Booz | Allen | Hamilton®

WHEN THE LIGHTS WENT OUT

A COMPREHENSIVE REVIEW OF THE 2015 ATTACKS ON UKRAINIAN CRITICAL INFRASTRUCTURE

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

CONTENTS

EXECUTIVE SUMMARY

On December 23, 2015, unknown cyber actors disrupted energy-grid operations for the first time ever,[a] causing blackouts for over 225,000 customers in Ukraine.[1] Among the most striking features of this attack were the complexity of organization and planning, the discipline in execution, and capability in many of the discrete tasks exhibited by the threat actors. Over the course of nearly a year prior to the attack, these unknown actors clandestinely established persistent access to multiple industrial networks, identified targets, and ultimately carried out a complex set of actions, which not only disrupted electricity distribution in Ukraine, but also destroyed IT systems, flooded call centers, sowed confusion, and inhibited incident response. The attackers used a malware tool, BlackEnergy 3, designed to enable unauthorized network access, then used valid user credentials to move laterally across internal systems, and ultimately shut down electricity distribution using the utilities' native control systems.

This report details the step-by-step process the actors took and seeks to highlight the opportunities for detection and prevention across the various steps of the attack. Combining open-source intelligence analysis of the attack and malware analysis of the tools used by the threat actors in their operation, we break down the integration of both human interaction and malware-executed processes as components of the December 2015 events.

This Booz Allen report expands on previous incident analysis published in spring 2016, going beyond by including additional detail about the attack chain based on malware execution, a more detailed mapping of targeted and affected infrastructure, and a much wider view on similar and potentially related Black Energy (BE) campaigns against Ukrainian infrastructure. This report provides a highly accessible and factual account of the incident. By providing this comprehensive view of the events, this report provides operators, plant managers, chief information security officers, and key industrial security decision makers a view of how an attack could be conducted against their networks and infrastructure, and—more importantly—some advice on how to mitigate attacks such as these in the future.

This attack was exceptionally well organized and executed, but the tools necessary to mitigate and minimize the impact of an attack such as this are not difficult to implement. By implementing a well-designed defense-in-depth protection strategy, industrial network and ICS/SCADA defenders can effectively address the threats facing their organizations. This report highlights the important components this strategy ought to include, based on the methods used in the Ukraine attack.

a. Despite early reporting indicating that disruptions in Brazil's electrical grid in 2007 were the result of a cyberattack, further investigation ultimately attributed the blackouts to inadequate maintenance.


ШКОЛА

INTRODUCTION

Shortly before sunset on December 23, 2015, hackers remotely logged into workstations at a power distribution company in western Ukraine, clicked through commands in the operators control system interface, and opened breakers across the electrical grid one by one. Before they were finished, they struck two more energy distribution companies, in rapid succession, plunging thousands of businesses and households into the cold and growing darkness for the next six hours.[2] These attacks were not isolated incidents, but the culmination of a yearlong campaign against a wide range of Ukrainian critical infrastructure operations. In addition to three energy distribution companies, Prykarpattyaoblenergo,[3] Kyivoblenergo,[4] and Chernivtsioblenergo,[5] threat actors had also previously targeted several other critical infrastructure sectors, including government, broadcast media, railway, and mining operators.

The attacks in Ukraine were a watershed moment for cybersecurity; for the first time, malicious cyber threat actors had successfully and publicly disrupted energy-grid operations, causing blackouts across multiple cities. The power outage was also one of the few known cyber-attacks against a supervisory control and data acquisition (SCADA) system, a type of system critical to automation in many sectors, including transportation, manufacturing, heavy industry, and oil and gas.

This report details the actions threat actors took in each step of the attack, including an analysis of associated malware and other identified indicators of compromise (IoC). This report also includes, as an appendix, detailed technical analysis of the associated malware's function and use. By tracing this attack from early exploration and target identification to turning the lights out on Ukrainian cities, this report serves as an aid to the security professionals charged with securing industrial control systems (ICS) and is equally relevant across a range of other critical infrastructure sectors.

By understanding the current tactics, techniques, and procedures (TTP) that the threat actors used in this attack, and those that are most likely to be used against ICS systems in the future, security professionals can use this case study to plan for future threats against their own systems. Though this attack targeted operators in the electricity distribution sector, the TTPs illustrated in this attack are applicable to nearly all ICS sectors including oil and gas, manufacturing, and transportation. A reconnaissance campaign against US ICS operators in 2011–2014 using the same malware family deployed across Ukraine's critical infrastructure raises the urgency of understanding this disruptive Ukrainian attack.

ADDRESSING THE THREAT

In a series of unique, discrete steps, the threat actors deployed malware; gained access to targeted corporate networks; stole valid credentials; moved into the operators' control environment; identified specific targets; and remotely disrupted the power supply. Each task was a missed opportunity for defenders to block, frustrate, or discover the attackers' operations before they reached their final objectives.

The Ukraine incident also demonstrates that no single mitigation can prevent an attack's success. The attackers followed multiple avenues to eventually overcome challenges and move onto the attack sequence's next components. The most effective strategy for repelling complex attacks, therefore, is defense in depth. Layering defenses can raise the adversary's cost of conducting attacks, increase the likelihood of detection by a network defender, and prevent a single point of failure. All mitigation techniques, from

INDUSTRIAL SECURITY THREAT BRIEFING

This attack on Ukraine's electric grid is the most damaging of the increasingly common attacks against ICS systems. ICS operators reported more security incidents in 2015 than in any other year. Complementing the detailed, procedural analysis provided in this report, Booz Allen's Industrial Security Threat Briefing provides a broader perspective on the cyber threat landscape ICS operators face. The Industrial Security Threat Briefing includes an overview of the emerging tactics and active threat actors observed in 2015 and 2016, as well as the threats most likely to affect ICS operators in the coming years. The report is available at http://www.boozallen.com/insights/2016/06/industrial-cybersecurity-threat-briefing.

Acknowledgments

Several in-depth reports have been released, each covering a different facet of the December 2015 attacks in Ukraine. The SANS Institute, in partnership with the Electricity Information Sharing and Analysis Center (E-ISAC),[6] as well as the US Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC)[7], have both produced detailed reports covering the incident. Security researchers at F-Secure[8] and ESET[9] have conducted extensive analysis of the BlackEnergy malware, and reporting produced by Cys-Centrum[10] and Trend Micro[11] have sought to lay out the common ties across the string of similar, and likely related, cyber attacks against Ukrainian critical infrastructure. Each of these accounts provides a different piece of the larger picture, which this report lays out.

architectural segmentation and network monitoring, to access control and threat intelligence, should be complementary efforts in a wide-reaching process and network defense strategy that aims to protect the environment, making it so difficult, expensive, or time consuming that it ultimately deters the attacker.

OUR RESEARCH METHODOLOGY

Though the attacks against Ukraine's electrical grid in December 2015 have been discussed widely in public reporting, this report seeks to build upon the analysis to provide a more comprehensive account. By analyzing the malware tools used in the attack and using open-source intelligence gathering, this report seeks to tie together the wide body of existing information on this event and fill the gaps in other reports.

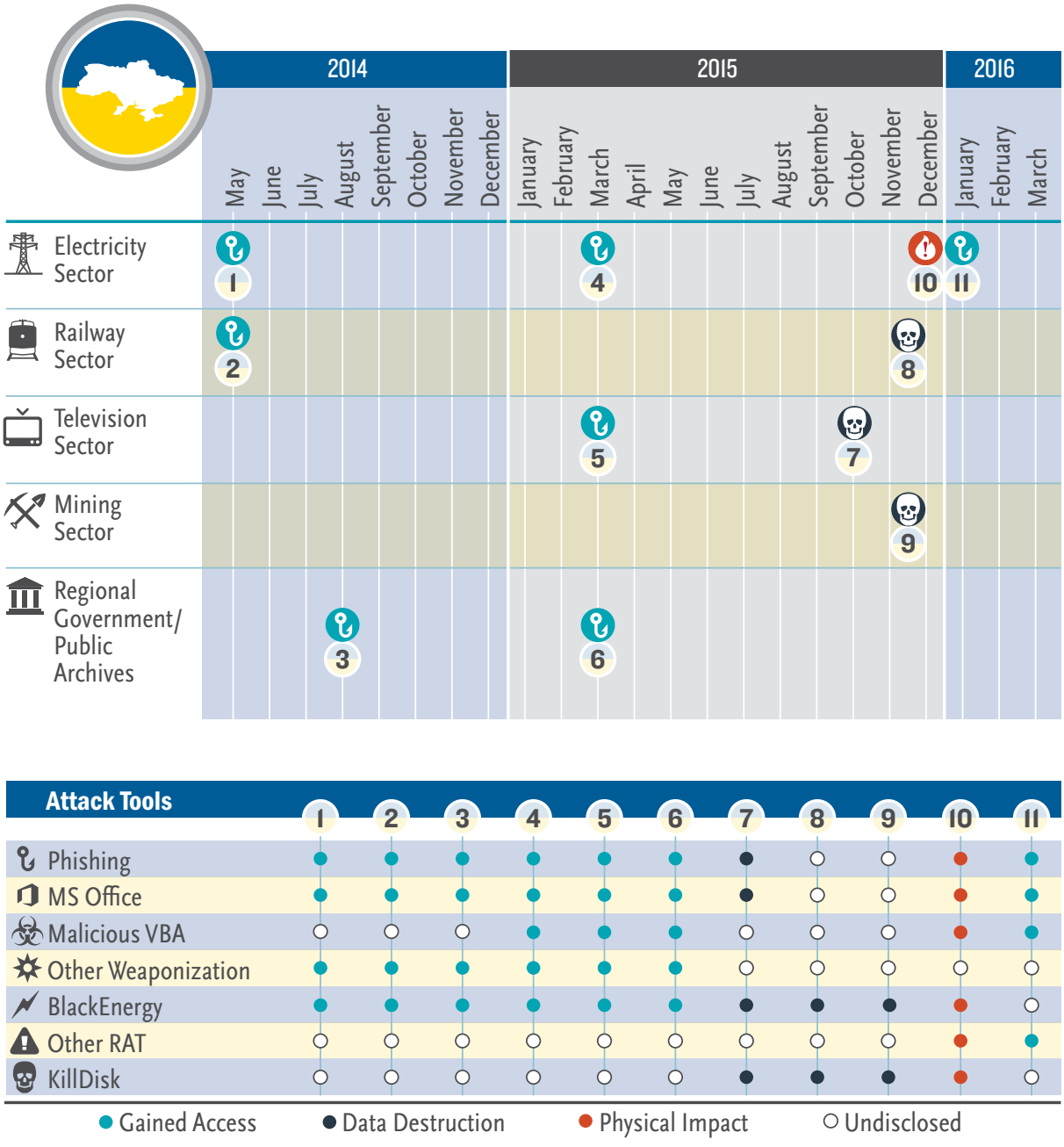
This report leverages an extensive analysis of publicly reported data on the attack, as well as our own deep-dive technical analysis of recovered malware samples used in the attack. Public reporting on the incident and related attack data was collected manually or through automated searches on publicly accessible internet sites. The sources included, but were not limited to, English and foreign language media, advisories and alerts from US and foreign government cybersecurity organizations, and analysis by independent security researchers. References to IoCs and other attack data were used to identify related incidents, then analyze and integrate their findings with this attack.

Analysis of public reporting was complemented with a thorough technical analysis of recovered malware samples used in the December 2015 attacks against the electrical distributors, as well as samples from related attacks. Our technical analysis was used to verify, corroborate, and expand on existing reports detailing threat actor activity leading up to and during the incident. Experienced reverse engineers used disassembler and debugger software to navigate through the malware code to identify its capabilities and unique characteristics. Reverse engineers used both static and dynamic analysis, allowing them to see how the malware behaves on a system with the freedom to run in a debugger in order to force or bypass certain conditions, thereby allowing the malware to take multiple paths. By recording system changes made by the malware, the reverse engineers were able to gather key data needed to identify further system infections, as well as potential mitigations. This investigation also emphasized analyzing the recovered samples within the context of their broader malware family. Using YARA, a tool to identify binary or textual signatures within malware, analysts pivoted to new samples in an effort to identify new capabilities and different variants of the malware. This comprehensive report completes the view of the attack sequence for this incident.

A REGIONAL CAMPAIGN

Our research and analysis of the December 2015 blackout showed that the attack against Ukraine's electricity grid was not an isolated incident, but in fact a continuation of a theme of a steady, deliberate attacks against Ukraine's critical infrastructure. This long-running campaign likely reflects a significant, concerted effort by a single threat actor with a well-organized capability and interest in using cyberattacks to undermine Ukraine's socio-political fabric. Each of the attacks used a common set of TTPs that had been used in earlier incidents in the previous months, detailed in Exhibit 1. To put the December 2015 attack in context, our research uncovered an additional 10 related attacks, the last of which occurred in January 2016. Exhibit 1 shows the timing, techniques and target sectors in this 18-month campaign.

EXHIBIT I. CYBER THREAT LANDSCAPE IN UKRAINE



1. May 2014 (Electricity) On May 12, 2014, threat actors targeted Ukrainian electricity distributor Prykarpattyaoblenergo in a phishing campaign using weaponized Microsoft (MS) Word documents.[12] The threat actors forged the sender addresses and modified the weaponized MS Word attachments with a malicious PE-executable file inserted into the icon image associated with file.[13]
2. May 2014 (Railway) On May 12, 2014, threat actors targeted all six of Ukraine's state railway transportation system operators in a phishing campaign using weaponized MS Word documents.[14] The threat actors forged the sender addresses and modified the weaponized MS Word attachments with a malicious PE-executable file inserted into the icon image associated with file.[15]
3. August 2014 (Ukrainian Regional Government, Archives) In August 2014, threat actors began a wide-reaching phishing campaign using weaponized MS Power Point files. The weaponized files exploited a zero-day vulnerability (CVE-2014-4114) to deliver BlackEnergy Malware to targeted systems.[16,17] Targets included five Ukrainian regional governments, and the state archive of Chernivtsi Oblast, one of the three oblasts targeted in the December 2015 Electricity distributor attacks.[18,19]
4. March 2015 (Media) In early March 2015, threat actors conducted a phishing campaign against Ukrainian television broadcasters, using weaponized MS Excel and MS PowerPoint documents (Додаток1.xls and Додаток2.pps).[20] The weaponized documents contained malicious Visual Basic Application (VBA) and JAR files designed to drop BlackEnergy malware on targeted systems.[21]
5. March 2015 (Electricity) In late March 2015, threat actors conducted a phishing campaign targeting electricity operators in western Ukraine using the weaponized MS Excel file (Додаток1.xls) used earlier that month against broadcast media targets. As with the earlier attack, the file included a malicious macro designed to install BlackEnergy.[22]
6. March 2015 (State Archives) Also in late March 2015, threat actors targeted Ukrainian state archives in phishing attacks using the same weaponized MS Excel file (Додаток1.xls), malicious macro, and BlackEnergy malware.[23]
7. October 2015 (Television Broadcast) On October 24 and October 25, 2015, Ukrainian election day, threat actors used KillDisk malware to destroy video data and server hardware, and render employee workstations inoperable at multiple Ukrainian television broadcasters.[24,25] Targeted systems were found to be infected with the same BlackEnergy and KillDisk samples observed in attacks against a railway operator, mining company, and electricity distributors in November and December 2015. Investigation of the incident indicated access to the network was established May 2015.[26]
8. November–December (Railway) In November–December 2015, an undisclosed Ukrainian Railway firm, operating under the Ukrainian State Administration of Railway Transport, was targeted in a cyberattack using BlackEnergy and KillDisk malware.[27] The method for establishing initial access to targeted networks was not disclosed.
9. November–December 2015 (Mining) In November–December 2015, an undisclosed Ukrainian Mining firm was targeted in a cyberattack using BlackEnergy and KillDisk malware.[28] The method for establishing initial access to targeted networks was not disclosed.
10. December 2015 (Electricity) On December 23, 2015, threat actors opened breakers and disrupted electricity distribution at three Ukrainian firms: Prykarpattyaoblenergo, Kyivoblenergo, and Chernivtsioblenergo. Full details of this attack are included in the Attack Walk Through section of this report.
11. January 2016 (Electricity) On January 19 and 20, 2016, threat actors targeted approximately 100 organizations, including many Ukrainian energy firms,[29] in a phishing campaign.[30] The malicious emails were designed to look as though they were sent by Ukrainian energy distributor NEC Ukrenergo.[31] The emails included a weaponized MS Excel document, which prompted users to enable macros; once enabled, a malicious VBA script installed GCat, an open-source, python-based trojan which disguises communications with the command-and-control (CC) server as Gmail email traffic.[32]

BLACKENERGY MALWARE

BlackEnergy is a remote-access trojan designed to provide unauthorized access to targeted networks via an HTTP connection with an external server. Its modular design allows it to accept additional plugins to carry out specific functions, such as stealing credentials or conducting network reconnaissance.

ATTRIBUTION

Though the Security Service of Ukraine (SBU) immediately implicated Russia in the attack,[33] there is no smoking gun which irrefutably connects the December 2015 attacks in Ukraine to a specific threat actor. The limited technical attribution data, such as the attackers using a Russia-based Internet provider and launching the telephony denial-of-service (TDoS) flood traffic from inside Russia,[34] point to Russian threat actors, though this evidence is not conclusive unto itself. Some inferences can be made based on the history of the tools used, how the attack was carried out, and the outcomes that were achieved.

Cybercriminal organizations and state-backed groups are often the most well-resourced, organized, and technically advanced cyber threat actors. BlackEnergy first emerged as a DDoS tool in 2007[35] and has a history of use by criminal organizations. The most notable criminal operation was a series of attacks in 2011 against Russian and Ukrainian banks, in which criminals used BlackEnergy 2 to steal online credentials and obfuscate the attacks with distributed denial-of-service (DDoS) floods.[36]

Despite these criminal roots, BlackEnergy often rears its head in attacks with particular political significance, typically targeting organizations and countries with adversarial relations with Russia. In 2008, during Russia's conflict with Georgia, Georgian networks were bombarded with a DDoS attack by a botnet constructed with the first iteration of BlackEnergy, and controlled by CC servers hosted on Russian state-owned companies.[37,38] BlackEnergy was also used in June 2014, targeting a French telecommunications firm, by a group known to conduct cyberattacks against NATO, Western European governments, and several regional Ukrainian governments.[39,40,b] In addition, the KillDisk malware, used in conjunction with BlackEnergy, was first observed in a data destruction attack against servers operated by several Ukrainian news outlets on October 24–25, 2015, Ukraine's election day.[41]

As security researchers have pointed out, the overlap in usage of the malware by multiple groups, including criminal organizations, would be convenient for a state-backed group as this provides a degree of plausible deniability.[42] As noted above though, the targets selected in previous campaigns using BlackEnergy often align to Russian political interests. Furthermore, the activity associated with the December 2015 attack does not appear to align to a criminal organization's likely goal of financial gain. Threat actors invested significant resources in establishing, maintaining, and expanding persistent access on targeted networks for nearly a year. They conducted extensive network reconnaissance, likely developed malicious firmware, familiarized themselves with the native control environment, and then ultimately revealed their presence in a destructive attack. The extensive resources invested, and no apparent financial return, indicate the attackers' likely objective was to use the attack to send a message.

b. Reporting did not specify whether if used BlackEnergy malware was used in the attacks against NATO or other European government targets.

INTENT

Several plausible theories that have been proposed may explain the threat actor's motivations for conducting the attacks, as well as its timing, target, and impact. It is possible that the adversary was motivated by several of the posited theories, though the attack was probably designed to send a message to the Ukrainian government, rather than gain a lasting benefit.

CONVEY DISPLEASURE WITH PLANS TO NATIONALIZE RUSSIAN-OWNED ASSETS

One theory that has circulated in cybersecurity circles is that the attackers may have intended to convey displeasure with a Ukrainian proposal[43,44] to nationalize assets owned by Russia and its citizens.[45] The policy would have harmed influential Russian oligarchs with investments in Ukraine's energy sector. For example, Alexander Babakov—a senior member of Russia's national legislature and a current target of EU sanctions[46]—is a main shareholder in VS Energy. It is one of the largest electricity distributors in the Ukrainian market, with ownership stakes in nine of the 27 oblenergos and a 19-percent electricity-distribution market share, as of 2010.[47]

Based on available evidence, however, we find the theory unconvincing. The timing of the attack and the particular target made it an unlikely symbolic target for expressing a position on nationalization. Discussions about nationalizing Russian assets had not been a headline issue since the spring of 2015, more than six months before the disruption; the lack of temporal proximity between the two events blurred or watered down the symbolic value of the attack vis-à-vis nationalization.

POLITICAL DESTABILIZATION; CULTIVATE GENERAL FEAR AND DISCONTENT

Another possible objective was to destabilize Ukraine politically. As indicated above, a wide swath of Ukrainian organizations were caught in the attacker's larger collection of networks compromised with BlackEnergy, including targets in the railway, mining, broadcast media and government sectors.[48] This trend indicates the objective may have been to disrupt a critical service provider or critical industry, rather than an energy company specifically. By disrupting operations in critical infrastructure, the threat actors may have sought to reduce confidence in the Ukrainian government. This strategy would be consistent with Russia's information warfare doctrine, which seeks to sow discontent in a target country or region in order to induce political and economic collapse.[49]

IN-KIND RETALIATION

Another possible objective may have been in-kind retaliation for perceived Ukrainian disruptions of electricity to Crimea. On November 21–22, 2015, Crimea lost power for more than six hours due to physical attacks on four pylons carrying transmission wires.[50] The identity of the saboteurs has not been publicly determined, but they are rumored to be Ukrainian nationalists.[51] Crimea is reliant on Ukraine, as the country supplies about 70 percent of Crimea's power.[52] Russia intends to obviate this risky reliance by constructing a new energy bridge between Crimea and Russia, which will be able to supply 70–80 percent of Crimea's power needs.[53] If this was the objective in the attack, it would indicate that Russia may actively seek to gain footholds in critical services providers with the intention to execute attacks at strategically useful times. This would be consistent with similar attacks against critical infrastructure in other adversarial nations in Western Europe[54] and the US[55] that have been attributed to Russia.

OUTLOOK

While politically motivated cyberattacks are not a novel foreign policy tool, the industries and organizations that serve as potential targets are expanding. Cyberattacks present a powerful political tool, particularly those against critical infrastructure providers. Industrial control systems operators are not above the fray in geopolitical rows, and may in fact be the new primary target.

ATTACK WALK THROUGH

The attack walk through provided in this report is informed by analytical frameworks published by cybersecurity industry organizations,[56,57] as well as proprietary methods for conducting open-source intelligence analysis and technical malware analysis. To provide as complete a picture as possible for this report, as with other reporting on this incident, some inferences on the threat actors' most likely method were required, as there does not exist a complete accounting of all actions the threat actors took in their campaign. Wherever possible, inferences were based on confirmed technical evidence, such as identified malware capabilities and known hardware and software vulnerabilities.

This section provides the step-by-step walk through of threat actor activity during the attack. Each step includes a high-level description, as well as a feature summary of the step with eight descriptors. The eight descriptors are as follows:

Location: This describes the network on which the activity occurred, including preparatory activity conducted outside of the targeted networks (listed as "external infrastructure"), as well as the logically or physically separated "corporate network" or "ICS network" operated by the electricity distributors.

Action: The December 2015 attacks were achieved using a combination of direct threat actor manipulation of systems deployed by the electricity distributors, as well as malware-executed tasks. "Active threat actor activity" highlights tasks that involved hands-on-keyboard interactions with systems deployed on the electricity distributor network. "Malware execution" highlights tasks completed by functions built into the malware tools used by threat actors.[c]

Timeline: This section provides the timeframe in which the step most likely occurred. This includes specific, known dates, as well as ranges of time defined by known threat actor activities.

Device/application: This section lists the device or application targeted or exploited by threat actors in the step. Wherever possible, specific model information is provided; in instances in which the model or application details were not found in open sources, analysts made assessments based on available evidence, such as operating system (OS) or application-specific services targeted by the reported malware. For the steps detailing preparatory tasks conducted external to the electricity distributors' networks, "activity conducted external to network" is listed rather than the targeted device or application.

Role in infrastructure: This section details the function of the targeted device or application within the electricity distributors' network. "Activity conducted external to network" is listed for preparatory activities conducted on external infrastructure.

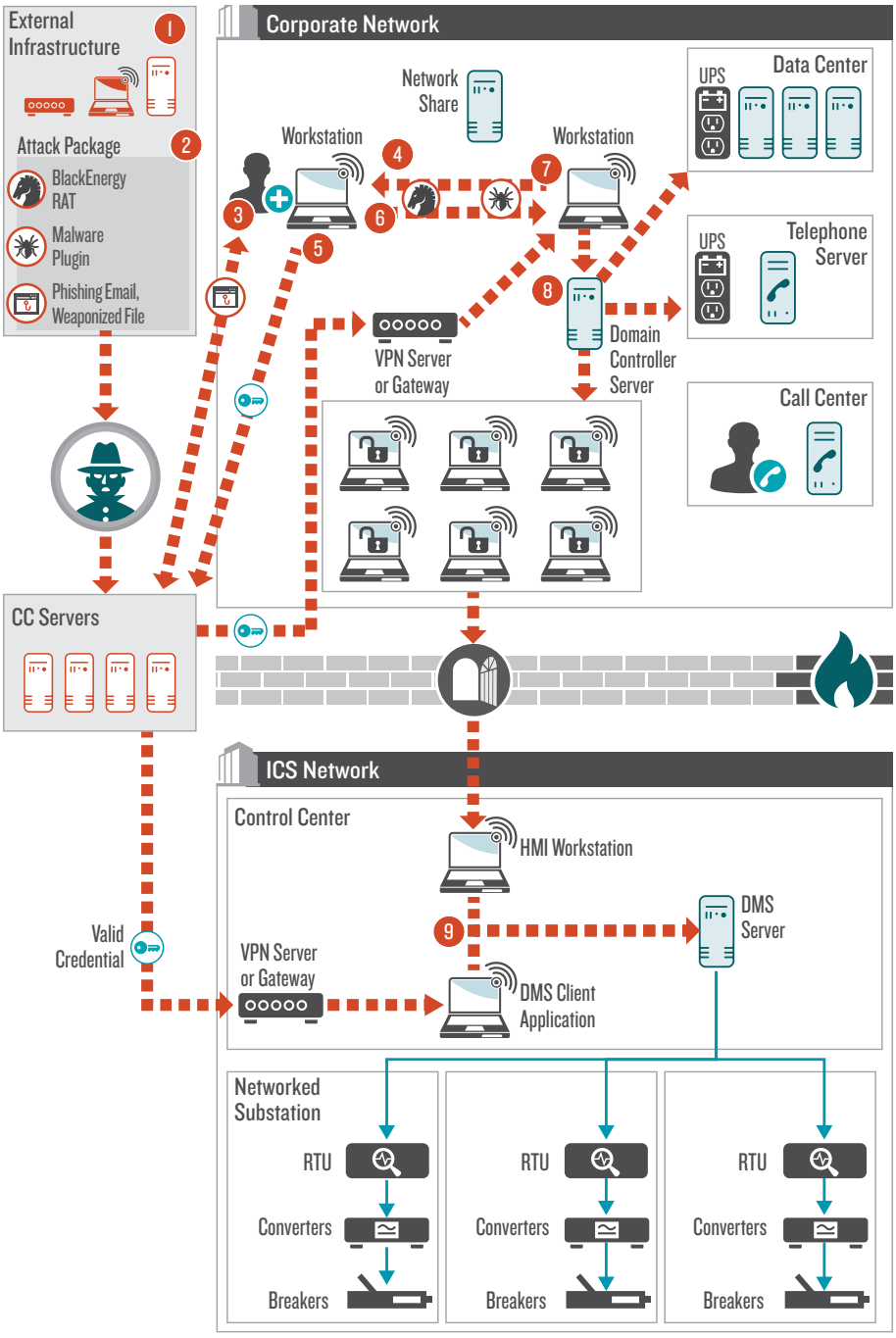
Exploitation method: This section includes a summary of the method used by threat actors to complete the step.

Impact: This section includes a brief summary of the capability achieved by threat actors, or any disruption or destruction of systems operated by the targeted operator, upon completion of the step.

Booz Allen's recommended mitigations: This section provides the technical or procedural security measures that would help prevent or limit the impact of the activities associated with the step.

c. *One step required employees to actively grant permissions that enabled the malware to execute. Another step manipulated a task scheduling service available on the targeted network.*

EXHIBIT 2. WALK THROUGH OF THREAT ACTOR ACTIVITY, STEPS I THROUGH 9



Steps 1–9

Step I: Reconnaissance and Intelligence Gathering. Prior to the attack, threat actors likely begin open-source intelligence gathering and reconnaissance on potential targets.

Step 2: Malware Development and Weaponization. Threat actors acquire or independently develop the malware to be used in the attack, as well as the weaponized documents to deliver the malicious files.

Step 3: Deliver Remote Access Trojan (RAT). Threat actors initiate phishing campaign against electricity distributors.

Step 4: Install RAT. Threat actors successfully install BlackEnergy 3 on each of the three targeted electricity distributors after employees open the weaponized MS Office email attachments and enable macros.

Step 5: Establish Command-and-Control (CC) Connection. Malware establishes connection from malicious implant on targeted network to attacker-controlled command-and-control (CC) server.

Step 6: Deliver Malware Plugins Following installation of BlackEnergy 3 implant, threat actors likely import plugins to enable credential harvesting and internal network reconnaissance.

Step 7: Harvest Credentials. Delivered BE3 malware plugins conduct credential harvesting and network discovery functions.

Step 8: Lateral Movement and Target Identification on Corporate Network. Threat actors conduct internal reconnaissance on corporate network to discover potential targets and expand access.[d]

Step 9: Lateral Movement and Target Identification on ICS network. Threat actors use stolen credentials to access the control environment and conduct reconnaissance on deployed systems.

d. In this step, the threat actors are not passing through the Domain Controller server in their lateral movements across the network, as they would, for example, a VPN gateway. In accessing the Domain Controller they are retrieving, or making, valid user credentials to enable expansive access across the corporate network and pivoting into the ICS network. The actual movement and network exploration would follow this compromise, would be conducted using the stolen credentials, and would occur on many machines across the network.

In addition to the high-level summary of each step provided in this section, each step has a corresponding textual summary provided in Appendix A. This textual summary provides the detailed overview of the evidence relating to each step, including citations for all referenced material and explanations of analyst assessments.

RECONNAISSANCE

STEP 1: RECONNAISSANCE AND INTELLIGENCE GATHERING

Prior to the attack, threat actors likely begin open-source intelligence gathering and reconnaissance on potential targets.

Location: External infrastructure

Action: Active threat actor activity

Timeline: May 2014 or earlier

Device/application: Activity conducted external to network

Role in infrastructure: Activity conducted external to network

Exploitation method: Threat actors likely gather publicly available information on deployed systems and network architecture, and may also use active discovery methods such as scanning of perimeter devices.

Impact: Threat actors gather targeting data on personnel and network infrastructure for use in future attacks.

Booz Allen's recommended mitigations:

- Implement information classification program to categorize critical system information that could be used by a threat actor. Sensitive information such as this should have restricted distribution and not be publicly available.
- Utilize open-source intelligence gathering to identify publicly accessible information on the organization or personnel that could be used by threat actors in social engineering attacks.
- Utilize open-source tools, such as Shodan, to monitor your organization's external IP address range for unexpected Internet-facing devices. Pay special attention to identified devices with common ICS ports, such as Modbus (502) or EtherNet/IP (44818).
- Maintain a detailed inventory of all assets and communication paths to develop an understanding of potential external attack vectors. Asset inventories should cover both equipment and applications, and should include such details as MAC ID, IP address, and firmware version, to prevent rogue network connections or modifications to network devices.
- Actively monitor perimeter network security devices to identify active reconnaissance techniques, such as port scanning.

WEAPONIZATION

STEP 2: MALWARE DEVELOPMENT AND WEAPONIZATION

Threat actors acquire or independently develop the malware to be used in the attack, as well as the weaponized documents to deliver the malicious files.

Location: External infrastructure

Action: Active threat actor activity

Timeline: May 2014 or earlier

Device/application: Activity conducted external to network

Role in infrastructure: Activity conducted external to network

Exploitation method: Threat actors acquire BlackEnergy remote access trojan (RAT), and weaponize Microsoft (MS) Word and Excel files with VBA scripts to drop the BlackEnergy RAT.

Impact: Combined with targeting data gathered during the reconnaissance phase, threat actors are able to develop tailored attack packages. At the completion of this step, threat actors have all the necessary tools to begin their attack.

Booz Allen's recommended mitigation:

- Implement application whitelisting to prevent unknown files from being executed and apply sandboxing to non-critical applications in order to reduce unintended modifications.

DELIVERY

STEP 3: DELIVER RAT

Threat actors initiate phishing campaign against electricity distributors.

Location: Corporate network

Action: Active threat actor activity

Timeline: May 2014–June 2015[e]

Device/application: Employee workstations, likely using MS Windows OS and provisioned with MS Internet Explorer web browser

Role in infrastructure: Support email communications and other IT services used in business operations.

Exploitation method: Threat actors send innocuous-looking emails containing the modified MS Office files as attachments to users on targeted networks. This tactic is known as phishing.

Impact: RAT is delivered to targeted network, but not installed. Installation requires employees to actively grant permission to the embedded VBA scripts to execute.

Booz Allen's recommended mitigations:

- Implement a position-specific cybersecurity awareness training program to ensure employees understand the organizational risks associated with cyberattacks and how to identify social engineering techniques such as phishing.
- Establish a Computer Incident Response Team (CIRT) and ensure all employees are aware that suspicious emails or attachments should be forwarded here for investigation. The CIRT should review any reports, perform malware analysis, and extract an indicator of compromise (IOC) to identify any infections on the organization's network.
- Use a network-based antivirus solution to detect and prevent known malware from entering the organization's network.
- Install and configure an anti-spam solution to screen incoming emails for suspicious content or abnormal senders.
- Subscribe to and monitor threat intelligence sources to be aware of ongoing campaigns. This information can be used to focus defense efforts and search for IOCs.

EXPLOITATION AND INSTALLATION

STEP 4: INSTALL RAT

Threat actors successfully install BlackEnergy 3 on each of the three targeted electricity distributors after employees open the weaponized MS Office email attachments and enable macros.

Location: Corporate network

Action: Employee-enabled malware execution

Timeline: May 2014–June 2015

Device/application: Employee workstations, likely using MS Windows OS and provisioned with MS Internet Explorer web browser

Role in infrastructure: Support email communications and other services used in business operations.

Exploitation method: In a social engineering attack, employees are prompted to enable macros when opening the file attached to phishing email. Once macros are enabled, the VBA script places multiple malicious files on the workstation, unbeknown to the employee.

Impact: Files placed on workstations within the corporate network can begin the communication process with external CC servers.

---

e. Ukrainian Deputy Energy Minister noted access was gained at least six months prior to the final attack. Earliest observed phishing attack matching TTP against electricity distributor was May 2014.

Booz Allen's recommended mitigations:

- Implement application whitelisting to prevent unknown files from being executed.
- Use host-based antivirus software to detect and prevent known malware from infecting organization systems.
- Set script execution policy to allow only signed VBA scripts and macros to be run.

COMMAND AND CONTROL

STEP 5: ESTABLISH CC CONNECTION

Malware establishes connection from malicious implant on targeted network to attacker-controlled CC server.

Location: Corporate network

Action: Malware execution

Timeline: May 2014–June 2015

Device/application: Employee workstations, likely using MS Windows OS and provisioned with MS Internet Explorer web browser

Role in infrastructure: Support email communications and other services used in business operations.

Exploitation method: The external connection is established as part of the execution routine following installation of the malicious files. Once permissions to execute macros are granted by employees, the malicious VBA script installs the malware implant, and the implant attempts to communicate with an external server via HTTP requests.

Impact: Threat actors gain unauthorized access to targeted networks, including the ability to deliver additional BlackEnergy plugins to enable internal network reconnaissance and credential harvesting.

Booz Allen's recommended mitigations:

- Configure firewall ingress and egress traffic filtering to block anomalous incoming and outgoing network communications.
- Blacklist known malicious IP addresses and monitor for any form of network communications to these addresses.

ACTION ON OBJECTIVES: INTERNAL RECONNAISSANCE AND LATERAL MOVEMENT

STEP 6: DELIVER MALWARE PLUGINS

Following installation of BlackEnergy 3 implant, threat actors likely import plugins to enable credential harvesting and internal network reconnaissance.

Location: Corporate network

Action: Active threat actor activity

Timeline: June 2015–December 2015

Device/application: Employee workstations, likely using MS Windows OS and provisioned with MS Internet Explorer web browser

Role in infrastructure: Support email communications and other services used in business operations

Exploitation method: The BlackEnergy 3 implant delivered in the initial attack functions as a receiver for additional malware plugins. After establishing a remote connection with delivered files via HTTPS, the threat likely delivers the additional malware components.

Impact: The delivered plugins enable additional BlackEnergy functionality, including harvesting user credentials, keylogging, and network reconnaissance.

Booz Allen's recommended mitigations:

- Implement application whitelisting to prevent unknown files from being executed.
- Configure firewall ingress and egress traffic filtering to block anomalous incoming and outgoing network communications.
- Blacklist known malicious IP addresses and monitor for any form of network communications to these addresses.
- Use host-based antivirus software to detect and prevent known malware from infecting organization systems.

STEP 7: HARVEST CREDENTIALS

Delivered BlackEnergy 3 malware plugins conduct credential harvesting and network discovery functions.

Location: Corporate network

Action: Active threat actor activity, malware execution

Timeline: June 2015–December 2015

Device/application: Windows OS workstations, Windows domain controllers, virtual private network (VPN) service deployed in control environment

Role in infrastructure: These systems support business operations, manage permissions and domain access, and provide remote network access respectively.

Exploitation method: Threat actors use delivered BlackEnergy 3 plugins to gather stored credentials or log keystrokes. After gathering valid credentials for user with administrator privileges, threat actors use the stolen administrator credentials to access the domain controller, recover additional credentials, and create new privileged accounts.

Impact: Threat actors obtain valid credentials enabling them to expand access across the corporate network and into the control environment, ensure persistent access, and blend into regular network traffic.

Booz Allen's recommended mitigations:

- Implement centralized logging and monitor audit logs for unusual logins or use of administrative privileges (e.g., abnormal hours, unsuccessful login attempts).
- Establish a baseline of user domain and local accounts and monitor for any account additions or privilege escalations outside of the organization's approved workflow.
- Implement least privilege policies across all systems to ensure administrative accounts are properly restricted and assigned to only those who require them.

STEP 8: LATERAL MOVEMENT AND TARGET IDENTIFICATION ON CORPORATE NETWORK

Threat actors conduct internal reconnaissance on the corporate network to discover potential targets and expand access.

Location: Corporate network

Action: Active threat actor activity, malware execution

Timeline: June 2015–December 2015

Device/application: Discovered systems, including networked uninterruptable power supply (UPS) devices, data center servers, a telephone communications server, and employee workstations

Role in infrastructure: Internal reconnaissance efforts could potentially include all deployed devices on the corporate network.

Exploitation method: Threat actors likely use a combination of valid user credentials and BlackEnergy 3 plugins developed to conduct network discovery. VS.dll plugin is likely used to leverage MS Sysinternals PsExec to establish remote connections to workstations and servers.

Impact: Threat actors are able to enumerate the systems deployed across the network, identify targets, and begin preparations for final attack.

Booz Allen's recommended mitigations:

- Implement active network security monitoring to identify anomalous network behavior.
- Ensure network is appropriately segregated to inhibit lateral movement.
- Monitor audit logs for unusual logins or use of administrative privileges (e.g., abnormal hours, unsuccessful login attempts).
- Establish production honeypots spread throughout the network to alert on any attempts to login or access files. These honeypot systems have no intentional purpose, and any attempt to access them is a notable security alert.

STEP 9: LATERAL MOVEMENT AND TARGET IDENTIFICATION ON ICS NETWORK

Threat actors use stolen credentials to access the control environment and conduct reconnaissance on deployed systems.

Location: ICS network

Action: Active threat actor activity

Timeline: June 2015–December 2015

Device/application: Discovered systems, including human machine interface (HMI) workstations, distributed management system (DMS) servers, UPS devices,[58] serial-to-Ethernet converters (Moxa UC 7408-LX-Plus,[59] IRZRUH2 3G[60]), remote terminal unit (RTU) devices (ABB RTU560 CMU-02), and the substation breakers

Role in infrastructure: HMI workstations provide a graphical user interface for operators to remotely monitor and control devices within the control environment. DMS applications enable centralized monitoring and issuing of commands within a control environment. UPS devices condition incoming power to downstream devices and provide temporary battery backup power. Serial-to-Ethernet converters convert serial data from field devices to digital packets, enabling communications with the control center. RTU devices function as a communication processor or a data concentrator in a substation, enabling communications and data transfer between field devices in the substations and the control center. Substation breakers are devices designed to physically interrupt current flows through an electrical circuit.

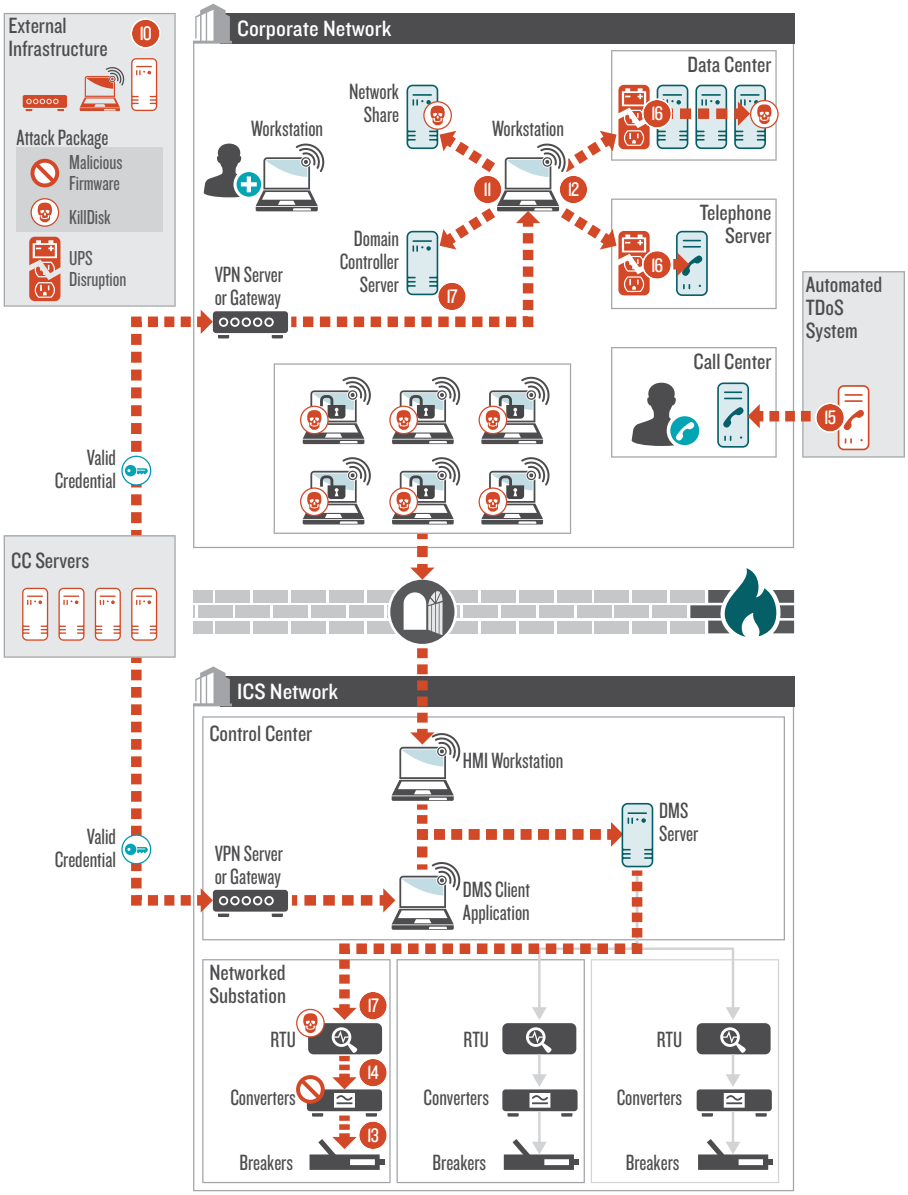
Exploitation method: Threat actors use valid credentials to interact directly with the client application for the DMS server via a VPN, and native remote access services to access employee workstations hosting HMI applications. This access likely enables threat actors to enumerate all networked devices within the control environment.

Impact: Threat actors gain access to critical systems, enabling them to begin target selection and preparations for final attack.

Booz Allen's recommended mitigations:

- Install and configure a stateful firewall or data diode device between the corporate network and ICS network.
- Configure an ICS network demilitarized zone (DMZ) and prohibit any direct traffic between the corporate and ICS networks. All traffic between these domains should be heavily controlled through the use of proxies and be actively monitored.
- Any access to systems within the control system DMZ should require the use of two-factor authentication.
- Implement network segregation of control system components within the ICS network using zone and conduit techniques. Use industrial firewalls between these network segments whereby only specified traffic can enter and exit. All traffic outside of what is explicitly allowed should trigger an alert.
- Take advantage of the predictability in control system traffic by establishing a baseline of normal ICS network communications and conduct active monitoring for anomalies.

EXHIBIT 3. WALK THROUGH OF THREAT ACTOR ACTIVITY, STEPS 10 THROUGH 17



Steps 10–17

Step 10: Develop Malicious Firmware. Threat actors develop malicious firmware update for identified serial-to-Ethernet converters.

Step 11: Deliver Data Destruction Malware. Threat actors likely deliver KillDisk malware to network share and set policy on domain controller to retrieve malware and execute upon system reboot.

Step 12: Schedule Uninterruptable Power Supply (UPS) Disruption. Threat actors schedule unauthorized outage of UPS for telephone communication server and data center servers.

Step 13: Trip Breakers. Threat actors use native remote access services and valid credentials to open breakers and disrupt power distribution to over 225,000 customers within three distribution areas.

Step 14: Sever Connection to Field Devices. After opening the breakers, threat actors deliver malicious firmware update to serial-to-Ethernet communications devices. The malicious updates render the converters inoperable, and sever connections between the control center and the substations.

Step 15: Telephony Denial-of-Service Attack. Threat actors initiate DoS attack on telephone call center at one of the targeted distributors.

Step 16: Disable Critical Systems via UPS Outage. Previously scheduled UPS outage cuts power to targeted telephone communications server and data center servers.

Step 17: Destroy Critical System Data. Scheduled execution of KillDisk malware erases the master boot records and deletes system log data on targeted machines across the victims' corporate and ICS network.

ACTION ON OBJECTIVES: ATTACK PREPARATION

STEP 10: DEVELOP MALICIOUS FIRMWARE

Threat actors develop malicious firmware update for identified serial-to-Ethernet converters.

Location: External infrastructure

Action: Active threat actor activity

Timeline: June 2015–December 2015

Device/application: Activity conducted external to network

Role in infrastructure: Activity conducted external to network

Exploitation method: After identifying deployed converts, threat actors begin a malware development and testing effort on infrastructure outside of the targeted network.

Impact: Upon completion of this step, threat actors would have target-specific malware designed to disrupt communications with field devices by disabling deployed converters.

Booz Allen's recommended mitigations:

- Implement information classification program to categorize critical system information that could be used by a threat actor. Sensitive information such as this should have restricted distribution and not be publicly available.
- Review publicly available information, including job announcements and new supplier agreements, to ensure they do not provide inadvertent information to a threat actor on deployed devices.

STEP 11: DELIVER DATA DESTRUCTION MALWARE

Threat actors likely deliver KillDisk malware to network share and set policy on domain controller to retrieve malware and execute upon system reboot.

Location: Corporate and ICS network

Action: Active threat actor activity

Timeline: December 2015, directly preceding attack

Device/application: Network share and Windows domain controller server

Role in infrastructure: The network share provides access to shared digital resources, and the Windows domain controller manages access control throughout the network.

Exploitation method: Threat actors likely use stolen credentials to place KillDisk malware on a network share, then set the retrieval and execution of the malicious files by implementing a policy on the compromised domain controller server.[f]

Impact: Prescheduling execution of malware enables coordination of multiple attack components, such that data destruction coincides with or shortly follows attacks against breakers.

Booz Allen's recommended mitigations:

- Utilize network- and host-based antivirus software to detect and prevent known malware from infecting organization systems.
- Regularly scan organizational machine images with YARA rules to detect malware prior to execution.
- Restrict and monitor network share access permissions.

STEP 12: SCHEDULE UPS DISRUPTION

Threat actors schedule unauthorized outage of UPS for telephone communication server and data center servers.

Location: Corporate and ICS network

Action: Active threat actor activity

Timeline: Directly preceding December 2015 attack

Device/application: Networked UPS devices with remote management interface

---

f. This tactic was observed in attacks against the Ukrainian television broadcaster in October 2015. Domain controllers and KillDisk execution upon reboot, observed in the December 2015 attacks, both indicate this tactic may have been repeated against the electricity distributors.

Role in infrastructure: Prevent power outages from disrupting continuous operation of critical systems.

Exploitation method: Threat actors likely use valid credentials to access privileged employee accounts, then use this access to remotely schedule unauthorized power outages.

Impact: Prescheduling outages enables coordination of multiple attack components, such that critical systems also go down as a result of the power outages, stifling potential restoration efforts.

Booz Allen's recommended mitigations:

- Isolate UPS systems, and other facility management systems, from both the ICS and corporate networks.
- Disable remote management services for UPS devices wherever possible.

ACTION ON OBJECTIVES: EXECUTE ATTACK

STEP I3: TRIP BREAKERS

Threat actors use native remote access services and valid credentials to open breakers and disrupt power distribution to more than 225,000 customers within three distribution areas.

Location: ICS network

Action: Active threat actor activity

Timeline: December 23, 2015, during

Device/application: HMI workstations, DMS servers, RTU, and the substation breakers

Role in infrastructure: HMI workstations provide a graphical user interface for operators to remotely monitor and control devices within the control environment. DMS applications enable centralized monitoring and issuing of commands within a control environment. Substation breakers are devices designed to physically interrupt current flows through an electrical circuit.

Exploitation method: Threat actors use valid credentials to seize control of operator workstations, access DMS client application via VPN, and issue unauthorized commands to breakers at substations.

Impact: Opening of breakers results in disruption of electricity service to customers.

Booz Allen's recommended mitigations:

- Disable remote access into an organization's ICS network wherever possible.
- Require direct operator action to allow a remote user connectivity into the ICS VPN.
- Restrict user accounts with remote access privileges to the minimum necessary and require two-factor authentication for all VPN connections.
- Restrict functions of users who remotely access the control system environment wherever possible (e.g., read-only privileges).
- Develop and practice incident response scenarios to understand how to disrupt remote connectivity and manually operate ICS equipment to bring operations back to a safe state.

STEP I4: SEVER CONNECTION TO FIELD DEVICES

After opening the breakers, threat actors deliver malicious firmware update to serial-to-Ethernet communications devices. The malicious updates render the converters inoperable and sever connections between the control center and the substations.

Location: ICS network

Action: Active threat actor activity

Timeline: December 23, 2015, during attack

Device/application: Serial-to-Ethernet converters (Moxa UC 7408-LX-Plus,[61] IRZRUH2 3G[62])

Role in infrastructure: Convert serial data from field devices to digital packets to be transmitted to remote monitoring and administration systems within the control network.

Exploitation method: Threat actors use network access to push the malicious update over the network to targeted devices.

Impact: Operators are unable to remotely close the breakers, requiring workers to manually close breakers at each substation. Forcing this manual response draws out recovery time.

Booz Allen's recommended mitigations:

- Actively monitor ICS network for spikes in traffic or anomalous communications associated with firmware updates or reprogramming.
- Use physical means to restrict remote reprogramming and firmware updates of field devices (e.g., jumper settings, remote/run/prog switches).
- Implement a patch and vulnerability management plan for all computer systems, field devices, and network infrastructure equipment.
- Maintain offline spares of common ICS devices within an organization to aid in the restoration of compromised devices.

STEP 15: TELEPHONY DENIAL-OF-SERVICE ATTACK

Threat actors initiate DoS attack on telephone call center at one of the targeted distributors.

Location: Corporate network[g]

Action: Likely automated process

Timeline: Dec 23, 2015, during attack

Device/application: Operator telephone call center

Role in infrastructure: Receive external telephone communications from customers.

Exploitation method: Threat actors likely use automated IP-based call generators to flood the targeted call center.

Impact: Automated calls overwhelm resources at call center, blocking legitimate communications from customers.

Booz Allen's recommended mitigations:

- Establish a relationship with the telecommunications provider to aid in filtering out malicious calls during response activities.

g. *Public reporting did not indicate whether the call center deployed an automated system to receive calls or whether calls were answered manually by call center personnel.*

STEP 16: DISABLE CRITICAL SYSTEMS VIA UPS OUTAGE

Previously scheduled UPS outage suspends temporary battery backup power to targeted telephone communications server and data center servers.

Location: Corporate and ICS network

Action: Execution of prescheduled process

Timeline: December 23, 2015, during attack

Device/application: Networked UPS devices with remote management interface, telephone communications server, and data center servers

Role in infrastructure: Prevent power outages from disrupting continuous operation of critical systems.

Exploitation method: Threat actors use network access to schedule the temporary backup power to be offline at the time of the power outages.

Impact: Power loss to telephone server disrupts communications across remote sites, and disruptions at control centers inhibit ability to monitor and respond to attack against breakers. The disruption at the data center and associated system reboot trigger execution of KillDisk malware.

Booz Allen's recommended mitigations:

- Isolate UPS systems, and other facility management systems, from both the ICS and corporate networks.
- Disable remote management services for UPS devices wherever possible.

STEP 17: DESTROY CRITICAL SYSTEM DATA

Scheduled execution of KillDisk malware erases the master boot records and deletes system log data on targeted machines across the victims' corporate and ICS network.

Location: Corporate network and ICS network

Action: Malware execution

Timeline: December 23, 2015, during attack

Device/application: RTU device (ABB RTU560 CMU-02),[63] servers and workstations used by management, human resources (HR), and finance staff

Role in infrastructure: The RTU functions as a communication processor or data concentrator in a substation, enabling communications and data transfer between field devices in the substations and the control center.[64] Servers and workstations are used by management, HR, and finance staff to conduct business administration operations.

Exploitation method: Malware is retrieved from the network share and executed on networked devices according direction received via domain controller policy or local Windows Task Scheduler.

Impact: Targeted systems are rendered inoperable, and critical data is destroyed.

Booz Allen's recommended mitigations:

- Utilize network- and host-based antivirus software to detect and prevent known malware from infecting organization systems.
- Regularly scan organizational machine images with YARA rules to detect malware prior to execution.
- Develop and practice contingency plans that include backup and restoration of critical data.

TOP 10 TAKEAWAYS

What to Consider When Protecting Your OT Environment

1. **Know your environment**. Identifying risk starts with the need to understand your operational environment, including the topology, network and wireless connection points, and connected devices and assets. Starting with a thorough understanding of the people, processes, and technology that comprise an operational environment provides the foundation to identifying what you need to defend.
2. **Identify the key OT processes and data that need to be protected**. All processes and data are not created equal, and cybersecurity professionals often do not understand the core operations of an ICS environment. Cybersecurity professionals need to partner with plant operators to identify and understand the essential operational processes that, when disrupted, can cause significant impact on operations. By assessing and prioritizing these key processes, focused mitigation strategies can be developed to both defend and recover from cyberattacks.
3. **Understand the threats**. Threats against ICS environments continue to increase, and cybercriminals see this as an opportunity to quickly monetize their trade through ransomware and other attacks. Stay informed about what's happening across the broader threat landscape, both within your industry vertical and beyond. Understand how malicious actors may compromise your environment, whether it's launching phishing attacks against operators in your plant or injecting malicious code in ICS devices at some point in the supply chain. Engage in an active dialog with your security team to ensure they are on the lookout for these types of events, and be prepared to quickly respond.
4. **Segment your OT and IT environments**. Like the Ukraine incident, many OT attacks originate in the enterprise environment. It is important that you understand your network boundaries and connection points. We recommend implementing network segmentation between your environment using VLANs and firewalls. Also, when necessary for ultimate protection, consider data diodes or other unidirectional technologies for one-way data transfer from sensitive environments to authorized systems.
5. **Focus on the Cyber security basics**. Often, we are making it easy on cybercriminals by forgetting about the basics. Treat your OT environment like you treat the enterprise. Remember to focus on basic cyber hygiene such as (a) strong passwords (or even a password if not already protected); (b) multifactor authentication for remote access, third parties, and maintenance providers; (c) access control to protect key processes and data; and (d) the principle of least privilege for user and admin accounts.
6. **Maintain your OT security posture**. We often find HMI and other connected devices in the OT environment to be outdated from a patching perspective—remember, keep your patches up to date if possible. We recognize there are cases where vendors will not support their product when new patches are applied. In these cases, get creative because you're still at risk. Consider alternative controls, such as whitelisting or network-based security appliances that block access based on known vulnerabilities.

7. **Focus on proactive monitoring and detection, not just compliance.** A wise person once said, "Compliance solves yesterday's problem today." In today's cybersecurity landscape, new vulnerabilities and threats emerge daily. We recommend instrumenting your environment with both traditional network and end-point security solutions, along with emerging real-time OT data collection sensors. We also recommend implementing an OT monitoring environment, such as Splunk, that captures and correlates events. For security operators, we recommend watching critical processes and data for firmware and configuration changes outside the proper change control process.

8. **Train your operators**. Remember, people are usually the weakest link in a cybersecurity attack. Educate your team about the cyber and technology risks facing OT and ICS—and build awareness of the impacts these threats can have on your OT environment. Cyber criminals are actively looking to exploit ICS operations; educate staff to watch out for phishing emails and immediately report them to your cyber response team.

9. **Develop an OT incident response (IR) plan**. Everyone is vulnerable to a cyberattack; it's important to be prepared. We recommend creating an OT IR plan that addresses safety and plant operations stability as its primary goal. The IR plan should include key stakeholders, such Health and Safety, Legal, Compliance, and Environmental. Once developed, it's important that you socialize and prepare to execute your plan. We recommend using scenario-driven exercises for operators to understand threats and how to react to a cyber incident. Practice and drill using the IR plan—and do it regularly!

10. **"Red Team" your environment**. Cybercriminals think differently from traditional network defenders. They are crafty and financially motivated. It's important to view your environment from the eyes of your adversary. We recommend engaging a professional team to assess your environment from an "attacker's view." While conventional red team practices may not work in an OT environment, a skilled team that understands the delicacies of operating in this space can use offline environments and built-in redundancy to conduct these activities without affecting your operations. Once completed, you can develop a mitigation plan based on findings and periodically re-engage the red team!

CONCLUSION

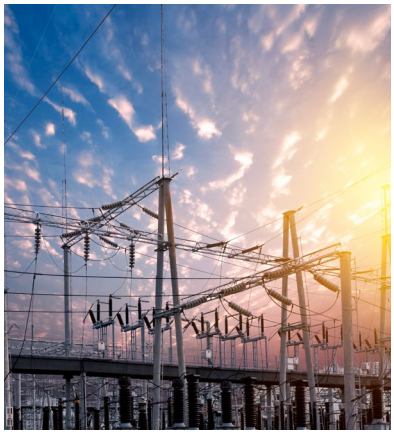
The attack against Ukraine's electricity distributors was unparalleled in its impact and demonstrated disciplined, professional execution. It is highly likely that this attack was politically motivated and conducted by a state-backed group.[h] As such, these threat actors were among the most well-resourced and well-organized adversaries an organization can face. ICS operators are capable of meeting these adversaries head-on, and the tools needed to mitigate and minimize the impact of an attack such as this are readily available.

WHAT COULD HAVE PREVENTED THE ATTACK FOR UKRAINE?

At the time of the attack, though the Ukrainian electrical distributors had exploitable holes in their security posture, they were not without defense. The Ukrainian operators had implemented firewalls between their internal networks and had segmented their ICS environment from their corporate network.[65] This segmentation should have forced attackers to search for vulnerabilities on the deployed systems, had they not already stolen valid credentials. The Ukrainian firms were also fairly well positioned to respond to the attacks; their extensive experience in manual operation of their infrastructure enabled them to get impacted systems up and running within hours of the attack, despite lacking a prepared system failure contingency plan.[66] Likewise, the firms were well prepared to investigate the incident, as they had extensive logging capability implemented across their systems and firewalls.[67] Despite these precautions, the attackers were ultimately successful. The biggest point of failure in the operator's security posture, which allowed attackers to interfere with the physical systems, was the enablement of remote access for their control environment and the lack of two-factor authentication.[68]

WHAT ABOUT THE UNITED STATES?

The risks demonstrated in the attacks in Ukraine are significant for the US for several reasons. Variants of BlackEnergy malware have been identified on multiple critical infrastructure networks in the US over the past several years.[69] Additionally, disruptions on the US grids would likely have a greater financial and social impact than in Ukraine. Given the right grid operating conditions and timing of a cyberattack, another Northeast Blackout or greater could occur. Restoration from such a blackout could be even longer if utilities were unable to remotely coordinate and operate key portions of their system.



Though a destructive attack like the Ukrainian event has not occurred in the US energy sector, various actors conduct reconnaissance and technical collection on the sector. In fiscal year 2015, members of the US energy sector reported 46 cybersecurity incidents[i] to ICS-CERT.[70] ICS-CERT does not publish a breakdown of the types of incidents by sector, but it revealed that 31 percent of total incidents reported across all sectors involved successful intrusion into operators' assets, a third of which included accessing control systems.[71] A few disclosed examples of reconnaissance targeting the US energy sector exist, the most relevant of which is a BlackEnergy campaign active from at least 2011 to 2014,[72] which the US government reportedly suspected to be Russian-government orchestrated.[73] In this case, the attackers who gained access to systems did not attempt to "damage, modify, or otherwise disrupt...processes."[74]

---

h. An in-depth analysis of the weaponized file samples and recovered VBA scripts recovered for this report are provided in Appendix B.

i. ICS-CERT defines an incident as "the act of violating an explicit or implied security policy." Examples of such incidents include the receipt of spear-phishing email messages, attempts to gain unauthorized systems access, and the existence of malware in either corporate or operational environments. Source: https://ics-cert.us-cert.gov/Report-Incident

In the near future, the likelihood of an attack against US electrical infrastructure on the scale of the Ukraine attack is very low. Based on previous research, we conclude that several nation states have the capability to conduct similar time-consuming, strategically complex attacks, but, based their current relations with the United States, these countries lack the intent to carry out such a brazen, destructive attack against US critical infrastructure.

In recent years, we have seen several government regulations and industry initiatives that have reduced the risk of such attacks. These efforts are designed and implemented to mitigate cyber risk and ultimately to protect the reliability and availability of the electrical grid.

That said, operators must remain vigilant as many threats do exist. Cybercriminals and other nonstate actors could use similar techniques and tactics to those in the Ukraine incident to deliver ransomware or other create other equally disruptive scenarios without attacking the grid directly. Additionally, global relations are in constant flux and a significant deterioration in relations with any of several countries could induce them to conduct a Ukraine-style attack in the US.

BOOZ ALLEN SERVICE OFFERINGS

Booz Allen operates at the intersection of risk and technology to deliver engineering, process, and domain-focused solutions for managing process and cybersecurity challenges in a sustainable manner. We bring the capability to work across the entire organization, from the C-Suite with business and regulatory perspectives to the plant manager and the realities of the industrial environment, to ensure business and process integrity. We have developed cutting-edge solutions to help you identify, understand, enumerate, and manage the risks in your industrial control systems (ICS) environment.

+ CyberM³™ for ICS. Booz Allen's unique assessment methodology for performing risk-based reviews of your operational technology (OT) environment. We use it to understand the key risk areas in your security posture. We focus on (1) identification and prioritization of your key industrial processes, telemetry, and data (2) identification and analysis of key industrial and plant systems, (3) risk assessment of plant, facility, and field operations, and (4) discovery to create a comprehensive view of digital systems in your OT environment. The output of CyberM³ is a picture of your current OT security maturity with a roadmap and actionable mitigation plans to improve your OT security posture.
+ Dark Labs Blacklight™ Assessment. Our security engineers employ decades of expertise shielding the world's most critical information to provide a red team assessment of your critical infrastructure and OT environment. Our Dark Labs team develops strategies to assess your systems by deploying the same techcraft malicious hackers apply to exploit them. Through binary reverse engineering, embedded security, network analysis and operations, and data science, we assess your ICS environment across a range of industries, manufacturers, and vendors to identify critical weaknesses—providing insights to preemptively secure your devices, infrastructure, and ICS systems before they're attacked.
+ Supply Chain Vendor Risk Analysis. Booz Allen provides risk-based and continuous monitoring of all aspects of the supply chain. We can work with you to define security requirements for your key technology, hardware, and software deployments; evaluate your suppliers; and embed security into your procurement process, maintenance procedures, and other aspects of your supply chain interactions to ensure that your ICS environment is not at risk.
+ ICS Security Architecture, Design, Review, and Analysis Capabilities. Booz Allen recognizes that the best way to secure your OT and ICS environment is to ensure security is embedded into the system's architecture. We provide technical leadership to architect and secure the control environment from the risks associated with cyber threats. We look at data flows, process interactions, different plant systems, and remote access and third-party access needs to create an architecture to support operational needs and protect critical assets. Our team of process and industrial systems engineers, using industry requirements and operational characteristics, will organize system components into a series of protective levels to allow secure exchange of information between systems that need it while at the same time protecting core industrial processes.

For More Information

BRAD MEDAIRY
Senior Vice President
medairy_brad@bah.com
+1-703-902-5948

SCOTT STABLES
Chief Cyber Technologist
stables_scott@bah.com
+1-630-776-7701

MATT THURSTON
Lead Associate
thurston_matthew@bah.com
+1-703-216-5259

+ ICS Monitoring (Powered by Splunk). Leveraging our intelligence community work and our commercial Cyber Fusion Center offering, we help clients implement an end-to-end ICS monitoring solution that (1) instruments critical processes and data, (2) presents an operational dashboard that provides situational awareness of security and ICS-related events, (3) actively hunts for adversary and malicious activity across the OT network. Our solution can be deployed not only to detect, flag, and manage OT incidents, but also provides insights into the plant's security, safety, reliability, and performance using advanced analytics.
+ Industrial Incident Response (IR). We work with clients to determine whether their OT IR strategy is sufficient to navigate a breach, developing a customized plan so you are ready to respond when a breach occurs. It covers the entire OT environment—from plant manager, chief information security officer, and operators to legal, HR, and communications—to clarify and test roles and procedures. If you think you've been breached, our incident response team can be on the ground within 12 hours, bringing the experience, technical expertise, and equipment to eradicate bad actors from your critical operations network and shield your organization's most valuable assets.
+ Security Programs, Training, and Awareness. We can provide the expertise to establish comprehensive training and awareness programs and to implement an overall security management framework. We provide leadership in creating and implementing end-to-end security management programs covering risk assessment, architecture and threat mitigation, and ongoing compliance and monitoring programs. As part of our training and awareness programs, we can create a training curriculum and communications plan targeted at education OT, ICS risk, and overall impact.

Booz Allen's solutions are not driven by "cyber for cyber's sake" but are focused on protecting your core operational functions; improving safety, reliability, and process integrity; and supporting regulatory compliance. Our differentiated position allows you to become safer and more secure—and able to compete in a challenging business and operational landscape.

APPENDIX A:

Detailed Textual Description of Attack Walk Through

This section is included to provide a more detailed textual summary of each of the steps outlined in the Attack Walk Through section of the report. This includes citations for all referenced sources and discussion of the analyst assessments behind each step.

RECONNAISSANCE

STEP 1: RECONNAISSANCE AND INTELLIGENCE GATHERING

It is currently unknown why the particular three power distribution companies were targeted, though reconnaissance and intelligence gathering were likely used by threat actors to identify targets. Threat actors may select several potential targets based on their strategic objectives, then use initial reconnaissance on these targets to narrow their focus and build their plan of attack. Reconnaissance can be conducted actively or passively. Active reconnaissance includes direct interactions with the targeted network, such as port scanning, whereas passive reconnaissance includes activities such as open-source intelligence gathering. Open-source intelligence gathering can also provide key situational information about the types of technologies deployed by potential targets, associated vulnerabilities, and possible attack vectors available to threat actors. Valuable targeting data, such as information on the type and kilo-voltage of hardware deployed at substations, specific model information on devices used in operator's control environment,[75,76,77,78] and likely types of operating systems used at workstations in the control environment,[79] is available on publicly accessible websites.

WEAPONIZATION

STEP 2: MALWARE DEVELOPMENT AND WEAPONIZATION

To gain unauthorized network access, attackers may target vulnerabilities in web-facing infrastructure, or develop weaponized files to deliver to users on the network. In taking a weaponization approach, attackers modify common file types, such as .pdf or .doc files, to exploit vulnerabilities in the programs used to view and edit the specific file type. Alternatively, the attackers may use social engineering tactics to encourage targeted users to enable content such as Visual Basic (VB) macro scripts. These weaponized files can be delivered to specific individuals in an organization or sent to large numbers of users, depending the level of targeting conducted by the threat actor. Ultimately, both techniques result in installation of malware, which can be used as a means to enable remote access.[80]

In the Ukraine attacks, threat actors gained access to targeted networks using weaponized Microsoft (MS) Office files, specifically Word and Excel,[81,82] by embedding BlackEnergy (BE) 3 malware in VB scripts.[j] The BE malware embedded in the weaponized files was also specifically modified for the attacks. Public reporting on BE3 samples gathered in 2015 indicates the attackers had added functionality to the malware to support specific,internalproxyserversinestablishingcommand-and-control (CC) connections.[83,84] This indicates the attackers had already gathered network infrastructure details prior to delivery of the updated malware[85] and modified the malware packages based on infrastructure at their targets.

j. An in-depth analysis of the weaponized file samples and recovered VBA scripts recovered for this report are provided in Appendix B.

DELIVERY

STEP 3: DELIVER REMOTE ACCESS TROJAN (RAT)

Public reporting consistently indicates that phishing was the initial delivery method, though the exact timeframe in which initial access was established is not confirmed. Ukraine's Deputy Energy Minister stated threat actors had access no less than six months prior to the attack.[86] Other reporting indicates the phishing campaign began on or around March 2015 and continued through January 20, 2016.[87] This March 2015 campaign used weaponized MS Office files to deliver malware via phishing attacks to many Ukrainian organizations, including the three distributors hit in the December 2015 attacks.[88] The earliest phishing attacks using weaponized MS Office documents to deliver BE malware against Prykarpattyaoblenergo were observed in May 12, 2014,[89] a year and a half before the grid disruptions in December 2015. This attack also targeted a range of Ukrainian businesses,[90] including all six of Ukraine's railway operators managed by "Ukrzaliznytsya," the State Administration of Railway Transport of Ukraine.[91] Each of these phishing attacks may have been part of a broad reconnaissance and intelligence gathering effort, and the ultimate objective of causing a destructive industrial control systems (ICS) attack may have developed later on.[92] In addition, while BE was the primary malware delivered to targeted networks, other RATs, including GCat,[93] Dropbear,[94] and Kryptik[95] were recovered in the investigation following the grid disruption in December 2015.[96,k]

EXPLOITATION AND INSTALLATION

STEP 4: INSTALL RAT

BE3 malware was embedded in malicious MS Office files, which were sent to operators in a wide-reaching phishing campaign. Upon delivery, when recipients opened the weaponized documents, they were presented with an onscreen prompt to enable the macro function for the weaponized files to execute.[97] No exploit code was used to initially deliver BE onto targeted networks.[98] Using permissions granted by the user when macros were enabled, the VBA script dropped the persistent malware files on disk at workstations of targeted employees.[l]

COMMAND AND CONTROL

STEP 5: ESTABLISH CC CONNECTION

The primary function of BE3 malware is to establish a hook into targeted networks, enable persistent, unauthorized access, and use this access to gather intelligence on the targeted systems. The first step in this process is establishing a connection with an external CC server. After installation, the BE implant modifies in-registry Internet settings and MS Internet Explorer security settings, then uses HTTP POST requests to contact an external CC server.[m]

---

k. Additional discussion of the alternate RATs observed on the electricity distributor networks is provided in Appendix D.

l. By analyzing the weaponized files, the step-by-step process the BE malware executed to insert itself into targeted networks is revealed. A detailed summary of the infection routine for recovered malware samples used in the Ukraine attacks in included in Appendix B.

m. Additional details on communication process are provided in Appendix B.

ACTION ON OBJECTIVES: INTERNAL RECONNAISSANCE AND LATERAL MOVEMENT

STEP 6: DELIVER MALWARE PLUGINS

After establishing connections to the delivered BE implant, attackers used this access to acquire employee credentials, allowing them to use existing remote access services to maintain a presence on the network.[99] Specific details on how the credentials were harvested are not publicly reported, though analysis of the BE malware provides some insight into the methods threat actors may have leveraged.

One of the key features of BE is its modular nature and ability to download plugins designed for many different tasks.[100,n] Once loaded onto a targeted system, and having established connections with the CC server, BE3 is capable of receiving a range of commands, including uninstall, load or unload plugin, update DLL, download and execute executable, download and execute a binary, or update configuration data.[101] After loading any plugins, the BE3 implant communicates with them internally using remote procedure calls (RPC) over named pipes.[102] The threat actors likely downloaded several plugins onto the targeted networks, following the initial infection, and used these plugins in several stages of the attack, including the harvest of user credentials.

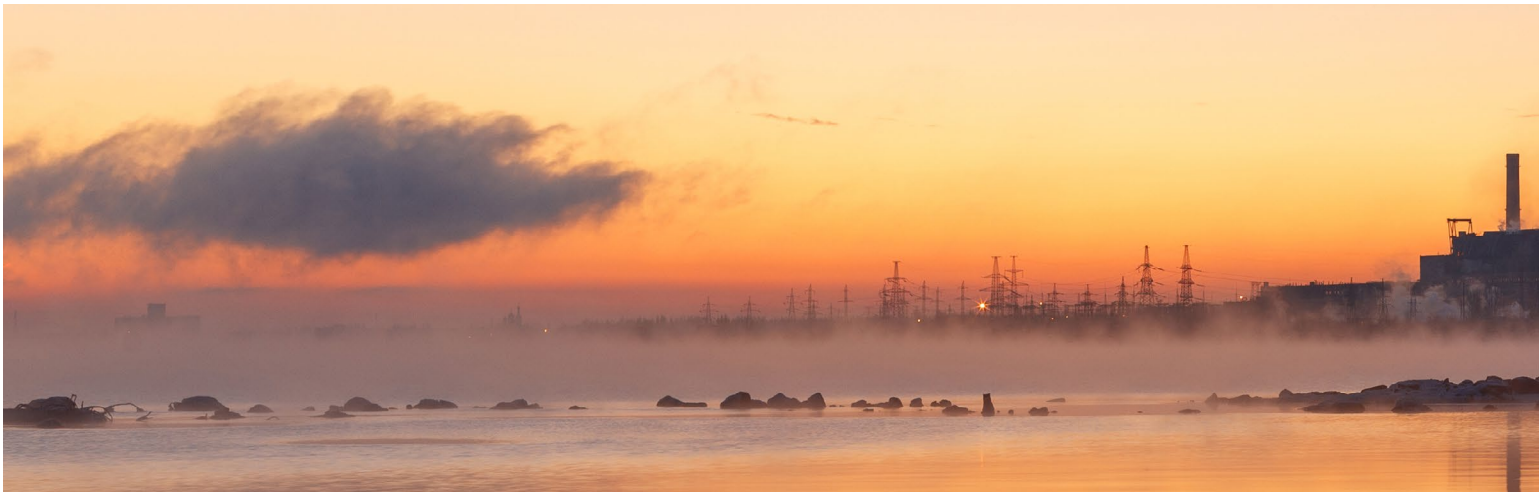
STEP 7: HARVEST CREDENTIALS

Credential harvesting was likely an iterative process beginning with malware exfiltration then shifting to direct interaction with deployed systems by the attackers. Credentials can be stolen using a wide range of the methods, such as social engineering, keylogging, or targeting of specific applications, such as password managers. In the Ukraine attacks, credentials were likely collected using associated BE plugins specifically designed for this task. The plugins likely used to harvest credentials in the Ukraine attack are the PS.dll plugin, designed to harvest stored user credentials,[103] SI.dll plugin, which gathers system data and stored passwords from a range of applications,[104] and the KI.dll plugin, which logs keystrokes.[105,o] In at least one instance, attackers used their access to create additional, unauthorized domain accounts.[106] Other reporting

---

n. An in-depth discussion of BE capabilities for receiving and communicating with plugins, as well as the capabilities and functions of identified plugins are detailed in Appendix B and Appendix C.

o. Additional detail on these plugins is provided in Appendix C.



indicates the attackers eventually gained access to Windows domain controllers, where they gathered credentials for the virtual private network (VPN) used by grid operators to access the control network remotely.[107] In the attack against the Ukrainian media outlets,[p] attackers used VPN to access an administrator account then used remote desktop protocol (RDP) service from the administrators' account to access the domain controller.[108] It is plausible that threat actors repeated this tactic against the electricity distributors.

Once the attackers had valid credentials, the attackers likely shifted away from this initial hook into the network provided by the BE implant in favor of native remote access services such as VPN.[109] The benefit of shifting away from the network access provided by the malware, and establishing multiple lines of communication, is that it supports persistent access and minimizes visibility of malicious activity.[110] If any one connection is discovered and removed, threat actors have redundant connections, and, by using trusted communications, threat actor activity blends in with normal traffic of authorized users.[111]

STEP 8: LATERAL MOVEMENT AND TARGET IDENTIFICATION ON CORPORATE NETWORK

Little information is publicly available on the lateral movement and internal reconnaissance efforts, though the list of targets in the final attack indicate extensive network discovery. Targeted systems include networked uninterruptable power supply (UPS) devices, data center servers, a telephone communications server, and employee workstations.[112] This movement likely involved a range of activities over a lengthy period, including gathering of credentials, and identification of potential targets and services to be leveraged in the attack.[113] As with the initial credential harvesting, network discovery was likely aided with dedicated BE plugins, specifically the VS.dll plugin. VS.dll scans for connected network resources, attempts to retrieve remote desktop credentials, and establishes connections to remote systems using the MS Sysinternals PsExec tool.[114] In the attack against Ukrainian media outlets,[q] anomalous use of PsExec to enumerate and establish remote access to networked systems was logged on administrator workstations.[115] Threat actors may have used this same tactic two months later against the three electricity distributors.

STEP 9: LATERAL MOVEMENT AND TARGET IDENTIFICATION ON ICS NETWORK

Ultimately, after gaining initial access to the corporate network and harvesting valid user credentials, the threat actors were able to navigate successfully from the corporate IT network into the control environment, hosting the human machine interface (HMI) workstations, distributed management system (DMS) servers, and networked field devices. Threat actors used valid credentials to establish at least two pathways into the control environment; these included remote administration tools to access operator workstations and VPN services to interact directly with the client application for the DMS server.[116] As noted above, public reporting indicates VPN credentials for the control environment may have been recovered from Windows domain controllers.[117] Access to the HMI workstations and DMS application was likely sufficient for threat actors to

p. *The original source did not explicitly mention the target in their summary of the investigation, though the blog indicated the attack was conducted on October 25, 2015, against a Ukrainian target, and used BE3 and KillDisk.*

q. *The original source did not explicitly mention the target in their summary of the investigation, though the blog indicated the attack was conducted on October 25, 2015, against a Ukrainian target, and used BE3 and KillDisk.*

enumerate all of the networked devices. Unlike corporate networks, ICS networks often follow a hub-and-spoke orientation, with a single, centralized control point. It is unlikely the threat actors used the associated BE network discovery plugins referenced above; using active discovery methods, such as scanning, may interfere with necessary communications or cause communication cards to fail.[118] Systems identified during this reconnaissance phase, and targeted in the final attack, include HMI workstations, DMS servers, control center UPS,[119] serial-to-Ethernet converters, and the substation breakers.[120]

Though this attack was conducted remotely using valid credentials, tampering with the physical network connections to field devices, such as RJ45 or Fiber cabling, can provide another method to gain network access. A mitigation strategy to prevent malicious code or a laptop from entering the network could be something as simple as a "sticky MAC" program, whereby the network switch port is configured to whitelist the unique MAC address of a specific intelligent controller, and becomes disabled in the event the field device gets disconnected. Similarly, if the network includes wireless telemetry, this could also provide an entry-point for attackers. This risk can be mitigated using FIPS 140-2 or similar encryption technology.

During their target selection process, threat actors likely used their network access to familiarize themselves with ICS configuration, interfaces, command processes, and other operational details of systems at each organization. Even if threat actors are familiar with the deployed devices and applications, often system configurations will be customized at individual facilities based on operator needs or preferences. Prior to the final attack, the attackers learned how to direct the DMS at each of the three companies, using the existing controls and HMI displays.[121] Because this activity was likely executed on the operator network, little forensic information on this process was generated.[122]

ACTION ON OBJECTIVES: ATTACK PREPARATION

STEP 10: DEVELOP MALICIOUS FIRMWARE

This incident was the first instance where threat actors developed malicious firmware update for a specific attack.[123] In conducting a firmware attack, threat actors will push an update that will either patch or completely replace the old firmware. This is often done in an unauthenticated manner without any verification that the new or updated firmware is valid. Alternatively, in some attacks threat actors have compromised vendor websites and hosted weaponized firmware to be downloaded and installed by operators.[124]

Typically, the system running the firmware will be rebooted for the new firmware to be fully installed and operational. At this point, anything malicious that has been added to the firmware will have a chance to execute, depending on how the code is designed; this could be immediately upon reboot, or may be based on some trigger. Samples of the malicious firmware used in the Ukraine attacks were not recovered, and specific detail on the execution process could not be derived.

Well-resourced and highly organized groups may also conduct testing of malware or exploit code intended for use on targeted systems.[125] Threat actors may obtain specific ICS hardware or

software, and configure them to match the operator environment.[126] Investigators assessed that it is unlikely the threat actors executed the attacks in Ukraine without some level of prior capability testing, particularly the malicious firmware updates.[127] Given the apparent resources and professionalism of the group, outside observers assessed the threat actors may have used systems of their own to confirm the effectiveness of the modified firmware used in the final stages of the attack.[128]

STEP II: DELIVER DATA DESTRUCTION MALWARE

In addition to opening breakers, the threat actors also used a data destruction malware, known as KillDisk, at all three distributors to wreak havoc on networked machines. Threat actors have used both KillDisk and BE3 malware together in multiple attacks,[129] but analysis of recovered samples of BE3 does not indicate any technical link between the two malware applications. KillDisk is a separate, standalone executable (.exe) file used in conjunction with BE3 during the attack. The malware was likely loaded onto targeted networks as one of the final preparations directly prior to attackers opening the breakers. Public reporting indicates that the KillDisk malware may have been set as a logic bomb when placed on targeted machines, with a specific time delay before the destructive functions of the malware executed.[130] This would ensure data destruction would coincide with, or shortly follow, the attacks against breakers.

The use of an internal scheduling function is unlikely; BE has an associated data destruction plugin, DSTR.dll, which includes an execution time in its configuration data, but recovered KillDisk samples did not include any such capability. In the attack against Ukrainian media outlets,[r] attackers placed KillDisk malware on a network share and used a compromised administrator account to access domain controller servers.[131] On the domain controller servers, they scheduled a policy for every workstation to retrieve and execute the file following reboot.[132] Public reporting indicates that, in the attack against electricity distributors, credentials were retrieved from compromised domain controllers[133] and that UPS disruptions triggered KillDisk execution on data center servers.[134] Both of these claims support the assessment that the tactic used in the media attack was also used against the electricity distributors. Attackers may have also used administrator access to remotely schedule retrieval and execution of the malware using Windows Task Scheduler on high-priority target machines.[135] This method was also used in

r. *The original source did not explicitly mention the target in their summary of the investigation, though the blog indicated the attack was conducted on October 25, 2015, against a Ukrainian target, and used BE3 and Killdisk.*

the Ukrainian media attack as a contingency measure to ensure the data destruction attack would be successful should the domain controller server crash.[136]

STEP I2: SCHEDULE UPS DISRUPTION

Attacks against operators' UPS systems were conducted against at least two of the three affected power distributors.[137] UPS outages were scheduled using remote management interfaces,[138] and affected devices included an internal telephony communications server at one firm and the main data center at a second operator.[139] Public reporting also indicates the UPS outages affected two of the control centers, disabling the ability of operators to monitor the control network.[140] In disrupting the telephony server, the attackers severed internal communications across the firm and with workers at remote sites. In the attack against the data center, the scheduled outage was entered directly preceding the malicious interactions with the firms' substation breakers, and was set to execute several hours following the attack.[141] In this attack, public reporting indicates that the server reboot caused by the power disruption also triggered the disk-wiping function of the KillDisk malware, which had been loaded onto the systems.[142]

Some UPS network management cards support remote monitoring and control via web browser, command line interface, or SNMP, enabling reboot and scheduling of shutdowns.[143] Details on the specific UPS devices deployed by each of the distributors was not found in public reporting, so the remote access services used to access the devices cannot be confirmed. In addition, while the threat actors likely used valid credentials in this attack, vulnerabilities such as cross-site scripting have been identified in some UPS management devices.[144]

This component of the attack is not technically complex, but it serves as an effective illustration of the level of organization exhibited in this multifaceted attack. Two of the reported UPS disruptions were essentially direct threat actor interactions with two systems, using remote access, to cause second-order effects (i.e., server backup power loss), which triggered malware execution upon reboot for one target, and mirrored the communication disruption (i.e., telephony denial of service [TDoS]) of a nearly simultaneous attack against another target. The attacks also highlight the dependencies of computer network components on peripheral systems, such as power supply, HVAC, or even physical security. Vulnerabilities in these systems may be used by threat actors as additional means of accessing or interfering with network devices.

ACTION ON OBJECTIVES: EXECUTE ATTACK

STEP I3: TRIP BREAKERS

After months of clandestine access, reconnaissance, and preparation, the threat actors executed the final step in their attack: disrupting operation of the electrical grid itself. Using existing remote access tools similar to RDP and Radmin,[145] threat actors took control of employee workstations hosting the HMI and actively issued commands to open individual breakers across the managed substations. During the attack, users sitting at the workstation could observe the commands being issued but were unable to use their mouse and keyboard to interfere with the attack.[146] In some instances, the attacks also used an existing DMS client application to send commands to open breakers directly to the DMS server using their VPN access.[147] The direct interactions with DMS

and employee workstations were conducted by multiple threat actors, and were all conducted within a 30-minute window[148] at some point between 15:30 and 16:30 local time.[149] Investigators noted that, prior to execution of the final attack, the threat actors modified passwords for some users to lock them out of the system during recovery.[150]

In all, the attackers opened breakers in at least 57 substations. Though complete details on the extent of the attack are not publicly available, one of the three operators, Prykarpattyaoblenergo, indicated that 27 of its substations were taken offline, resulting in complete blackouts across 103 cities and partial blackouts in an additional 186 cities.[151] Kyivoblenergo indicated that seven of its 110kV substations and 23 of its 35kV substations were taken offline, disconnecting power for 80,000 customers.[152] Impacts on the infrastructure of Chernivtsioblenergo were not found in public reporting.

STEP 14: SEVER CONNECTION TO FIELD DEVICES

Public reporting indicates that the updates were pushed to each of the devices within a short period, and the firmware itself was uniform across the targeted converters.[153] With the communications between the control center and field devices severed, even after control of the network was restored, the breakers could not be closed remotely and technicians had to manually close them at each substation.[154] Manually resetting the breakers, the technicians were able to restore power to customers within three to six hours.[155]

Ultimately, neither the operator nor the manufacturer was able to restore the devices following the malicious update, which forced operators to replace all targeted devices.[156] At least 16 substations were disconnected from the control network using the malicious firmware updates.[157]

The two converters targeted in the attack were the Moxa UC 7408-LX-Plus and the IRZRUH2 3G.[158] While both of these devices support firmware updates by authorized users, indicating the attackers may have used the credentials harvested earlier in the attack to push the malicious updates,[159] they are also both susceptible to known vulnerabilities.

The Moxa device includes an extensive number of vulnerabilities, and the source code itself is publicly available; access to the source code is of particular concern, as it would allow threat actors to directly examine the code for vulnerabilities. The identified Moxa firmware vulnerabilities included arbitrary code execution[160] and multiple remote denial-of-service (DoS) vulnerabilities;[161,162] in addition, several of the fixes for the device were incomplete, leading to follow-on vulnerabilities.[163,164] Though the iRZ-RUH2 was relatively more secure and source code for the firmware did not appear to be publicly available, the device still included a least one vulnerability that would allow an authorized user to remotely update the firmware with an unvalidated patch.[165]

STEP 15: TDOS ATTACK

In an apparent attempt to block incoming communications, threat actors also conducted a

TDoS attack against at least one operator. TDoS attacks are similar to DoS attacks against webservers or other data network systems; a flood of communication traffic is used to block legitimate communications by overwhelming infrastructure bandwidth or call-center staff.[166]

Public reporting indicates that directly prior to opening breakers, one of the operators began receiving thousands of calls at its call centers that appeared to be coming from Moscow.[167,168] By preventing operators from receiving outage reports, threat actors may have intended to mask the impact of the outage and possibly draw out recovery time. Alternatively, investigators also noted the TDoS attacks may have been focused on blocking callers from receiving information, in order to create greater confusion and frustration toward the operators among their customer base.[169]

It is highly likely the TDoS attack in Ukraine was conducted using automated tools, though specific details regarding how the TDoS attack was conducted are not documented in public sources. While not as common as DoS attacks against data networks, there are existing tools to automate the process. Free software, including Asterisk IP PBX and SIP call generator, can be used by attackers to send floods of robocalls at targeted systems.[170] Similar to DoS attacks, TDoS floods can be amplified using distributed botnets, and paid services to launch TDoS attacks have also been observed in criminal forums.[171] Previously, TDoS attacks have been used to target firms in the financial sector and emergency responder call centers in the US.[172] The attacks against emergency responders were principally conducted by criminal groups as part of extortion operations.[173]

STEP 16: DISABLE CRITICAL SYSTEMS VIA UPS OUTAGE

As noted above, the UPS disruptions were likely scheduled in advance of the final attack on the substation breakers. The targeted systems included a telephone communication server and data center servers.[174] Public reporting also indicated the disruption impacted control center systems, though specific details on targeted devices were not provided.[175]

STEP 17: DESTROY CRITICAL SYSTEM DATA

KillDisk was retrieved and executed on networked devices at all three distributors.[176] The malware overwrote the master boot record (MBR), and in some instances continued to overwrite additional data on disk. Several variants of KillDisk malware were used in the attack; execution routine and extent of data destruction varied.[s] Affected machines were rendered completely inoperable, adding an additional burden on incident responders and ultimately driving up recovery costs to replace targeted devices.

Disk-wiping attacks were not executed against all network devices. Targets were primarily on operators' enterprise networks, particularly servers and hosts used by management, human resources, and finance staff, though the attackers also destroyed at least one remote terminal unit (RTU) with an embedded windows HMI card.[177]

s. *An in depth analysis of each of the recovered Killdisk samples is provided in Appendix B, including assessments of key variations between execution routines.*

APPENDIX B:

Malware Samples

The malware samples analyzed for this report can be categorized into four distinct groups. These groups include:

- Weaponized files used to deliver malware to targeted systems
- Malicious scripts embedded in the weaponized files used to install a persistent implant
- Persistent implants used to provide remote access onto the network
- Additional destructive malware, specifically the KillDisk malware, used to overwrite data during the final stages of the attack.

Samples from each of these categories are detailed in the following sections. Though predominantly BlackEnergy (BE) samples, a weaponized version of Dropbear server, and an associated Visual Basic (VB) dropper are also detailed. Multiple samples of the KillDisk malware were analyzed for this report. Samples analyzed for this report were gathered using the Virus Total Intelligence (VTI) service. The "First Upload," "Final Modification," "Language Settings," and "File Name" data in the malware analysis tables were gathered from the VTI summary for the reported sample.

DELIVERY MALWARE

Most public reporting on the December 2015 attacks indicate that the malware was initially delivered to targeted networks using weaponized Microsoft (MS) Office documents. Several recovered samples indicate attackers had some variation in their delivery method. Recovered samples included both a weaponized MS Excel[t] file and a weaponized MS Word document.[u] Samples of BE2 recovered following an attack on a Ukrainian news outlet in October 2015[178] indicate the threat actors may have also embedded malware in a compromised Cyberlink PowerDVD 10 binary[v] (a movie/media player) or a file designed to look like Cyberlink PowerDVD 10 via string analysis. This particular sample file functioned as an installer, delivering a BE2 implant[w] and encrypted configuration[x] file to the targeted system. Though not definitively conducted by the same group behind the attacks against the electricity distributors, the attack on the Ukrainian media outlet, which was conducted on Ukraine's election day, shared the common tactics, techniques, and procedures (TTP) of using a combination of BE malware and KillDisk malware to destroy critical data.[179]

t. *Appendix B.1: Weaponized MS Excel (Додаток1.xls) (MD5: 97b7577d13cf5e3bf39cbe6d3f0a7732)*

u. *Appendix B.2: Weaponized MS Word ($RR143TB.doc) (MD5: e15b36c2e394d599a8ab352159089dd2)*

v. *Appendix B.5: BE2 Installer (Undisclosed) (MD5: 1d6d926f9287b4e4cb5bfc271a164f51)*

w. *Appendix B.11: Implant (adpu160m.sys) (MD5: e60854c96fab23f2c857dd6eb745961c)*

x. *Appendix B.12: Encrypted Configuration/On-disk-store (ieapflrt.dat) (MD5: 01215f813d3e93ed7e3fc3fe369a6cd5)*

APPENDIX B.1:
WEAPONIZED MS EXCEL (ДОДАТОК1.XLS)[y]

SHA1: aa67ca4fb712374f5301d1d2bab0ac66107a4df1	
SHA-256: 052ebc9a518e5ae02bbd1bd3a5a86c3560aefc9313c18d81f6670c3430f1d4d4	
MD5: 97b7577d13cf5e3bf39cbe6d3f0a7732	
Type: Microsoft Office Excel[180]	**First Upload:** 2015-08-03 10:37:19[181]
Compile Timestamp: 2015-02-04 07:35:08[182]	Final Modification Timestamp: 2015-03-18 07:41:04[183]
File Size: 734720 bytes[184]	**Language Settings:** Code_page is Cyrillic[185]
File Names: Додаток1.xls[186]	
Technical Notes: This is a weaponized MS Excel file used to deliver BE3 malware.[187] Upon opening the file, users are prompted to enable macros. The spreadsheet includes an embedded VBA macro that executes when users enable the macro functionality. The associated VBA macro is a BE3 installer.[188]	
Related Samples: 1. Appendix B.4: BE3 Installer (VBA_macro.exe, Sample 2) (MD5: abeab18ebae2c3e445699d256d5f5fb1) 2. Appendix B.6: Dropbear Installer (DropbearRun.vbs) (MD5: 0af5b1e8eaf5ee4bd05227bf53050770)[189]	

APPENDIX B.2:
WEAPONIZED MS WORD ($RR143TB.DOC)[z]

SHA1: 28719979d7ac8038f24ee0c15114c4a463be85fb	
SHA-256: 39d04828ab0bba42a0e4cdd53fe1c04e4eef6d7b26d0008bd0d88b06cc316a81	
MD5: e15b36c2e394d599a8ab352159089dd2	
Type: Microsoft Office Word[190]	**First Upload:** 2016-01-20 08:03:52 UTC[191]
Compile Timestamp: 2015-07-27 10:21:00[192]	Final Modification Timestamp: 2015-07-27 10:21:00[193]
File Size: 1194496 bytes	**Language Settings:** Code_page is Cyrillic[194]
File Names: $RR143TB.doc[195]	
Technical Notes: This is a weaponized MS Word file, with an embedded BE3 installer.[196] Upon opening the file, users are prompted to enable macros, allowing the execution of the BE3 installer.[197] Additional details on the infection routine are provided in Appendix B.6: BE3 Installer (VBA_macro.exe, Sample 1).	
Related Samples: 1. Appendix B.6: BE3 Installer (VBA_macro.exe, Sample 1) (MD5: ac2d7f21c826ce0c449481f79138aebd)	

y. A sample of this file was not recovered. The technical notes provided are based on the cited reporting.

z. A sample of this file was not recovered. The technical notes provided are based on the cited reporting.

MALWARE INSTALLERS

In an analysis of a weaponized MS Excel file[aa] first observed in August 2015 and most recently reported in January 2015, BE3 malware was found embedded in VB code attached as a macro title: "M 609230 '_VBA_PROJECT_CUR/VBA/Workbook_____".[198] By using weaponized macros as the attack vector, the threat actors were reliant on users actively enabling macros before they could execute. Samples of the malicious VBA scripts recovered are detailed in Appendix B.3 and Appendix B.4.

Following delivery, users enabled macros in the weaponized document, allowing the embedded macros to execute. The executable calls ENVIRON('TMP') and saves the file, vba_macro.exe in the Widows TMP directory.[199] Once saved to disk, the file drops FONTCACHE.DAT (which is a dynamic-link library file), rundll32.exe (which is the standard utility for running .dll files on machines with Windows operating system [OS]), NTUSER.LOG (which is an empty file) and desktop.ini, the default file used to determine folder displays on windows machines.[200]

FONTCACHE.DAT serves as the primary BE3 implant, and as noted above, some observed samples have been packed with the tElock packer. FONTCACHE.DAT is dropped into the local application data folder, and a .lnk file is created in the startup folder, which functions as a shortcut to execute using rundll32.exe.[201] The .lnk file name is generated off the volume serial number.[ab,202,203] Following delivery of FONTCACHE.DAT, and the associated .lnk file, the original executable, vba_macro.exe, is deleted.[204]

aa. Analysis details for this sample provided in Appendix B.1.

ab. An example path for the .lnk file would be: C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\{9980061D-64BB-46BC-8AC6-D9AC3DB67577}.lnk

APPENDIX B.3:

BE3 INSTALLER (VBA_MACRO.EXE, SAMPLE 1)

SHA1: 4184888c26778f5596d6e8d83624512ed2f045dd	
SHA-256: ca7a8180996a98e718f427837f9d52453b78d0a307e06e1866db4d4ce969d525	
MD5: ac2d7f21c826ce0c449481f79138aebd	
Type: Win32 Executable[205]	**First Upload:** 2016-01-29 01:59:28 UTC[206]
Compile Timestamp: 1979-01-28 00:25:53[207]	**Final Modification Timestamp:** Undisclosed
File Size: 110592 bytes[208]	**Language Settings:** Japanese[209]
File Names:[210] CPLEXE.EXE (original name) MS-IME (Internal Name) virus_04.exe vba_macro.exe	

Technical Notes:
At execution:

1. The installer drops a .dll file at C:\Documents and Settings\useradm\Local Settings\Application Data\FONTCACHE.DAT (size 56,832)
2. And installs persistence:
    a. C:\Documents and Settings\useradm\Start Menu\Programs\Startup\{C323A392-5BB0-47D5-9518-E60202A85B5C}.lnk (size 1,682)
3. Weakens Internet settings in registry to lower Internet security:
    a. HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass (sets to 1)
    b. HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName (sets to 1)
    c. HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet (sets to 1)
4. It launches (in this case PID: 936) Command line: "C:\WINDOWS\system32\rundll32.exe" "C:\Documents and Settings\useradm\Local Settings\Application Data\FONTCACHE.DAT",#1
    a. Further weakening Internet Explorer settings:
        i. HKCU\Software\Microsoft\Internet Explorer\PhishingFilter\Enabled (sets to 0)
        ii. HKCU\Software\Microsoft\Internet Explorer\Recovery\NoReopenLastSession (sets to 1)
        iii. HKCU\Software\Microsoft\Internet Explorer\Main\NoProtectedModeBanner (sets to 1)
        iv. [Amongst some other I.E. settings]
    b. And loads BE into "svchost.exe -DcomLaunch"

5. It then launches (in this case PID: 1804) Command line: /s /c "for /L %i in (1,1,100) do (attrib +h "C:\DOCUME~1\useradm\Desktop\CA7A81~1.EXE" & del /A:h /F "C:\DOCUME~1\useradm\Desktop\CA7A81~1.EXE" & ping localhost -n 2 & if not exist "C:\Documents and Settings\useradm\Local Settings\Application Data\FONTCACHE.DAT" Exit 1)"
    a. This self deletes it's installer
6. "svchost.exe -DcomLaunch" launches iexplorer.exe
    a. "C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
        i. which beacons to 5.149.254.114:80

This sample differs only slightly from Sample 2 (MD5:abeab18ebae2c3e445699d256d5f5fb1), in that this sample (MD5:ac2d7f21c826ce0c449481f79138aebd) has a rundll32.exe that remains visible in the process list on the victim throughout the initial infection and following every reboot. The following sample does not have this indicator of compromise, as the rundll32 process is only visible for a short period following the initial infection.

Related Samples:

1. Appendix B.7: BE3 Implant (Fontcache.dat, Sample 1) (MD5: 3fa9130c9ec44e36e52142f3688313ff)
2. Appendix B.9: BE3 Implant (.LNK Persistence Mechanism, Sample 1) (MD5: 40c74556c36fa14664d9059ad05ca9d3)

APPENDIX B.4:
BE3 INSTALLER (VBA_MACRO.EXE, SAMPLE 2)

SHA1: 4c424d5c8cfedf8d2164b9f833f7c631f94c5a4c	
SHA-256: 07e726b21e27eefb2b2887945aa8bdec116b09dbd4e1a54e1c137ae8c7693660	
MD5: abeab18ebae2c3e445699d256d5f5fb1	
Type: Win32 Executable[211]	**First Upload:** 2015-08-03 10:37:19[212]
Compile Timestamp: 1979-01-28 00:25:53[213]	**Final Modification Timestamp:** Undisclosed
File Size: 98304 bytes[214]	**Language Settings:** Japanese[215]
File Names:[216] vba_macro MS-IME icshextobin.exe BlackEnergy.exe vba_macro.exe CPLEXE.EXE 1.exe	

Technical Notes:
This installer follows a routine very similar to the sample detailed in Appendix B.4 (MD5: ac2d7f21c-826ce0c449481f79138aebd); in fact, 33% of its code is shared with that sample.

At execution:

1. The installer drops a .dll file at C:\Documents and Settings\useradm\Local Settings\Application Data\FONTCACHE.DAT (size 55,808)
2. The installer then delivers the persistent .link file at C:\Documents and Settings\useradm\Start Menu\Programs\Startup\{C323A392-5BB0-47D5-9518-E60202A85B5C}.lnk (size 1,682)
    a. this .lnk calls rundll32.exe to execute FONTCACHE at system startup
3. Weakens internet settings in registry to lower Internet security:
    a. HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass (sets to 1)
    b. HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName (sets to 1)
    c. HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet (sets to 1)
4. Launches (in this case PID: 2696) Command line: "C:\WINDOWS\system32\rundll32.exe" "C:\Documents and Settings\useradm\Local Settings\Application Data\FONTCACHE.DAT",#1
    a. Further weakens Internet Explorer settings:
        i. HKCU\Software\Microsoft\Internet Explorer\PhishingFilter\Enabled (sets to 0)
        ii. HKCU\Software\Microsoft\Internet Explorer\Recovery\NoReopenLastSession (sets to 1)
        iii. HKCU\Software\Microsoft\Internet Explorer\Main\NoProtectedModeBanner (sets to 1)
        iv. [Amongst some other I.E. settings]
    b. Loads BE into "svchost.exe -DcomLaunch"
5. Launches (in this case PID: 2704) Command line: /s /c "for /L %i in (1,1,100) do (del /F "C:\DOCUME~1\useradm\Desktop\07E726~1.EXE" & ping localhost -n 2 & if not exist "C:\DOCUME~1\useradm\Desktop\07E726~1.EXE" Exit 1)"
    a. Deletes BE on-disk installer
6. Fontcache (from within svchost.exe -DcomLaunch) launches "C:\Program Files\Internet Explorer\iexplore.exe -Embedding"
    a. Which beacons to 5.149.254.114:80

Related Samples:

1. Appendix B.8: BE3 Implant (FONTCACHE.DAT, Sample 2)
   (MD5: cdfb4cda9144d01fb26b5449f9d189ff)
2. Appendix B.9 BE3 Implant (.LNK Persistence Mechanism, Sample 2)
   (MD5: bffd06a38a46c1fe2bde0317176f04b8)

APPENDIX B.5:

BE2 INSTALLER (UNDISCLOSED)

SHA1: 896fcacff6310bbe5335677e99e4c3d370f73d96	
SHA-256: 07a76c1d09a9792c348bb56572692fcc4ea5c96a77a2cddf23c0117d03a0dfad	
MD5: 1d6d926f9287b4e4cb5bfc271a164f51	
Type: Win32 Executable[217]	**First Upload:** 2015-10-11 04:17:36 UTC[218]
Compile Timestamp: 0000:00:00 00:00:00[219]	Final Modification Timestamp: Undisclosed
File Size: 155648 bytes[220]	**Language Settings:** English[221]
File Names: Undisclosed	

Technical Notes:
This is a BE2 dropper, installer, and RAT bundle. It is either a modified Cyberlink PowerDVD 10 binary or is designed to look like one during string analysis.

The installer appears to be packed, possibly with tElock.
The associated implant is packed with tElock 0.99.
This bundle includes an encrypted file, which is likely the configuration file stored on disk.

Infection Routine:

1. Installer 1d6d926f9287b4e4cb5bfc271a164f51.exe (in this case PID 596) executes
2. Installer creates file c:\windows\adpu160ms then pings localhost "-n 2" (effectively a 2 second sleep)
3. Installer pings localhost "-n 3" (effectively a 3 second sleep)
4. Installer launches a cmd.exe (in this case PID 880) with the following command line:
   a. PID: 880, Command line: /c "ping localhost –n 8 & move /Y "C:\WINDOWS\adpu160ms" "C:\WINDOWS\system32\drivers\adpu160m.sys" & ping localhost –n 3 & net start adpu160m"
5. Services.exe (in this case PID 768) writes the registry keys for apdu160m and loads adpu160m.sys into "svchost.exe –DcomLaunch" (in this case PID 988)

6. Once loaded into "svchost.exe –DcomLaunch" (PID 988) the malware writes a 203-byte, encoded, and timestamped file to c:\windows\system32\ieapflrt.dat, which is likely a configuration file.
7. The implant then performs a reverse lookup to 5.9.32.230 and attempts to initiate a TCP connection over port 443. The implant goes through this routine frequently, nearly every two minutes.

Related Samples:

1. Appendix B.7: Implant (adpu160m.sys)
   (MD5: e60854c96fab23f2c857dd6eb745961c)
2. Appendix B.8: Encrypted Configuration/On-disk-store (ieapflrt.dat)
   (MD5: 01215f813d3e93ed7e3fc3fe369a6cd5)

APPENDIX B.6:
DROPBEAR INSTALLER (DROPBEARRUN.VBS)[ac]

SHA1: 72d0b326410e1d0705281fde83cb7c33c67bc8ca	
SHA-256: b90f268b5e7f70af1687d9825c09df15908ad3a6978b328dc88f96143a64af0f	
MD5: 0af5b1e8eaf5ee4bd05227bf53050770	
Type: ASCII text[222]	**First Upload:** 2015-10-13 10:51:25 UTC[223]
Compile Timestamp: Undisclosed	Final Modification Timestamp: 2015-03-17 06:41:04 UTC+0[224]
File Size: 165 bytes[225]	**Language Settings:** Undisclosed
File Names: DropbearRun.vbs[226] VBS/Agent.AD trojan[227]	
Technical Notes: This script launches the Dropbear SSH server from directory C:\\WINDOWS\TEMP\DROPBEAR\, and sets the server to listen on port 6789.[228] The modified version of the Dropbear server includes two backdoors, a hardcoded public key authentication process, and a hardcoded username and password.[229]	

Related Samples:

1. Appendix B.4: BE3 Installer (VBA_macro.exe, Sample 2)
   (MD5: abeab18ebae2c3e445699d256d5f5fb1)
2. Appendix B.13: Dropbear Implant (Dropbear.exe)
   (fffeaba10fd83c59c28f025c99d063f8)

ac. A sample of this file was not recovered. The technical notes provided are based on the cited reporting.

PERSISTENT MALWARE IMPLANTS

After dropping FONTCACHE.DAT into the application data directory and inserting the associated .lnk file in the startup directory, the installer takes steps to modify the Internet security setting and initiate the process of connecting to the command-and-control (CC) server. The installer first modifies in-registry Internet settings to lower the Internet security, then uses rundll32.exe to launch FONTCACHE.DAT, which in turn further weakens Internet security settings, specifically targeting MS Internet Explorer. FONTCACHE.DAT is then loaded into svchost.exe, the standard process used for hosting services running off .dll files, which then launches iexploerer.exe and attempts to use Internet Explorer to establish an HTTP connection with an external host.[ad] In the analyzed sample, the implant attempted to connect to IP address 5.149.254.114.[ae] This IP address was identified as a potential CC server in other BE3 analysis reporting.[230]

Communications between the infected host and the CC server are conducted using HTTP POST requests.[231] During the initiation of the connection, BE3 requests will contain fields such as a SHA1 hash of the bot_id, domain security identifier (SID), host name and serial number, as well as build_id from the samples configuration data, and a series of hardcoded values representing the associated version number.[232] The CC server then sends a decrypted response as a series of 509_ASN encoded values.[233]

In the initial POST request sent to the CC server, the hashed build_id is a unique text string associated with each individual infection.[234,235] These build_ids, as well as a list of the CC servers, are stored in the embedded configuration data within the binary of the .dll implant.[236] Publicly reported analysis of the BE3 samples indicate that at least 12 build_ids had been identified in 2015, and the strings included in the build_ids are likely significant.[237] The 12 build_ids recovered in 2015 included strings such as "kiev_o" and "2015telsmi," and the authors of the report speculate "SMI" is an acronym representing Sredstva Massovoj Informacii.[238] Sredstva Massovoj Informacii (Сре́дства массово́й информа́ции) is the Russian term for mass media, which may be referring to the attack on the Ukrainian media outlet in October 2015.

ad. This summary is based on the infection routine observed in VBA_macro.exe, Sample 1. Additional details on specific setting modifications can be found the full infection routine summary in Appendix B.4: BE3 Installer (VBA_macro.exe, Sample 1).

ae. This summary is based on the infection routine observed in VBA_macro.exe, Sample 1. Additional details on specific setting modifications can be found the full infection routine summary in Appendix B.4: BE3 Installer (VBA_macro.exe, Sample 1).

APPENDIX B.7:
BE3 IMPLANT (FONTCACHE.DAT, SAMPLE 1)

SHA1: 899baab61f32c68cde98db9d980cd4fe39edd572	
SHA-256: ef380e33a854ef9d9052c93fc68d133cfeaae3493683547c2f081dc220beb1b3	
MD5: 3fa9130c9ec44e36e52142f3688313ff	
Type: Win32 Dynamic Link Library[239]	First Upload: 2015-10-13 10:51:25 UTC[240]
Compile Timestamp: 1979-01-28 00:25:53[241]	Final Modification Timestamp: 1979:01:28 01:25:53+01:00[242]
File Size: 56832 bytes[243]	Language Settings:[244] Neutral English US
File Names:[245] FONTCACHE.DLL FONTCACHE.DAT.174093.DROPPED FONTCACHE.DAT packet.dll	
Technical Notes: This is the implant file associated with Appendix B.3: BE3 Installer (VBA_macro.exe, Sample 1). Full infection routine details are provided in Appendix B.3: BE3 Installer (VBA_macro.exe, Sample 1).	
Related Samples: 1. Appendix B.3: BE3 Installer (VBA_macro.exe, Sample 1) (MD5: ac2d7f21c826ce0c449481f79138aebd)	

APPENDIX B.8:
BE3 IMPLANT (FONTCACHE.DAT, SAMPLE 2)

SHA1: 315863c696603ac442b2600e9ecc1819b7ed1b54	
SHA-256: f5785842682bc49a69b2cbc3fded56b8b4a73c8fd93e35860ecd1b9a88b9d3d8	
MD5: cdfb4cda9144d01fb26b5449f9d189ff	
Type: Win32 Dynamic Link Library[246]	**First Upload:** 2015-07-27 13:17:32[247]
Compile Timestamp: 1979-01-28 00:25:53[248]	Final Modification Timestamp: 1979-01-28 00:25:53[249]
File Size: 55808 bytes[250]	Language Settings:[251] Neutral English US
File Names:[252] FONTCACHE.DAT 63.dll packet.dll	
Technical Notes: This is the implant file associated with Appendix B.4: BE3 Installer (VBA_macro.exe, Sample 2). Full infection routine details are provided in Appendix B.4: BE3 Installer (VBA_macro.exe, Sample 2).	
Related Samples: 1. Appendix B.4: BE3 Installer (VBA_macro.exe, Sample 2) (MD5: abeab18ebae2c3e445699d256d5f5fb1 2. Appendix B.10: BE3 Implant (.LNK Persistence Mechanism, Sample 2) (MD5: bffd06a38a46c1fe2bde0317176f04b8)	

APPENDIX B.9:
BE3 IMPLANT (.LNK PERSISTENCE MECHANISM, SAMPLE 1)[af]

SHA1: f89ce5ba8e7b8587457848182ff1108b1255b87f	
SHA-256: 2872473b7144c2fb6910ebf48786c49f9d4f46117b9d2aaa517450fce940d0da	
MD5: 40c74556c36fa14664d9059ad05ca9d3	
Type: Microsoft Windows LiNK	**First Upload:** Not Submitted
Compile Timestamp: Not Submitted	Final Modification Timestamp: Not Submitted
File Size: 1682 bytes	**Language Settings:** Not Submitted
File Names: Not Submitted	

af. This is an embedded file dropped during malware execution. This file was not publicly reported as an independent malware sample. "Not Submitted" is listed in fields that would otherwise have been populated with data from public sources.

Technical Notes: This is the shortcut file inserted in the startup folder and used to launch the FONTCACHE.DAT implant. Full infection routine details associated with this file are provided in Appendix B.3: BE3 Installer (VBA_macro.exe, Sample 1).
Related Samples: 1. Appendix B.3: BE3 Installer (VBA_macro.exe, Sample 1) (MD5: ac2d7f21c826ce0c449481f79138aebd) 2. Appendix B.4: BE3 Implant (FONTCACHE.DAT, Sample 1) (MD5: 3fa9130c9ec44e36e52142f3688313ff)

APPENDIX B.10:
BE3 IMPLANT (.LNK PERSISTENCE MECHANISM, SAMPLE 2)[ag]

SHA1: 3feb426ac934f60eee4e08160d9c8bbe926c917e	
SHA-256: 22735ffeb3472572f608e9a2625ec91735482d9423ea7a43ed32f8a39308eda8	
MD5: bffd06a38a46c1fe2bde0317176f04b8	
Type: Microsoft Windows LiNK	First Upload: Not Submitted
Compile Timestamp: Not Submitted	Final Modification Timestamp: Not Submitted
File Size: 1682 bytes	Language Settings: Not Submitted
File Names: Not Submitted	
Technical Notes: This is the shortcut file inserted in the startup folder and used to launch the FONTCACHE.DAT implant. Full infection routine details associated with this file are provided in Appendix B.4: BE3 Installer (VBA_macro.exe, Sample 2).	
Related Samples: 1. Appendix B.4: BE3 Installer (VBA_macro.exe, Sample 2) (MD5: abeab18ebae2c3e445699d256d5f5fb1) 2. Appendix B.9: BE3 Implant (FONTCACHE.DAT, Sample 2) (MD5:cdfb4cda9144d01fb26b5449f9d189ff)	

ag. This is an embedded file dropped during malware execution. This file was not publicly reported as an independent malware sample. "Not Submitted" is listed in fields that would otherwise have been populated with data from public sources.

APPENDIX B.II:
BE2 IMPLANT (ADPU160M.SYS)

SHA1: 4bc2bbd1809c8b66eecd7c28ac319b948577de7b	
SHA-256: 244dd8018177ea5a92c70a7be94334fa457c1aab8a1c1ea51580d7da500c3ad5	
MD5: e60854c96fab23f2c857dd6eb745961c	
Type: Win32 Executable[253]	**First Upload:** 2015-10-09 16:26:08 UTC[254]
Compile Timestamp: Not Submitted	**Final Modification Timestamp:** 0000:00:00 00:00:00[255]
File Size: 60928 bytes[256]	**Language Settings:** English[257]
File Names:[258] FILE_208 acpipmi.sys aliides.sys	
Technical Notes: This is the implant file associated with Appendix B.5: BE2 Installer (Undisclosed). The name is listed here (adpu160m.sys) is taken from a legitimate, unused driver on the system, and will potentially vary between executions. Full infection routine details are provided in Appendix B.5: BE2 Installer (Undisclosed).	
Related Samples: 3. Appendix B.5: BE2 Installer (Undisclosed) (MD5: 1d6d926f9287b4e4cb5bfc271a164f51) 4. Appendix B.12: Encrypted Configuration/On-disk-store (ieapflrt.dat) (MD5: 01215f813d3e93ed7e3fc3fe369a6cd5)	

APPENDIX B.I2:
BE3 ENCRYPTED CONFIGURATION/ON-DISK-STORE (IEAPFLRT.DAT)[ah]

SHA1: 63bf25190139bd307290c301304597bdeffa4351	
SHA-256: ad2e333141e4e7a800d725f06e25a58a683b42467645d65ba5a1cf377b4adcbe	
MD5: 01215f813d3e93ed7e3fc3fe369a6cd5	
Type: Not Submitted	**First Upload:** Not Submitted
Compile Timestamp: Not Submitted	**Final Modification Timestamp:** Not Submitted
File Size: Not Submitted	**Language Settings:** Not Submitted
File Names: Not Submitted	
Technical Notes: This is the encrypted configuration and on-disk-store file associated with Appendix B.5: BE2 Installer (Undisclosed). Full infection routine details are provided in Appendix B.5: BE2 Installer (Undisclosed).	

ah. This is an embedded file dropped during malware execution. This file was not publicly reported as an independent malware sample. "Not Submitted" is listed in fields that would otherwise have been populated with data from public sources.

Related Samples:

1. Appendix B.5: BE2 Installer (Undisclosed (MD5:1d6d926f9287b4e4cb5bfc271a164f51)
2. Appendix B.7: BE3 Implant (adpu160m.sys) (MD5: e60854c96fab23f2c857dd6eb745961c)

APPENDIX B.13:
MODIFIED DROPBEAR SERVER IMPLANT (DROPBEAR.EXE)[ai]

SHA1: 166d71c63d0eb609c4f77499112965db7d9a51bb	
SHA-256: 0969daac4adc84ab7b50d4f9ffb16c4e1a07c6dbfc968bd6649497c794a161cd	
MD5: fffeaba10fd83c59c28f025c99d063f8	
Type: Win32 Executable[259]	**First Upload:** 2015-06-25 09:16:03[260]
Compile Timestamp: 2013-12-10 06:08:44[261]	Final Modification Timestamp: 2013:12:10 07:08:44+01:00[262]
File Size: 303152 bytes	**Language Settings:** Undisclosed
File Names: dropbear.exe[263] Win32/SSHBearDoor.A trojan[264]	
Technical Notes: This file is the Dropbear server program. Analysis identified that this Dropbear binary code was modified from its source code to include a backdoor and authentication processes.[265] The first authentication process uses a hardcoded credential set of "user" and "passDs5Bu9Te7" and the second process uses a RSA public key.[266]	
Related Samples: 1. Appendix B.1: Weaponized MS Excel (Додаток1.xls) (MD5: 97b7577d13cf5e3bf39cbe6d3f0a7732) 2. Appendix B.6: Dropbear Installer (DropbearRun.vbs) (MD5: 0af5b1e8eaf5ee4bd05227bf53050770)	

ai. A sample of this file was not recovered. The technical notes provided are based on the cited reporting.

KILLDISK SAMPLES

Five KillDisk samples were recovered and analyzed for this report. Two of the samples[aj,ak] drop a file "C:\windows\svchost.exe" and create a process "C:\WINDOWS\svchost.exe –service," which runs as a child of services.exe. The process overwrites the first 131072 bytes of \Device\Harddisk0\DR0 with zeros, effectively rendering the OS unusable upon reboot. The infected machine then sustains a critical error, displays a blue screen of death, and reboots with the message "Operating System not found." A third observed sample[al] executes nearly identically, though the sample runs as its own process as opposed to dropping an embedded file onto the targeted system to overwrite the data.

A key point of variance between recovered samples is the level of additional data destruction beyond overwriting the master boot record. Though all samples ultimately rendered the machines inoperable, in the samples[am,an] described above, a critical system error and forced reboot occurred without overwriting any additional data on disk. This indicates that valuable data stored on the device may be recoverable, even if the machine itself is inoperable.

Two other analyzed samples[ao,ap] included additional data destruction beyond the MBR. The first[aq] runs as its own process and overwrites the first 131072 bytes of \Device\Harddisk0\DR0 with spaces, rendering the OS unusable upon reboot. The sample then continues to overwrite thousands of files while the system remains powered on but unusable. The other sample follows a nearly identical execution, though it runs as a child process to services.exe

---

aj. Appendix B.14: KillDisk (Sample 1) (MD5: 108fedcb6aa1e79eb0d2e2ef9bc60e7a)

ak. Appendix B.14: KillDisk (Sample 2) (MD5: 72bd40cd60769baffd412b84acc03372)

al. Appendix B.16: KillDisk (Sample 3) (MD5: 7361b64ddca90a1a1de43185bd509b64)

am. Appendix B.14: KillDisk (Sample 1) (MD5: 108fedcb6aa1e79eb0d2e2ef9bc60e7a)

an. Appendix B.17: KillDisk (Sample 4) (MD5: cd1aa880f30f9b8bb6cf4d4f9e41ddf4)

and also drops hundreds of 5-byte .tmp files in C:\windows\temp\ with incrementing numeric file names.

Public reporting indicates that some observed KillDisk samples would not execute properly in malware sandboxes, requiring analysts to conduct static analysis.[267] This could possibly indicate functionality to identify the use of malware sandboxes, a feature that would be included to hinder forensic analysis. In initial analysis of one of the recovered samples,[ar] analysts found it would not run in a Windows XP virtual machine, though patching with Ollydbg corrected this issue. This may have been the same issue discussed by other analysts encountered.

At least one machine destroyed by KillDisk was functioning as a remote terminal unit (RTU), and some public reporting indicated that a process executed by the malware (sec_service.exe) may have been a standard process in several applications used in control environments.[268] Despite this, specific targeting of industrial control systems (ICS) devices was not a behavior observed in any of the KillDisk samples analyzed. The samples observed did not include inherent features to discover ICS components, and the reported disk destruction against the RTU was likely accomplished by the threat actors, actively delivering the malware to the targeted system.

In addition to targeting the electricity distributors in December 2015, several of the KillDisk samples analyzed for this report were also reported in attacks against a Ukrainian railway operator[as] and Ukrainian mining company[at,au] in November and December 2015.[269]

---

ao. Appendix B.18: KillDisk (Sample 5) (MD5: 66676deaa9dfe98f8497392064aefbab)

ap. Appendix B.16: KillDisk (Sample 3) (MD5: 7361b64ddca90a1a1de43185bd509b64)

aq. Appendix B.18: KillDisk (Sample 5) (MD5: 66676deaa9dfe98f8497392064aefbab)

ar. Appendix B.16: KillDisk (Sample 3) (MD5: 7361b64ddca90a1a1de43185bd509b64)

as. Ibid

at. Appendix B.15: KillDisk (Sample 2) (MD5: 72bd40cd60769baffd412b84acc03372)

au. Appendix B.17: KillDisk (Sample 4) (MD5: cd1aa880f30f9b8bb6cf4d4f9e41ddf4)

APPENDIX B.I4:
KILLDISK (SAMPLE 1)

SHA1: aa0aaa7002bdfe261ced99342a6ee77e0afa2719	
SHA-256: 30862ab7aaa6755b8fab0922ea819fb48487c063bea4a84174afbbd65ce26b86	
MD5: 108fedcb6aa1e79eb0d2e2ef9bc60e7a	
Type: Win32 Executable[270]	**First Upload:** 2016-03-22 11:54:29 UTC[271]
Compile Timestamp: 2015-10-24 18:19:30[272]	Final Modification Timestamp: 2015:10:24 19:19:30+01:00[273]
File Size: 110592 bytes[274]	**Language Settings:** English US[275]
File Names: 1.1[276]	
Technical Notes: This KillDisk sample executes a destructive disk overwrite function. Following execution, data may be recoverable. Execution Routine: 1. Shortly after running, the executable creates a process "C:\WINDOWS\svchost.exe -service" that runs as a child of services.exe; it runs in such fashion because it is installed as service "msDefenderSvc". 2. The executable then overwrites (with zeros) the first 131072 bytes of \Device\Harddisk0\DR0, effectively rendering the OS unusable upon reboot. 3. While running, the machine sustains a critical error, and upon reboot displays "Operating system not found." The machine sustains this critical system error before additional files are overwritten, indicating some data may be recoverable. Dropped files include: c:\windows\svchost.exe	
Related Samples: N/A	

APPENDIX B.I5:
KILLDISK (SAMPLE 2)

SHA1: 8ad6f88c5813c2b4cd7abab1d6c056d95d6ac569	
SHA-256: f52869474834be5a6b5df7f8f0c46cbc7e9b22fa5cb30bee0f363ec6eb056b95	
MD5: 72bd40cd60769baffd412b84acc03372	
Type: Win32 Executable[277]	**First Upload:** 2015-11-10 09:31:41[278]
Compile Timestamp: 2015-10-24 18:19:30[279]	Final Modification Timestamp: 2015:10:24 19:19:30+01:00[280]

File Size: 110592 bytes[281]	Language Settings: English US[282]
File Names: svchost.exe[283]	
Technical Notes: The execution process for this sample is identical to the process detailed in Appendix B.14: KillDisk (Sample 1).	
Related Samples: 1. Appendix B.14: KillDisk (Sample 1) (MD5:108fedcb6aa1e79eb0d2e2ef9bc60e7a)	

APPENDIX B.16:
KILLDISK (SAMPLE 3)

SHA1: f3e41eb94c4d72a98cd743bbb02d248f510ad925	
SHA-256: c7536ab90621311b526aefd56003ef8e1166168f038307ae960346ce8f75203d	
MD5: 7361b64ddca90a1a1de43185bd509b64	
Type: Win32 Executable[284]	First Upload: 2015-12-23 22:34:19[285]
Compile Timestamp: 1999:01:06 23:02:00+01:00[286]	Final Modification Timestamp: 1999:01:06 23:02:00+01:00[287]
File Size: 98304 bytes[288]	Language Settings: English US[289]
File Names:[290] tsk.exe danger Ukranian.bin.exe	
Technical Notes: This KillDisk sample executes a destructive disk overwrite function. In addition to destroying critical OS data, the sample also overwrites thousands of additional files, including log files.[291] Following execution, data is not likely recoverable. In initial analysis, the executable would not run from cmdline on Win5.1. The file was patched using Ollydbg, allowing it to run as a child of services.exe as "<Binary_Name> -LocalService". Execution Routine: 1. The executable overwrites (with blanks/spaces) first 131072 bytes of \Device\Harddisk0\DR0, effectively rendering the OS unusable upon reboot. 2. After overwriting OS data, the executable continues to overwrite thousands of files, causing the system to remain powered but unusable. Data destruction takes long time and does not immediately trigger a critical system error. 3. Following reboot, the system displays reboot error: "Operating system not found." The executable also drops hundreds of 5-byte files in C:\windows\temp\==00####=.tmp, where "####" is an incrementing numeric.	
Related Samples: N/A	

APPENDIX B.I7:
KILLDISK (SAMPLE 4)

SHA1: 16f44fac7e8bc94eccd7ad9692e6665ef540eec4	
SHA-256: 5d2b1abc7c35de73375dd54a4ec5f0b060ca80a1831dac46ad411b4fe4eac4c6	
MD5: cd1aa880f30f9b8bb6cf4d4f9e41ddf4	
Type: Win32 Executable	**First Upload:** 2015-10-25 01:31:24[292]
Compile Timestamp: 2015:10:24 14:23:02[293] +01:00	Final Modification Timestamp: 2015:10:24 14:23:02+01:00[294]
File Size: 90112 bytes[295]	**Language Settings:** English US[296]
File Names:[297] crab.exe ololo 2.exe ololo.exe	
Technical Notes: This KillDisk sample executes a destructive disk overwrite function. Following execution, data may be recoverable. Execution Routine: 1. The executable runs as own process rather than running an embedded file as a child process, as was observed in other samples. 2. Upon execution, the first 131072 bytes of \Device\Harddisk0\DR0 are overwritten with zeros, effectively rendering the OS unusable upon reboot. 3. While running, the machine sustains a critical error, and upon reboot displays "Operating system not found." The machine sustains the critical system error before additional files are overwritten, indicating some data may be recoverable.	
Related Samples: N/A	

APPENDIX B.18:
KILLDISK (SAMPLE 5)

SHA1: 6d6ba221da5b1ae1e910bbeaa07bd44aff26a7c0	
SHA-256: 11b7b8a7965b52ebb213b023b6772dd2c76c66893fc96a18a9a33c8cf125af80	
MD5: 66676deaa9dfe98f8497392064aefbab	
Type: Win32 Executable[298]	**First Upload:** 2015-10-25 23:07:26[299]
Compile Timestamp: 2015-10-24 13:49:03[300]	Final Modification Timestamp: 2015:10:24 14:49:03+01:00[301]
File Size: 126976 bytes[302]	**Language Settings:** English US[303]
File Names:[304] trololo.exe 123.txt ololo.exe ololo.txt virus_ololo.dat	
Technical Notes: This KKillDisk sample executes a destructive disk overwrite function. In addition to destroying critical OS data, the sample also overwrites thousands of additional files, including log files.[305] Following execution, data is not likely recoverable. Execution Routine: 1. The executable runs as own process rather than running an embedded file as a child process, as was observed in other samples. 2. The executable overwrites (with blanks/spaces) the first 131072 bytes of \Device\Harddisk0\DR0, effectively rendering the OS unusable upon reboot. 3. After overwriting OS data, the executable continues to overwrite thousands of files, causing the system to remain powered but unusable. Data destruction takes long time and does not immediately trigger a critical system error. 4. Following reboot, the system displays reboot error: "Operating system not found."	
Related Samples: N/A	

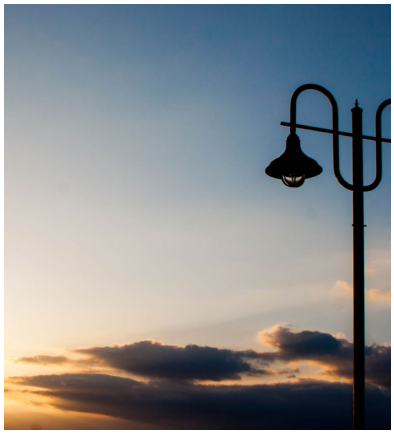
APPENDIX C:

BlackEnergy Plugins

BlackEnergy (BE) was first observed in 2007 and has since been used by a wide range of threat actors, predominantly criminal groups, to conduct a diverse collection of malicious campaigns.[306] BE has been observed as an enabling tool in distributed denial-of-service (DDoS) attacks, theft of banking credentials, widespread reconnaissance and cyberespionage,[307] and ultimately disruptive industrial control systems (ICS) attacks in Ukraine. The BE plugins identified reflect the diverse use of this malware, and the significant overlap in functionality across different plugins indicates that several distinct groups are actively using the tool. At least 14 BE plugins have been identified in public reporting, including:[308,309]

- FS.dll: Functions as a data exfiltration tool; gathers documents and private keys by search for specific file extensions
- SI.dll: Searches infected machines for specific configuration and operational data
- JN.dll: Functions as a parasitic infector; fixes checksum values in PE headers, fixes CRC32 Nullsoft value, and deletes digital signatures to avoid invalidation
- KI.dll: Records user key strokes on infected machines
- PS.dll: Searches infected machines for user credentials
- SS.dll: Captures screenshots on infected machines
- VS.dll: Functions as a network discovery and remote execution tool. Scans the infected network to identify connected network resources, retrieves remote desktop credentials, and attempts to establish connections. Uses PsExec, which is embedded in the plugin, to gather system information and launch executables on remote machines
- TV.dll: Searches for TeamViewer versions 6–8. If the targeted application is identified, the plugin sets an additional password, creating an additional backdoor into the compromised system
- RD.dll: Functions as a pseudo "remote desktop" server
- UP.dll: Used to update the hosted malware
- DC.dll: Identifies Windows accounts on the infected system
- BS.dll: Conducts system profiling through queries of system hardware, BIOS, and Windows information
- DSTR.dll: Functions as a logic bomb. At a specified time, the plugin rewrites files with specific extensions with random data, deletes itself, and deletes the first 11 sectors of system drive, then rewrites all remaining data
- SCAN.dll: Functions as a network scanner on infected systems.

Of particular interest in the attacks against Ukrainian electricity distributors are the SI and PS plugins. As plugins designed specifically to search for credential data, SI or PS are the likely plugins used following the initial infection. Data destruction was also a component of the final stages of the attack, and though BE has a dedicated data destruction plugin, DSTR.dll, public reporting indicates that the disk-wiping component of the attack was achieved using the KillDisk malware.



The SI plugin gathers a wide range of systems data. Using the systeminfo.exe utility, SI gathers configuration information, including OS version, privileges, current time, up time, idle time, and proxy.[310] SI also identifies:[311]

- Installed applications, using the uninstall program registry
- Process list, using the tasklist.exe utility
- IP configurations, using the ipconfig.exe utility
- Network connections, using the netstat.exe utility
- Routing tables, using the route.exe utility
- Traceroute and Ping information to Google, using tracert.exe and ping.exe
- Mail, browser, and instant messaging clients.

Of particular interest is its targeting of password managers and stored user credentials.[312] SI is designed to pull credentials from The Bat! email client, Mozilla password manager, Google Chrome password manager, Outlook and Outlook Express, Internet Explorer, and Windows Credential Store, including credentials for Windows Live messenger services, Remote Desktop, and WinINET.[313] If any of these applications or services were deployed on the targeted systems, they would present a viable avenue for gathering the valid user credentials that the threat actors ultimately obtained in their attack. The PS.dll plugin is also specifically designed to search and exfiltrate credentials,[314] and may have been used in the attack. Similarly, the KI.dll may have been used to record and transfer keystrokes during user authentication, as some public reporting speculates.[315] Detail on the specific function of these two plugins was not listed in public sources, and samples of the .dll files were not located for analysis.

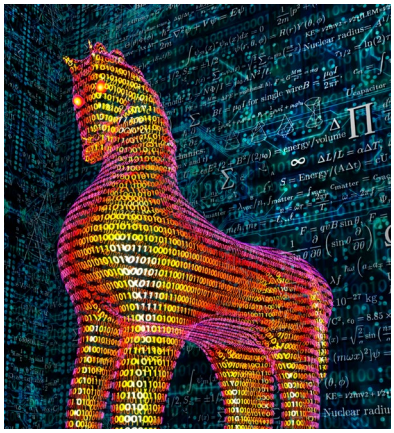
Of the 15 plugins mentioned in this report, most were initially developed for BE2, though they could be recompiled for use with BE3.[316] According to reporting in September 2015, SI was the only plugin analyzed by security researchers that had been updated for use with BE3 at that time;[317] this indicates SI may have been the tool used in the December 2015 attacks. Later reporting, in January 2015, indicated that all 14 of the plugins had been modified for compatibility with BE3.[318]

APPENDIX D:

Alternate Remote Access Trojans

Though the primary tool in the Ukraine attacks was BlackEnergy (BE) 3, as noted above, several other remote access trojans (RAT) were observed in the phishing campaign leading up to the attacks.[319] Several reports discussed the use of a modified version of Dropbear,[320,321,322] an open-source SSH server and client executable designed as a lightweight server primarily for Linux-based embedded systems.[323] As with BE3, the modified Dropbear was launched using a Visual Basic (VB) script[av] delivered via a weaponized Microsoft (MS) Excel document.[324] At launch, the server is set to listen at port 6789.[325] The modified version of the Dropbear server contained two backdoors, a hardcoded public key authentication process, and a hardcoded username and password, allowing threat actors to authenticate into the targeted system.[326] One of the benefits, from an attacker's perspective, of using a RAT such as the modified Dropbear server, is that it is not inherently malicious, and unlike other RATs, it may not be recognized by automated scanners designed to recognize potentially malicious files.[327] Using an open-source SSH client like Dropbear in the initial infection would also limit the risk of exposing a more complex and valuable piece of malware, such as BE3; if the malware is discovered, it would not represent a significant loss from the attacker's perspective.

During analysis of BE3 malware samples, analysts did not find any technical link between BE3 and the other referenced RATs: GCat, Dropbear, and Kryptik. It is possible, as some public reporting indicates, that these additional trojans were used by the same threat actors that conducted the attack on the electrical grid; in the attack the threat actors used at least two separate malware applications, BE3 and KillDisk. There is no technical evidence to confirm these additional trojans were used by the same group though, and it is possible they had been delivered to the targeted systems as part of separate, unrelated attacks.



av. Appendix B.6: Dropbear Installer (DropbearRun.vbs) (MD5: 0af5b1e8eaf5ee4bd05227bf53050770)

APPENDIX E:

Sources

1. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*
2. *"ИЗ-ЗА ХАКЕРСКОЙ АТАКИ ОБЕСТОЧИЛО ПОЛОВИНУ ИВАНО-ФРАНКОВСКОЙ ОБЛАСТИ," TSN, December 24, 2015, accessed April 13, 2016, http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html.*
3. *"Енергетики ліквідовують наслідки масштабної аварії на Прикарпатті,"* Прикарпаттяобленерго, *December 23, 2015, accessed July 12, 2016, hxxp://www.oe.if.ua/showarticle.php?id=3413.*
4. *"Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины,"* Cys Centrum, *June 1, 2016, accessed July 12, 2016, hxxps://cys-centrum.com/ru/news/black_energy_2_3.*
5. *Blake Sobczak and Peter Behr, "Inside the diabolical Ukrainian hack that put the U.S. grid on high alert," Environment & Energy Publishing, July 18, 2016, accessed July 21, 2016, hxxp://archive.is/InnBf.*
6. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*
7. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*
8. *"Blackenergy & Quedagh: The convergence of crimeware and APT attacks," F-Secure Labs Security Response, accessed July 12, 2016, hxxps://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.*
9. *Robert Lipovsky and Anton Cherapanov, "Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland ," Virus Bulletin, September 25, 2015, accessed July 12, 2016, hxxps://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland.*
10. *"Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины,"* Cys-Centrum, *June 1, 2016, accessed August 15, 2016, hxxp://cys-centrum.com/ru/news/black_energy_2_3.*
11. *Kyle Wilhoit, "KillDisk and BlackEnergy Are Not Just Energy Sector Threats," Trend Micro, February 11, 2016, accessed July 20, 2016, hxxp://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.*
12. *"Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины,"* Cys-Centrum, *June 1, 2016, accessed August 15, 2016, hxxp://cys-centrum.com/ru/news/black_energy_2_3.*
13. *Ibid.*
14. *Ibid.*
15. *Ibid.*
16. *Ibid.*
17. *Stephen Ward, "iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign," iSight-Partners, October 14, 2014, accessed August 15, 2016, hxxps://www.isightpartners.com/2014/10/cve-2014-4114/.*
18. "Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины," Cys-Centrum, *June 1, 2016, accessed August 15, 2016, hxxp://cys-centrum.com/ru/news/black_energy_2_3.*
19. *Stephen Ward, "iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign," iSight-Partners, October 14, 2014, accessed August 15, 2016, hxxps://www.isightpartners.com/2014/10/cve-2014-4114/.*
20. "Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины," Cys-Centrum, *June 1, 2016, accessed August 15, 2016, hxxp://cys-centrum.com/ru/news/black_energy_2_3.*
21. *Ibid.*

22. *Ibid.*

23. *Ibid.*

24. *Ibid.*

25. *"Українські ЗМІ атакують за допомогою Black Energy," CERT-UA, September 11, 2012, accessed July 19, 2016, hxxp://cert.gov.ua/?p=2370.*

26. *Aleksey Yasinskiy, "DISMANTLING BLACKENERGY, PART 3 – ALL ABOARD!" SOCPrime, March 29, 2016, accessed August 19, 2016, hxxps://socprime.com/en/blog/dismantling-blackenergy-part-3-all-aboard/.*

27. *Kyle Wilhoit, "KillDisk and BlackEnergy Are Not Just Energy Sector Threats," Trend Micro, February 11, 2016, accessed July 20, 2016, hxxp://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.*

28. *Ibid.*

29. *"Атака на энергетические объекты 19-20 января 2016 года. Постфактум," Cys-Centrum, January 29, 2016, accessed August 22, 2016, hxxps://cys-centrum.com/ru/news/attack_on_energy_facilities_jan_ps.*

30. *Robert Lipovsky, "New wave of cyberattacks against Ukrainian power industry," We Live Security, January 20, 2016, accessed August 22, 2016, hxxp://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/.*

31. *"Атака на энергетические объекты 19-20 января 2016 года. Постфактум," Cys-Centrum, January 29, 2016, accessed August 22, 2016, hxxps://cys-centrum.com/ru/news/attack_on_energy_facilities_jan_ps.*

32. *Ibid.*

33. *"Russian Hackers plan energy subersion in Ukraine," Ukrinform, December 28, 2015, accessed July 19, 2016, hxxp://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html.*

34. *Pavel Polityuk, "Ukraine sees Russian hand in cyber attacks on power grid," Reuters, February 12, 2016, accessed August 22, 2016, hxxp://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E.*

35. *Jose Nazario, "BlackEnergy DDoS Bot – Analysis Available," Arbor Networks, October 12, 2007, accessed July 14, 2016, hxxps://www.arbornetworks.com/blog/asert/blackenergy-ddos-bot-analysis-available/.*

36. *Kelly Jackson Higgins, "New BlackEnergy Trojan Targeting Russian, Ukrainian Banks," DarkReading, March 4, 2010, accessed July 14, 2016, hxxp://www.darkreading.com/vulnerabilities---threats/new-blackenergy-trojan-targeting-russian-ukrainian-banks/d/d-id/1133120.*

37. *Brian Prince, "Russian Banking Trojan BlackEnergy 2 Unmasked at RSA," eWeek, March 4, 2010, accessed July 14, 2016, hxxp://www.eweek.com/c/a/Security/Russian-Banking-Trojan-BlackEnergy-2-Unmasked-at-RSA-883053.*

38. *Brian Prince, "Security Researcher Asserts Russian Role in Georgia Cyber-attacks," eWeek, August 13, 2008, accessed July 14, 2016, hxxp://www.eweek.com/c/a/Security/Security-Researcher-Asserts-Russian-Role-in-Georgia-Cyber-Attacks.*

39. *John Hultquist, "Sandworm Team – Targeting SCADA Systems," iSight Partners, October 21, 2014, accessed July 14, 2016, hxxps://www.isightpartners.com/tag/blackenergy-malware/.*

40. *Jim Finkle, "Russian hackers target NATO, Ukraine and others: iSight," Reuters, October 14, 2014, accessed July 14, 2016, hxxp://www.reuters.com/article/us-russia-hackers-idUSKCN0I308F20141014.*

41. *"Українські ЗМІ атакують за допомогою Black Energy," CERT-UA, September 11, 2015, accessed July 13, 2016, hxxp://cert.gov.ua/?p=2370.*

42. *"Blackenergy & Quedagh: The convergence of crimeware and APT attacks," F-Secure Labs Security Response, accessed July 12, 2016, hxxps://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.*

43. *"Ukrainian Lawmakers Introduce a Bill on Nationalizing Russia's Assets," Russia Insider, April 23, 2015, accessed July 14, 2016, hxxp://russia-insider.com/en/ukrainian-lawmakers-introduce-bill-nationalizing-russias-assets/5993.*

44. *"Ukrainian MPs propose to nationalize Russian assets," People Investigator, April 4, 2015, accessed July 14, 2016, hxxp://peopleinvestigator.us/politics/308-ukrainian-mps-propose-to-nationalize-russian-assets.html.*

45. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

46. *"List of persons and entities under EU restrictive measures over the territorial integrity of Ukraine," Council of the European Union, September 15, 2015, accessed July 14, 2016, hxxp://www.consilium.europa.eu/en/press/press-releases/2015/09/pdf/150915-sanctions-table---persons--and-entities_pdf/.*

47. *Brad Well, "Corporte Governance in Ukraine: Passing Go," Concorde Capital, October 2011, accessed July 14, 2016, hxxp://concorde.ua/en/getfile/129/3/.*

48. *Pierluigi Paganini, "BlackEnergy infected also Ukrainian Mining and Railway Systems," Security Affairs, February 13, 2016, accessed July 14, 2016, hxxp://securityaffairs.co/wordpress/44452/hacking/blackenergy-mining-and-railway-systems.html.*

49. *Maria Snegovaya, "Putin's information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Institute for the Study of War, September 2015, accessed July 14, 2016, hxxp://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.*

50. *Anna Shamanska, "Explainer: Why Ukraine Supplies Electricity To Crimea, And Why It Stopped," Radio Free Europe, Radio Liberty, July 14, 2016, accessed July 14, 2016, hxxp://www.rferl.org/content/ukraine-crimea-power-supply-electricity-explainer/27384812.html.*

51. *Neil MacFarquhar, "Crimea in Dark After Power Lines Are Blown Up," New York Times, November 22, 2015, accessed July 14, 2016, hxxp://www.nytimes.com/2015/11/23/world/europe/power-lines-to-crimea-are-blown-up-cutting-off-electricity.html?_r=0.*

52. *"Crimea hit by power blackout and Ukraine trade boycott," BBC News, November 23, 2015, accessed July 14, 2016, hxxp://www.bbc.com/news/world-europe-34899491.*

53. *Anna Shamanska, "Explainer: Why Ukraine Supplies Electricity To Crimea, And Why It Stopped," Radio Free Europe, Radio Liberty, July 14, 2016, accessed July 14, 2016, hxxp://www.rferl.org/content/ukraine-crimea-power-supply-electricity-explainer/27384812.html.*

54. *"Dragonfly: Cyberespionage Attacks Against Energy Suppliers," Symantec, July 7, 2014, accessed July 19, 2016, hxxps://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf.*

55. *"Alert (ICS-ALERT-14-281-01E)," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, December 10, 2014, modified March 2, 2016, accessed July 12, 2016, hxxps://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.*

56. *Michael J. Assante and Robert M. Lee," The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed July 12, 2016, hxxps://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.*

57. *Eric M. Hutchins, Michael J. Clopperty, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed martin Corporation, 2011, accessed September 12, 2016, hxxp://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.*

58. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

59. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

60. *Ibid.*

61. *Ibid.*

62. *Ibid.*

63. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

64. *"Remote Terminal Unit RTU560 System Description Release 6.2," ABB Utilities GmbH, May 2003, accessed August 22, 2016, vfservis.cz/files/000290_RTU560_SD_R6.pdf.*

65. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

66. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

67. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

68. *Peter Behr and Blake Sobczak, "Grid hack exposes troubling security gaps for local utilities," Environment and Energy Publishing, July 20, 2016, accessed August 22, 2016, hxxp://www.eenews.net/stories/1060040519.*

69. *Ibid.*

70. *"ICS-CERT Monitor," ICS-CERT, November/December 2015, accessed October 26, 2016, hxxps://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.*

71. *Ibid.*

72. *"Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)," ICS-CERT, last updated November 17, 2015, accessed October 26, 2016, hxxps://web.archive.org/web/20151117164746/https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.*

73. *Bill Gertz, "Moscow Suspected in Hack of U.S. Industrial Control Systems," Washington Free Beacon, October 31, 2014, accessed October 26, 2016, hxxp://freebeacon.com/national-security/moscow-suspected-in-hack-of-u-s-industrial-control-systems/.*

74. *"Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)," ICS-CERT, last updated November 17, 2015, accessed October 26, 2016, hxxps://web.archive.org/web/20151117164746/https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.*

75. *"Інформація щодо трансформаторних підстанцій 35-110 кВ," PJSC Kyivoblenergo, January 2, 2016, accessed August 22, 2016, hxxp://www.koe.vsei.ua/koe/documents/Zvedena_forma_I_2016(14-03-16).pdf.*

76. *"Компанія сьогодні," PJSC EK Chernivtsioblenergo, accessed August 22, 2016, hxxp://www.oblenergo.cv.ua/about.php.*

77. *"Company Overview of Public Joint Stock Company Prykarpattyaoblenergo," Bloomberg, accessed August 22, 2016, hxxp://www.bloomberg.com/Research/stocks/private/snapshot.asp?privcapid=2559975.*

78. *"ОАО Прикарпатьеоблэнерго," Galician Computer Company, accessed August 22, 2016, htxxtp://galcomcomp.com/index.php/ru/nashi-proekty.*

79. *"Comprehensive Analysis Report on Ukraine Power System Attacks," Antiy Labs, March 16, 2016, accessed July 12, 2016, hxxp://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/.*

80. *Michael J. Assante and Robert M. Lee," The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed July 12, 2016, hxxps://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.*

81. *GReAT, "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents," SecureList, January 28, 2016, accessed July 12, 2016, hxxps://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/.*

82. *Udi Shamir, "Analyzing a New Variant of BlackEnergy 3 Likely Insider-Based Execution," SentinelOne, 2016, accessed July 12, 2016, hxxps://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf.*

83. *Robert Lipovsky and Anton Cherapanov, "Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland," Virus Bulletin, September 25, 2015, accessed July 12, 2016, hxxps://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland.*

84. *"Blackenergy & Quedagh: The convergence of crimeware and APT attacks," F-Secure Labs Security Response, accessed July 12, 2016, hxxps://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.*

85. *Ibid.*

86. *Pavel Polityuk, "Ukraine sees Russian hand in cyber attacks on power grid," Reuters, February 12, 2016, accessed August 22, 2016, hxxp://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E.*

87. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

88. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

89. *"Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины," Cys Centrum, June 1, 2016, accessed July 12, 2016, hxxps://cys-centrum.com/ru/news/black_energy_2_3.*

90. *Ibid.*

91. *Ibid.*

92. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

93. *byt3bl33d3r, "Gcat," GitHub, June 9, 2016, accessed July 14, 2016, hxxps://github.com/byt3bl33d3r/gcat/blob/master/README.md.*

94. *Matt Johnston, "Dropbear SSH," University of Western Australia University Computer Club, accessed July 12, 2016, hxxps://matt.ucc.asn.au/dropbear/dropbear.html.*

95. *Dianne Lagrimas, "TROJ_KRYPTIK," Trend Micro, October 9, 2012, accessed July 14, 2016, hxxp://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TROJ_KRYPTIK.*

96. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

97. *"Конференция UISGCON11. Итоги по киберугрозам в Украине в 2015 году," Cys-Centrum, June 12, 2015, accessed August 22, 2016, hxxps://cys-centrum.com/ru/news/uisgcon11_2015#pic-5.*

98. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

99. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

100. *Robert Lipovsky and Anton Cherapanov, "Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland," Virus Bulletin, October 14, 2014, accessed July 12, 2016, hxxps://www.youtube.com/watch?v=I77CGqQvPE4.*

101. *"Blackenergy & Quedagh: The convergence of crimeware and APT attacks," F-Secure Labs Security Response, accessed July 12, 2016, hxxps://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.*

102. *Ibid.*

103. *Robert Lipovsky and Anton Cherapanov, "Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland," Virus Bulletin, September 25, 2015, accessed July 12, 2016, hxxps://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland.*

104. *"Blackenergy & Quedagh: The convergence of crimeware and APT attacks," F-Secure Labs Security Response, accessed July 12, 2016, hxxps://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.*

105. *Robert Lipovsky and Anton Cherapanov, "Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland," Virus Bulletin, September 25, 2015, accessed July 12, 2016, hxxps://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland.*

106. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

107. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

108. *Aleksey Yasinskiy, "DISMANTLING BLACKENERGY, PART 3 – ALL ABOARD!" SOCPrime, March 29, 2016, accessed August 19, 2016, hxxps://socprime.com/wp-content/uploads/2016/03/blackenergy-p3_16-1.jpg.*

109. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

110. *Michael J. Assante and Robert M. Lee," The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed July 12, 2016, hxxps://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.*

111. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

112. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

113. *Michael J. Assante and Robert M. Lee," The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed July 12, 2016, hxxps://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.*

114. *Robert Lipovsky and Anton Cherapanov, "Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland," Virus Bulletin, September 25, 2015, accessed July 12, 2016, hxxps://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland.*

115. *Aleksey Yasinskiy, "DISMANTLING BLACKENERGY, PART 3 – ALL ABOARD!" SOCPrime, March 29, 2016, accessed August 19, 2016, hxxps://socprime.com/en/blog/dismantling-blackenergy-part-3-all-aboard/.*

116. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

117. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

118. *Michael J. Assante and Robert M. Lee," The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed July 12, 2016, hxxps://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.*

119. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

120. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

121. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

122. *Ibid.*

123. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

124. *"Dragonfly: Western Energy Companies Under Sabotage Threat," Symantec, June 30, 2014, accessed July 14, 2016, hxxp://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat.*

125. *Michael J. Assante and Robert M. Lee," The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed July 12, 2016, hxxps://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.*

126. *Ibid.*

127. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

128. *Ibid.*

129. *"Українські ЗМІ атакують за допомогою Black Energy," CERT-UA, September 11, 2015, accessed July 13, 2016, hxxp://cert.gov.ua/?p=2370.*

130. *Robert Lipovsky and Anton Cherepanov, "BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry," welivesecurity, January 4, 2016, accessed July 12, 2016, hxxp://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.*

131. *Aleksey Yasinskiy, "DISMANTLING BLACKENERGY, PART 3 – ALL ABOARD!" SOCPrime, March 29, 2016, accessed August 19, 2016, hxxps://socprime.com/en/blog/dismantling-blackenergy-part-3-all-aboard/.*

132. *Ibid.*

133. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

134. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

135. *Aleksey Yasinskiy, "DISMANTLING BLACKENERGY, PART 3 – ALL ABOARD!" SOCPrime, March 29, 2016, accessed August 19, 2016, hxxps://socprime.com/en/blog/dismantling-blackenergy-part-3-all-aboard/.*

136. *Ibid.*

137. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

138. *Ibid.*

139. *Ibid.*

140. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

141. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

142. *Ibid.*

143. *"UPS Network Management Cards," Schneider Electric, accessed July 13, 2016, hxxp://www.schneider-electric.com/en/product-range/61936-ups-network-management-cards/.*

144. *"Vulnerability Note VU#166739APC Network Management Card web interface vulnerable to cross-site scripting and cross-site request forgery," Carnegie Mellon University Computer Emergency Response Team, February 24, 2010, modified April 29, 2010, accessed July 13, 2016, hxxps://www.kb.cert.org/vuls/id/166739.*

145. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

146. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

147. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

148. *Ibid.*

149. *Robert M Lee, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," SANS, January 9, 2016 hxxps://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.*

150. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

151. *Jose Pagliery, "Scary questions in Ukraine energy grid hack," CNN Money, January 18, 2016, accessed July 13, 2016, hxxp://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/.*

152. *Robert M Lee, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," SANS, January 9, 2016 hxxps://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.*

153. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

154. *Rich Heidorn, "How a 'Phantom Mouse' and Weaponized Excel Files Brought Down Ukraine's Grid," March 28, 2016, hxxp://www.rtoinsider.com/nerc-phantom-mouse-cyberattack-24232/.*

155. *Ellen Nakashima, "Russian hackers suspected in attack that blacked out parts of Ukraine," Washington Post, January 5, 2016, accessed July 14, 2016, hxxps://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html.*

156. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

157. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

158. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

159. *Ibid.*

160. *"Vulnerability Summary for CVE-2014-6271," National Vulnerability Database, September 24, 2014, modified June 28, 2016, accessed July 14, 2016, hxxps://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271.*

161. *Vulnerability Summary for CVE-2014-7186," National Vulnerability Database, September 28, 2014, modified October 9, 2015, accessed July 14, 2016, hxxps://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7186.*

162. *"Vulnerability Summary for CVE-2014-7187," National Vulnerability Database, September 28, 2014, modified October 9, 2015, accessed July 14, 2016, hxxps://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7187.*

163. *"Vulnerability Summary for CVE-2014-6277," National Vulnerability Database, September 28, 2014, modified October 9, 2015, accessed July 14, 2016, hxxps://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6277.*

164. *"Vulnerability Summary for CVE-2014-6278," National Vulnerability Database, September 30, 2014, modified June 14, 2016, accessed July 14, 2016, hxxps://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6278.*

165. *"Advisory (ICSA-16-138-01) IRZ RUH2 3G Firmware Overwrite Vulnerability," US Department of Homeland Security Industrial computer Emergency Response Team, May 17, 2016, accessed July 14, 2016, hxxps://ics-cert.us-cert.gov/advisories/ICSA-16-138-01.*

166. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

167. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

168. *"The Surging Threat of Telephony Denial of Service Attacks," SecureLogix, Ocotber 21, 2014, accessed July 13, 2016, hxxp://www.cisco.com/c/dam/en/us/products/collateral/unified-communications/unified-border-element/tdos_brochure.pdf.*

169. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

170. *Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed July 13, 2016, hxxps://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.*

171. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

172. *"The Surging Threat of Telephony Denial of Service Attacks," SecureLogix, Ocotber 21, 2014, accessed July 13, 2016, hxxp://www.cisco.com/c/dam/en/us/products/collateral/unified-communications/unified-border-element/tdos_brochure.pdf.*

173. *Ibid.*

174. *"TDoS Attacks on Public Safety Communications," Cook County Department of Homeland Security Emergency Management, March 16, 2013, accessed July 13, 2016, hxxp://krebsonsecurity.com/wp-content/uploads/2013/04/DHSEM-16-SAU-01-LEO.pdf.*

175. *Ibid.*

176. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

177. *Ibid.*

178. *"Українські ЗМІ атакують за допомогою Black Energy," CERT-UA, September 11, 2015, accessed July 19, 2016, hxxp://cert.gov.ua/?p=2370.*

179. *Ibid.*

180. *"052ebc9a518e5ae02bbd1bd3a5a86c3560aefc9313c18d81f6670c3430f1d4d4," Virus Total, July 6, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/052ebc9a518e5ae02bbd1bd3a5a86c3560aefc9313c18d81f6670c3430f1d4d4/analysis/.*

181. *Ibid.*

182. *Ibid.*

183. *Ibid.*

184. *"Analysis Report," joeSandboxCloud, accessed July 12, 2016, hxxps://www.document-analyzer.net/analysis/4073/16856/0/html.*

185. *"052ebc9a518e5ae02bbd1bd3a5a86c3560aefc9313c18d81f6670c3430f1d4d4," Virus Total, July 6, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/052ebc9a518e5ae02bbd1bd3a5a86c3560aefc9313c18d81f6670c3430f1d4d4/analysis/.*

186. *Ibid.*

187. *Robert M Lee, "Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered," SANS Institute, January 1, 2016, accessed July 15, 2016, hxxps://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered.*

188. *Udi Shamir, "Analyzing a New Variant of BlackEnergy 3 Likely Insider-Based Execution," SentinelOne, 2016, accessed July 12, 2016, hxxps://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf.*

189. *"Malicious Code Analysis on Ukraine's Power Grid Incident," Beijing Knownsec Information Technology Co., Ltd., January 10, 2016, accessed July 12, 2016, hxxp://blog.knownsec.com/wp-content/uploads/2016/01/Malicious-Code-Analysis-on-Ukraines-Power-Grid-Incident-L150113.pdf.*

190. *"39d04828ab0bba42a0e4cdd53fe1c04e4eef6d7b26d0008bd0d88b06cc316a81," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/39d04828ab0bba42a0e4cdd53fe1c04e4eef6d7b26d0008bd0d88b06cc316a81/analysis/.*

191. *GReAT, "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents," SecureList, January 28, 2016, accessed July 12, 2016, hxxps://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/.*

192. *"39d04828ab0bba42a0e4cdd53fe1c04e4eef6d7b26d0008bd0d88b06cc316a81," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/39d04828ab0bba42a0e4cdd53fe1c04e4eef6d7b26d0008bd0d88b06cc316a81/analysis/.*

193. *Ibid.*

194. *Ibid.*

195. *Ibid.*

196. *GReAT, "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents," SecureList, January 28, 2016, accessed July 12, 2016, hxxps://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/.*

197. *Ibid.*

198. *Udi Shamir, "Analyzing a New Variant of BlackEnergy 3 Likely Insider-Based Execution," SentinelOne, 2016, accessed July 12, 2016, hxxps://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf.*

199. *Ibid.*

200. *Ibid.*

201. *"Blackenergy & Quedagh: The convergence of crimeware and APT attacks," F-Secure Labs Security Response, accessed July 12, 2016, hxxps://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.*

202. *Ibid.*

203. *"Analysis Report," joeSandboxCloud, accessed July 12, 2016, hxxps://www.document-analyzer.net/analysis/4073/16856/0/html.*

204. *Udi Shamir, "Analyzing a New Variant of BlackEnergy 3 Likely Insider-Based Execution," SentinelOne, 2016, accessed July 12, 2016, hxxps://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf.*

205. *"ca7a8180996a98e718f427837f9d52453b78d0a307e06e1866db4d4ce969d525," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/ca7a8180996a98e718f427837f9d52453b78d0a307e06e1866db4d4ce969d525/analysis/.*

206. *Ibid.*

207. *Ibid.*

208. *Ibid.*

209. *Ibid.*

210. *Ibid.*

211. *"07e726b21e27eefb2b2887945aa8bdec116b09dbd4e1a54e1c137ae8c7693660," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/07e726b21e27eefb2b2887945aa8bdec116b09dbd4e1a54e1c137ae8c7693660/analysis/.*

212. *Ibid.*

213. *Ibid.*

214. *Ibid.*

215. *Ibid.*

216. *Ibid.*

217. *"07a76c1d09a9792c348bb56572692fcc4ea5c96a77a2cddf23c0117d03a0dfad," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/07a76c1d09a9792c348bb56572692fcc4ea5c96a77a2cddf23c0117d03a0dfad/analysis/.*

218. *Ibid.*

219. *Ibid.*

220. *Ibid.*

221. *Ibid.*

222. *"b90f268b5e7f70af1687d9825c09df15908ad3a6978b328dc88f96143a64af0f," Virus Total, February 12, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/b90f268b5e7f70af1687d9825c09df15908ad3a6978b328dc88f96143a64af0f/analysis/.*

223. *Ibid.*

224. *"Malicious Code Analysis on Ukraine's Power Grid Incident," Beijing Knownsec Information Technology Co., Ltd., January 10, 2016, accessed July 12, 2016, hxxp://blog.knownsec.com/wp-content/uploads/2016/01/Malicious-Code-Analysis-on-Ukraines-Power-Grid-Incident-L150113.pdf.*

225. *"b90f268b5e7f70af1687d9825c09df15908ad3a6978b328dc88f96143a64af0f ," Virus Total, February 12, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/b90f268b5e7f70af1687d9825c09df15908ad3a6978b328dc88f96143a64af0f/.*

226. *Ibid.*

227. *Anton Cherepanov, "BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry," welivesecurity, January 3, 2016, accessed July 15, 2016, hxxp://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/.*

228. *"Malicious Code Analysis on Ukraine's Power Grid Incident," Beijing Knownsec Information Technology Co., Ltd., January 10, 2016, accessed July 12, 2016, hxxp://blog.knownsec.com/wp-content/uploads/2016/01/Malicious-Code-Analysis-on-Ukraines-Power-Grid-Incident-L150113.pdf.*

229. *Ibid.*

230. *Udi Shamir, "Analyzing a New Variant of BlackEnergy 3 Likely Insider-Based Execution," SentinelOne, 2016, accessed July 12, 2016, hxxps://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf.*

231. *"Blackenergy & Quedagh: The convergence of crimeware and APT attacks," F-Secure Labs Security Response, accessed July 12, 2016, hxxps://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.*

232. *Ibid.*

233. *Ibid.*

234. *Anton Cherepanov, "BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry," welivesecurity, January 3, 2016, accessed July 15, 2016, hxxp://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/.*

235. *Chintan Shah, "Evolving DDoS Botnets: 1. BlackEnergy," McAfee Labs Blog, February 28, 2011, accessed July 19, 2016, hxxps://blogs.mcafee.com/business/security-connected/evolving-ddos-botnets-1-blackenergy/.*

236. *Anton Cherepanov, "BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry," welivesecurity, January 3, 2016, accessed July 15, 2016, hxxp://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/.*

237. *Ibid.*

238. *Ibid.*

239. *"ef380e33a854ef9d9052c93fc68d133cfeaae3493683547c2f081dc220beb1b3," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/ef380e33a854ef9d9052c93fc68d133cfeaae3493683547c2f081dc220beb1b3/analysis/.*

240. *Ibid.*

241. *Ibid.*

242. *Ibid.*

243. *Ibid.*

244. *Ibid.*

245. *Ibid.*

246. *"f5785842682bc49a69b2cbc3fded56b8b4a73c8fd93e35860ecd1b9a88b9d3d8," Virus Total, July 11, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/f5785842682bc49a69b2cbc3fded56b8b4a73c8fd93e35860ecd1b9a88b9d3d8/analysis/.*

247. *Ibid.*

248. *Ibid.*

249. *Ibid.*

250. *Ibid.*

251. *Ibid.*

252. *Ibid.*

253. *"244dd8018177ea5a92c70a7be94334fa457c1aab8a1c1ea51580d7da500c3ad5," Virus Total, June 21, 2016, accessed July 15, 2016. hxxps://www.virustotal.com/en/file/244dd8018177ea5a92c70a7be94334fa457c1aab8a1c1ea51580d7da500c3ad5/analysis/.*

254. *Ibid.*

255. *Ibid.*

256. *Ibid.*

257. *Ibid.*

258. *Ibid.*

259. *"0969daac4adc84ab7b50d4f9ffb16c4e1a07c6dbfc968bd6649497c794a161cd," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/0969daac4adc84ab7b50d4f9ffb16c4e1a07c6dbfc968bd6649497c794a161cd/analysis/.*

260. *Ibid.*

261. *Ibid.*

262. *Ibid.*

263. *Ibid.*

264. *Anton Cherepanov, "BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry," welivesecurity, January 3, 2016, accessed July 15, 2016, hxxp://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/.*

265. *Anton Cherepanov, "BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry," welivesecurity, January 3, 2016, accessed July 15, 2016, hxxp://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/.*

266. *"Malicious Code Analysis on Ukraine's Power Grid Incident," Beijing Knownsec Information Technology Co., Ltd., January 10, 2016, accessed July 12, 2016, hxxp://blog.knownsec.com/wp-content/uploads/2016/01/Malicious-Code-Analysis-on-Ukraines-Power-Grid-Incident-L150113.pdf.*

267. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

268. *Robert Lipovsky and Anton Cherepanov, "BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry," welivesecurity, January 4, 2016, accessed July 12, 2016, hxxp://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.*

269. *Kyle Wilhoit, "KillDisk and BlackEnergy Are Not Just Energy Sector Threats," Trend Micro, February 11, 2016, accessed July 20, 2016, hxxp://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.*

270. *"30862ab7aaa6755b8fab0922ea819fb48487c063bea4a84174afbbd65ce26b86," Virus Total, March 22, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/30862ab7aaa6755b8fab0922ea819fb48487c063bea4a84174afbbd65ce26b86/analysis/.*

271. *Ibid.*

272. *Ibid.*

273. *Ibid.*

274. *Ibid.*

275. *Ibid.*

276. *Ibid.*

277. *"f528694748 34be5a6b5df7f8f0c46cbc7e9b22fa5cb30bee0f363ec6eb056b95," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/f52869474834be5a6b5df7f8f0c46cbc7e9b22fa5cb30bee0f363ec6eb056b95/analysis/.*

278. *Ibid.*

279. *Ibid.*

280. *Ibid.*

281. *Ibid.*

282. *Ibid.*

283. *Ibid.*

284. *"c7536ab90621311b526aefd56003ef8e1166168f038307ae960346ce8f75203d," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/c7536ab90621311b526aefd56003ef8e1166168f038307ae960346ce8f75203d/analysis/.*

285. *Ibid.*

286. *Ibid.*

287. *Ibid.*

288. *Ibid.*

289. *Ibid.*

290. *Ibid.*

291. *"Malicious Code Analysis on Ukraine's Power Grid Incident," Beijing Knownsec Information Technology Co., Ltd., January 10, 2016, accessed July 12, 2016, hxxp://blog.knownsec.com/wp-content/uploads/2016/01/Malicious-Code-Analysis-on-Ukraines-Power-Grid-Incident-L150113.pdf.*

292. *"5d2b1abc7c35de73375dd54a4ec5f0b060ca80a1831dac46ad411b4fe4eac4c6," Virus Total, July 15, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/5d2b1abc7c35de73375dd54a4ec5f0b060ca80a1831dac46ad411b4fe4eac4c6/analysis/.*

293. *Ibid.*

294. *Ibid.*

295. *Ibid.*

296. *Ibid.*

297. *Ibid.*

298. *"11b7b8a7965b52ebb213b023b6772dd2c76c66893fc96a18a9a33c8cf125af80," Virus Total, June 21, 2016, accessed July 15, 2016, hxxps://www.virustotal.com/en/file/11b7b8a7965b52ebb213b023b6772dd2c76c66893fc96a18a9a33c8cf125af80/analysis/.*

299. *Ibid.*

300. *Ibid.*

301. *Ibid.*

302. *Ibid.*

303. *Ibid.*

304. *Ibid.*

305. *"Malicious Code Analysis on Ukraine's Power Grid Incident," Beijing Knownsec Information Technology Co., Ltd., January 10, 2016, accessed July 12, 2016, hxxp://blog.knownsec.com/wp-content/uploads/2016/01/Malicious-Code-Analysis-on-Ukraines-Power-Grid-Incident-L150113.pdf.*

306. *"Blackenergy & Quedagh: The convergence of crimeware and APT attacks," F-Secure Labs Security Response, accessed July 12, 2016, hxxps://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.*

307. *Ibid.*

308. *Raj Samani and Christiaan Beek, "Updated BlackEnergy Trojan Grows More Powerful,"McAfee Labs, January 14, 2016, accessed July 13, 2016, hxxps://blogs.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/.*

309. *Robert Lipovsky and Anton Cherapanov, "Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland," Virus Bulletin, September 25, 2015, accessed July 12, 2016, hxxps://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland.*

310. *"Blackenergy & Quedagh: The convergence of crimeware and APT attacks," F-Secure Labs Security Response, accessed July 12, 2016, hxxps://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.*

311. *Ibid.*

312. *Ibid.*

313. *Ibid.*

314. *Raj Samani and Christiaan Beek, "Updated BlackEnergy Trojan Grows More Powerful,"McAfee Labs, January 14, 2016, accessed July 13, 2016, hxxps://blogs.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/.*

315. *Robert M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute and Electricity Information Sharing and Analysis Center, March 18, 2016, accessed July 12, 2016, hxxps://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.*

316. *Robert Lipovsky and Anton Cherapanov, "Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland," Virus Bulletin, September 25, 2015, accessed July 12, 2016, hxxps://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland.*

317. *Ibid.*

318. *Raj Samani and Christiaan Beek, "Updated BlackEnergy Trojan Grows More Powerful,"McAfee Labs, January 14, 2016, accessed July 13, 2016, hxxps://blogs.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/.*

319. *"IR-ALERT-H-16-043-01AP Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security Industrial Control System Computer Emergency Response Team, March 7, 2016, accessed July 12, 2016, hxxps://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.*

320. *Paul Ducklin, "Ukraine power outages blamed on "hackers and malware" – the lessons to learn," nakedsecurity by Sophos, January 6, 2016, accessed July 12, 2016, hxxps://nakedsecurity.sophos.com/2016/01/06/ukraine-power-outages-blamed-on-hackers-and-malware/.*

321. *Eduard Kovacs, "BlackEnergy Malware Used in Ukraine Power Grid Attacks," SecurityWeek, January 4, 2016, accessed July 12, 2016, hxxp://www.securityweek.com/blackenergy-group-uses-destructive-plugin-ukraine-attacks.*

322. *"Malicious Code Analysis on Ukraine's Power Grid Incident," Beijing Knownsec Information Technology Co., Ltd., January 10, 2016, accessed July 12, 2016, hxxp://blog.knownsec.com/wp-content/uploads/2016/01/Malicious-Code-Analysis-on-Ukraines-Power-Grid-Incident-L150113.pdf.*

323. *Matt Johnston, "Dropbear SSH," University of Western Australia University Computer Club, accessed July 12, 2016, hxxps://matt.ucc.asn.au/dropbear/dropbear.html.*

324. *"Malicious Code Analysis on Ukraine's Power Grid Incident," Beijing Knownsec Information Technology Co., Ltd., January 10, 2016, accessed July 12, 2016, hxxp://blog.knownsec.com/wp-content/uploads/2016/01/Malicious-Code-Analysis-on-Ukraines-Power-Grid-Incident-L150113.pdf.*

325. *Ibid.*

326. *Ibid.*

327. *"BlackEnergy and the Ukraine: Signals vs. Noise," Cylance, January 12, 2016, accessed July 12, 2016, hxxps://blog.cylance.com/blackenergy-and-the-ukraine-signals-vs.-noise.*

AUTHORS

JAKE STYCZYNSKI
Jake Styczynski is an associate at Booz Allen Hamilton specializing in cyber threat research. He has conducted cyber threat landscape and organizational risk assessments for commercial and government clients. Jake has led project teams in open-source research efforts evaluating threats to space-based systems, maritime navigation and communication systems, and industrial control systems. Jake earned an M.I.A. in international security policy from Columbia University and a B.A. in political science from University of Massachusetts at Amherst.

NATE BEACH-WESTMORELAND
Nate Beach-Westmoreland (@NateBeachW) is a lead associate at Booz Allen Hamilton with nearly a decade of experience in cyber intelligence, open-source research, and geopolitical analysis. Nate leads a team of multidisciplinary analysts in producing strategic cyber threat intelligence for commercial and government clients. He has helped mature or establish several Booz Allen open-source intelligence teams, including the firm's first commercial cyber threat intelligence offering in 2011. He earned an M.A. in international relations from Yale University and a B.A. in history from Cornell University.

About Booz Allen

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision. With global headquarters in McLean, Virginia and more than 80 offices worldwide, our firm employs more than 26,100 people and had revenue of $6.7 billion for the 12 months ending March 31, 2019. To learn more, visit BoozAllen.com. (NYSE: BAH))

For More Information

BRAD MEDAIRY
Executive Vice President
medairy_brad@bah.com
+1-703-902-5948

JANDRIA ALEXANDER
Principal
alexander_jandria@bah.com
+1-630-776-7701

MATT THURSTON
Lead Associate
thurston_matthew@bah.com
+1-703-216-5259

boozallen.com/ics

Authors

JAKE STYCZYNSKI
Lead Author

NATE BEACH-WESTMORELAND
Author