DOI: http://dx.doi.org/10.14236/ewic/ICS2016.7

Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid

Rafiullah Khan, Peter Maynard, Kieran McLaughlin, David Laverty and Sakir Sezer
Queen's University Belfast, Belfast, United Kingdom
{*rafiullah.khan, pmaynard01, kieran.mclaughlin, david.laverty, s.sezer*} *@qub.ac.uk*

The BlackEnergy malware targeting critical infrastructures has a long history. It evolved over time from a simple DDoS platform to a quite sophisticated plug-in based malware. The plug-in architecture has a persistent malware core with easily installable attack specific modules for DDoS, spamming, info-stealing, remote access, boot-sector formatting etc. BlackEnergy has been involved in several high profile cyber physical attacks including the recent Ukraine power grid attack in December 2015. This paper investigates the evolution of BlackEnergy and its cyber attack capabilities. It presents a basic cyber attack model used by BlackEnergy for targeting industrial control systems. In particular, the paper analyzes cyber threats of BlackEnergy for synchrophasor based systems which are used for real-time control and monitoring functionalities in smart grid. Several BlackEnergy based attack scenarios have been investigated by exploiting the vulnerabilities in two widely used synchrophasor communication standards: (i) IEEE C37.118 and (ii) IEC 61850-90-5. Further, the paper also investigates protection strategies for detection and prevention of BlackEnergy based cyber physical attacks.

BlackEnergy, Malware, Cyber Attacks, Synchrophasors, Smart Grid, IEEE C37.118, IEC 61850-90-5.

1. INTRODUCTION

Synchrophasor based systems play a vital role in real-time and wide-area monitoring, protection and control in modern power grids. It involves measurement of electrical quantities in real-time at different points in the grid, time-stamped using a common precise time source (e.g., GPS) and transmitted to the control center using a suitable communication framework. Synchrophasor applications range from simple grid dynamics visualization/recording to protection in distributed generation and synchronous islanding (Schweitzer et al. (2011)). At present, two communication frameworks are available for synchrophasor technology: IEEE C37.118 and IEC 61850-90-5. Both have their own unique features and limitations (Khan et al. (2016)). Due to involvement of critical infrastructure in synchrophasor based systems and possible transmission of data over insecure wide-area network, a strong protection mechanism against cyber attacks is necessary.

The role of malware in modern sophisticated multi-stage cyber attacks cannot be ignored. The success of a cyber attack depends on the attacker's ability to install malware on a targeted system without being noticed by the system owner. The time a malware can disguise itself and persist inside an infected system is also an important factor for successful cyber attacks. BlackEnergy evolved as one of the most sophisticated and modular malware for targeting critical infrastructures since its first discovery. It has been involved in several major cyber attacks including coordinated DDoS attack on Georgia's finance, military and government agencies (Hollis (2011)), fraudulent bank transactions and the Ukraine power grid. Its concealment ability inside an infected system is evident from the US Department of Homeland Security revelation in 2014 that the software controlling several national critical infrastructures remained compromised by BlackEnergy since 2011 (ThreatSTOP (2016)).

Based on the capabilities and success stories of BlackEnergy, it is also a major threat for synchrophasor applications. Any cyber attack on synchrophasor based systems can lead to extreme consequences including blackout, financial loss and physical damage to the grid. This paper investigates key features and capabilities of BlackEnergy and analyzes threats against synchrophasor based control and monitoring systems. It presents a basic attack model used previously in BlackEnergy based cyber attacks and analyzes it for synchrophasor technology. In particular, this paper investigates vulnerabilities in both IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks which could be exploited through cyber attacks including reconnaissance, DDoS, Man-In-The-Middle (MITM) and replay attacks. The paper presents several attack scenarios which alone or in combination could severely impact monitoring and control functionalities of synchrophasor applications. The aim of paper is to investigate potential BlackEnergy threats which could aid the development of cyber security solutions.

The remainder of the paper is organized as follows: Section 2 presents background and related work. Section 3 presents formal analysis of BlackEnergy variants evolved over time. Section 4 analyzes threats of BlackEnergy for synchrophasor based systems. Section 5 presents possible protection strategies. Finally, Section 6 concludes the paper.

2. BACKGROUND AND RELATED WORK

This section presents background and related work on (i) synchrophasor technology and its security challenges and (ii) BlackEnergy based cyber attacks.

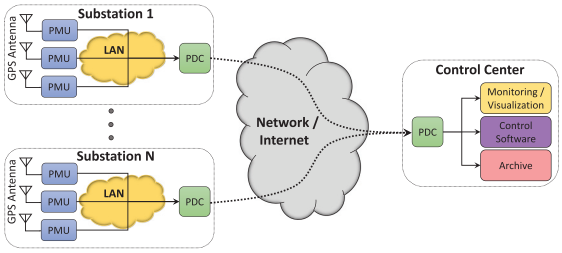

Figure 1: *Generic synchrophasor communication system.*

2.1. Synchrophasor Technology

Synchrophasor technology is used for real-time grid monitoring and control (Schweitzer et al. (2011)). Fig. 1 depicts a generic synchrophasor based system consisting of the following basic components: Phasor Measurement Units (PMUs), Phasor Data Concentrators (PDCs), communication network and control center. The PMUs are placed at different points in the grid and measure voltage and current waveforms in real-time which are transmitted to the control center. They are equipped with GPS antenna for time-stamping synchrophasor data before transmission. The PDC is a device that receives data from multiple PMUs, aggregates it based on GPS timestamps and sends as a single output stream. The control center processes data for real-time grid monitoring, control or simply archive for post-analysis in case of any disaster.

Synchrophasor technology requires a suitable communication framework for transmitting grid status information in real-time over a wide area network (Martin (2013)). IEEE developed the IEEE 1344 standard which was improved over the time and ultimately replaced by IEEE C37.118-2 (Martin et al. (2008)). The IEEE C37.118-2 has several limitations including (i) lack of security mechanism, (ii) limited interoperability and integration support and (iii) no defined transport protocol and multicast features. IEC recently established a working group for development of IEC 61850-90-5 standard (Madani et al. (2015)). IEC 61850-90-5 has a security mechanism based on Group Domain Of Interpretation (GDOI) that ensures highest level of communication security. To protect communication from cryptanalysis, GDOI periodically refreshes security policies and keying material. However, IEC 61850-90-5 adaptation is quite limited and most commercially available PMUs still support IEEE C37.118. Khan et al. (2016) presented detailed comparison of IEEE C37.118 and IEC 61850-90-5.

Laverty et al. (2013) presented an OpenPMU project, the first open source PMU project that integrates latest features and supports both IEEE C37.118 and IEC 61850-90-5. The literature mostly focuses on vulnerabilities in IEEE C37.118 due to lack of built-in security mechanism (Khan et al. (2016)). Allgood et al. (2011) highlighted that synchrophasors are transmitted over wide-area networks and an insecure communication protocol raises serious threats against potential cyber attacks. Stewart et al. (2011) addressed best practice strategies and explained the role of Virtual Private Network (VPN) and firewall in protection against cyber attacks. Morris et al. (2011) tested the resilience of PMUs against Denial of Service (DoS) attacks and monitored their degree of unresponsiveness when flooded with ARP requests and IPv4 packets. Coppolino et al. (2014) also augmented the work on PMU vulnerabilities when using IEEE C37.118. Shepard et al. (2012) addressed GPS spoofing that can severely impact power system. In short, cyber attacks on a synchrophasor based system could lead to extreme consequences. Several survey articles (Yan et al. (2012), Boyer et al. (2009), Beasley et al. (2014)) have addressed security challenges for synchrophasors and smart grid in general.

An investigation is necessary to determine resilience of IEEE C37.118 and IEC 61850-90-5 against BlackEnergy based attacks. Further, countermeasures or protection strategies also need to be investigated.

2.2. History of Black Energy

The history of BlackEnergy and its involvement in different cyber attacks is depicted in Fig. 2. It was

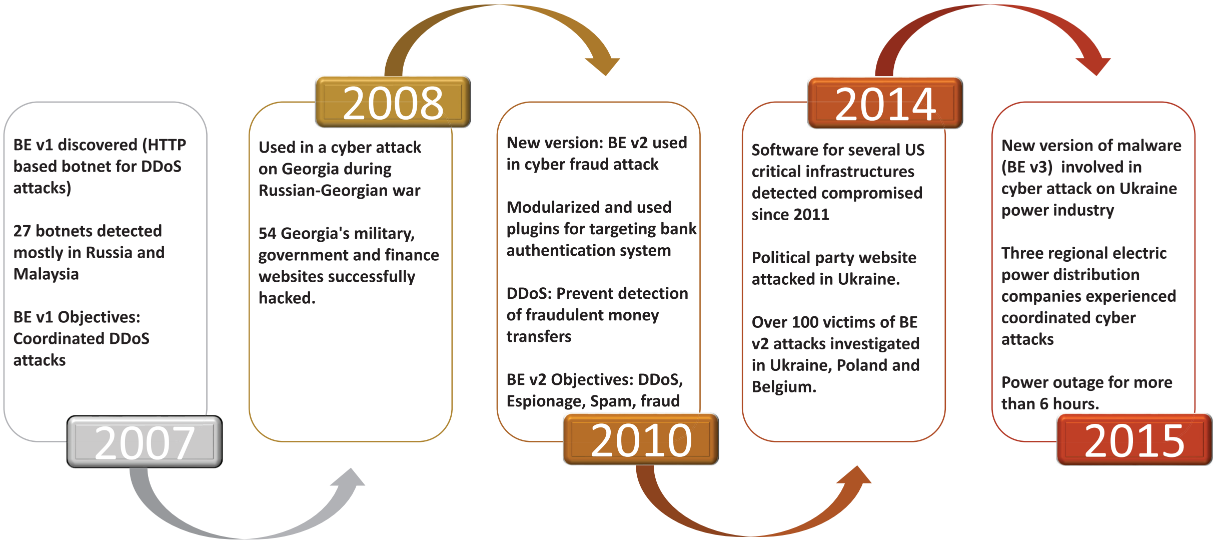
2007
BE v1 discovered (HTTP based botnet for DDoS attacks)
27 botnets detected mostly in Russia and Malaysia
BE v1 Objectives: Coordinated DDoS attacks
2008
Used in a cyber attack on Georgia during Russian-Georgian war
54 Georgia's military, government and finance websites successfully hacked.
2010
New version: BE v2 used in cyber fraud attack
Modularized and used plugins for targeting bank authentication system
DDoS: Prevent detection of fraudulent money transfers
BE v2 Objectives: DDoS, Espionage, Spam, fraud
2014
Software for several US critical infrastructures detected compromised since 2011
Political party website attacked in Ukraine.
Over 100 victims of BE v2 attacks investigated in Ukraine, Poland and Belgium.
2015
New version of malware (BE v3) involved in cyber attack on Ukraine power industry
Three regional electric power distribution companies experienced coordinated cyber attacks
Power outage for more than 6 hours.

Figure 2: *History of Black Energy.*

first discovered by Arbor Networks (Nazario (2007)) as a simple HTTP based botnet. It is regarded as BlackEnergy version 1 (BE1) and specifically designed for DDoS attacks. It provides an attacker an easy to control HTTP based bot with minimal syntax for control functionalities. Arbor Networks detected that most BE1 Command & Control (C&C) servers were located in Malaysia and Russia. A distinguishing feature of BE1 DDoS is its capability to target more than one destination IP address per hostname (Nazario (2007)). This makes the coordinated DDoS much more effective even if the target is using DNS load balancing. The bot also uses encryption at runtime to prevent detection by anti-virus software. The victims of BE1 are of two types: (i) several distributed compromised systems with BE1 Trojan for launching coordinated DDoS, and (ii) the end targeted system of DDoS attack. The connection between both types of victims was unclear. Arbor Networks identified 27 active DDoS networks based on BE1 Trojan located in Malaysia and Russia, whereas, their main targets were also located in Russian IP address space.

It is widely believed that BE1 was used for a DDoS attack on Georgia in 2008 during the Russian-Georgian war. However, there is insufficient information to prove this speculation. The attack was highly successful resulting in 54 websites inaccessible (Hollis (2011)). The attack left Georgia's government, military, finance and news agencies unable to communicate with citizens from affected areas. It is believed that reconnaissance attack took place several weeks prior to actual DDoS attack.

In 2010, BlackEnergy version 2 (BE2) was discovered with new espionage, spam and fraud capabilities. SecureWorks research team revealed that BE2 was involved in stealing financial and authentication data from Russian banks (Russian botnets targeting local banks) (ThreatSTOP (2016)). SecureWorks further revealed that BE2 has a modular design that uses plugins for carrying out a specific malicious activity without re-writing completely new code. After stealing authentication data, BE2 utilized a DDoS plug-in against the same bank to take authentication system offline for customers and distract them from noticing the fraudulent transactions. Further, BE2 was also accompanied with a plug-in designed to destroy the filesystem on compromised machine.

BlackEnergy is also a major threat to critical infrastructures. US Department of Homeland Security revealed in 2014 that the software controlling several national critical infrastructures including nuclear plants, electric grids, water filtration systems and oil and gas pipelines had been compromised by BlackEnergy since 2011 (ThreatSTOP (2016)). F-Secure labs researched two BE2 samples in 2014. The main victim of first sample was a political website in Ukraine while NATO headquarters in Belgium was the main target of second sample. In the same year, ESET also researched more than 100 BE2 victims mostly in Poland and Ukraine (ThreatSTOP (2016)).

The story of BlackEnergy continues and three regional electric power distribution companies of Ukraine experienced coordinated cyber attacks in December 2015. The attacker utilized a new variant of malware, BlackEnergy version 3 (BE3) for illegal entry into the company's computer and SCADA systems. Attackers opened the breakers of seven 110 kV and 2335 kV substations resulting in blackout for more than 225,000 people which took 6+ hours to restore. To remove attack traces and elongate

Table 1: *BlackEnergy features and capabilities.*

Feature	BE1	BE2	Lite	BE3
GUI Build Tools	X	X	X	X
Plugin Support		X	X	X
Denial of service	X	X	X	X
C2C Controller	X	X	X	X
AV Obfuscation	X	X	X	X
Kernel rootkit			X	X
x64 support			X	X
bypass driver signing				X
Reside only in memory				X
rundll			X	X
Detection of virtual environment				X
Anti-debugging methods				X
Detect security countermeasures				X

the blackout period, attackers also utilized KillDisk malware to wipe/erase several systems and corrupt master boot records in all three companies. In addition, a custom firmware was deployed for serial to Ethernet converters that bricked the devices and prevented technicians from restoring power until converters were bypassed.

3. FORMAL ANALYSIS OF BLACKENERGY

The use of BlackEnergy for targeted attacks is attributed to a Russian based cyber gang known as Sandworm. Sandworm uses spear phishing as their preferred infection tactic and the latest version of BlackEnergy as signature malware. BlackEnergy enumerates all installed drivers on a system and identifies those which are disabled. It randomly selects a disabled driver, maliciously replaces it with its own driver and enables it on the compromised system. The driver needs to have a valid signature. BlackEnergy bypasses such security features by modifying system boot configuration data to enable testing signatures and patches the user32.dll.mui or bypasses the UAC through shim. Table 1 describes how BlackEnergy features evolved over time and is discussed in the following sections.

3.1. BlackEnergy 1

The BE1 is HTTP based botnet used for coordinated DDoS attacks. It provides the attacker an easy to control interface with minimal syntax and structure. The BE1 botnet configurations are stored and loaded from MySQL database (db.sql). Unlike traditional botnets, it does not communicate with botnet master using Internet Relay Chat (IRC). Further, BE1 lacks the exploit functionalities and relies on external tools to load the bot. BE1 botnet uses HTTP POST messages to communicate with its controlling servers and specifies the bot's ID inside each message. Key features of BE1 include (Nazario (2007)): (i) ability to target more than one IP address per hostname, (ii) a runtime encrypter to prevent detection by antivirus software, and (iii) disguises itself by hiding its processes in a system driver (syssrv.sys). The BE1 bot has three different types of commands: (i) DDoS attack commands e.g., ICMP flood, TCP SYN flood, UDP flood, HTTP get flood, DNS flood, etc, (ii) download commands to fetch and launch a new or updated executable from its server and (iii) control commands e.g., stop (to freeze DDoS), wait (a placeholder) or die (kill or exit).

3.2. BlackEnergy 2

BE2 provided extended functionalities with easily loadable attack-specific plugins for espionage, fraud, stealing user credentials or key logger, scanning network, sending spam and more. BE2 is a superset of BE1 and also contains plugin for the original DDoS functionality. The plugins are downloaded/updated from its C&C servers on compromised system in an encrypted format as drivers. BE2 also contains a Trojan plugin that can destroy the complete filesystem of a compromised system on kill command (ThreatSTOP (2016)). The capabilities of BE2 include: (i) execute local files, (ii) download and execute remote files, (iii) update itself and plugins with C&C servers and (iv) die or destroy. The plugins and update features of BE2 make it highly evasive with a much longer survival time on compromised systems. If the bot is detected by antivirus software, the attacker only rewrites the discovered part.

3.3. BlackEnergy 3

The BE3 is highly simplified version of BE2, first discovered in 2014. Compared to BE2, BE3 bears minor changes and uses a different protocol for communication with its plugins (ThreatSTOP (2016)). Further, the BE3 installer drops the main DLL component directly into user processes (specifically in svchost.exe) rather than using driver/rootkit component as in BE2. BE3 was also found scanning the internet for a specific HMI, the GE Intelligent Platforms HMI/SCADA - CIMPLICITY. The HMI was known to have a directory traversal vulnerability in CimWebServer.exe (the WebView component) which allows remote attackers to execute arbitrary code via a crafted message to TCP port 10212, (ZDI-CAN-1623). BE3 targeted this service after detecting its network interface. Once it detected an exploitable server, it has two options; download devlist.cim or config.bak which would then use to deploy BE3. Once on a system, BE3 scans the network and local machines for data to exfiltrate.

3.4. BlackEnergy Lite

The BE Lite (also known as BE Mini) has different build ID format, different plugin interface and has much lighter footprint. Unlike BE2 and BE3, it does not use a driver for loading the main DLL but instead uses more standard way for loading DLLs (e.g., rundll32.exe). The configuration data of BE Lite is stored as X.509 certificates unlike other BlackEnergy variants which store in XML files.

4. SECURITY CHALLENGES FOR SYNCHROPHASOR BASED APPLICATIONS

BlackEnergy is one of the most sophisticated malware evolved over time and played key role in several high profile cyber attacks on critical infrastructures in the past. It is also a major threat to synchrophasor technology which is particularly used for monitoring and control of critical infrastructure. Depending on the type of cyber attack on synchrophasors, the potential impact could be different. The BE3 with DDoS plugin could lead to failure in a power grid leaving PMUs unable to communicate with the control centers. BE3 with fs.dll and dstr.dll plugins could destroy entire filesystem on compromised system and leave devices completely inoperable. BE3 with ps.dll and kd.dll plugins could provide an attacker key logging and password stealing functionalities which could be necessary for remote access to critical system components e.g., the PMU, and alter the configurations. BE3 with scan.dll, vs.dll and rd.dll plugins could help attacker remotely access the compromised system, scan the entire network and discover the devices of interest and launch MITM, replay or other traffic manipulation attack on communication between PMUs and the control center. Traffic manipulation attacks could severely damage physical equipment and result in complete shutdown of grid components.

Depending on the synchrophasor communication framework (IEEE C37.118 or IEC 61850-90-5), BlackEnergy kill chain process could be slightly different. This section presents a basic cyber attack model derived from the analysis of previous BlackEnergy based cyber attacks. Further, several attack scenarios have been addressed in which BlackEnergy could play lead-role in executing cyber attacks on synchrophasor based systems.

4.1. Basic Cyber Attack Model

A proper anatomy of cyber attack could help detect and prevent future attacks. Fig. 3 illustrates steps involved in the launch of a successful cyber attack based on BlackEnergy in particular but equally applicable to any malware in general.

4.1.1. Reconnaissance

It is the first step in any cyber attack to identify and exploit vulnerabilities in the targeted system including organizational structure, OS and software types and version, security credentials and any misconfigurations. It is the identification of a weak initial target that is either inside or connected to the targeted organization.

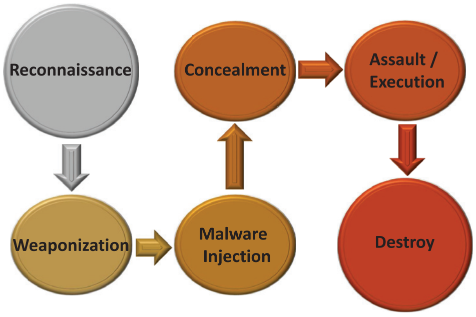

Figure 3: *The anatomy of cyber attack.*

4.1.2. Weaponization

Once a weak target is identified, a weapon is prepared for initial attack. Weaponization often means trojanization of a genuine application, document or file with malicious code. E.g., weaponization may exploit macros in Microsoft word document or use PDF files in malicious way.

4.1.3. Malware Injection

The next step is injection of malware or weaponized application/document into the targeted system. The most common method is spear phishing i.e., sending weaponized document as email attachment or link to weaponized application in email by impersonating it as a link for necessary updates of a genuine application already installed on the system. The BlackEnergy attack on Ukraine power companies was based on spear phishing (ThreatSTOP (2016)). Another common malware injection strategy is pharming or driveby pharming i.e., redirecting traffic to fraudulent website through exploiting vulnerabilities in DNS server.

4.1.4. Concealment

Once malware is successfully injected and executed, the next step is to disguise and remain undetected by defense mechanisms on targeted system. BlackEnergy successfully replaces genuine system drivers to conceal itself. Concealment is necessary to get enough time for attack preparation, testing and validation before final execution to get best results.

4.1.5. Assault

It is the actual execution of an attack based on the BlackEnergy version and plugins used. The concealed malware executes the final attack only when instructed by C&C servers e.g., coordinated DDoS attack on Georgia (Hollis (2011)).

4.1.6. Destroy

Post attack after achieving objectives, the attacker destroys all traces leaving behind no clues of attack process. Cleaning logs and injecting mis-leading information into the system could obfuscate forensic team from revealing attack success reasoning. The BlackEnergy attack on Ukraine power companies used a KillDisk plugin to destroy the entire file system, destroy forensic evidences and significantly increase recovery time for power companies.

4.2. Coordinated DDoS Attack on Synchrophasor-Based System

The DDoS attack floods target systems with traffic originating from potentially thousands of different sources. The distributed nature makes it difficult to differentiate between legitimate packets and flood packets. Further, attack prevention cannot be achieved by simply blocking packets from a single origin IP. The DDoS attack leaves target system irresponsive by consuming all of its processing resources.

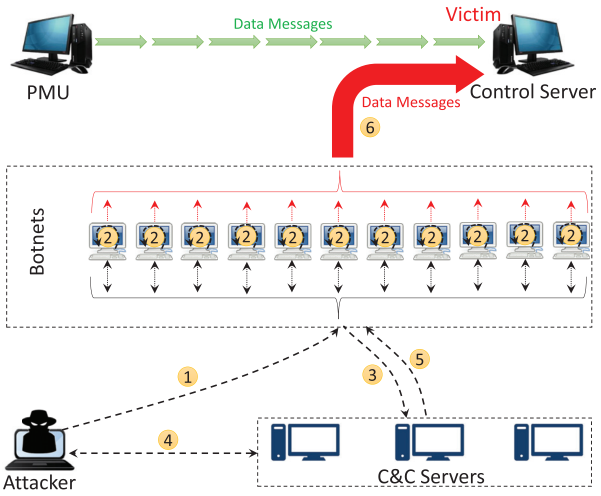

Figure 4: *Coordinated DDoS Attack on IEEE C37.118 using BlackEnergy DDoS plugin.*

Several synchrophasor applications involve local communication or use of secure VPNs which make DDoS attacks on a specific device difficult. The attack scenario in Fig. 4 is limited to certain specific synchrophasor applications involving transmission over Internet without using VPN tunnels. It is similar to the DDoS attack on Georgia (Hollis (2011)) and consists of following steps:

Step:1 It involves reconnaissance, weaponization and malware injection (i.e., BE3 with DDoS plugin) steps of attack model shown in Fig. 3.

Step:2 Execution of injected malware and concealment.

Step:3 The victim sends basic information about compromised system to C&C servers.

Step:4 The attacker gets information about compromised systems from C&C servers and instructs them when to execute actual attack.

Step:5 C&C servers send attacker commands to victims.

Step:6 The victims execute coordinated DDoS when instructed by attacker through C&C servers.

Fig. 4 demonstrates DDoS by flooding ‘data’ messages; a specific IEEE C37.118 message carrying actual synchrophasor measurements. Without knowing PMU configurations, the botnets could not construct correctly formated data messages. In case of IEC 61850-90-5, the botnets will flood Sampled Value (SV) packets. However, botnet operators will most likely lack knowledge about security policies and keying material. Thus, incorrectly formated packets or packets with invalid signatures will be immediately discarded by the control server without being fully processed. This results in the reduced strength of DDoS attack. For a much stronger DDoS attack with correctly formated flood packets, a multi-stage attack is addressed in Section 4.6.

4.3. Reconnaissance/Eavesdropping Attack on Synchrophasor-Based System

Reconnaissance is unauthorized discovery of network and equipment configurations, system topology and system dynamics. Since synchrophasors carry real-time dynamics about the power system, eavesdropping could reveal critical information to the attacker. Reconnaissance itself is not harmful but can help discover system dynamics and vulnerabilities, steal secrets (e.g., login credentials for remote access devices) and can help determine the right time for more severe attacks.

A reconnaissance attack could be launched by eavesdropping on network traffic or by directly accessing the physical device. Depending on the attack strategy, the attacker could use BlackEnergy with one or more plugins such as scan.dll (i.e., network scanning), kl.dll (i.e., key-logger), vs.dll (i.e., network discovery & remote execution), ss.dll (i.e., screenshot), ps.dll (i.e., password stealer), tv.dll (i.e., teamviewer) or rd.dll (i.e., remote desktop). Fig. 5 depicts the attack scenario for reconnaissance and consists of the following steps:

Step:1-5 Corresponds to steps 1-5 as in Fig. 4.

Step:6 The victim scans for an internal server or HMI device that has the ability to access/control field devices. Attacker uses remote execution vulnerability to implant BlackEnergy on internal server which then

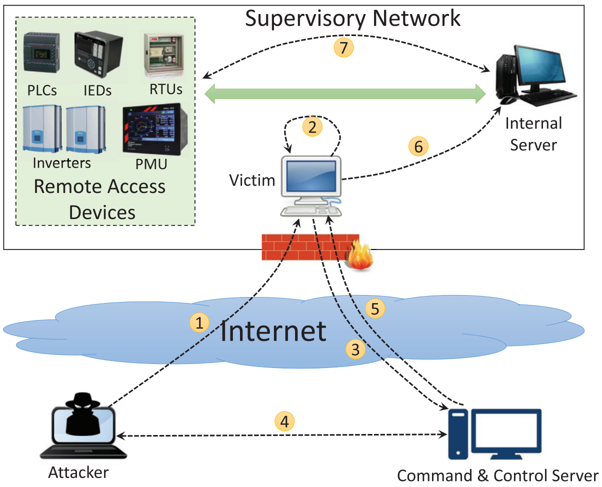

Figure 5: *Reconnaissance/Eavesdropping attack scenario on synchrophasor System.*

opens a SSH backdoor on a specific port. This provides the attacker more flexibility to control internal server/HMI.

Step:7 The actual reconnaissance attack execution by remotely accessing and monitoring the device or sniffing and monitoring its traffic (e.g., using traffic diversion demonstrated in Fig. 6).

The attacker will acquire PMU configurations (i.e., necessary for IEEE C37.118) or security credential for IEC 61850-90-5 by either remotely accessing the PMU from a compromised server or by monitoring its traffic. Such information will also enable an attacker to control PMU operations. To eavesdrop on traffic, the compromised internal server needs to implement local traffic diversion mechanism (depicted in Fig. 6), which is one possible approach described as follows:

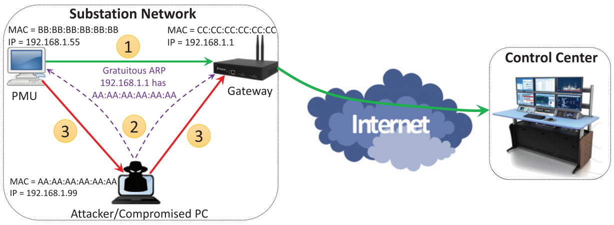

Figure 6: *Traffic diversion based on ARP spoofing.*

Step:1 Normal operations scenario when no traffic diversion is activated.

Step:2 The attacker broadcast Gratuitous ARP inside local network to update ARP caches of all LAN devices. Gratuitous ARP associates PMU or gateway IP (i.e., one way traffic diversion) or both IP addresses (i.e., two way traffic diversion) with attacker's MAC address.

Step:3 Final delivery of packets inside local network is based on MAC address. Thus, all traffic to/from PMU goes to attacker who then forwards to correct destination.

The attack scenario in Fig. 5 is also very similar to recent BlackEnergy attack on Ukraine power companies (Lee et al. (2016)). During step 6, BlackEnergy malware opened an SSH backdoor by listening on port 6789. During step 7, attackers altered configurations of inverters and created blackout. The attackers took an additional step by executing KillDisk plugin to format/destroy the entire file system of internal server. This left the attack impact over a longer period and more time and efforts were required to recover the system from attack. The attackers also launched a DDoS attack (similar to Fig. 4) on control center in parallel to prevent customers from reporting the blackout.

4.4. Man In The Middle Attack on Synchrophasor-Based System

The MITM attack hijacks communication between two devices and makes them believe that they are connected to each other directly. Instead, the attacker lies in the middle, sniffs and manipulates packets in transit. The attacker may alter packets in transit or drop them or inject new packets.

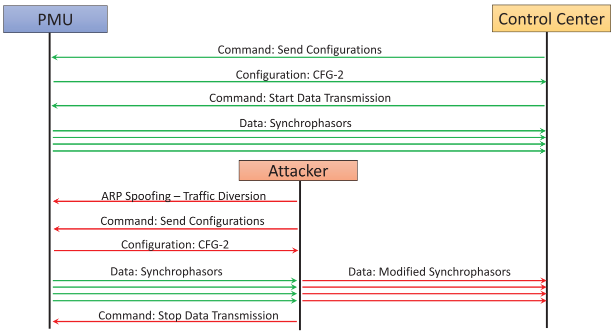
PMU
Control Center
Command: Send Configurations
Configuration: CFG-2
Command: Start Data Transmission
Data: Synchrophasors
Attacker
ARP Spoofing – Traffic Diversion
Command: Send Configurations
Configuration: CFG-2
Data: Synchrophasors
Data: Modified Synchrophasors
Command: Stop Data Transmission

Figure 7: *MITM attack: Hijacking of IEEE C37.118 communication.*

For a MITM attack, the attacker first needs to get access inside supervisory network by compromising an internal server (i.e., similar to Steps 1-6 in Fig. 5). The next step is to implement traffic diversion (depicted in Fig. 6) to get access to packets in both directions. Further steps after traffic diversion depend on the communication framework: IEEE C37.118 or IEC 61850-90-5. The basic scenario to successfully hijack IEEE C37.118 communication and perform MITM attack is depicted in Fig. 7. To initiate communication with PMU, the control center sends a command message to request configurations from PMU. The PMU replies with a configuration message that contains information about the PMU as well as necessary decoding information for the upcoming synchrophasor data messages. Afterwards, the control center sends another request to the PMU to start the transmission of synchrophasor data messages. If an attacker sits in the middle by implementing traffic diversion, it cannot understand/decode synchrophasor data messages without the knowledge of PMU configurations. Thus, the attacker sends command message to PMU to request the configurations. After storing configurations, the configuration message from PMU should be dropped and prevented from traveling to the control center. At this point, the attacker can successfully decode synchrophasor data messages in transit and manipulate/modify them before being forwarded to the control center. An attacker may also interrupt communication by sending command message to PMU to stop transmission of synchrophasors and generate packets from its own and transmit to the control center. For synchrophasor control applications, it can cause severe damage to physical equipments and financial loss as the deceived control center unintentionally performs decisions on incorrect data.

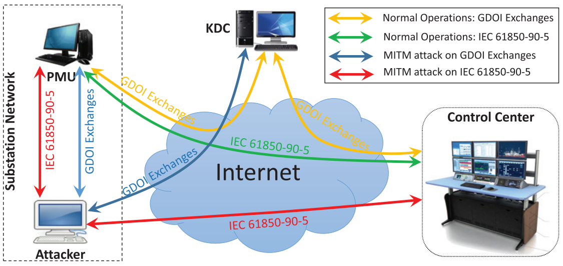

Figure 8: *MITM attack: Hijacking of IEC 61850-90-5 communication.*

Unlike IEEE C37.118, the IEC 61850-90-5 communication cannot be hijacked easily due to GDOI security mechanism. As depicted in Fig. 8, both the PMU and control center first need to acquire security policies and keying material from the Key Distribution Center (KDC) through specific GDOI exchanges. The acquired security credentials then enable the PMU and control center to securely communicate with each other. For an attacker to play a MITM role, it needs to hijack both GDOI exchanges as well as IEC 61850-90-5 communication. Both GDOI exchanges and IEC 61850-90-5 messages are encrypted leaving the attacker unable to decrypt and manipulate the messages in transit. To acquire security credentials for decryption, the attacker may adopt one of two strategies: (i) compromise the PMU as well and steal security credentials, or (ii) persist inside the substation network until a new PMU or existing disconnected PMU (e.g., due to maintenance) reconnects to the network and authenticates with the KDC. The authentication phase with KDC can be successfully hijacked by an attacker by a MITM attack on GDOI authentication exchanges (e.g., MITM attack on Diffie Hellman authentication mechanism). The attacker masquerades as the PMU to the KDC, and as the KDC to the PMU. Thus, two authentications take place: (i) between PMU and attacker and (ii) between attacker and KDC. Once GDOI phase 1 (i.e., Diffie Hellman) has been compromised, an attacker can successfully decrypt and manipulate IEC 61850-90-5 packets in transit between PMU and control center by using acquired security credentials.

4.5. Replay/Reflection Attack on Synchrophasor-Based System

The procedure and requirements of replay/reflection attack are similar to the MITM attack as addressed in Section 4.4. It can hide the real-time power system dynamics by storing/recording communication between a PMU and control center and plays it back to the control center later on. It can lead to incorrect decisions by the control center due to processing out-dated packets. It is particularly risky for real-time synchrophasor control applications such as synchronous islanding and could cause physical damage to substation resulting in local blackout. For replay attack on IEEE C37.118, the attacker does not need to acquire configurations from PMU. However, the Second Of Century (SOC) count inside each recorded packet should be adjusted by attacker before replaying to the control center. For a replay attack on IEC 61850-90-5, the attacker still needs to acquire security credentials as addressed in Section 4.4. The attacker needs to decrypt packets and update session PDU numbers and security information inside each packet before transmitting to control center. This step is necessary as the GDOI security credentials have certain validity and replaced periodically upon expiry.

4.6. Multistage DDoS Attack on Synchrophasor-Based System

As addressed in Section 4.2, the packets in simple DDoS for IEEE C37.118 and IEC 61850-90-5 are partially processed by control center and ignored. To launch a strong DDoS attack by enabling control center to process flood packets completely, knowledge of PMU configurations for IEEE C37.118 and security credentials for IEC 61850-90-5 is strictly necessary. This requires a multi-stage attack utilizing BlackEnergy DDoS plugin along with other plugins (e.g., scan.dll, ps.dll, re.dll, etc) for information stealing. The first stage attack is on the substation network by compromising an internal server and stealing necessary information from PMU. In second

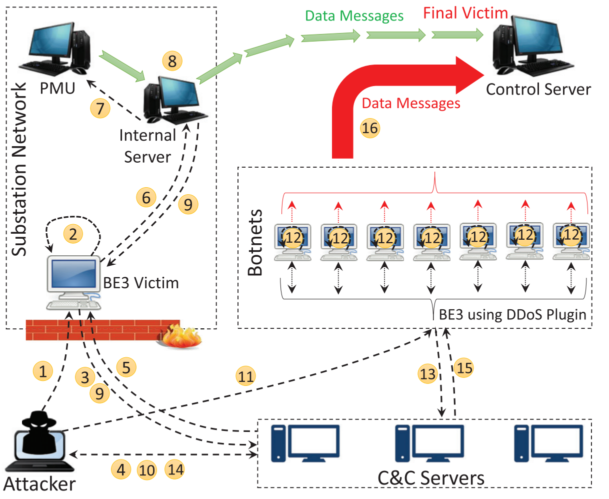

***Figure 9:** Strong DDoS attack based on two-stage interim attacks utilizing BlackEnergy plugins for credential theft and DDoS.*

stage, DDoS botnets utilize stolen information and launch coordinated DDoS attack on control server.

The two stage attack scenario on synchrophasor based system (depicted in Fig. 9) consists of the following steps:

Step:1-6 Corresponds to steps 1-6 as in Fig. 5.

Step:7 Attacker implements traffic diversion to gain access to PMU messages.

Step:8 Attacker through reconnaissance finds the PMU configurations for IEEE C37.118 communication framework which is necessary to build and decode synchrophasor data messages. In case of IEC 61850-90-5, security credentials are also hacked as described in Fig. 8.

Step:9 Necessary synchrophasor information is returned to the C&C servers.

Step:10 Attacker instructs C&C servers to provide stolen synchrophasor information to DDoS botnets when discovered.

Step:11-15 Corresponds to steps 1-5 as in Fig. 4.

Step:16 The DDoS botnets use stolen synchrophasor information provided by the C&C servers and build correctly formated IEEE C37.118 or IEC 61850-90-5 messages and flood on the control server for a very strong DDoS attack.

5. PROTECTION STRATEGIES

A basic level of protection can be achieved with anti-virus software and firewall configurations. An updated anti-virus software may detect known variants of BlackEnergy but cannot guarantee protection against its future updates. Also firewalls block incoming connections at non-open ports but are not effective in case of spear phishing emails. Sandboxes can also provide protection while testing/executing unverified applications/documents. This section presents protection strategies in a generalized way with flexibility in mind to tackle with unforeseen future behavior changes in BlackEnergy.

5.1. Black-Listing and White-Listing Connections

The blacklisting and whitelisting of external destination IP addresses can be one of the most effective protection strategy against BlackEnergy. The unforeseen future updates of BlackEnergy make impossible to create a blacklist for its C&C servers. Instead, a whilelist of trusted destinations should be created for PMU and control center. Such defense may be local to device or system-wide. A device's local defense system will monitor its inbound and outbound traffic and check with the whilelist. Whereas, a system-wide defense system will monitor the entire network traffic. Blocking inbound as well as outbound connections which are not specified in whitelist will prevent BlackEnergy victim (e.g., if any compromised through spear phishing emails or infected websites) to communicate with the C&C servers. This leaves the attacker unable to communicate with victim in order to execute the attack. This strategy will become ineffective if any future variant of BlackEnergy performs its job without requiring communication with C&C servers.

5.2. Event Monitoring and Logging

Event monitoring and logging for both users and SCADA applications could help detect or identify security breaches or perform forensic analysis. First, a baseline should be defined for defense system based on device routine activities. The baseline for a synchrophasor based system can be PMU configurations, messaging rate, drivers and firmware updates etc. An alert should be raised if non-scheduled event is detected.

5.3. End-to-End Encryption

The PMUs are specialized devices and the likelihood of direct infection by BlackEnergy is very low. However, the malware can target a general purpose office PC and launch traffic hijacking, MITM and replay attacks on PMU traffic. Such attacks can be launched on unencrypted IEEE C37.118 packets and GDOI security mechanism in IEC 61850-90-5. The attacks can be easily prevented if end-to-end encryption is used by communicating devices without relying on external KDC. Without the knowledge of security credentials, the attacker cannot manipulate PMU traffic in transit.

5.4. Remote Access to PMUs

Cyber attacks normally involve remote access to field devices and altering their configurations e.g., cyber attack on Ukraine power companies remotely opened breakers (Lee et al. (2016)). The specialized devices like PMUs are better to be controlled locally with remote access features disabled. Eliminating network interface will prevent attacker to gain direct access to PMUs. This strategy is particularly useful if PMU communication is using end-to-end encryption and its traffic cannot be manipulated in transit.

5.5. Protocol Specific Strategies

The defense mechanism on field devices should also raise an alert if any non-routine packet is detected. E.g., to implement reconnaissance or MITM attack on IEEE C37.118, the compromised local system requests configurations from PMU to understand the data messages. These request packets are normally spoofed with the genuine recipient IP address. However, such activity should be marked suspicious by a PMU as it has already provided configurations to the recipient. For IEC 61850-90-5, the attacker may attempt to disconnect a PMU from the KDC and then attempt MITM on communication between the PMU and KDC. The PMU should be suspicious on such events and raise an alert. Further, the PMU should also detect gratuitous ARP packets (i.e., used for traffic diversion) and raise an alert.

6. CONCLUSIONS

BlackEnergy is one of the most sophisticated malware in active development and has been used in high profile cyber attacks on critical infrastructures. Its concealing ability in infected systems, bypassing of UAC settings, bypassing driver signing policy and plugin nature of its recent variant increased its scope to virtually unlimited cyber criminal activities. A cyber attack may use more than one plugin based on attacker intension where each plugin performs a specific task e.g., scan.dll (i.e., network scanning), kl.dll (i.e., key-logger), vs.dll (i.e., network discovery & remote execution), ss.dll (i.e., screenshot), ps.dll (i.e., password stealer), si.dll (i.e., stealing information), rd.dll (i.e., remote desktop) etc.

This paper addressed BlackEnergy malware in detail and highlighted its features and capabilities. It analyzed how BlackEnergy can be utilized for targeting critical infrastructures. Particularly, threats were analyzed for the synchrophasor technology which is used for real-time monitoring and control in smart grids. The paper demonstrated DDoS, reconnaissance, MITM and replay attacks on the communication frameworks used in synchrophasor based systems. A successful DDoS attack could impair real-time monitoring and control functionalities. The reconnaissance attack could help attacker to launch more sophisticated attacks by stealing configurations and security credentials from PMU. The MITM and replay attacks are most critical as they can leave control center performing decisions on incorrect data. Based on the synchrophasor control application e.g., synchronous islanding, such attacks can cause severe physical damage to grid and cause blackout.

The paper also addressed possible protection strategies for shielding synchrophasor based systems against BlackEnergy. Absolute protection against BlackEnergy could not be guaranteed due to unforeseen future updates to its functionalities, plugins/capabilities and infection strategy. However the task can become more challenging for attackers if they must evade protection strategies such as Blacklisting/Whitelisting external IP addresses, end-to-end communicating encryption, eliminating/disabling network interface for field devices (e.g., PMUs). Regular monitoring of system logs and events could also help detect security breaches e.g., unscheduled update/installation of driver or firmware.

ACKNOWLEDGMENT

This work was funded by the EPSRC CAPRICA project (EP/M002837/1).

REFERENCES

Schweitzer, E. O. et al. (2011). Advanced real-time synchrophasor applications. *SEL Journal of Reliable Power*, 2(2).

Khan, R. et al. (2016). Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks. In: *IEEE PES-GM*.

Hollis, D. (2011). Cyberwar case study: Georgia 2008. *Small Wars Journal*.

ThreatSTOP (2016). Black energy. *Security Report by ThreatSTOP*.

Martin, K. E. (2013). Synchrophasor standards and guides for the smart grid. In: *IEEE PES-GM*.

Martin, K. E. et al. (2008). Exploring the IEEE Standard C37.118-2005 synchrophasors for power systems. *IEEE Transactions on Power Delivery*.

Madani, V. et al. (2015). Challenges and Lessons Learned from Commissioning an IEC 61850-90-5 based Synchrophasor System. In: *68th Annual Conference for Protective Relay Engineers*.

Laverty, D. M. et al. (2013). The OpenPMU project: Challenges and perspectives. In: *IEEE PES-GM*.

Khan, R. et al. (2016). IEEE C37.118-2 synchrophasor communication framework: Overview, cyber vulnerabilities analysis and performance evaluation. In: *ICISSP*.

Allgood, G. et al. (2011). Security profile for wide area monitoring, protection and control. in: *UCAIug SG Security Working Group*.

Stewart, J. et al. (2011). Synchrophasor security practices. In: *14th Georgia Tech Fault and Disturbance Analysis Conference*.

Morris, T. et al. (2011). Cybersecurity testing of substation phasor measurement units and phasor data concentrators. In: *7th ACM CSIIRW*.

Coppolino, L. et al. (2014). Exposing vulnerabilities in electric power grids: An experimental approach. *Int. Journal of Critical Infrastructure Protection*, 7(1), 51–60.

Shepard et al. (2012). Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. In: *Critical Infrastructure Protection Conference*.

Yan, Y. et al. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys and Tutorials*.

Boyer, W. F. and McBride, S. A. (2009). Study of security attributes of smart grid systems - Current cyber security issues. Battelle Energy Alliance LLC., Rep INL/EXT-09-15500.

Beasley, C. et al. (2014). A survey of electric power synchrophasor network cyber security. In: *PES ISGT-Europe*.

Nazario, J. (2007). BlackEnergy DDoS Bot analysis. *Arbor Networks Technical Report*.

Lee, R. M. et al. (2016). Analysis of the cyber attack on the Ukrainian power grid. In: *SANS ICS Report*.