Analysis Report

iTrust-Analysis-001

May 2016

iTrust
Centre for Research
in Cyber Security

BlackEnergy - Malware for Cyber-Physical Attacks

About iTrust

iTrust is a multidisciplinary research centre located in the Singapore University of Technology and Design (SUTD), established collaboratively by SUTD and the Ministry of Defence, Singapore (MINDEF). The focus of iTrust is on cyber security, spanning across three research areas:

a. Cyber Physical System (CPS);
b. Enterprise Networking / Security; and
c. Internet of Things (IoT).

iTrust researchers focus on the development of advanced tools and methodologies to ensure security and safety of current and future cyber physical systems and Internet of Things (IoT) systems. Systems of interest include large infrastructure of national importance such as power grid, water treatment, and oil refineries as well as cyber-devices such as smart watches, pacemakers, defibrillators, insulin pumps, and VNS implants.

Cyber physical systems is one of the many areas we are working on. The focus of the proposed research is to improve our understanding of cyber threats to CPSs and to develop and experiment with strategies to mitigate such threats. Our approach is based on well understood technical foundations borrowed from the interdisciplinary fields of control theory, artificial intelligence, game theory, networking, and software engineering.

The techniques propose will be evaluated against, and demonstrated in our Secure Water Treatment (SWaT) Testbed, Water Distribution System (WADI) testbed, and Electric Power and Intelligent Control (EPIC) testbed. Similarly, shielded room laboratory for IoT research.

iTrust researchers are drawn from across SUTD and with a strong collaboration with Massachusetts Institute of Technology (MIT), enrich the depth, breadth, and quality of research. Academic collaborators include MIT, Imperial College, University of Illinois at Urbana-Champaign (UIUC)/Advanced Digital Sciences Center (ADSC), Ben Gurion University, Israel and Nanyang Technological University, Singapore (NTU).

For more information, please refer to http://itrust.sutd.edu.sg.

Thank you.

iTrust, Centre for Research in Cyber Security
Singapore University of Technology and Design

Malware for Cyber-Physical Attacks

Siddhant Shrivastava, iTrust Centre for Research in Cyber Security

Cyber-Physical Systems are increasingly being used in critical infrastructures. Recent attacks on these systems have resulted in adverse consequences on an international level. Contemporary malware has expanded its scope from conventional cyberspace to the physical space by attacking Cyber-Physical Systems. One such popular malware family, *BlackEnergy*, is studied in detail here to better understand the scope of Malware in facilitating Cyber-Physical Attacks.

Contents

1 Introduction

Recent malware-facilitated attacks on criticial public infrastructure bolster the need to understand the relation between malware and cyber-physical attacks. This report studies the BlackEnergy malware family in detail and its involvement in attacks on industries in Ukraine (media, power). The uniqueness of the attack strategies lies in the employment of different versions of the same malware family to achieve different end results. The attacks in this paper are reportedly the first in the history of power-sector related cyber-physical attacks. It is important to note that the versatility of the BlackEnergy malware family enables it to be a persistent threat to the industries. The attacks were coordinated with much fewer resources and lesser sophistication than previous attacks on critical infrastructure by malware such as Stuxnet.

The report is organised as follows. Section 2 discusses concepts of cyber-physical systems. Criticial Infrastructures and Malware are considered in Sections 3 and 4 respectively. A comprehensive study of the BlackEnergy malware family is described in Section 5. Details about the Ukraine Power Sector Attacks are mentioned in Section 6. Finally, the current state of the security landscape is discussed in Section 7.

2 Cyber-Physical Systems

Cyber-Physical Systems (CPS) entail all possible systems which exist in the cyber Domain as well as the physical Domain. Examples include intelligent transportation systems, water treatment and distribution systems, automobiles, pacemakers and the power grid. CPS integrates computing, networking, and physical processes. The physical process is integrated, monitored and controlled by computers [17]. The intelligence programmed in the cyber domain decides the steps that the physical process should take given the state of the system. This enables automation, control and quality assurance of processes which would otherwise require humans in the loop. Thus, cybersecurity becomes increasingly important in the case of CPS as all critical infrastructures are built on this model. The security of CPS depends on more factors than conventional networked cyber systems. A secure CPS has at least the following features:

- Confidentiality
- Integrity
- Availability
- Authenticity

Thus, it suffices to say that an insecure cyber system is also a vulnerable CPS. The risk is not limited to data and services but includes physical and biological risks to the people who are affected by the CPS. Since the physical process can be attacked physically by adversaries, defence mechanisms need to take physical security into consideration as well. Components of CPS are referred in Table 1. The vulnerable points of entry of attack are identified in Figure 2. CPS technology is increasingly being utilised as the model for designing and engineering public critical infrastructures of nations.

3 Critical Infrastructure

CPS is increasingly being utilised for designing and engineering Critical Infrastructures. Critical Infrastructure [23] is a set of commonly accessible services that fulfills the basic needs of a nation's society and economy. Every country has certain services that fall under the Critical National Infrastructure. ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) [30] has defined 16 sectors as critical infrastructures as shown in Table 2.

3.1 Threats to Public Infrastructure

Due to distributed design, increased network connectivity and technology readiness, contemporary critical infrastructures face the following threats:

- **Cyber Attacks** - An attack purely in the cyber domain, in which one of confidentiality, integrity, availability is compromised
- **CPS Attacks** - An attack in the cyber domain with consequences in the physical domain, e.g., unauthorised actuation, espionage, delayed actuation
- **Physical Attacks** - An attack purely in the physical domain, e.g., drilling a hole in a water tank
- **Physical-Cyber Attacks** - An attack in the physical domain with consequences in the cyber domain, e.g., pulling out wires connecting to the historian server

These attacks may not be mutually exclusive; the overlap between these domains is represented in Figure 1.

Note that even further specialised types of attack such as cyber-physical-cyber can be carried out by a determined adversary. However, the impact of the malware on CPS domains is the primary focus of this report.

3.2 Points of Attack

The points of attack for a generic CPS are represented in Figure 2. For a specific CPS, the descriptions are presented in Table 1.

Table 1: *Examples of CPS.*

CPS Systems	Sensors/ Actuators	Control Devices	Utility Devices
Water Treatment SCADA System	Level sensor, Pumps, Flow sensor	PLCs	SCADA workstation, Historian server
Pacemaker	Pulse monitor, Pulse amplifier	Timing controller	Mobile application, Pulse logger
Automobile	Odometer / Throttle	ECUs using CAN Bus, i2c, FlexRay	Dashboard computer, Mobile application

Table 2: *Critical Infrastructures defined by ICS-CERT.*

Energy	Water	Chemical	Finance
Food and Agriculture	Communications	Commerce	Government
Nuclear	Defence	Manufacturing	Dams
Transportation	Information Technology	Emergency Services	Healthcare

4 Malware

Malware is a portmanteau for *mal*icious soft*ware*, and refers to all the practices that are meant to cause harm to the normal operations of a cyber-system. Malware can be classed as a source of cyber-physical attacks when used against a CPS.

4.1 Types of Malware

The most common types of malware are listed below:

- **Rootkit** - Programmes which utilise privilege escalation to grant stealth / anti-forensics capabilities to other malware. Rootkits are not malicious in isolation but are used to subvert the perceived impact of the actual damage caused by the CPS attack, thereby aiding in the persistence of the threat

- **Backdoor** - Backdoors are communication channels which are used by the attacker to penetrate the system even when the preferred channels are shut down, adding persistence and redundancy to a CPS Attack. Backdoors typically make use of vulnerabilities on the host system such as open ports. They can also be created by another malware once the dropper is successful in its attack delivery. Backdoors are the medium through which Command-and-Control (C&C) servers remotely monitor and control the compromised system. Backdoors are typically used in *Supply Chain Attacks* in which counterfeit hardware have physical backdoors to allow for future command and control

- **Worm** - A computer software written for self-replication without an external trigger and it spreads from machine to machine over the network until it reaches the desired host. Historically, worms have been identified for their notoriety in CPS Attacks - Stuxnet(centrifuges), Slammer(nuclear plant) and most recently BlackEnergy (power)

- **Botnet** - A malware strategy in which a set of compromised infected computer nodes act as unaware victims for a C&C Server. The bots can be then made for Distributed Denial of Service Attacks (DDoS), phishing email servers, Tor relays, etc. BlackEnergy began its foray as a botnet malware

- **Trojan** - A computer programme designed to be useful for the unsuspecting human user while at the same time affecting the confidentiality, integrity and availability of the target computer system. The direct impact to the host system is not relevant but a trojan can be used as a *dropping* technique to set up Backdoors and Rootkits

- **Virus** - Viruses are the most famous and the least implemented form of malware. Computer programmes which spread from device to device depending on certain human triggers. Viruses are host-specific, while the spreading mechanism is as device-agnostic as possible

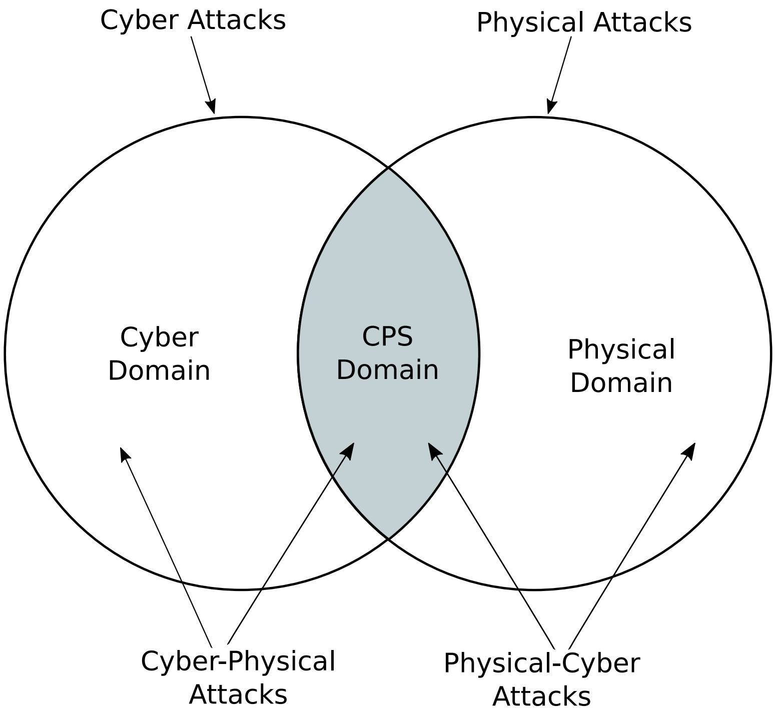

Figure 1: *The relationship between the origins of attacks and the consequential impact on different domains. CPS (CPS) Domain is the most vulnerable of all domains.*

4.2 Attack Strategies Used

Every CPS attack involving malware has an attack kill chain [29] associated with it. A successful CPS Malware Attack is carried out in the following sequence of steps:

- **Reconnaissance / Survey** - Capturing credentials of authorised personnel. This is done with a supporting malware which acts as a keylogger or can be accomplished through various phishing methods
- **Vulnerability Discovery** - Exploring loopholes in the compromised system
- **Intrusion / Dropping** - Obtaining access to the compromised system. This step is where the malware is introduced into the system
- **Installation** - The malware is installed and execution is initiated in the system
- **Persistence** - Maintaining access until the attack is complete. This is where the malware enables the adversaries to stay connected to the infected system
- **Delivery** - Executing the attack. This step is where the malware performs the attack
- **Cleanup** - Performing anti-forensics to eliminate attack traces

5 BlackEnergy

BlackEnergy is a malware family that first came to public view in 2007 as an HTTP-based botnet for DDoS attacks. Its current version allows for various plugins that affect system resources.

5.1 Infection Vectors and Targets

BlackEnergy has been reported to be delivered via the following payloads:

- Microsoft Word Documents (.doc, .docx), TeamViewer [9]
- Microsoft Powerpoint Slideshows (.pps files) [32]
- Infected Juniper Installer [32]
- Java Update Scams [32]
- Bogus Flash Player Installer [31]
- Compromised TeamViewer Installer [32]
- Bogus Microsoft System Executables (svchost.exe)
- Backdoor Files (aliide.sys, amdide.sys, acpimi.sys, adpu320.sys)
- Fake Integrated Drive Electronics Controller [27]

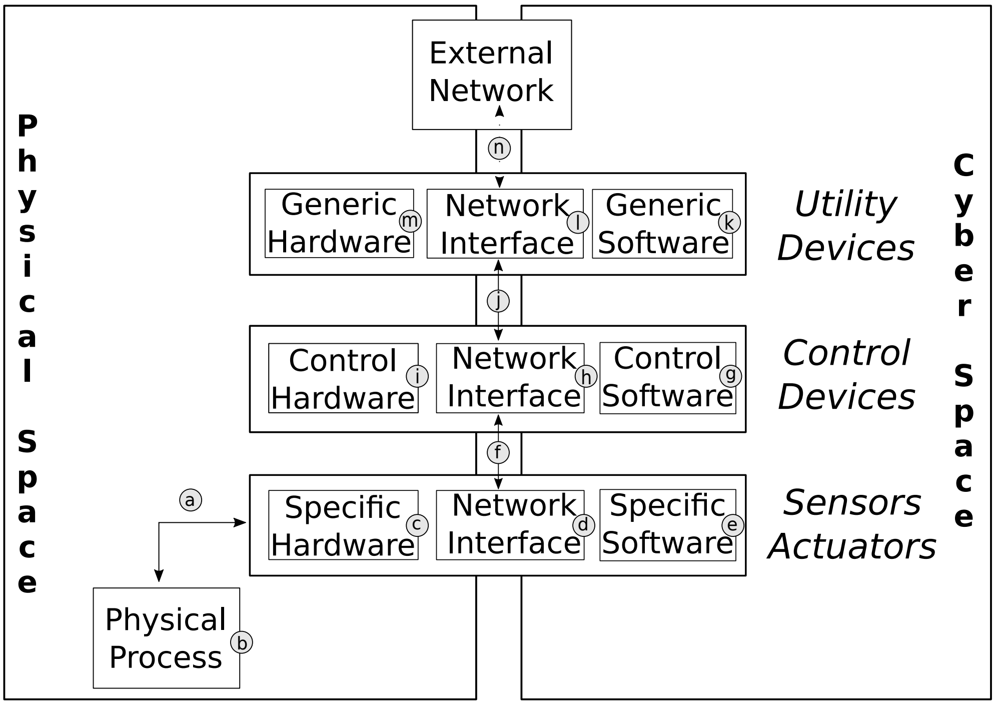

Figure 2: *Representation of a generic CPS system with components and points of attack.* a *: Physical-Cyber Attack,* b *: Physical Attack,* c,i,m *: Supply-Chain Attack, Side-Channel Attack;* d,h,l *: Firmware Modification Attack;* f,j,n *: Network-based Attacks;* e,g,k *: Code Injection, Replay Attack*

- Fake CPU Drivers [27]

These files are placed in locations such as `Windows/System32/drivers` which require root privileges for execution. This prompts administrators to force execute the seemingly innocuous executables [27]. According to [3], all BlackEnergy3 malware used for targeted attacks infect the Human-Machine-Interface (HMI) workstations in ICS plant networks. The companies whose products have been targeted and used as infection vectors to deliver the BlackEnergy3 payload include [19] GE Cimplicity, Advantech/Broadwin WebAccess and Siemens WinCC.

Analysis by CyberX reveals that the CVE-2014-0751 vulnerability in GE CIMPLICITY software and Proficy [20] was utilised to upload shell code from remote locations to deliver the BlackEnergy payload. It also enabled adversaries to execute an infected *.cim* file (CIMPLICITY) on HMI workstations from the attacker's remote server. BlackEnergy utilised the SMB (Server Message Block) resource-sharing protocol (which is allowed in most firewall servers) to facilitate exfiltration of data even in firewall-protected networks. SMB enables network file-sharing services for smooth operation of the network. BlackEnergy used this to its advantage by spreading from an Internet-connected HMI to an isolated ICS-Network (shown in Figure 3).

5.2 Architecture

BlackEnergy has undergone several architectural design changes since its first iteration (version 1.0) [32]:

- Version 1.0 - Dropper, Driver/Rootkit, `MainDLL`
- Version 2.0 - Dropper, Driver, `MainDLL`, Downloadable Plugins
- Version 3.0 - Dropper, `MainDLL (rundll32.exe)`, Downloadable Plugins (BlackEnergy3 Lite)

The dropping mechanism of BlackEnergy is as follows:

1. The Dropper drops and loads the driver
2. Enumerates all drivers already installed in the system
3. Selects a disabled driver at random
4. Replaces it with a malicious driver and restarts
5. Self-signs to create a signature

6. Enables 'Test' mode in Boot menu
7. Blanks out indications of booting up in text mode
8. Bypasses UAC (authentication check) and gets highest privileges

BlackEnergy3 'Lite' has a different architecture as it has no driver component. It also supports a different build ID format from previous versions. The configuration files are stored as an encrypted x.509 cert file whereas the previous versions used xml files. The plugin interface for the *Lite* variant is different in that it uses pipes to communicate with the infected system. Unlike the *Big* variants, this has no dependencies on dll files.

BlackEnergy has a Remote Procedure Call (RPC) communications module [3] which is used as the interface between the C&C server and the infected host. The main *si* module and the other plugins use these extensively to facilitate data exfiltration. The four exposed RPC functions achieve the following functions:

- Get Command from Remote Server
- Send String to Remote Server
- Send Command Result to Remote Server
- Send File to Remote Server

It has been found that each BlackEnergy backdoor is carefully constructed for the event that it is designed for. The mode of operation of the malware is quite similar according to its reported activity in 2014 and 2015. The payload is delivered to the host months before the actual date of the event (sometimes more than six months before the event). The malware is mostly innocuous for the entire period, performing basic reconnaissance operations. At the desired date of attack, the malware starts delivering the payload and wipes off the disks. This has been witnessed in all the Ukraine attacks reported so far.

Reverse analysis of BlackEnergy3 [27] indicates that it is written in Visual C++ with over 309 functions and 140 variables that it analyzes. The payloads are written in the scripts that the vulnerable hosts support such as Visual Basic Advanced Macros for Microsoft Word, OLE loaders for Microsoft PowerPoint, shell scripts for GE CIMPLICITY. Reports state that such a level of sophistication makes BlackEnergy an *intelligent* malware.

5.3 Features

The *features* timeline from [26] summarises the growth of the malware. It is replicated here in Figure 3.

The original BlackEnergy malware uses Remote Procedure Calls via named pipes over the SMB (Server Message Block) protocol to facilitate exfiltration of data even in firewall-protected networks.

BlackEnergy2 had unique features which were not found in either previous or successive variants. In addition to the features mentioned in 5.4 such as Linux and Cisco Router support, it supported additional channels to connect to C&C servers using Google+ accounts. The plugins were consistent across different target architectures and used the same C&C IP addresses.

The C&C IP addresses are scattered throughout the globe and include Tor exit nodes correlated with suspicious malware activity [31].

BlackEnergy3 has various reconnaissance features [32], which are achieved with the following plugins:

1. **FS Plugin** - File operations (enumerate files, directories, upload, overwrite, delete, download, execute files

2. **SI Plugin for BlackEnergy Lite** - Different interface uses pipes for communication. Collects *systeminfo* output , Windows version, privileges, time and zone, proxy settings, installed applications, running processes

   The plugin can collect passwords from different applications (The Bat!, Rambler Broswer, Mozilla Thunderbird, Firefox, Seamonkey, Comodo IceDragon, Opera, Chrome, Chromium, Yandex, Sleipnir, Outlook. Internet Explorer, Application passwords in Microsoft Credential Store (remote desktop and Windows live messenger)

3. **VS Plugin - Network Discovery** - Enumerates connected network resources and attempts to obtain remote desktop credentials to connect to the infected host. Use psexec to gather system information from remote computers and launch executables on remote computers

4. **JN Plugin (introduces trojan-like capabilities)** - This plugin helps to fix header checksums and CRC32 in Nullsoft windows installers

Table 3: *Features for the BlackEnergy malware.*

Early 2007	v1.0 Source Code Released - DDoS tool.
Late 2007	Credential Stealer Added.
Early 2008	v1.8 Custom Implant Builder [7].
Early 2010	v2 surfaces (with Linux support, Windows plugins, encryption, rootkit) [5].
Late 2012	64-bit support added [16].
Early 2014	v2 - User Account Control Bypass On Windows (msiexec.exe installer) [16].
Early 2014	v3 surfaces (regedt32.exe installer) [32].
Early 2014	BlackEnergy Lite surfaces[32].
Late 2015	v3 linked to KillDisk.

5. **Team Viewer Plugin** - Sets up an additional unattended password to create a backdoor

6. **DSTR Plugin (when a particular daytime is reached; enable self-destruction of system)** - The KillDisk component serves this purpose in the recent versions of BlackEnergy3

BlackEnergy3 is also reported to be location and time-aware [27]. When the malware sample was tested in different sandboxes around the world, one particular instance attempted to connect to a particular server in U.S.A at a certain timestamp. This hints that a version of the malware is being used against a specific target.

5.4 Versions

BlackEnergy has evolved significantly over the years as is evident from Table 3.

5.4.1 Version 1.0

Version 1.0 is the most documented version of the BlackEnergy malware [24] since the DDoS Bot Builder Tool was made publicly available on Russian forums. It enabled a user to set parameters for conducting a DDoS attack, thereby allowing anyone to launch attacks using a compromised botnet.

Version 1.8 [7] introduced an implant-building mechanism in which a payload could be encrypted and unpacked before transmitting to an infected host. The plugins were restricted to a DDoS plugin [6], a syn plugin (to trigger attacks), and a `http` plugin.

5.4.2 Version 2.0

BlackEnergy2 was a significant improvement over the previous versions [4]. The introduction of modular architecture made it possible to write plugins for the malware. To this end, several plugins began to surface which bolstered the malware family. The salient features of BlackEnergy version 2 are:

- Support for ARM and MIPS architectures
- Support for compromising Cisco Network devices
- Support for Linux and Windows Operating Systems

The difference in the coding styles of reverse-engineered malware samples suggests that there was a group of programmers behind the effort.

5.4.3 Version 3.0

BlackEnergy3 has been used in targeted attacks in Ukrainian industries so far. It specifically targets generic Microsoft Windows platforms and servers such as Active Directory Domain Controllers (servers which are responsible for authorisation requests and user management) and desktop workstations. Version 3 has been responsible for different attacks since 2014.

5.5 Attacks

The timeline of BlackEnergy based attacks is presented in Table 4.

5.6 KillDisk Component

BlackEnergy3 has a KillDisk component that has been thoroughly analysed by SOC Prime in its report [15]. Security experts noted that KillDisk did not feature explicitly in the BlackEnergy malware family in versions 1 and 2. KillDisk has been extensively used in the attack campaigns against Ukraine for wiping disks after reconnaissance efforts and clearing Master Boot Records to render systems unusable. This serves an important anti-forensics purpose in the BlackEnergy family by deleting the payload and the dropper after the attack is successful.

5.7 BlackEnergy in the Ukraine Attacks

The BlackEnergy malware family has targeted Ukraine-based media companies, power companies, railways, mining industry and airports.

5.7.1 Media Industry

Reports on attacks in the Ukrainian media industry started streaming in on October 25th, 2015 when computers in a media company were restarted and rendered unbootable. The malware has infected the computers long before the attack date through fake self-signed CPU drivers [27]. BlackEnergy circumvented detection by running in the 'Test Mode' which allows unsigned / self-signed drivers to be loaded on booting up the Microsoft Windows distribution [32]. The payload files were executable files (`ololo.exe` and `svchost.exe`). It suffices to note that the backdoor mechanism of BlackEnergy was established and on the day of the attack, BlackEnergy changed the malware process's start-up parameters from "Force Start" to "Auto-Start on Boot." The C&C servers orchestrated this process and therefore attacked several companies at the same time.

The malware code considered the context and the privilege level of the user onto which it was running. In order to gain administrator access, a non-admin process filled up the Temporary directory in Windows with 16 MB files until disk space reached a critical point when the process prompted for an Administrator User's intervention. Meanwhile, reconnaissance efforts happen in the background, scanning for more than two thousand types of files (media files).

Before the day of the attack, the malware set up tunnels and backdoors throughout the infected network, thereby ensuring persistence. It is important to note that it went undetected by Anti-Virus programmes throughout this period. After the attack was over, the malware filled the targeted files with zeros (e.g. shredded the disks) and issued a reboot command after formatting the Master Boot Records to prevent anti-forensics operations.

5.7.2 Power Industry

According to [14], the Prykarpatty power company was reported to have been attacked in early 2015. Later reports suggest that two more power companies were attacked, BlackEnergy played a significant role in facilitating the Ukraine Blackouts. Its specific role in the Ukraine 2015 Blackout Incident is analysed in a report by SOCPrime [14]. Unlike in the media industry, BlackEnergy played a more supporting role. It primarily facilitated the adversaries access into the operator's workstations and consequently the plant network. It also aided them in anti-forensics operations by removing the traces after the attack was completed. The direction of infection is represented in Figure 3. Domain Controllers are Microsoft Servers responsible for access control and authorisation of users on a network and respond to security authentication. BlackEnergy3 infected the Domain Controllers and rendered it unusable during the course of the attack, by disabling access to the workstations.

Event logs from [14] report the series of events that led to the entire CPS Kill Chain of BlackEnergy in the recent Ukraine attacks:

1. Deliver BlackEnergy malware using spear phishing emails with documents attached.

2. Microsoft Word uses VBA Macros to deliver payload whereas Microsoft PowerPoint uses OLE objects to load malware from a remote server

3. BlackEnergy performs reconnaisance (keylogging) and captures VPN credentials for Enterprise-network workstations

4. Connect to the VPN, access RDP and move laterally to enter the ICS Network while infecting as many hosts as possible

Table 4: *Attacks aided by BlackEnergy.*

2007	Distributed Denial of Service attacks [6].
2008	Network cyberattack against Dnipropetrovsk, Georgia [16].
2009	Attacks against Citibank [8].
2010	Used as Rootkit [13].
2014	Attacks against Ukraine Goverment [27].
2014	SandWorm group's HMI attacks [32].
2014	Cisco Routers attacked [4].
2015	Steel Mill attacked, Germany [12].
2015	Media Industry, Ukraine [10].
2015	Power Sector, Ukraine [25].
2016	Discovered in mining companies, railway industry, airports [22].

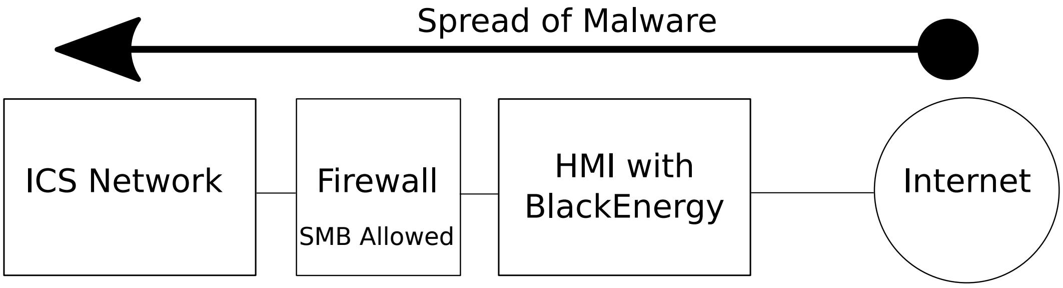

Figure 3: *Spread of BlackEnergy through an Industrial Control System.*

5. Establish RDP session to Domain Controllers. Exploit privilege escalation vulnerability in VirtualBox to bypass Driver Signature Enforcement

6. Control SCADA systems from the infected HMI

7. Enable KillDisk by `ololo.exe` to auto-start on boot

8. Modify the drivers for Serial-to-Ethernet devices to become unresponsive for remote maintenance

9. Install BlackEnergy drivers (`acpimi.sys`) on Domain Controllers

10. Perform reconnaissance to obtain any important files and authorisation files from Domain Controllers

11. Perform wipeout on Domain Controllers

12. Perform wipeout on Application Servers

13. Remove traces of malware and wipeout Master Boot Records

6 Ukraine Power Sector Attacks

The Ukraine blackout incident is the first recorded CPS attack on the power infrastructure of a city in a coordinated manner. It was a successfully executed attack in that it made use of several techniques and adhered to the CPS Attack Kill Chain.

6.1 Events Timeline

The attacks occurred on the afternoon of December 23, 2015 in the Kiev Power Distribution company in Ukraine. According to the official analysis, a total of 30 substations of different capacities (seven 110kV and twenty-three 35kV substations) were disconnected for *three hours* due to external intrusion into the SCADA network. Blackouts lasted for several hours in three distribution-level service territories in the Lavno-Fraknlvst regions of Ukraine.

6.2 Attack Workflow

There are several *Kill Chain* models available to depict Cyber Attacks such as Lockheed Martin's Cyber Kill Chain [11]. Since CPS Attacks on the Industrial Control System are different from conventional Cyber Attacks, the one used in this report is the *ICS Cyber Kill Chain* [29].

The first stage of the Kill Chain for the Ukraine Blackout looks like this:

- **Planning** - Reconnaissance
- **Preparation** - Weaponisation/Training
- **Cyber Intrusion** - Delivery, Exploit, Modification
- **Management** - Command and Control
- **Sustainment** - Act

According to open source intelligence sources, the attackers first gained access to the plant resources and initiated *reconnaissance* more than *six months* before the time of the attack. Reports by SOCPrime [14] corroborate this fact. The level of coordination and the wide range of hardware/software targeted is a certain indicator that the attackers had knowledge about the power distribution system and the infrastructure available. It was discovered that the Remote Terminal Unit models used by the power companies were available online with vendor and version details.

The next natural step was to **target** the organisations by **delivering** the malware payload. Spear Phishing was employed to send the documents via email in the hope that the infected documents would be downloaded into a computer inside the organisation's business network. Microsoft Excel and Microsoft Word documents were embedded with the BlackEnergy3 malware which was installed when the users enabled Office macros. This connected the BlackEnergy3 malware to the C&C IP addresses required for the next stages of the attack. BlackEnergy was also used as a keylogger to obtain credentials and exfiltrate the network details. It was discovered that with the help of the access provided by BlackEnergy3, privilege escalation and lateral movement through the network environment were enabled. The directory service infrastructure was targeted at this step. This enabled the attackers to enable authorisation for themselves so that the need for temporary C&C Servers was minimised. The authorisation enabled the adversaries to monitor all system usage and network traffic, thereby allowing access to the VPN system for the ICS network from the demilitarised business network.

This set up access channels to the SCADA workstations which consequently led the attackers to Stage 2 of the CPS Kill Chain. It was proven that the attackers performed an internal discovery in the ICS network and reconfigured the network connected to the Uninterrupted Power Supply to be affected by the blackout as well. This second stage of the Kill Chain has the following classifications:

- **Attack Development** - Develop
- **Validation** - Test
- **ICS Attack** - Deliver, Install/Modify, Execute

It was observed that at least one of the power companies used *Dropbear SSH* as the remote administration tool for the workstations. The attackers made use of this opportunity and set up a modified native version of Dropbear SSH server with a backdoor and password to remotely administer the workstations for attacks. Remote screen sharing enabled the attackers to understand the workings of the plant and the Data Management System environments (the SCADA software in place for automation of controls from the sensors and actuators level to the SCADA level.) The attackers were also able to modify the firmware for the serial-to-ethernet devices. The final act of modification was to gain total access to the operator workstations so that the legitimate operators were not able to access the systems.

The **attack execution** was initiated by opening the breakers by accessing the HMIs. The power outages were a direct consequence of the opening of breakers. According to reports, this caused an outage across 27 substations in 3 energy companies. Remote access to the operator workstations was disabled as a consequence of the firmware modification of serial-to-ethernet drivers of gateway devices. The coordination aspect of the attack was further bolstered by the telephoic denial-of-service attack to the power company's call centers. It was reported that the call centers received thousands of calls from the attackers to ensure disconnectedness between the customers and the company.

Finally, the UPS systems were disconnected from the network as configured and KillDisk performed wipe-outs on infected devices (workstations, servers, and on an HMI card inside of an RTU).

6.3 Impact on CPS

The most visible impact of the 2015 Ukraine attacks was the blackout in the Ivano-Frankivsk regions of Ukraine which affected approximately 225,000 households. The primary targets of the attack were Windows-based machines that were used in the plant network as HMIs and power administration. The power circuit breakers for the regional substations were affected directly by remote access to the HMI. The breakers were remotely opened in a number of affected substations. The SCADA system was remotely controlled by a remote user with *administrator* privileges. The UPS was configured to remain switched off even in the case of a power cut. In addition, the disks were wiped out with the use of malware which made it difficult to restore the physical state of the power system. The call center service was disrupted due to a telephonic denial-of-service effort by the attackers on the power company's call center. That further delayed the time it took to estimate the scope of the attack, in terms of affected regions and people.

It is clear that malware facilitated the first and last stages of the attack, e.g. preparation and execution. BlackEnergy3 and a modified Dropbear SSH server were used for C&C operations. The KillDisk component of BlackEnergy3 enabled the master boot record (MBR) wipeout which made it impossible for systems to be restored without manual intervention (using tools such as Testdisk).

6.4 Analysis

The following array of coordinated techniques were used to execute the attack:

- Spear Phishing
- Keylogging
- VPN Access
- Command and Control
- Remote HMI Workstation
- Cleaning Traces
- Firmware Modification of Communication Devices
- Disconnecting Uninterrupted Power Supply Systems
- Telephonic Denial-of-Service Attacks

The VPNs lacked two-factor authentication. The firewall configuration made it possible for the attackers to remotely control the environment by using a Dropbear SSH client that connected to the affected computers. There were no active network security monitoring tools in place, evident from the fact that the reconnaissance efforts were being undertaken for more than six months before the attack by a variety of external public IP addresses as well as the Tor network addresses.

According to the report by E-ISAC, the credibility rating of the malware-induced CPS attack is *5*, which confirmed that the Ukraine attacks were indeed CPS Attacks. This reasoning is based on the analysis of malware samples, direct interviews of the U.S. Government's DHS ICS-CERT with the staff who had first-hand experience of the event and the reports published by organisations who had access to the public, non-government data of the event.

Surprisingly, there was another attempt to recreate the blackouts in January 2016 using an open source backdoor known as *gcat* which uses GMail as the SMTP Command-and-Control Server [25].

6.5 Open-Source Knowledge

ICS-Alert ICS-ALERT-14-281-01 [19] covered the malware campaign of BlackEnergy against Industrial Control Systems. The exact details of the malware-induced attacks are still not available. The report by E-ISAC assigns a score of 4 which implies that there are *extensive details* available about the incident but the comprehensive details with supporting evidence are still lacking. This report bases its facts on open-source knowledge available on the Internet through several reports that are cited. The reports were released, building up on one another soon after the incident. The release of open-source information is represented in Table 5.

Table 5: *Events leading to open-source knowledge of the Ukraine Attacks.*

May '15	BlackEnergy3 disclosure report by CyberX.
Oct 29	ICS-CERT issues ICS-ALERT-14-281-01A hinting at BlackEnery being used against Industrial Control Systems.
Dec 23	Kiev Company Power Cut.
Jan 3	ESET Report establishing involvement of BlackEnergy and KillDisk.
Jan 7	iSIGHT report suggesting "Sandworm" Link and Dropbear SSH.
Jan 9	SANS-ICS report suggesting SCADA Attacks.
Jan 15	CERT-UA report discovering BlackEnergy Samples in Ukraine's Kiev Borispol Airport.
Jan 20	Another series of attacks using the open-source tool *gcat* as a backdoor.
Jan 28	Kaspersky Labs report malware similarity with Ukraine STB television attacks.
Feb 16	KillDisk component found in Ukraine's Mining and Railway Industries.
Feb 25	DHS ICS-CERT Issues Alert IR-ALERT-H-16-056-01.
Mar 16	Antiy Labs Comprehensive Analysis Report released.
Mar 18	SANS-ICS Defence Use Case Whitepaper released.

6.6 Significance

The Ukraine attacks were the first recorded event in the history of a wide-scale coordinated attack in the power sector. A wide range of CPS Attack techniques were employed to realise the blackouts. It shed light on the security flaws that exist in conventional Industrial Control Systems. The cost of executing the attacks was fairly low compared to coordinated malware-based attacks in the past (like Stuxnet). This attack did not use any known zero-day vulnerabilities but rather misused the legitimate features of the systems such as macros in Microsoft Office products to execute the attack. An alert was soon issued after the attack [19].

7 Current State of ICS Security

An increasing number of these physical services are administered and controlled by cyber-systems. This is due to the organic requirement of automation and maintainability. Since these computer systems in the cyber-domain have an impact on elements in the physical domain (real world), they are ideal examples of CPS. Having a CPS in place enables distributed and supervisory control to the physical elements. The number of cyber and physical elements increases the points of attack for an adversary, thereby amplifying the security threat on the the CPS in question. For instance, the elements of a CPS that are vulnerable to attacks can be well ascertained from Figure 2.

ICS-CERT issued 14 advisories and one alert in the first two months of 2016 alone. The incidents across other sectors far outweigh the threats faced in an industrial setting. Recent reports [18] suggest a rise in sector-wise attacks on critical infrastructures. As reliance on CPS increases, addressing safety and security concerns become more important than ever. Both safety and security are paramount concerns, the need for which is demonstrated by the recent attacks on several industries in Ukraine.

Five-year plans like the *The National Cyber Security Masterplan 2018* [28] are expected to increase system resilience by preventing attacks like BlackEnergy.

7.1 Defence Mechanisms

The recent attacks provide a fresh perspective on defence against malware-aided CPS Attacks. Defence mechanisms against these are provided in the Defence Use Case [2]:

- **YARA Signatures** [21] - It is important for the latest Indicators of Compromise to detect the presence of malware in workstations
- **Segmented Communication** - Spear Phishing and other forms of social engineering can be prevented if the workstations connected to the Internet are not connected to the plant network
- **User Account Analysis** - BlackEnergy exploited authentication controller servers and file sharing protocols that were allowed by default in firewalls. It is important to analyse the flow of information from the user accounts. Priority-based alarms for anomalous events allow early detection of malware attempting to move laterally through an organisation's network
- **Network Security Monitoring** - Active Monitoring enables anomaly detection in presence of backdoors / malwares utilising the internet. Monitoring should be implemented not just for the plant network devices but the enterprise network as well
- **VPN Access** - RDP ports should be closed for Internet connections and VPN connections should be limited to the enterprise network
- **Remote HMI Access** - HMI should not be made remotely accessible to non-plant networks. Application Whitelisting should enable only trusted processes to use remote connections
- **Hardware Security** - Firmware should be verified periodically and hardware attestation mechanisms must be set in place

7.2 Security by Design

It is imperative to have security as a design priority right in the *Design Thinking* stage of building a system. The iterative design process approach is described in recent work [1]. It considers the security problem from the view of the attacker and the possible attack scenarios.

8 Conclusion

Malware poses a significant threat to the CPS. Recent attacks on Ukraine facilitated by the BlackEnergy malware family support this claim. BlackEnergy is a popular malware family from recent years. The cyber-physical attacks attributed

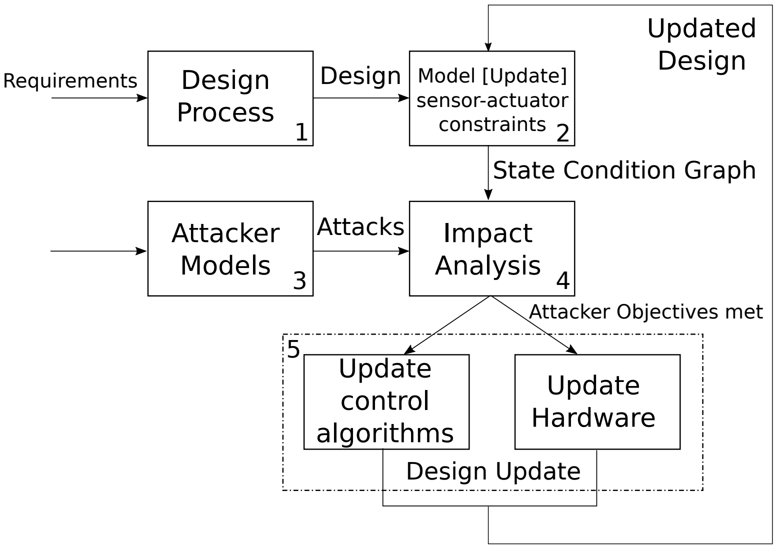

Figure 4: *An iterative design process to strengthen hardware and control algorithms to mitigate the effect of CPS attacks.*

to BlackEnergy are described in this report. Defence mechanisms to mitigate against a possible coordinated attack on cricial public infrastructures in the future are presented.

References

[1] Sridhar Adepu and Aditya Mathur. "CSD&M Asia 2016". In: Springer International Publishing. Chap. Introducing Cyber Security at the Design Stage of Public Infrastructures: A Procedure and Case Study.

[2] *Analysis of the Cyber Attack on the Ukrainian Power Grid.* SANS ICS. URL: `https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf` (visited on 03/20/2016).

[3] David Atch. "BlackEnergy 3 Exfiltration of Data in ICS Networks - Malware Report". In: *CyberX* (2015).

[4] *BE2 Custom Plugins, Router Abuse, and Target Profiles - Securelist.* URL: `https://securelist.com/blog/research/67353/be2-custom-plugins-router-abuse-and-target-profiles/` (visited on 02/29/2016).

[5] *BE2 extraordinary plugins, Siemens targeting, dev fails - Securelist.* URL: `https://securelist.com/blog/research/68838/be2-extraordinary-plugins-siemens-targeting-dev-fails/` (visited on 02/29/2016).

[6] *Black DDoS - Securelist.* URL: `https://securelist.com/blog/research/36309/black-ddos/` (visited on 02/29/2016).

[7] *Black Energy Bot v 1.8 Analysis.* Edisun Industries. URL: `http://edisunindustries.blogspot.sg/2012/02/black-energy-bot-v-18-analysis.html` (visited on 04/02/2016).

[8] *Black Energy Bot v 1.8 Analysis.* Antiy Labs. URL: `http://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/` (visited on 03/20/2016).

[9] *BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents - Securelist.* URL: `https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/` (visited on 02/29/2016).

[10] *BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry.* URL: `http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/` (visited on 02/29/2016).

[11] *Cyber Kill Chain.* Lockheed Martin. URL: `http://cyber.lockheedmartin.com/solutions/cyber-kill-chain` (visited on 03/20/2016).

[12] *Cyberattack on German Steel Plant Caused Significant Damage: Report.* SecurityWeek. URL: http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report (visited on 03/20/2016).

[13] *Dell SecureWorks Threat Report for 2012.* Dell SecureWorks. URL: https://www.secureworks.com/research/2012-threat-review (visited on 04/04/2016).

[14] *Dismantling BlackEnergy3.* SOC Prime. URL: https://socprime.com/en/blog/dismantling-blackenergy-part-3-all-aboard/ (visited on 03/23/2016).

[15] *Dismantling KillDisk - Reverse of BlackEnergy.* SOC Prime. URL: https://socprime.com/en/blog/dismantling-killdisk-reverse-of-the-blackenergy-destructive-component/ (visited on 03/23/2016).

[16] F-Secure. *BlackEnergy & Quedagh: The convergence of crimeware and APT attacks.* URL: https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf (visited on 02/29/2016).

[17] Helen Gill. "From vision to reality: Cyber-Physical Systems". In: *Presentation, HCSS National Workshop on New Research Directions for High Confidence Transportation CPS: Automotive, Aviation and Rail.* 2008.

[18] Dan Goodin. *First known hacker-caused power outage signals troubling escalation.* Ars Technica. Jan. 4, 2016. URL: http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/ (visited on 02/29/2016).

[19] ICS-CERT. *ICS-ALERT-14-281-01E - Ongoing Sophisticated Malware Campaign Compromising ICS.* 2014.

[20] ICS-CERT. *ICSA-14-023-01 - GE Proficy Vulnerabilities.* 2014.

[21] ICS-CERT. *YARA Signatures for BlackEnergy.* URL: https://ics-cert.us-cert.gov/sites/default/files/file_attach/ICS-ALERT-14-281-01E.yara (visited on 02/29/2016).

[22] *KillDisk and BlackEnergy Are Not Just Energy Sector Threats.* TrendMicro. URL: http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/ (visited on 03/29/2016).

[23] George Loukas. *Cyber-Physical Attacks: A Growing Invisible Threat.* Butterworth-Heinemann, 2015.

[24] Jose Nazario. "Blackenergy DDoS bot analysis". In: *Arbor Networks* (2007).

[25] *New wave of cyberattacks against Ukrainian power industry.* We Live Security. URL: http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/ (visited on 02/29/2016).

[26] Kyle OMeara et al. "Malware Capability Development Patterns Respond To Defenses: Two Case Studies". In: (2016).

[27] *Results Of Initial Investigation And Malware Reverse Analysis Of Fire Sale Ukraine.* SOC Prime. URL: https://socprime.com/en/blog/results-of-initial-investigation-and-malware-reverse-analysis-of-fire-sale-ukraine/ (visited on 04/08/2016).

[28] Infocomm Development Authority of Singapore. *National Cyber Security Masterplan 2018.* 2014. URL: https://www.ida.gov.sg/Programmes-Partnership/Store/National-Cyber-Security-Masterplan-2018.

[29] *The Industrial Control System Cyber Kill Chain.* SANS Institute. URL: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297 (visited on 03/20/2016).

[30] *The Industrial Control Systems Cyber Emergency Response Team.* ICS-CERT. URL: https://ics-cert.us-cert.gov/ (visited on 03/20/2016).

[31] *Threat Hunting Assisted by BlackEnergy.* SOC Prime. URL: https://socprime.com/en/blog/threat-hunting-assisted-by-blackenergy-mark/ (visited on 03/23/2016).

[32] *Virus Bulletin :: Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland.* URL: https://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland (visited on 02/29/2016).