# Summary Report of the paper: Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid

Okoye Emeka Elvis
*40274904*
Montreal, Canada
emeka.okoye@mail.concordia.ca

***Abstract*—This report provides a comprehensive analysis of the research paper on BlackEnergy Malware and its implications for Synchrophasor-based Real-time Control and Monitoring in Smart Grids. The study delves into the technical aspects of the reported malware, its operational mechanisms, and the potential threats it poses to the stability and security of smart grids. The findings of the summarized report contribute to the ongoing discourse on cybersecurity in the context of smart grid technology and offer insights into mitigating such sophisticated cyber threats.**

***Index Terms*—BlackEnergy, Denial of service, SmartGrid, Malware**

## I. INTRODUCTION AND EVOLUTION OF BLACK ENERGY

Black Energy, a notorious malware family, has undergone significant transformations since its inception around 2007. Initially, it was a simple Trojan used primarily for denial-of-service attacks. However, its evolution over time has been marked by increasing complexity and versatility. Around 2010, Black Energy experienced a complete code rewrite. This metamorphosis elevated it from a simple Trojan to a sophisticated, modular malware. The new architecture allowed for expanded functionality, enabling it to be used not only for denial-of-service attacks but also for bank fraud and spam.

Fast forward to 2014, Black Energy was still active and had found a new purpose: targeted attacks. This evolution led to the emergence of two main variants: the regular Black Energy and a newer version called Black Energy Light. The regular version included a driver component, while the Light version simplified the process by not using a driver at all. The driver component in Black Energy has also evolved over time. In the 2010 version, the driver contained rootkit functionality, which allowed it to hide elements on the system. By 2014, the driver in the regular Black Energy versions had shed its rootkit functionality and was used solely to inject the main DLL into system processes. The Light variant took a more standard approach, loading the DLL without the use of a driver. One of the key features of any malware is its dropper, which is responsible for dropping other components. In the case of Black Energy, the dropper drops and loads the driver by enumerating all drivers already installed in the system, selecting one at random, replacing it with its own malicious driver, and attempting to start it.

To bypass the security feature on 64-bit versions of Windows that requires drivers to have valid digital signatures, Black Energy modifies the system's configuration data to allow testing signatures. To stay under the radar and hide the resulting system notification, Black Energy patches the user32.dll.mui, part of the multilingual user interface. In its quest to remain undetected, Black Energy employs a variety of stealth techniques. It has the ability to blank out certain texts, making them invisible to the user. Furthermore, it ensures that the User Account Control (UAC) prompt does not appear by using a shim database that it carries with itself. This is achieved through the Microsoft Application Compatibility Toolkit. However, it's worth noting that Black Energy does not escalate privileges and needs to be running under an administrative account. Interestingly, despite not escalating privileges, Black

Identify applicable funding agency here. If none, delete this.

Energy does elevate to the highest possible privileges it can get. It achieves this using shims, which are the official way of achieving this task. This is a testament to the malware's adaptability and its ability to exploit official system features for malicious purposes.

## II. INTRODUCTION TO BLACK ENERGY LITE

At the beginning of the year, a significant modification of Black Energy was spotted. This variant, referred to as Black Energy Light or Mini, was characterized by the absence of a kernel mode driver, lesser support of plugins, and an overall lighter footprint. This was not a minor version update; the changes were very significant. The build IDs of the malware variants revealed a trend. The numbers for the regular Black Energy were essentially timestamps, indicating when the samples were built. Both the Black Energy Light variants and the regular variants were actively developed and used, sometimes even in tandem in attacks. An interesting difference between Black Energy Light and the regular Black Energy is how they store their configuration data. The regular Black Energy stores it in the form of XML files, whereas Black Energy Light stores it in an X509 certificate, a unique approach. It uses a crypto API to parse this configuration data.

There's also a different plugin interface and means of communication between the plugins and the main DLL. The plugins are not compatible between the different kinds of Black Energy variants. The Light version communicates all through a pipe, and its main DLL only has two export functions: make cache and start. In contrast, a plugin written for the regular Black Energy is dependent on imports from the main DLL and calls these functions directly, not using a pipe. An interesting hybrid case was found that contains features of both the regular Black Energy and the Mini version. It doesn't use a driver and contains some features attributed to the Light versions, but it contains the exports as in the regular version. The timestamp indicates that this hybrid was likely developed when the attackers were starting the development of these versions. Most of the plugins encountered while tracking the malware are for the regular Black Energy. However, it wouldn't be a problem for the attackers to reuse them for the Light versions if needed. The functionality in a number of these plugins overlaps, suggesting that many different third parties are writing these plugins

## III. BLACK ENERGY PLUGINS FOR EXPLOIT

The Black Energy plugins were designed for various malicious activities, including remote access, data theft, network discovery, parasitic infection, remote control software manipulation, and self-destructive actions. These plugins play a crucial role in facilitating the malware's capabilities and executing targeted cyber-attacks.

- File Stealing Plugin: The file stealing plugin is a crucial component of Black Energy, enabling attackers to remotely access and steal sensitive data from victim drives. Notably, attackers primarily target documents and private keys, highlighting their focus on valuable information.
- Site Login Plugin: This plugin is unique to Black Energy Lite and is used to gather system information, network-related data, and passwords from various applications, particularly browsers. It allows attackers to gain insights into the victim's system and access sensitive information.
- VS Plugin (Vulnerability Scanner): Designed for network discovery, this plugin enumerates resources connected to the network and attempts to obtain RDP credentials from the Microsoft credential store. Additionally, it utilizes PSExec to gather system information and execute commands on remote computers, making it challenging to remove the infection from an infected LAN.
- Parasitic Infection Plugin: This plugin is responsible for infecting executables, exhibiting typical viral behavior. It fixes checksums in the P header and CRC32 values in infected installers to avoid invalidating digital signatures. Notably, it deletes the TeamViewer plugin, creating an additional backdoor for remote access.
- TV Plugin (TeamViewer): This plugin checks for the presence of TeamViewer versions 6, 7, or 8, creating an additional backdoor for remote unattended access. It allows attackers to establish persistent access to compromised systems, enhancing their control over the infected environment.

- Destroy Plugin: Acting as a self-destruct mechanism, this embedded plugin executes destructive actions at a specified date and time. It rewrites files with random data, wipes the first 11 sectors of the system drive, deletes itself, and renders the system unbootable, causing significant disruption to the victim's environment.

## IV. BLACKENERGY CAMPAIGNS OR EXPLOIT OVER THE YEARS

In April, a document exploiting the CV-2014-1761 vulnerability in Microsoft Word was discovered. This exploit was also used in other targeted attacks involving different malware families, such as Dukes, Sednit, and others. The successful execution of the payload or shell code drops the Black Energy dropper and displays a decoy document to the victim. These decoy documents often contained controversial or diplomatic texts to lure victims into opening them. In one case, an executable file named "spiesok parole" (Ukrainian for password list) was found. Despite being an executable, it also contained an embedded decoy document and was disguised with a Word icon, leading many victims to open it. This file did contain a list of passwords.

In August 2014, an interesting case was noticed due to the exploit used and the actual email used to spread the malware. The email contained a controversial text, and the attachment contained a list of potential terrorist supporters that should be checked. Opening the attachment would eventually lead to the infection and installation of Black Energy Light. The PowerPoint package used in these attacks contains two embedded OLE objects, both of which contain a remote path to where the resource is located. This is a dangerous feature of PowerPoint that allows it to load these files. Microsoft addressed this issue over two years ago in MS-12005 and updated the object packager DLL, the module responsible for loading these. However, no warning is displayed at all for the PPSX PowerPoint slideshow files, even in Office PowerPoint versions 2007, 2010, 2013 with all the latest patches installed.

## V. HISTORY OF BLACK ENERGY

The BlackEnergy malware, first discovered by Arbor Networks in 2007, has evolved through three major variants, each more sophisticated and dangerous than the last.

The initial variant, BlackEnergy 1 (BE1), was a simple botnet based on the Hypertext Transfer Protocol (HTTP). Its primary function was to execute Denial of Service attacks on Synchrophasor-based systems. What set BE1 apart was its ability to evade antivirus software detection through the use of a runtime encrypter, which effectively concealed its malicious activities within the network. Additionally, BE1 could target multiple destination IP addresses per hostname, enabling it to attack all or most redundant IP addresses of a target, such as Google's load balancing IP addresses. Command and Control servers, predominantly located in Malaysia and Russia, utilized BE1 in the DDoS attack on Georgia during the Russian-Georgian war in 2008. This attack rendered 54 websites inaccessible, leading to misinformation due to the lack of legal communication channels between the government and its citizens.

In 2010, Secure Works' research team discovered a new variant, BlackEnergy 2 (BE2). This version was a complete rewrite of the original code, transforming the malware into a modular framework capable of loading attack-specific plugins. This new structure enabled BE2 to steal financial and authentication data from Russian banks. The malware used a variety of plugins to enhance its attacks. For instance, the DDoS plugin was used to disable the authentication server, preventing customers from detecting fraudulent activities in their accounts. A 'kill and destroy' plugin was also employed to erase the filesystem on compromised systems, eliminating any trace of the attacker's activities and rendering the system unusable by deleting core system files. Around the same time, ESET, a security research company, found that over 100 BlackEnergy victims were primarily located in Ukraine and Poland. In 2014, BE2 was used to disable a political website in Ukraine and to attack the NATO headquarters in Belgium.

The most recent variant, BlackEnergy 3 (BE3), was discovered in 2014 when it was used to attack three regional electric power distribution companies in Ukraine. BE3 had evolved into a more potent and deadly threat, using advanced modules for its attacks. It introduced a different protocol for communicating with its built-in plugins and had a feature that dropped the main DLL component into

user processes. This evolution of BlackEnergy malware underscores the escalating threat posed by such cyber weapons in our increasingly interconnected world.

## VI. COORDINATED (MULTI-STAGE) DDOS ATTACK ON SYNCHROPHASOR-BASED SYSTEM

The architecture of Synchrophasor-based Systems and their networks is designed to make them resilient against Denial of Service (DoS) attacks. This resilience is primarily due to the communication protocols used within the system. Local Area Network (LAN) is employed for internal or short-range communications, while Virtual Private Network (VPN) is used for long-distance or external communications. This setup significantly reduces the likelihood of botnets infiltrating the network via the public internet.

For a DoS attack to be effective, the attacker must first gain access to a system within the network infrastructure. The attacker can then move laterally within the network, compromising other systems and converting them into botnets. These botnets can then access the internal network and disrupt its operation, resulting in a denial of service. The process of executing an attack on the Synchrophasor-based System is illustrated in Fig 1.

The attack follows the stages of the cyber kill chain, which includes reconnaissance, weaponization, and malware injection into the network. The subsequent stage involves executing the injected malware and concealing it to avoid detection by antivirus software. The malware then establishes a connection with the command-and-control server, providing the attacker with necessary information. The attacker collects this information, sends instructions back to the server to be executed by the botnets or compromised systems within the infrastructure, and the compromised system then carries out a coordinated DDoS attack on the Synchrophasor Systems.

However, this type of attack has limitations based on the protocol used by the Synchrophasor-based System. The two protocols in question are the IEEE C37.118 protocol and the more recent IEC-61850-90-5 protocol. In the case of the IEEE C37.118 protocol, the effectiveness of a DDoS attack is limited. Although the botnets can flood the network with data messages, without knowledge of the PMU configuration or the language it uses, the botnets cannot generate correctly formulated data messages. For the IEC-61850-90-5 protocol, the botnets can flood the network with Sampled Value (SV) packets. However, if the attacker does not know the security policies and keying materials used in the communication between the PMUs and the control system, incorrectly generated packets will be immediately dropped by the control system and PMU upon arrival.

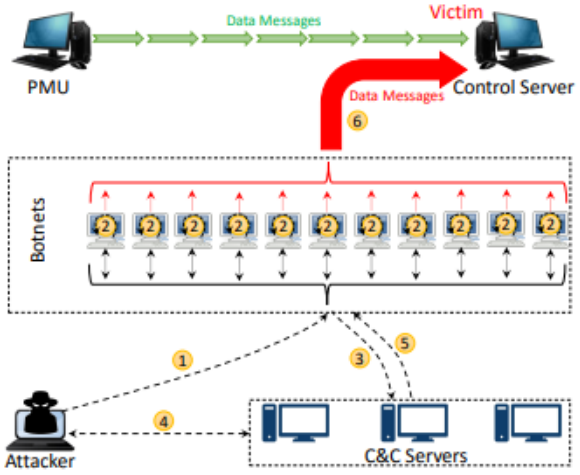



Fig. 1.
Coordinated DDoS Attack on IEEE C37.118 using BlackEnergy DDoS plugin.[1]

## VII. REPLAY/REFLECTION ATTACK ON SYNCHROPHASOR-BASED SYSTEM

A replay or reflection attack is a type of cyber threat where an attacker captures previously leaked, unauthenticated, or unencrypted data or information and reintroduces it into the network. This can disrupt the system's functionality or render it unavailable. In the context of Synchrophasor-based Systems, such an attack could lead to erroneous decisions by the control center due to the processing of outdated information. For example, if a Phasor Measurement Unit (PMU) is supposed to receive data instructing it to shut down some generators due to an excess of power in the grid network, an attacker within the network could send outdated but valid data to the PMU. Consequently, the PMU might do the opposite of the intended instruction and bring more generators online, disrupting the

power grid and potentially causing an outage in the affected area.

In the case of a replay attack on the IEEE C37.118 protocol, the attacker does not need to acquire any configuration data from PMUs. However, they would need to obtain the Second of Century (SOC) count, which must be altered by the attacker before sending or replaying the data to the control center.

On the other hand, for a replay attack on the IEC-61850-90-5 protocol, the attacker would need to have certain security credentials. This is necessary because the attacker would need to decrypt the previous communication between the PMU and the control center to update the Protocol Data Unit (PDU) number and other security information. If this update is not carried out, the Group Domain of Interpretation (GDOI) security in place would thwart the attack, as it performs validity and periodic checks on the information transmitted between the PMU and the control center.

## VIII. RECONNAISSANCE/EAVESDROPPING (MITM) ATTACK ON SYNCHROPHASOR-BASED SYSTEM

A successful Man-In-The-Middle (MITM) attack is characterized by an attacker's ability to modify packets exchanged between two parties, leading to a breach of integrity. Alternatively, the attacker may drop packets sent between the parties, resulting in a denial of service, or inject new packets into the communication, causing both a breach of integrity and potential disruption. In the context of Synchrophasor-based Systems, which carry real-time dynamics about power systems, an attacker eavesdropping on the communication could gain access to critical information. The BlackEnergy malware, equipped with multiple plugins, provides the necessary tools for executing such an attack.

The attack unfolds in stages, with the initial penetration into the infrastructure network resembling the phases of a coordinated DDoS attack. A spear-phishing attack is used for malware injection, and the command-and-control server facilitates communication between the attacker and the victim. To execute the eavesdropping attack, the victim receives commands from the attacker to scan the network for an internal server or a Human Machine Interface (HMI) device. The attacker can then use a BlackEnergy plugin to perform remote execution on the internal server or HMI device, opening a backdoor SSH port and enabling the attacker to monitor communications between the control center and the PMUs. If successful, the attacker can acquire PMU configurations for the IEEE C37.118 protocol and security credentials for the IEC-61850-90-5 protocol, paving the way for the next stage of the attack.

In this subsequent phase, having gained access to the infrastructure network, the attacker broadcasts gratuitous Address Resolution Protocol (ARP) messages within the local network. This updates the network router's internal cache, allowing the attacker to associate the PMU or gateway IP address with the attacker's Media Access Control (MAC) address, illustrated in Fig 2. If successful, the attacker can monitor all traffic between the PMUs and the control center. After successfully implementing this traffic diversion (ARP spoofing) attack, the attacker can proceed to the final phase of the attack, which is to execute a successful MITM attack.

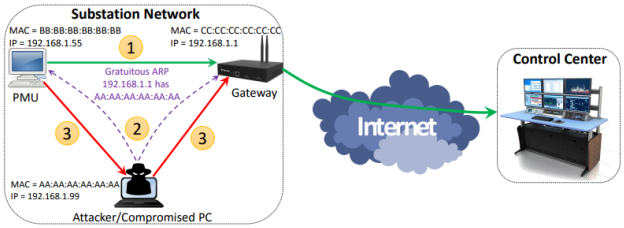



Fig. 2.
Traffic diversion based on ARP spoofing using during the network takeover phase. [1]

For the IEEE C37.118 protocol, the control system sends a common message requesting configuration data from the PMUs and simultaneously sends another request to initiate the transmission of this data. At this stage, the attacker, positioned in the middle of the communication, cannot decode Synchrophasor-based data messages without knowledge of the PMU configurations. Therefore, the attacker sends its own command messages to the PMU requesting configuration data. With this information, the attacker can decode Synchrophasor-based messages in transit and modify them. Simultaneously, the attacker can send command messages to the PMU to halt the transmission of

Synchrophasor-based data, enabling the attacker to generate its own data messages or configuration messages and send them to the respective party Fig 3.

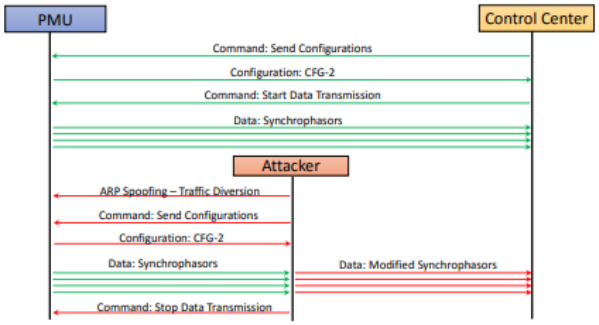



Fig. 3.
MITM attack: Hijacking of IEEE C37.118 communication. [1]

In the context of the IEC-61850-90-5 protocol, executing a Man-In-The-Middle (MITM) attack is considerably more challenging due to the robust security mechanisms in place. For this protocol, the Phasor Measurement Unit (PMU) and the control center must first obtain security policies and keying materials from the Key Distribution Center (KDC) via specific Group Domain of Interpretation (GDOI) exchanges. An attacker aiming to disrupt this communication and assume a MITM role would need to intercept both the GDOI exchanges and the IEC-61850-90-5 communications between the two parties. However, since both forms of communication are encrypted, the attacker is unable to decrypt or manipulate the data.

To successfully execute a MITM attack, an attacker would need to implement one of the following strategies:

- Compromise the PMUs and steal security credentials.
- Remain within the substation or infrastructure network and wait for a new or existing PMU to connect to the network and authenticate with the KDC.
- Given that the attacker is positioned between the KDC and PMU communication, they can intercept these messages and use the key generated between the PMU and KDC to decrypt further communications between the two parties.
- Once the above steps have been successfully executed, the attacker can then decrypt and manipulate IEC-61850-90-5 packets transmitted between the PMU and the control center.

The Fig 4 below highlights the complexity and sophistication required to launch a successful MITM attack on systems using the IEC-61850-90-5 protocol.

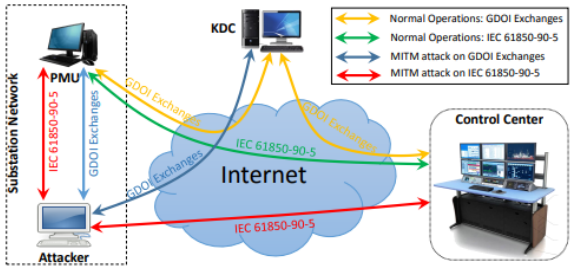



Fig. 4.
MITM attack: Hijacking of IEC 61850-90-5 communication. [1]

## IX. COMMENT ON THE ORIGINALITY'S AND/OR SIGNIFICANCE'S OF THE PAPER

Novel analysis of BlackEnergy malware: The paper investigates the evolution, features and capabilities of BlackEnergy, a sophisticated and modular malware that has been involved in several cyber-attacks on critical infrastructures, especially the power grid. The paper presents a basic cyber-attack model used by BlackEnergy and analyzes its threats for Synchrophasor based systems, which are used for real-time control and monitoring in smart grid.

Synchrophasor communication frameworks: The paper compares and contrasts two communication frameworks for Synchrophasor technology: IEEE C37.118 and IEC 61850-90-5. The paper highlights the strengths and weaknesses of both frameworks in terms of security, interoperability and performance. The paper also demonstrates how BlackEnergy can exploit the vulnerabilities in both frameworks to launch different types of cyber-attacks, such as reconnaissance, DDoS, MITM and replay attacks.

Attack scenarios and protection strategies: The paper presents several attack scenarios that illustrate how BlackEnergy can compromise, manipulate or disrupt Synchrophasor based systems and cause severe consequences for the power grid. The paper

also proposes possible protection and prevention strategies to mitigate the impact of BlackEnergy based cyber-attacks, such as encryption, authentication, firewall, VPN, anomaly detection and forensic analysis.

## X. COMMENT ON NOTABLE STRENGTH/WEAKNESS/APPLICABILITY OF THE PAPER

Strength: The paper provides a comprehensive analysis of the evolution, features and capabilities of BlackEnergy malware, which has been involved in several cyber-attacks on critical infrastructures. The paper also investigates the potential threats of BlackEnergy for Synchrophasor based systems, which are used for real-time monitoring and control of power grids. The paper presents several attack scenarios and possible protection strategies, which could help the development of cyber security solutions for Synchrophasor technology.

Weakness: The paper does not provide any experimental results or empirical evidence to support the proposed attack scenarios and protection strategies. The paper also does not address the impact of BlackEnergy on other smart grid components or applications, such as smart meters, distributed generation, demand response, etc. The paper could benefit from a more rigorous evaluation and validation of the proposed methods and techniques.

Applicability: The paper is relevant and timely for the research community and practitioners working on cyber security of smart grid and Synchrophasor technology. The paper raises awareness of the serious cyber threats posed by BlackEnergy malware and provides useful insights and recommendations for mitigating them. The paper could also inspire further research on developing more robust and resilient Synchrophasor based systems and applications.

## XI. CONCLUSION

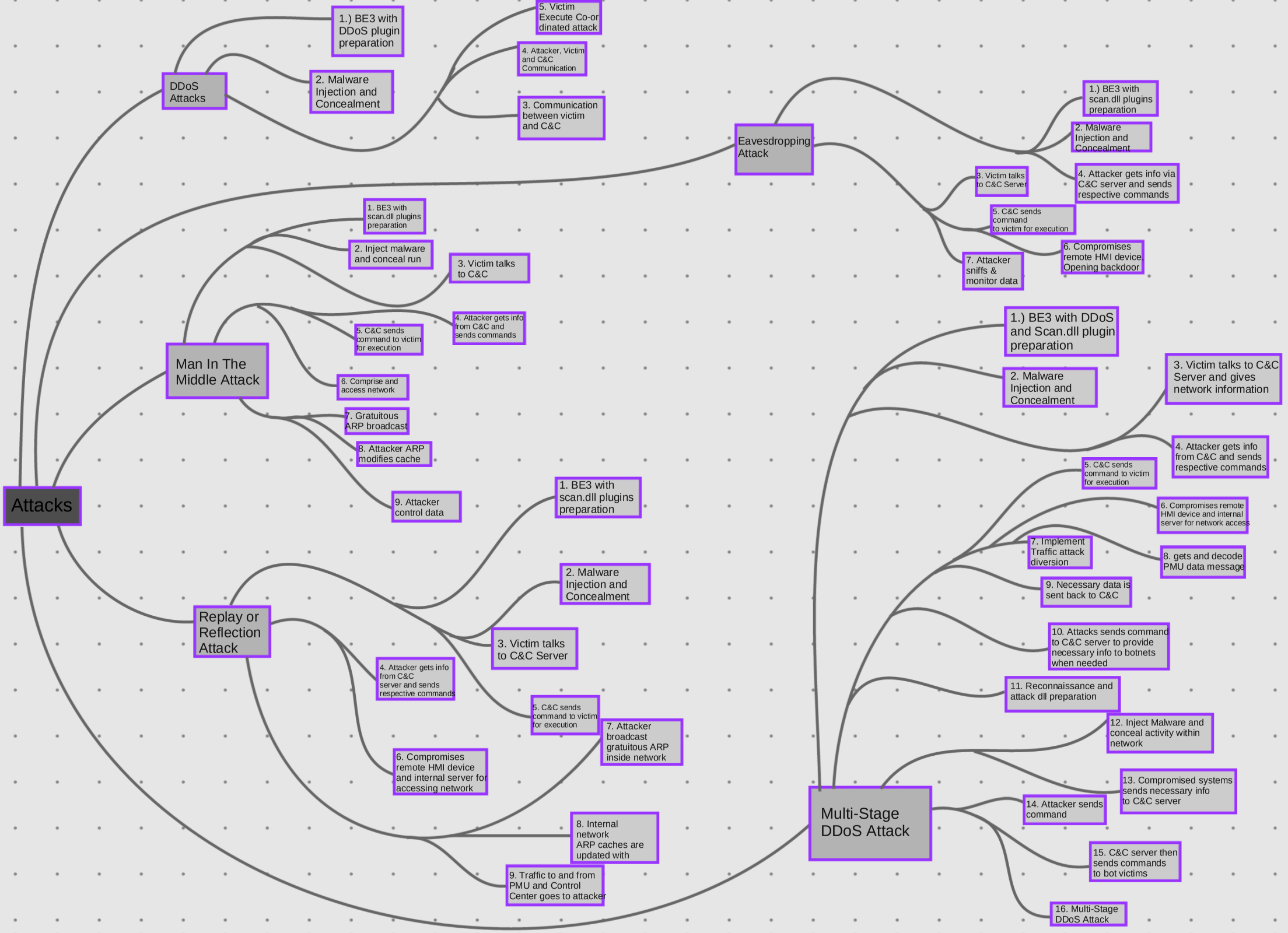
In conclusion, Black Energy represents a significant and evolving threat in the landscape of cybersecurity. Its inception as a simple Trojan used for denial-of-service attacks has given way to a sophisticated, modular malware capable of expanded functionality. The stealth techniques employed by Black Energy, such as blanking out certain texts, bypassing User Account Control prompts, and using shims for privilege elevation, highlight the complexity of its operation. Furthermore, the use of decoy documents and controversial texts in its campaigns demonstrates the psychological manipulation tactics employed by the attackers. The plugins used by Black Energy for exploitation, including those for stealing files, collecting system information, network discovery, infecting executables, and creating additional backdoors, illustrate the breadth of its capabilities. The existence of a self-destruct plugin further emphasizes the destructive potential of this malware.

The evolution of Black Energy, its stealth techniques, the emergence of a lighter variant, the changes in build IDs, and the various campaigns and exploits over the years all highlight the ongoing challenges in cybersecurity. The paper has explored various attack strategies, including Denial of Service, Man-In-The-Middle, and replay or reflection attacks, highlighting their complexities and the sophisticated techniques used by attackers. It has also examined the protective measures that can be implemented to guard against such threats, ranging from basic mechanisms like firewalls and antivirus software to more specific countermeasures such as IP address blacklisting or whitelisting, event monitoring and logging, and disabling remote monitoring of PMUs.

The fight against malware like Black Energy is a continuous one, requiring vigilance, continuous learning, and innovation in defense strategies. This case study report serves as a stark reminder of the adaptability of malware and the need for robust and evolving cybersecurity measures.

## REFERENCES

[1] R. Khan, P. Maynard, K. McLaughlin, D. Laverty and S. Sezer, "Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid," in 4th International Symposium for ICS and SCADA Cyber Security Research 2016, 2016, pp. 53-63, doi: 10.14236/ewic/ICS2016.7


Attacks
DDoS Attacks
1.) BE3 with DDoS plugin preparation
2. Malware Injection and Concealment
3. Communication between victim and C&C
4. Attacker, Victim and C&C Communication
5. Victim Execute Co-or dinated attack
Man In The Middle Attack
1. BE3 with scan.dll plugins preparation
2. Inject malware and conceal run
3. Victim talks to C&C
4. Attacker gets info from C&C and sends commands
5. C&C sends command to victim for execution
6. Comprise and access network
7. Gratuitous ARP broadcast
8. Attacker ARP modifies cache
9. Attacker control data
Replay or Reflection Attack
1. BE3 with scan.dll plugins preparation
2. Malware Injection and Concealment
3. Victim talks to C&C Server
4. Attacker gets info from C&C server and sends respective commands
5. C&C sends command to victim for execution
6. Compromises remote HMI device and internal server for accessing network
7. Attacker broadcast gratuitous ARP inside network
8. Internal network ARP caches are updated with
9. Traffic to and from PMU and Control Center goes to attacker
Eavesdropping Attack
1.) BE3 with scan.dll plugins preparation
2. Malware Injection and Concealment
3. Victim talks to C&C Server
4. Attacker gets info via C&C server and sends respective commands
5. C&C sends command to victim for execution
6. Compromises remote HMI device, Opening backdoor
7. Attacker sniffs & monitor data
Multi-Stage DDoS Attack
1.) BE3 with DDoS and Scan.dll plugin preparation
2. Malware Injection and Concealment
3. Victim talks to C&C Server and gives network information
4. Attacker gets info from C&C and sends respective commands
5. C&C sends command to victim for execution
6. Compromises remote HMI device and internal server for network access
7. Implement Traffic attack diversion
8. gets and decode PMU data message
9. Necessary data is sent back to C&C
10. Attacks sends command to C&C server to provide necessary info to botnets when needed
11. Reconnaissance and attack dll preparation
12. Inject Malware and conceal activity within network
13. Compromised systems sends necessary info to C&C server
14. Attacker sends command
15. C&C server then sends commands to bot victims
16. Multi-Stage DDoS Attack