CIO PMA

Student ID or IDs for group work	2126529
Words	3061

Date set	28/04/2023
Submission date (excluding extensions)	30/05/2023 by 12:00pm (UK Time)
Submission guidance	To be submitted electronically as a single PDF document in Tabula
Late submission policy	If work is submitted late, penalties will be applied at the rate of 5 marks per University working day after the due date, up to a maximum of 10 working days late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). “Late” means after the submission deadline time as well as the date – work submitted after the given time even on the same day is counted as 1 day late. For Postgraduate students only, who started their current course before 1 August 2019, the daily penalty is 3 marks rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

Module title & code	Cyber Intelligence and Operations WM090-15
Module owner	Sandy Taramonli
Module tutor	Sandy Taramonli, Sarah Aktaa
Assessment type	Coursework
Weighting of mark	100%

Table of Contents

1. Executive Summary

This section offers readers a succinct overview of the report's purpose and discoveries.

1.1 Scope of the Study

The study delves into the background, attack strategies, and repercussions of cyberattacks occurring throughout the Russian-Ukrainian conflict, with particular emphasis on those targeting Ukraine's infrastructure. We present a timeline of cyberattacks on Ukraine and a comprehensive analysis of the Industroyer2/CaddyWiper malware attack. By gaining insights into these cyberattacks, we equip ourselves to be prepared for potential future onslaughts.

1.2 Problems Need to be Addressed

In the face of the hazards ushered in by the cyberattacks of the Russian-Ukrainian conflict, we propose a stepwise approach to tackle the ensuing problems. Primarily, it is vital to acquire a thorough understanding of these cyberattacks, encapsulating their timing, the threat actors involved, the targeted entities, and their impact. Following this, an in-depth exploration of the information pertaining to the cyberattacks is required to discern how we can devise intricate countermeasures against them.

1.3 Assessment and Outline of Key Findings

We will utilise a timeline and the MITRE ATT&CK framework to evaluate the cyberattacks associated with the Russian-Ukrainian conflict. This encompasses the attack's timing, threat actor, victimised unit, its impact, the tactic employed, and a detailed description. The principal findings include: The majority of cyberattacks are carried out by hacker groups affiliated with the Russian Federation. Furthermore, DDoS attacks now constitute a significant chunk of all cyberattack incidents. As for the impact, the attackers primarily seek to either disrupt the services and operations of Ukrainian institutions or exfiltrate sensitive data (CyberPeace Institute, 2023).

1.4 Primary Conclusions and Recommendations

We have curated a list of practical and highly pertinent recommendations to combat the Industroyer2/CaddyWiper malware attack. These recommendations have been categorised under administrative and technical sections, inclusive of curtailing the duration of system audits, updating the incident response policy, implementing the separation of IT and OT, and stringent monitoring and restriction of remote access. These measures are designed to effectively stave off the network attacks emanating from the Russian-Ukrainian conflict.

2. Background

This section offers readers with an overview of the backdrop concerning cyberattacks launched against Ukrainian infrastructure.

2.1 The Evolution of the Situation Amidst (and Prior to) the Conflict

The low-intensity confrontation between Russia and Ukraine sparked off on 20th February 2014. It was only on the 24th of February 2022 that this low-intensity face-off escalated into a full-fledged armed conflict. Apart from Russia's military siege of Ukraine via land, sea, and air, cyber-information warfare has emerged as an integral part of the battlefield. Preceding the outbreak of the conflict, Ukraine had frequently experienced substantial DDoS attacks on their governmental websites and banking systems, thereby causing service disruptions. With the formal declaration of war, issues began surfacing in crucial infrastructure sectors such as water, electricity, and transport due to cyberattacks (Wikipedia, 2023).

2.2 Timeline of Comprehensive Cyber Attacks in Ukraine

We have integrated the number of cyber attacks from January 2022 to April 2023 into a comprehensive timeline showcasing the instances of intrusion, as shown in Table [1].

Table [1]. Timeline of Comprehensive Cyber Attacks in Ukraine (CyberPeace Institute, 2023)

2022	Jan.	Feb.	Mar.	Apr.	May	June	July	Aug.	Sep.	Oct.	Nov.	Dec.
Attacks	6	29	32	11	7	7	22	31	35	23	45	8
2023	Jan.		Feb.		Mar.		Apr.		Total			
Attacks	20		64		21		12		373			

2.3 Timeline of Key Cyber Attacks in Ukraine

We will provide a timeline outlining pivotal events within Ukraine's cyber-attacks. The details included encompass the event's date, the type of the attack, the threat actor, the victimised unit, the modus operandi, and the impact, as illustrated in Table [2].

Table [2]. Timeline of Key Cyber Attacks in Ukraine (CyberPeace Institute, 2023)

Date	Attack	Threat Actor	Victimised Unit	Modus Operandi	Impact
2022-01-13	HermeticWiper Malware Attack	Sandworm (Russian Federation)	IT company	Caused damage to computer or networked data	The operation of hundreds of computer systems was disrupted
2022-02-15	DDoS Attack	TBD (Russian Federation)	Government and Financial Organisations	Utilised an overwhelming amount of traffic to exceed the system's original capacity	Several websites went down but were recovered within a few hours

Date	Attack	Threat Actor	Victimised Unit	Modus Operandi	Impact
2022-02-24	AcidRain Malware Attack	TBD (Russian Federation)	ICT Company	Sabotaged the satellite internet's communication function	Nearly 10,000 satellite service providers lost internet connectivity, affecting around 10,000 users
2022-03-14	CaddyWiper Malware Attack	Sandworm (Russian Federation)	Government, Financial and Energy organisations	Damaged the system's AD server	Numerous systems experienced slowed down recovery processes
2022-04-08	Attempted Industroyer2 Malware Attack	Sandworm (Russian Federation)	Energy Organisation	The attack was detected and halted before it was deployed	If the attack had been successful, it would have left millions without electricity
2022-06-24	DarkCrystal Malware Attack	Sandworm (Russian Federation)	ICT Company	Took remote control of infected computers or systems	Several systems suffered data leaks
2022-08-16	DDoS Attack	People's CyberArmy (Russian Federation)	Energy Organisation	Employed an excessive amount of traffic to overload the system's original capacity	No harm was incurred
2022-11-08	Phishing Attack	Gamaredon (Russian Federation)	ICT Organisation	Disseminated malicious links and software via phishing emails	Data leakage was experienced in numerous systems
2023-02-23	Webshell with Malware Attack	DEV-0586 (Russian Federation)	Ukrainian Government Entities	Installed and executed malware through the webshell of the website, performed data collection and remote access operations	Resulted in the leakage and random alteration of data across various systems
2023-04-01	Phishing Attack	APT28 (Russian Federation)	Ukrainian Government Entities	Spread scripts via phishing emails	Data breaches occurred in multiple systems

2.4 Intelligence Brief

We will provide an intelligence brief on the cyber attacks Ukraine has suffered since the start of the Russian-Ukrainian war, divided into four parts:

Attack Incidents: There have been approximately 370 cyber attack incidents against Ukraine, with a significant fluctuation in the number of attacks (CyberPeace Institute, 2023). This variation in incident numbers could potentially be influenced by war strategies, attack methodologies, and stealth techniques.

Threat Actors: Threat actors involved in cyber attacks on Ukraine can be classified into state-sponsored actors, cybercriminals, and collective hacker organisations. As observed in Table [1], the majority of cyber attacks are launched by hacker groups affiliated with the Russian federation, including entities such as People's CyberArmy and Sandworm (CyberPeace Institute, 2023).

Attack Type: The types of cyber attacks on Ukraine include wipers, DDoS, cyberespionage, malware, phishing, financial fraud, and ransomware. Upon detailed examination, DDoS attacks account for two-thirds of total cyber attack incidents (CyberPeace Institute, 2023). This data suggests that the prevalence of DDoS might be due to its ease of execution, anonymity, and relative high levels of destruction.

Modus Operandi and Impact: The relationship between the modus operandi and impact of cyber attacks on Ukraine can be gleaned from Table [2]. In other words, a significant portion of the attackers' modus operandi involves disrupting services and operations of Ukrainian institutions or purloining sensitive data.

3. Industroyer2/CaddyWiper Malware Attack Analysis

This section offers readers an all-encompassing understanding of the Industroyer2/CaddyWiper malware attack that targeted Ukrainian infrastructure amid the Russian-Ukrainian War.

3.1 Background of the Malware Attack

Indeed, the precursor of the Industroyer2 malware, known as Industroyer, was already present as early as December 2016. During that period, an attack led to a substantial power outage that affected Ukrainian energy suppliers, serving as a crucial event in the annals of cybersecurity (Mandiant, 2022).

The Industroyer2/CaddyWiper malware attack was originally slated to be initiated on the 8th of April 2022 in the afternoon, with the infamous Russian entity, Sandworm, being the attacker. Industroyer2, like its forerunner, primarily targeted energy suppliers, but was more focused on distinct infrastructure communication configurations, granting it the benefit of considerable adaptability. Furthermore, the plan included the incorporation of CaddyWiper into the attack, which would make tracking it a more challenging task. Comfortingly, the attack was detected and halted before its deployment, hence no damage was inflicted upon Ukraine (MITRE, 2023).

From the above, it's apparent that the attackers have used this malware for two attacks, suggesting a high probability of further refinements for subsequent attacks. This is the reasoning behind our decision to technically analyse this particular attack, in the hope that it enables readers to gain a more profound comprehension of this malware.

3.2 Timeline of the Malware Attack

We will provide a timeline of the attack events so as to facilitate a better comprehension of the sequence of attacks among the readers, as shown in Table [3].

Table [3]. Timeline of Industroyer2/CaddyWiper Malware Attack (ESET, 2023)

Time	Description
2022-04-08 14:58 UTC	Attackers deploy CaddyWiper on energy provider's Windows systems.
2022-04-08 15:02 UTC	Attackers gear up to execute preliminary tasks for Industroyer2.
2022-04-08 16:10 UTC	Attackers strategise to initiate Industroyer2 on Windows systems, leading to power outages for energy suppliers.
2022-04-08 16:20 UTC	Attackers envision executing CaddyWiper on the Windows system, eliminating traces of Industroyer2 execution on the system.

As evident from the Table [3], it appears that the attacker planned to execute the assault in under two hours. However, following a thorough investigation, it is evident from the malware's compilation timestamp that the attacker meticulously planned this attack weeks in advance (ESET, 2023).

3.3 Glossary

We will provide a specific glossary to help deepen the understanding of Industroyer2/CaddyWiper attack techniques.

International Electrotechnical Commission 104 (IEC-104): The IEC-104 protocol is based on TCP/IP networks to achieve reliable data transmission. In addition, the IEC-104 protocol also defines the roles and communication processes between the TCP client and the remote station TCP server.

Application Service Data Unit (ASDU): In the IEC-104 protocol, it is a structured communication unit used to transmit different types of data, commands and control information in the IEC-104 protocol.

Information Object Addresses (IOA): IOA is a unique number or address used to identify specific data elements. It can correspond to equipment or components in the control system.

MBR (Master Boot Record): MBR is an old partition table format, and the partition table is located in the first sector of the hard disk, used to store information such as the boot program and the partition table.

GPT (GUID Partition Table): GPT is a new partition table format that was developed to overcome the limitations of the MBR format.

Active Directory Service Interface (ADSI): ADSI is an interface used to access and manage resources in Active Directory.

Group Policy Objects (GPO): Group Policy Objects are tools used to manage computer and user settings in a Microsoft Active Directory environment.

3.4 Attack Techniques of the Malware Attack

Industroyer2 is a malware targeting Windows systems, implementing the IEC-104 communication protocol, unlike its predecessor, Industroyer, which utilised multiple Industrial Control Systems (ICS) communication protocols. The IEC-104 protocol is used for communicating with ICS devices, enabling the malware to connect and monitor power equipment via TCP. Industroyer2 is capable of creating Application Service Data Units (ASDUs) and transmitting these customised ASDUs to the TCP server through the IEC-104 communication protocol from the TCP client. These ASDUs can alter the Information Object Addresses (IOA) status of the TCP server. A change in IOA status can potentially result in the interruption or failure of power equipment or components in the corresponding control system (Mandiant, 2022).

Further, CaddyWiper is employed to erase traces left by Industroyer2 on the Windows system, consequently prolonging the system recovery time. To be more specific, the attacker uses the enterprise's Active Directory Service Interfaces (ADSI) and Group Policy Objects (GPO) to deploy CaddyWiper. This is done to eliminate attack traces by wiping out disk contents of the C and D drives, among others. The malware also removes the system's Master Boot Record (MBR) and GUID Partition Table (GPT) partition tables, causing the system to fail to start properly (ESET, 2023).

3.5 MITRE ATT&CK Framework Analysis

We will utilise the MITRE ATT&CK Framework to thoroughly analyse Industroyer2/CaddyWiper. This analysis will incorporate both the Enterprise and Industrial Control Systems (ICS) frameworks, offering a comprehensive understanding of the attack's extent, as shown in Table [4][5].

Industroyer2:

Table [4]. MITRE ATT&CK Framework Analysis of Industroyer2 (Mandiant, 2022), (MITRE, 2023)

Domain	Tactic	ID	Name	Description
ICS	Discovery	T0888	Remote System Information Discovery	Industroyer2 is capable of establishing a connection with Windows systems using a TCP client, leveraging TCP to gather data. Through this process, crucial information such as the target IP address can be verified.
ICS	Collection	T0801	Monitor Process State	Due to Industroyer2's high configurability, it can connect to Windows systems via TCP and monitor the process state through specific commands. This action provides a more detailed understanding of the steps required for each target.
ICS	Collection	T0868	Detect Operation Mode	Because of Industroyer2's highly configurable characteristics, it can connect with Windows systems using TCP and control the operation mode via specific commands. Through this step, a more precise understanding of the actions required for each target can be ascertained.
ICS	Impair Process Control	T0836	Modify Parameter	Industroyer2 can manufacture ASDUs, which can alter the IOA status on the TCP server. A change in the IOA status could lead to disruptions or malfunctions in the corresponding control system's power equipment or components.

CaddyWiper:

Table [5]. MITRE ATT&CK Framework Analysis of CaddyWiper (ESET, 2023), (MITRE, 2022)

Domain	Tactic	ID	Name	Description
Enterprise	Discovery	T1082	System Information Discovery	The attacker accesses the Active Directory of the Windows system through ADSI, and acquires system information through controlling and managing the system via GPO. Through this step, the attacker can accurately identify the infected systems and better deploy CaddyWiper.
Enterprise	Discovery	T1083	File and Directory Discovery	The attacker accesses the Active Directory of the Windows system through ADSI, and acquires files and directories through controlling and managing the system via GPO. Through this step, the attacker can accurately identify the infected systems and better deploy CaddyWiper.
Enterprise	Privilege Escalation	T1222	File and Directory Permissions Modification	After deploying CaddyWiper on the system, the attacker elevates privileges to facilitate the subsequent elimination and destruction of data.
Enterprise	Impact	T1485	Data Destruction	After acquiring system information, files and directories, and elevated privileges of the Windows system, the attacker can damage files under the targeted directories and paths to better conceal their traces.
Enterprise	Impact	T1561.001	Disk Content Wipe	CaddyWiper can erase the contents of disks like the C and D drives in the Windows system. Through this step, the attacker can erase traces of the attack, increasing the difficulty of investigating this attack incident.
Enterprise	Impact	T1561.002	Disk Structure Wipe	CaddyWiper can erase the MBR and GPT of the Windows system, causing the system to fail to start smoothly. Through this step, the attacker slows down system recovery, increasing the complexity of the investigation.

3.6 Review of the Analysis

Upon our analysis of the Industroyer2/CaddyWiper malware attack, we have developed an understanding that international and complex issues such as the Russian-Ukrainian War can be approached differently by various authors, institutions, or publishers in their literature. The background, event timeline, attack methods, and the MITRE ATT&CK Framework presented herein are the product of our meticulous consideration regarding the timeliness, credibility, and diverse perspectives of the data, accompanied by our professional reflection using cybersecurity knowledge. This approach ensures the data we offer is accurate, unbiased, and upholds a high degree of professionalism.

4. Recommendations

This section offers a comprehensive list of practical and highly relevant suggestions to counter the Industroyer2/CaddyWiper malware attack. These recommendations provide an understanding of how to tackle the evolving threats identified in the preceding sections. For better comprehension and implementation, the suggestions have been categorised into administrative and technical sections.

4.1 Administrative Recommendations

Refresh the Cyber Security Department: During the ongoing Russian-Ukrainian conflict, refreshing the Cyber Security Department is crucial. This includes setting the objective to thwart Industroyer2/CaddyWiper malware attacks, bolstering the team in the network security department, and ensuring the protection of the organisation's operations and information systems.

Reduce System Audit Duration: Given the critical stage of the Russian-Ukrainian conflict, it's essential to lessen the duration taken for system audits, to promptly identify any unauthorised operations or potential vulnerabilities. For instance, early detection can prevent a potential Industroyer2/CaddyWiper malware attack (MITRE, 2023).

Revise the Incident Response Policy: In the case of a power system breach or equipment failure, it's crucial to update and review the Incident Response Policy. Furthermore, during this sensitive period, conducting Incident Response Policy drills more frequently can ensure seamless business recovery.

Re-evaluate Backup Policy: Review what data the organisation needs to back up, the method of backup, and the storage location. Increasing the frequency of backup tests will ensure vital data remains unaffected during a network attack.

Employee Training: Offer comprehensive training to employees about the Industroyer2/CaddyWiper malware attack. This includes providing a detailed overview of the attack background, methods, and MITRE ATT&CK framework analysis.

4.2 Technical Recommendations

Separate IT and OT: It's critical to segregate IT and OT for energy providers, including establishing different domains or virtual networks to prevent unauthorised remote access. Enhancing this with the application of firewalls, routers, and IDS/IPS will secure network traffic and communications.

Monitor and Restrict Remote Access: Implement restrictions and detailed monitoring of remote access for Windows systems. This includes utilising VPNs for secure remote connections, two-factor authentication, and the deployment of tools to closely monitor remote access behaviour.

Detect Abnormal Behaviour: Establish an effective system for detecting abnormal behaviour within Windows systems. This involves defining the scope of file access, network connection, and user login according to the organisation's operations. Furthermore, implement real-time surveillance and notifications to promptly alert the team when any suspicious activity is detected.

Strengthen Firewall Protection: Enhance the firewall rules for Windows system connections based on the specific requirements of the organisation, allowing connections exclusively from verified, trusted IP addresses.

Employ Hard Drive Encryption: Utilise hard drive encryption for Windows systems to add an extra layer of protection against unauthorised access or modification of drive data, including C, D drive, MBR, or GPT.

Regular Updates and Patches: Keep Windows systems and software updated and promptly patch known security vulnerabilities. Specifically, updates and patches should be prioritised for software that requires remote connectivity and system data access.

Reference:

CyberPeace (2023) Cyber Attacks in Times of Conflict | CyberPeace Institute. Available at: https://cyberconflicts.cyberpeaceinstitute.org/ (Accessed: 30 May 2023).

ESET (2023) Industroyer2: Industroyer Reloaded | WeLiveSecurity. Available at: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (Accessed: 30 May 2023).

MITRE (2022) CaddyWiper, Software S0693 | MITRE ATT&CK®. Available at: https://attack.mitre.org/software/S0693/ (Accessed: 30 May 2023).

MITRE (2023) Industroyer2, Software S1072 | MITRE ATT&CK®. Available at: https://attack.mitre.org/software/S1072/ (Accessed: 30 May 2023).

Mandiant (2022) INDUSTROYER.V2 : Old malware learns new tricks, Mandiant. Available at: https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks (Accessed: 30 May 2023).

Wikipedia (2023) Russo-Ukrainian War. Available at: https://en.wikipedia.org/wiki/Russo-Ukrainian_War (Accessed: 30 May 2023).