Destructive Malwares on MITRE ATT&CK Tactics for Cyber Warfare : A Brief Survey and Analysis

Seongmin Park[1*], Myeongsu Lee[2], Sarang Na[1] and Joonhyung Lim[1]
[1] Korea Internet & Security Agency, Republic of Korea
{smpark, no.1.nasa, lim}@kisa.or.kr
[2] AhnLab, Republic of Korea
myeongsu.lee@ahnlab.com

Abstract

Most types of malware are spy-on that seek to collect and steal sensitive information by infecting target systems. However, some malware, such as Stuxnet that was the alleged creation of a state-level sponsored attack in 2010, has been used for cyber warfare. Particularly, malware taking aim at an opposing nation does not just serve for espionage, but actually shuts up and sabotages an enemy's critical infrastructure, the real-world examples of which are Saudi Aramco hacking in 2012 and Ukraine's power outage in 2015. Critical infrastructure of a nation, which is vital as it provides crucial services, requires a set of robust security measures in place, but is often left lacking security in terms of equipment deployed, workforce and expertise. To protect critical infrastructure from malicious actors during times of conflict, there must be manpower capable of monitoring, analyzing and responding to internal and external threats, with consistent security posture against ever-changing cyber threats. As a means of ensuring staying cyber-secure, the MITRE ATT&CK framework is a best-practice tool to understand techniques and trends used in previous cyberattacks. This paper takes a look into the framework, to investigate and categorize what tactics and techniques have been used by key types of malware amidst cyber warfare.

Keywords: Destructive Malware, Cyber Warfare, MITRE ATT&CK, TTPs, Tactics

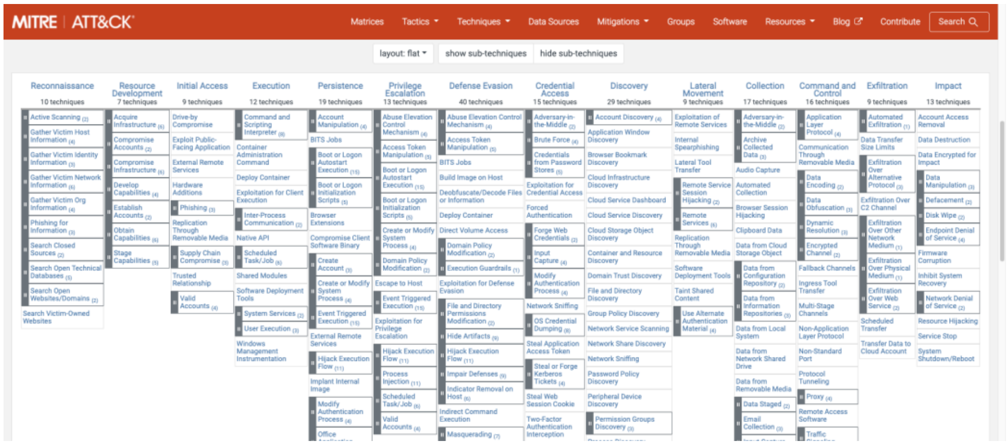
1 Introduction

Whereas the cyber-threat landscape continues to be sophisticated and advanced at a dizzying pace, traditional cybersecurity solutions often lend themselves to limitations. According to the latest statistics on the trend of cyber threats, damages incurred from cyberattacks costed the world approx. USD 3 trillion 968 billion in 2017, soaring up to approx. USD 6 trillion 939 billion in 2021. SANS, a US-based cybersecurity training and certification organization, reported that about 68% of cyberattacks in 2017 failed to be detected [1]. These served as a reminder of the need for continued vigilance, such as

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No. 66

[*] Corresponding author: Infrastructure Security Technology Team, Korea Internet & Security Agency, 9 Jinheung-gil, Najusi, Jeollanam-do, 58324, Republic of Korea, Tel: +82-61-820-1315

identifying ever-evolving malicious cyber activities and techniques. In this context, the ENISA established the cybersecurity threat landscape methodology, aiming to set a baseline for the sharing of thematic and sectorial cybersecurity threat landscapes. The methodological approach focuses on collaboration, starting with the collection of various inputs, performing analysis and interacting with key stakeholders to provide clear recommendations for the improvement of cybersecurity threat landscapes. This methodology involves two questions, to wit, (1) What is the scope of the threat landscape, and (2) What is the target audience and the aim. By answering these questions, elements belonging to the threat landscape could be identified. They will also support decision-making on how the threat landscape is analyzed and how strategic insight is inferred. On the other hand, a research institute MITRE, the US, has analyzed TTPs (Tactics, Techniques and Procedures) of malicious behaviors APT (Advanced Persistent Threat) groups have used in real-world cyberattacks, and developed a documented collection of information related thereto, called ATT&CK, which is a framework that classifies, and describes by attack attribution, potential TTPs various APT groups use [2]. As shown in Figure 1, the MITRE ATT&CK Framework consists of 14 tactics and 193 techniques.



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (6)	Hide Artifacts (9)	Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application		Impair Defenses (9)	Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Remote Access Software		
						Indicator Removal on Host (6)		Password Policy Discovery		Input Capture	Traffic Signaling		
						Indirect Command Execution		Peripheral Device Discovery					
						Masquerading (7)		Permission Groups Discovery (3)					
								Process Discovery					

Figure 1: MITRE ATT&CK Framework

Despite such outcomes, there has been no research done before on what tactics and techniques are used by attackers in cyber warfare. Given the situation like that, this paper analyzes key types of malware that are active in cyber warfare as well as the trend of techniques used to execute attacks.

2 Types of malware for cyber warfare

This Chapter looks into what types of malware have been used in the cyber warfare, and the characteristics each of them has. Cyber weapons, i.e. malware, to be noted one by one hereunder are selected based on whether the weapon of interest was used in a state level since 2009, a year provoking a wave of cyberattacks, whether it aimed to disrupt and destroy target systems, and whether it became the significant global issue. As a result, a total of 8 types of malware are selected, consisting of Trojan.Naid, Trojan.Hydraq, Stuxnet, Duqu, Shamoon, Mimikatz, WannaCry, and Gh0st RAT. But this paper classifies them into 7 in total, as both Trojan.Naid and Trojan.Hydraq were used in single cyber operation dubbed Operation Aurora.

2.1 Trojan.Naid, Trojan.Hydraq

Trojan.Naid and Trojan.Hydraq are Trojan hoses-type malware used by the Hidden Lynx group that was launched in 2009 to steal data from a range of corporate targets in the US such as Google, Microsoft and Adobe. This hacking gang has carried out espionage activities called “Operation Aurora”, using cutting-edge attack techniques at that time and a consistent methodology.

According to Symantec’s security response, Hidden Lynx attacks using Trojan.Naid bear the hallmarks of a campaign that involved yet another Microsoft Internet Explorer zero-day exploits in December, 2009. Trojan.Naid was used in the infamous attacks, Operation Aurora, on organizations in the financial, technology, Internet and media sectors. These attacks are linked with another Trojan called Trojan.Hydraq, which were used in stage two of the operation. Since then, Trojan.Hydraq along with Trojan.Naid was executed in stage three of the operation. Trojan.Hydraq disappeared from the targeted attack landscape after the Operation Aurora as key enterprises in the US strengthened their security attention against it. To the contrary, Trojan.Naid did not follow the same fate as it is still being used in sophisticated targeted attacks to this day [3].

2.2 Stuxnet Malware

Stuxnet is believed to have been developed in 2010 to destroy a uranium enrichment facility at Natanz, Iran. The malware achieved its goals successfully by causing physical damage to the Natanz facility, resulting in its centrifuge facility operation set back by up to four years. Stuxnet specifically targets PLCs (Programmable Logic Controllers) employed in industrial control systems. In particular, this malicious code functions by targeting the Microsoft Windows operating system that uses Siemens Step-7 software. Stuxnet malware destroyed an Iranian nuclear plant by manipulating PLC codes, causing the centrifuges to fast-spin at a speed outside limits to tear themselves apart. The attackers are believed to have designed Stuxnet to be air-gap bridged via portable flash drives. Once an infected USB stick was plugged into a Microsoft Windows operating system, Stuxnet automatically executed itself and dropped files onto the system by using zero-day vulnerabilities [4].

According to T. Chen et al., Stuxnet malware had three C2 servers, including a rootkit code designed to hide binaries on the infected Windows system. For development of such sophisticated exploit codes, a test bed fitted with all equipment associated with the target shall be accessible. Moreover, understanding of the Iranian nuclear facility is necessary along with experts for the installation, configuration and operation of special equipment. In particular, skilled developers and research personnel are essential for developing zero-day vulnerabilities applicable for the corresponding PLCs. Putting these in place could be made not possible without the government-level support [5]. Indeed, a malware sample dubbed as Stuxnet 0.5, which has been in existence from 2005, succeeded in part in damaging the centrifuges [6].

2.3 Duqu Malware

Duqu malware is extremely similar to Stuxnet malware [7]. Duqu is a modular malware platform as identical to Stuxnet malware, and uses a forged digital certificate to make it difficult to detect. Duqu’s primary purpose is to gather or exfiltrate sensitive data, rather than destroying the target. Duqu malware propagates itself using a crafted Microsoft Word document, and does not self-replicate. Upon successful installation, the attackers are able to continuously issue commands for a necessary period of time, thus manually infecting or attacking another system on the same network, using the compromised host. The malware uses the user designated protocol to communicate with its C2 server. This protocol, which is encrypted to evade detection by security products, is featured by using steganography that encodes data in a JPEG image file. This malware, although first discovered in September, 2011, could have been active as early as February, 2010 [8].

2.4 Shamoon Malware

Shamoon was malware designed to attack in 2012 Saudi Aramco which is the largest refinery in the world and Qatari RasGas which is the second largest producer of liquified natural gas in the world. It affected almost 300,000 of Aramco workstations, destroying hard disks of host computers on the operating network [9]. In the attack against Saudi Aramco, Shamoon wiped data by rewriting the hard drive MBR (Master Boot Records) of infected hosts, and the threat actor behind the Shamoon malware was able to selectively upload to the attacker or delete files stored in Aramco's corporate PCs [10].

Shamoon as a wiper malware targeted 32-bit NT kernel types of Microsoft Windows operating systems whereby files wiped out were replaced with a partial image of burning American flag [11].

2.5 Mimikatz

Mimikatz was initially developed in 2011 by Benjamin Delpy also known as gentilkiwi, which is an open source utility that turned out how protocols used for authentication of Microsoft Windows were at severe risk to cyberattacks. Attackers behind Mimikatz make use of the vulnerability on a MS Window system to access its hard disk. Modules provided by Mimikatz to gather MS Windows credentials on targeted systems include recapture of plain text passwords, LAN Manager, NTLM (New Technology LAN Manager), and Kerberos tickets including golden Kerberos ticket and silver Kerberos ticket [12].

During the 2016 cyberattack targeting Ukraine electric power network resulting in a 1-hour outage, the attackers used Mimikatz to capture legitimate credentials to disrupt the power stations. This tool can run on all versions of Windows from XP forward, except 8.1, 10 and 11, enabling the gathering of credential information from the Windows LSASS (Local Security Authority Subsystem Service) through its sekurlsa module which includes plain text passwords, Kerberos tickets and much more. Most security products will detect the presence of Mimikatz and delete it, but it is possible to go around that. Furthermore, Mimikatz can be executed locally from the command line and remotely, wherein mimikatz.exe and sekurlsa.dll are needed on the target system to run Mimikatz from the command line. However, this approach is not desirable in such a situation that it is required to use USB Rubber Ducky and bypass hard disk drive of the target. To run it remotely, one must first establish a connection to the servers, copy over sekurlsa.dll and run it [13].

2.6 WannaCry Ransomware

WannaCry ransomware, also known as Wanna DecryptOr, WCry, WannaCry, WannaCrypt, and WannaCryptOr, was observed during a massive attack across multiple countries on May 12, 2017 [14]. According to multiple reports from security vendors, the total of 300,000 systems in over 150 countries had been severely damaged. The attack affected a wide range of sectors, including healthcare, government, telecommunications and gas/oil production, the typical victims of which include NHS (National Health Service) of the UK, Telefonica that is a Spanish telecommunication company, and FedEx that is a North American provider of freight services.

The difficulty in protecting against WannaCry ransomware stems from its ability to spread to other systems by using a worm component. Along with this feature, the public-key cryptography-based encryption component of WannaCry makes the attacks more effective and requires defense mechanisms that can react quickly and in real time. WannaCry ransomware used by an attacker group called the Shadow Brokers uses the “Eternal-Blue” and “Double-Pulsar” exploits during the infection phase. With Eternal-Blue that exploits SMB (Server Message Block) vulnerability in MS Windows, the adversaries can execute a remote code on the infected systems by sending specially crafted messages to an SMB v1 server connected to TCP ports 139 and 445. This vulnerability affects all Microsoft Windows versions starting from Windows 8.1. Double-Pulsar is a persistent backdoor that may be used to access and execute code on previously compromised systems, thus allowing the attackers to install additional malware on the target system. In other words, during the malware distribution process, WannaCry’s worm component uses Eternal-Blue for initial infection through the SMB vulnerability, by actively probing appropriate TCP ports and, if successful, tries to implant the Double-Pulsar backdoor on the infected systems [15].

2.7 Gh0st RAT Malware

Gh0st RAT is a well-known Chinese remote control malware which was originally made by C. Rufus Security team. Just as with other well-featured “off-the-shelf” trojan viruses like Poison Ivy, Hupigon and DarkComet, it has often been used to compromise a targeted host computer which, if successfully infected, is changed to a state of zombie, giving the server/attacker the ability to execute various commands on the zombie’s computer [16].

Gh0st RAT is a most predominant malware used by APT groups, which has been out for around 10 years with diplomatic, political, economic or military agenda. This malware has a variety of capabilities and has been used usually by hacking groups in the Asia-Pacific region including China and North Korea [17].

In reality, the North Korean hacker group named Ryugyong-dong Team in Pyeongyang attacked in 2016 South Korean conglomerates like Korean Air Lines that is the state’s largest airline and four SK group affiliates, using gh0st RAT. The attacker group placed gh0st RAT malware through PC management systems within the targeted corporations, and stole over 42,000 documents, including classified files, such as photos of medium/high-altitude UAV parts, F15 fighter jets’ maintenance manuals and wing design blueprints military network materials, etc [18].

The fact of gh0st RAT’s source code being publicly available from e.g. Github, implies not only that it can be used to carry out illicit activities set by any actor to accomplish, but also that many flaws in design of the gh0st RAT toolset can be fixed and updated by anyone.

3 MITRE ATT&CK Tactics used in malwares for cyber warfare

Given that matrices for ICS are limited to Stuxnet malware, we perform the analysis narrowing down Enterprise Matrices. Furthermore, 3 tactics are excluded from the analysis, out of Enterprise Tactics available, since the tactics “Reconnaissance” and “Resource Development” on the mainframe series are preparatory techniques used by malicious actors before initiating the attack, and the tactic “Initial Access” needs to be performed before using malware.

Table 1 above shows the nuts and bolts of what and how many tactical techniques in light of MITRE ATT&CK have been observed in the wild use by type of malware each briefly described in Chapter 2. Main tactics/techniques used by malicious actors to exploit vulnerabilities are outlined in MITRE ATT&CK framework [19]. This Chapter dives into how respective MITRE tactics have been employed by destructive malwares.

Table 1: Number of MITRE ATT&CK Tactical techniques used in Destructive Malwares for Cyber warfare

MITRE Tactics	Trojan.Nid, Trojan.Hydraq	Stuxnet	Duqu	Shamoon	Mimi katz	Wann Cry	Gh0st RAT	Sum
Execution	2	3	0	1	0	1	4	11
Persistence	0	1	0	0	1	0	0	2
Privilege Escalation	3	6	4	5	2	1	2	23
Defense Evasion	5	11	3	5	1	2	6	33
Credential Access	0	0	1	0	11	0	1	13
Discovery	8	10	5	5	0	4	3	35
Lateral Movement	0	6	1	2	2	3	0	14
Collection	2	1	2	0	0	0	1	6
Command and Control	2	5	5	2	0	2	5	21
Exfiltration	1	1	0	0	0	0	0	2
Impact	0	0	0	4	0	3	0	7
Sum	23	44	21	24	17	16	22	167

3.1 Execution

“Execution” is a tactic that executes attack commands after gaining a foothold within a network through Initial Access. In particular, gh0st RAT malware has used 4 techniques (T1059, T1106, T1129, T1569) only in the phase of “Execution” of an attack, where it was able to open a remote shell to execute commands for data theft or load the DLL library into memory. Trojan.Hydraq created a backdoor through which remote attackers could load and call DLL functions. And, Stuxnet malware used WMI with an explorer.exe token to execute on a remote share.

3.2 Persistence

“Persistence” is a tactic that gives an attacker a persistent presence on the target through automatically executing program, task scheduler, malware configured to run in the background, account manipulation, etc. This tactic uses Mimikatz and Stuxnet only, out of 7 malwares. The Mimikatz credential dumper has been extended to include skeleton key domain controller authentication bypass functionality. The LSADUMP module the dumper created also manipulated the password hash of an account with the use of T1098 (Account Manipulation) technique. On the other hand, Stuxnet malware carried out the tactic by executing SQL code, using T1505 (SQL Stored Procedures) technique.

3.3 Privilege Escalation

“Privilege Escalation” is a tactic attackers use to acquire elevated rights to follow through on their objectives by bypassing user account control or taking advantage of security vulnerability. This tactic has been used in all types of malware investigated, mostly relying on techniques of T1543 (Create or Modify System Process: Windows Service) or T1053 (Scheduled Task/Job). With regard to T1543, Shamoon malware created a new service named “ntssrv”, “MaintenaceSrv" or “hdv_725x” to execute the attack payload. In addition, WannaCry ransomware creates a service named “msecsvc2.0”. With regard to T1053, Duqu malware was used to obtain legitimate credentials via keylogging or other means and infect the remote host by using the compromised credentials to schedule a task executing the malware.

3.4 Defense Evasion

“Defense Evasion” is a tactic to avoid detection by defense mechanisms like security debugger, or bypass the built-on detection mechanisms by creating obfuscation or cloud instances. This tactic has also been employed in all types of malware investigated, using very diverse techniques. While Duqu malware used T1055 (Process Injection), Gh0stRat and Stuxnet used a total of 11 techniques, mostly using T1070 (Indicator Removal). Trojan.Naid, Trojan.Hydraq and Shamoon malware used T1112 (Modify Registry) technique to enable the RemoteRegistry service for remote access. Moreover, Mimikatz performed credential dumping using T1555 (Credentials from Password Stores) to obtain account and password information useful in gaining access to targeted network resources.

3.5 Credential Access

“Credential Access” is a tactic used to steal passwords, sessions or tokens using phishing websites, network sniffing, etc. Almost all of techniques relying on this tactic (11 out of 13 in total) have been used to run Mimikatz on the victim machine. Mimikatz obtains account and password information for access to targeted network resources by using T1003 (OS Credential Dumping: Security Account Manager), and acquires information about credentials from the SAM (Security Account Manager) table. In addition, it can acquire credentials from the Windows Credential Manager, using T1555 (Windows Credential Manager), or create kerberos golden or silver tickets using T1558 (Steal or Forge Kerberos Tickets).

3.6 Discovery

“Discovery” is a tactic used to gain knowledge about the local/remote systems, accounts, applications and cloud services. This tactic has also been instilled in all types of malware investigated, except one (Mimikatz), where in the case of Stuxnet malware, a variety of 10 techniques were used. Discovery modules used together with Duqu malware enable adversaries to get a listing of network connections as well as detailed information about running processes on a system and valid accounts and privileges, using such techniques as T1049 (System Network Connections Discovery), T1057 (Process Discovery) and T1087 (Account Discovery), respectively. Gh0st RAT malware has the capability of performing process enumeration, while Trojan.Hydraq creates a backdoor through which remote attackers can retrieve system information, such as CPU speed, from registry keys. Meanwhile, Shamoon and Stuxnet malware families use T1082 (System Information Discovery) to fetch OS version, keyboard layout, etc. of the target system and transmit the information to a C2 server.

3.7 Lateral Movement

“Lateral Movement” is a tactic that transfers/installs remote access tools, such as malware and other files, to enter/control remote systems on a network. Malwares of Duqu, Shamoon and Stuxnet use T1021 (Remote Services). Duqu allows adversaries to obtain legitimate credentials via keylogging or other means and then infect the remote host using the compromised credentials. Shamoon copies an executable payload to the target system on a network share and uses a Scheduled Task/Job to execute the malware. WannaCry ransomware uses T1570 (Lateral Tool Transfer), attempting to copy itself to a remote host after gaining access privilege via an SMB exploit.

3.8 Collection

“Collection” is a tactic trying to gather data from target sources such as audio, video, screenshot, clipboard and email. Gh0st RAT and Trojan.Hydraq can capture the screen of an infected host remotely and stream live webcam feed by using T1113 (Screen Capture). In addition, Duqu and Stuxnet malwares use T1560 (Archive Collected Data: Archive via Custom Method) to XOR encrypt data of the target system.

3.9 Command and Control

“Command and Control” is a tactic trying to perform command and control through various communication channels, using encoding, encryption communication, etc. This tactic has also been employed in all types of malware investigated, except one (Mimikatz), using various techniques. In particular, most malwares can encrypt communication streams of command and control protocols transferred from C2 to the agent, using T1573 (Encrypted Channel). Trojan.Hydraq, Duqu and Stuxnet malwares use symmetric encryption algorithms while WannaCry ransomware uses asymmetric cryptography.

3.10 Exfiltration

“Exfiltration” is a tactic that steals data out of a target system through various communication channels. This tactic has been used only by Trojan.Hydraq and Stuxnet, out of 7 types of malware. First, Trojan.Hydraq connects to a predefined domain on port 443 using T1048 (Exfiltration Over Alternative Protocol) to exfil gathered information. On the other hand, Stuxnet malware uses T1041 (Exfiltration Over C2 Channel) to send compromised information to C2 servers via HTTP protocols.

3.11 Impact

"Impact" is a tactic actually mobilized to follow through on the adversary's end goal, such as manipulating, deleting or interrupting services and data, or demanding a ransom to be paid. This tactic has also been used in Shamoon malware and WannaCry ransomware only, out of 7 types of malware. Shamoon has been seen overwriting functions of disk structure such as wiping and rebooting MBR of a target system, using 4 techniques (T1485, T1486, T1529, T1561). WannaCry uses 3 techniques (T1486, T1489, T1490), and has a function of deleting and disabling operating system recovery features, in addition to a function of encrypting user files and demanding that a ransom be paid in Bitcoin to decrypt those files.

4 Conclusion

Gartner's 2021 report addressed that key goals of intelligent cyberattacks are to gain privileged credentials to follow through on the intent of cyber adversaries. In 2022, one year later, lots of high-profile organizations rushed to introduce ITDR (ID Threat Detection and Response) solutions that offer the analysis functions identical to those of EDR (Endpoint Detection and Response) tools, and further provide deep insights into corporate policies against identity-based threats and methodologies to restore any impacted services or capabilities [20]. On the flip side, advanced attackers actively target IAM (Identity and Access Management) systems. A typical instance is the SolarWinds hack where the adversary has gained the high-level administrative privileges and leveraged them to fully access a global admin account, or forged a valid SAML token for lateral movement, using the organization's SAML signing certificate. Moreover, they compromised an Active Directory Federation Server by injecting customized backdoor malware. Credential abuse has become a primary attack vector for identity systems, whereby as measures to respond thereto, organizations use the MITRE ATT&CK framework to incorporate ITDR technology into common attack scenarios. Despite the foregoing, ITDR does not take into account the response to cases where alternative techniques are employed other than those used to obtain credentials. Therefore, we need a security posture earnest to understand what tactics and techniques have been used by major attack groups, as well as their trends.

This paper explores what tactics and attack techniques have been made most of by classified types of malware mobilized in the cyber warfare. As demonstrated in Chapter 2, attacker groups, each formed as an organized team, often aim to bring about nation-level widespread damage. In this context, the MITRE ATT&CK framework would be a vital tool enabling one to simulate tactics and techniques used so far by major attacker groups into assets requiring protection therefrom, thereby drawing out methods to detect or mitigate threats/incidents. Future research is needed towards designing and validating a framework capable of creating attack scenarios by utilizing MITRE ATT&CK techniques.

Acknowledgments

This work was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korean government (MSIT) (RS-2023-00220303).

References

[1] Matt Bromiley, SANS 2022 ATT&CK and D3FEND Report, SANS, 2022

[2] MITRE, “Enterprise matrix.” [Online]. Available: https://attack.mitre.org/matrices/enterprise/

[3] Doherty S, Gegeny J, Spasojevic B, Baltazar J. Hidden lynx–professional hackers for hire. 17 Sep. 2013, [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf

[4] Lemos, R., Infoworld., 19 Jan. 2011, [Online]. Available: http://www.infoworld.com/t/alware/stuxnet-attack-more-effective-bombs-888

[5] Chen, T., Abu-Nimeh, S.: 2011. Lessons from Stuxnet. Computer 44, 4 Apr. 2011, pp. 91-93. http://dx.doi.org/10.1109/MC.2011.115

[6] Symantec, “Stuxnet 0.5: The missing link.”, 2013

[7] B. Bencsath, G. Pek, L. Buttyan, M. Felegyhazi, “Duqu: Analysis, detection, and lessons learned”, in Proc. of the 2nd ACM European Workshop on System Security, 2012

[8] Symantec, “W32.Duqu - The precursor to the next Stuxnet.", 2011

[9] S. Alshathry, “Cyber attack on saudi aramco,” International Journal of Management and Information Technology, vol.11, pp. 3037–3039, Dec. 2016

[10] C. Bronk and E. Tikk, “The cyber attack on saudi aramco,” Survival, vol. 55, no. 2, pp. 81-96, 2013

[11] N. Perlroth and C. Krauss, "A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try," The New York Times, vol. 15, 2018

[12] Lgu, S. Malik, E. A. Azeem, “The Secrets to MIMIKATZ - The Credential Dumper”, 2023

[13] Mimikatz, https://github.com/gentilkiwi/mimikatz.

[14] Symantec, "What you need to know about the WannaCry ransomware", Threat Intelligence, Oct. 2017, [Online]. Available: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

[15] Akbanov, M., Vassilakis, V. G., & Logothetis, M. D.,WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. Journal of Telecommunications and Information Technology, pp. 113–124, 2019

[16] Norman, A. S. A. "The many faces of Gh0st Rat.", 2012

[17] W. Grange, “Digital Vengeance: Exploiting the Most Notorious C&C Toolkits.”, Briefing presented at the Black Hat USA, Las Vegas, 27 Jul. 2017

[18] REUTERS, “North Korea mounts long-running hack of South Korea computers, says Seoul”, J. Kim, 13 Jun. 2016, https://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE

[19] MITRE, “Software.” [Online]. Available: https://attack.mitre.org/software/

[20] Gartner, “2023 Planning Guide for Identity and Access Management”, M. Ruddy, H. Farahmand, E. Wahlstrom, P. Rabinovich, D. Chase, N. Krishnan, G. Mudra, 10 Oct. 2022