CYBER THREAT INTELLIGENCE REPORT

AN OVERVIEW OF THE DOPPLEPAYMER RANSOMWARE

Image Courtesy: SOCPrime

Prepared by: Gaurav Manohar Suryawanshi (for Health Service Executive, Ireland)
as a part of CYBERSEC 510 coursework

Document Version Control

Version	Changelog summary	Reviewed by	Approved by	Comments
v1.0 (final)				
v0.1 (draft)	Uploaded the initial report for submission	Gaurav Suryawanshi (Self)	Gaurav Suryawanshi (Self)	Waiting for Prof. Art's feedback and comments before final presentation.

Table of Contents

Executive Summary 3
Increase of Threats and Attacks in the Healthcare Sector 3
Background and resemblance to the BitPaymer family 4
Overview & Analysis 5
Breaking down the technical analysis 6
Channeling the attack 6
Behavioral Patterns 7
Target audience for attacks 8
Recent Attacks & Operations carried out by DopplePaymer 8
Diving into DopplePaymer's intricacies 9
Tactics, Techniques and Procedures (TTPs) employed by DopplePaymer 9
Mapping of DopplePaymer's TTPs to the MITRE ATT&CK Framework 11
Indicators of Compromise (IOCs) leveraged by DopplePaymer 13
Conclusion 14
Inference from the Conti group's attack on HSE 14
Fortifying HSE against the DoppelPaymer threat actor 14
Effective recommendations & next steps for HSE 15
Cyber hygiene advised for HSE 16
Citations & References 16
Appendix 17

Executive Summary

Our cybersecurity landscape is evolving fast, and the healthcare industry has cropped up as one of the primary targets for cyber criminals, threat actors and adversaries. Quite recently, the Irish Health Service Executive (HSE) suffered along these lines when the notorious Conti Group attackers mounted a ransomware attack in 2021, crippling health services across the country. This report is intended to brief the HSE stakeholders on the nature of the current cyber threat landscape, with an emphasis on the transition from Conti to other major actors such as DoppelPaymer. We draw on lessons from past incidents and emerging threats to inform and refine HSE's cybersecurity posture as it may witness threats, while reducing the risk to the delivery of its essential healthcare services.

Conti, one of the notorious ransomware groups known for aggressive methods, conducted an attack on Ireland's Health Service Executive in May 2021. It brought about widespread disruption and exposed inner vulnerabilities related to health care information technology systems. The Conti cyber-attack was focused on data theft, encrypting vital systems, while the group asked for a hefty ransom since it kept the decryption keys along with all the compromised data.

Conti emerged in 2020 as a major ransomware player, with its fast-rising attacks on huge sectors that included health among others. The operations are under a RaaS model, and the group allows affiliates to carry out ransomware attacks, while core operators share profits. The attack on Ireland's Health Service Executive showed how Conti was able to cause massive disruptions through the encryption of systems and exfiltration of sensitive data.

With Conti on the decline, one of the more formidable threat actors is: DoppelPaymer. DoppelPaymer has been found to target health care, emergency services and education using state-of-the-art infiltration techniques and methods of extortion.

With Conti's activities having waned, DoppelPaymer has become one of the more active threats. Born from the BitPaymer ransomware family, DoppelPaymer has been attacking organizations with valuable data using advanced phishing campaigns and methods of network compromise since at least. It has been identified to use high ransom demands and threats of leaking data to strong-arm its victims into agreeing to its demands.

Thus, these threats and their methodologies vary such that their understanding will help a lot in preparing the defenses against such cyberattacks. This report analyses the impact DoppelPaymer has on the healthcare sector, the TTPs and IoCs while discussing the ways to enhance cybersecurity resilience for healthcare organizations such as HSE.

Increase of Threats and Attacks in the Healthcare Sector

The health sector has become a more and more attractive target for cybercriminals, and the frequency and sophistication of cyberattacks have been rising dramatically during recent years. The value of the information in this sector, critical business operations, and often poorly implemented cybersecurity measures form a vicious triangle driving this trend. Of all types of cyber threats, ransomware is probably the most prevalent type of cyberattack affecting healthcare providers.

Ransomware attacks have more than doubled from 2016 through 2021, with the PHI of close to 42 million patients being exposed. Normally, these attacks have involved the encryption of critical files and systems, thus holding them for ransom until such time as one pays. When this attack occurs, operational impacts may include downtime for electronic systems, canceled appointments and surgeries, and even diversions of ambulances. Disruptions even extended so far as to jeopardize patient safety and outcomes in many cases. HHS reported that there has been a 264 percent increase in the ransomware attacks on health providers in just the last five years. Due to its urgent need to restore access to critical systems and data, the providers, mostly the hospitals, are particularly vulnerable ones. Theft of PHI is a growing concern as this data can be used for identity theft besides conducting several other frauds.

Data breaches in the healthcare industry are both frequent and expensive: for instance, the average cost of data breaches in healthcare was about $10.10 million per incident. Large-scale data breaches have often come because of vulnerabilities within the IT system or due to human error, such as phishing attacks that have employees inadvertently giving credentials to the attackers. With so much complexity in healthcare IT networking, there are many potential attack vectors.

There have been numerous high-profile data breaches, affecting many millions of patients. For example, the Tricare data breach compromised the records of 5 million patients (about twice the population of Mississippi) through the theft of backup tapes. Other significant cyberattacks due to software vulnerability were obtained by cyber thieves against Community Health Systems, UCLA Health, and others.

One of the most pervasive ways in which health care systems are compromised is through phishing. An attack through opening malicious links or infected attachments grants them access to sensitive information, or it loads malware. Vulnerabilities in third-party vendors or supply chains with relationships to the health care organizations also provide an indirect entry point for an attack.

The attacker has moved from just being opportunistic to making use of advanced tools and techniques. Ransomware attacks have grown targeted and sophisticated, as attackers conduct reconnaissance to identify targets that are most vulnerable. The attackers then zero in on high-value systems and data. There is the case of double-extortion tactics where an attacker would threaten to release stolen data should the ransoms not get paid that have become common in ransomware attacks on healthcare.

Cyberattacks have much graver consequences for healthcare organizations than merely financial. Delays in medical procedures may occur, hospitalization may be prolonged, and even mortality rates may increase due to the disturbance in services. Other reputational damages could arise from the breach that could lead to distrust by the patients and may even extend to some legal ramifications.

Considering such threats, cybersecurity measures should be a priority of healthcare organizations. This involves the creation of solid security protocols: multi-factor authentication, periodic vulnerability testing, and an incident response plan. Training on phishing attempts and staying updated on the latest software to minimize vulnerabilities goes hand in hand.

The healthcare sector also needs to invest in easing their security infrastructure: consolidate security functions, centralize monitoring, and manage activities. The health sector organizations may be in a better position to safeguard against such continued threats by being aware of the threat landscape, which is evolving, and adapting their cybersecurity strategy accordingly.

This is in relation to the ever-increasing cyberattacks on the health sector, and thus there is an increased need to raise the cybersecurity bar. In as much as cyber attackers are constantly working on more effective methodologies, health organizations must be abreast of protecting sensitive data and critically essential functions.

Background and resemblance to the BitPaymer family

DoppelPaymer is believed to be from the BitPaymer ransomware that originally appeared in the year 2017, due to the code similarity it has along with ransom notes and payment portals. It should be important to note that differences still exist between DoppelPaymer and BitPaymer. For instance, DoppelPaymer uses encryption of 2048-bit RSA + 256-bit AES, whereas BitPaymer has used 4096-bit RSA + 256-bit AES, though it was 1024-bit RSA + 128-bit RC4 for the older version. DoppelPaymer also enhances the speeds at which BitPaymer can encrypt files through the use of threaded file encryption. Another difference between the two is the fact that DoppelPaymer requires the proper command-line parameter to run its malicious routines. Our experience with the samples shows different parameters for different samples. This might be one of the techniques attackers use to bypass sandbox analysis and make it difficult for security researchers to analyze the samples.

One of the distinguishing peculiarities of DoppelPaymer is the tool called Process Hacker, which it uses to kill services and processes of security, email server, backup, and database software to disrupt defenses and prevent access violation during encryption.

Like many ransomware families of recent times, DoppelPaymer's ransom demands for decrypting the file are high, ranging from US$25,000 to US$1.2 million. This is coupled with the fact that, since February 2020, the cybercriminals operating DoppelPaymer have been running a data leak site, where they publish files stolen from their victims as a threat, apart from demanding ransoms as a form of extortion by the ransomware.

Overview & Analysis

DoppelPaymer and BitPaymer are two ransomware strains that share a common origin but have evolved to exhibit distinct differences in their technical characteristics, encryption methods, and operational tactics. Both are linked to the Dridex malware family and are distributed by the INDRIK SPIDER cybercrime group. Here's a detailed comparison of the key differences between DoppelPaymer and BitPaymer.

Point of Comparison	**DopplePaymer**	**BitPaymer**
Encryption Techniques	Uses 2048-bit RSA and 256-bit AES for encryption.	Uses 4096-bit RSA and 256-bit AES in newer versions; older versions used 1024-bit RSA.
Encryption Speed and Efficiency	Utilizes threaded file encryption for rapid encryption across endpoints.	Encryption is less efficient without threaded file methods.
Execution Requirements	Requires specific command-line parameters for execution.	Does not require specific command-line parameters for execution.
Process Termination Techniques	Employs Process Hacker to terminate security-related processes.	Terminates processes but does not specifically use Process Hacker.
Data Exfiltration and Extortion Strategies	Introduced double extortion tactics by exfiltrating data and threatening to publish it.	Primarily focuses on encryption without double extortion tactics.
Historical Context and Evolution	Emerged in mid-2019 as an evolution from BitPaymer, focusing on enhancing efficiency.	Served as the predecessor to DoppelPaymer, sharing its codebase

DoppelPaymer ransomware has posed a complicated and aggressive cyber threat since its appearance in 2019. A modification of BitPaymer ransomware, this is part of the malware family Dridex spread by the INDRIK SPIDER cybercrime group. The following technical and behavioral analysis pointing to the sophistication of DoppelPaymer's attack patterns show the high impact of the attack due to its precise and effective execution.

Breaking down the technical analysis

The basis of DoppelPaymer is a strong encryption mechanism involving 2048-bit RSA and 256-bit AES algorithms. As such, without a key, files could hardly be decrypted. Most of the time, the ransomware reaches the target through phishing or spam emails that contain a malicious attachment or link. These phishing/spam emails contain JavaScript or VBScript code that downloads the DoppelPaymer loader once executed on the victim's machine. [1]

Once inside, DoppelPaymer starts a multi-stage infection process. Using the Emotet malware as a loader of sorts, it loads Dridex, which facilitates the deployment of DoppelPaymer. Dridex is involved in credential harvesting and lateral movement with tools like Mimikatz to dump passwords from system memory. The ransomware uses PowerShell Empire for Active Directory brute-forcing and PsExec for remote execution.

DoppelPaymer uses Process Hacker to kill processes and services that might interfere with the encryption of files. This ensures that security applications and vital applications are turned off before encryption. The DoppelPaymer ransomware also makes use of ADS to conceal the presence of their malicious executable files within NTFS file systems, which complicates the detection of this malware by most antivirus solutions.

Channeling the attack

DoppelPaymer leverages ProcessHacker, a legitimate tool, to terminate targeted processes on Windows systems. This is achieved by hijacking ProcessHacker's functionality through a series of sophisticated steps, allowing the ransomware to disable antivirus (AV) and endpoint detection and response (EDR) applications, even those protected by Protected Process Light (PPL). [3]

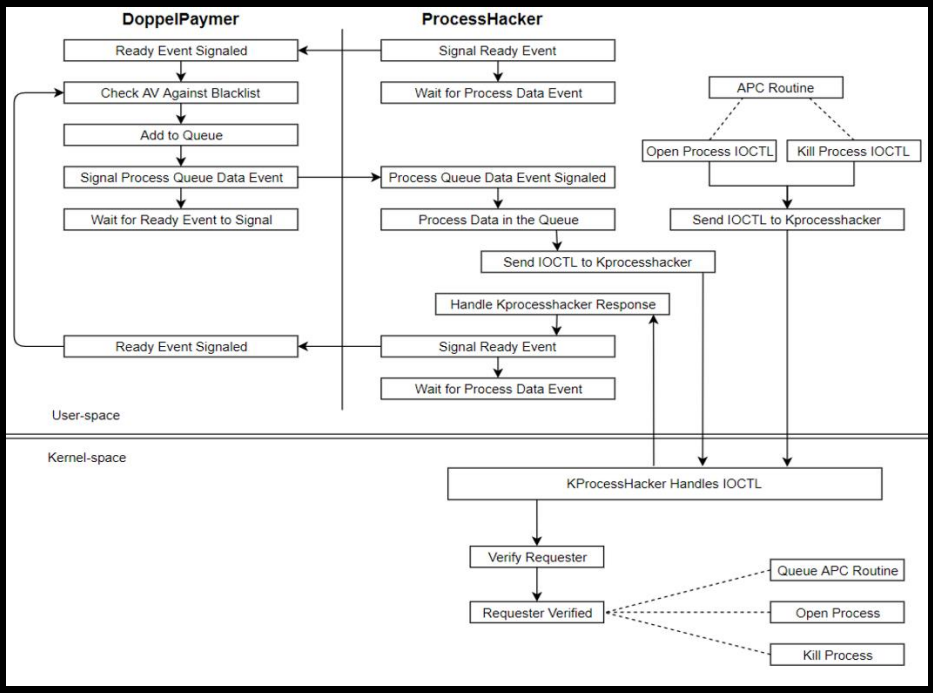


Figure 1.1: Architecture diagram to kill a target process (Original credits to CrowdStrike)

Order of Events

DLL Search Order Hijacking:

- DoppelPaymer uses a technique called DLL search order hijacking to inject a malicious stager DLL into ProcessHacker. This involves placing a malicious version of a DLL in the directory from which ProcessHacker loads its DLLs, causing it to load the malicious DLL instead of the legitimate one.

Process Creation and IPC Setup:

- The ransomware writes the ProcessHacker executable, KProcessHacker driver, and stager DLL into a subdirectory within %APPDATA%. It then launches ProcessHacker with specific arguments to facilitate inter-process communication (IPC) between DoppelPaymer and ProcessHacker.

Loading and Initializing the Stager DLL:

- The stager DLL is loaded into ProcessHacker, bypassing its normal startup routines. Several initialization steps are required, including modifying ProcessHacker's entry point and initializing the KProcessHacker service.

Verification and Communication:

- The stager DLL ensures that ProcessHacker is verified as a valid client for the KProcessHacker service. This involves complex verification processes using IOCTL requests and digital signature checks.

Killing Blocklisted Applications:

Once initialized, DoppelPaymer enumerates processes and services on the system, hashing their names with CRC32. These hashes are compared against a blocklist stored in memory. If a match is found, DoppelPaymer writes commands to terminate these processes into an IPC queue for the stager DLL to execute. The termination process involves opening a handle to the process and then killing it using specific IOCTL requests.

Behavioral Patterns

The takedown routine in DoppelPaymer is very strategic in causing high-impact takedowns with high extortion possibilities. It exfiltrates sensitive data from the network of the victim before encrypting the files, handily used later for double extortion-scenarios in which the attackers threaten to publish or sell it if they don't get paid. This does add pressure on the victims to comply with the ransom demand.

The ransomware also drops a ransom note on the compromised systems, which provides the victims with instructions on making the ransom demand, in most instances, ranging between $25,000 to over 1 million dollars. The typical set of instructions provided to the victim includes the need to download the Tor browser to get to a dark web-based payment portal, where the victim is further instructed with a countdown clock for the payment.

The ransom note dropped by DoppelPaymer is very similar to the ransom note dropped by BitPaymer in 2018. The ransom amount is not part of the ransom note, but it does include a .onion domain that is used for payment and communicating with the actors behind the attack. Similar to the ransom note, the payment portal of DoppelPaymer is an almost exact clone of the original BitPaymer payment portal. [4]

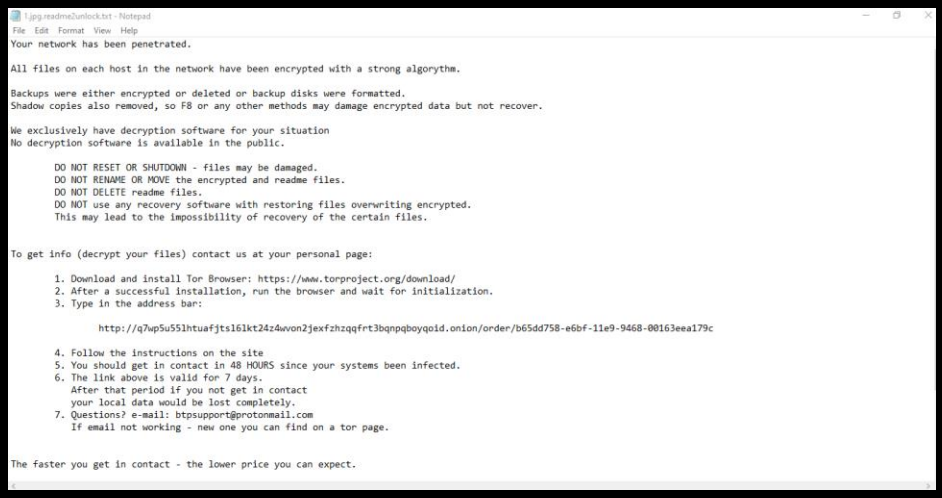


Figure 1.2: DoppelPaymer ransom note which was displayed on the compromised hosts

Target audience for attacks

Historically, DoppelPaymer targets large organizations across many different sectors mainly healthcare, emergency services, education, and government institutions. Traditionally, the group has leveraged vulnerabilities in remote desktop protocols, insecure configurations, and outdated software for gaining initial access. They have also been known to leverage botnets and deceptive downloads as part of their distribution strategy.

Many current attack patterns continue to focus on high-value targets, where disruption to operations can result in significant physical or financial harm. Healthcare remains particularly vulnerable because it requires continuous access to patient data and other critical systems.

With its technical sophistication and aggressive approach, DoppelPaymer has become one of the most powerful threat actors in the TA and APT networks. It's because it can merge advanced encryption techniques with strategic extortion methods underlines the appropriateness of cybersecurity measures in place to protect sensitive data and ensure operational integrity. Therefore, routine software updates, employee training regarding phishing, and planning incident responses are some of the areas of concentration for organizations looking to reduce the risks associated with such a threat.

Recent Attacks & Operations carried out by DopplePaymer

DoppelPaymer ransomware has been involved in various high-profile attacks against the healthcare sector, proving its great capability to disrupt essential services and outline the vulnerabilities within this industry. Among the attacks carried out by DoppelPaymer, two of the most relevant ones provide a clear vision of its tactics and impact, which it might leverage to attack or compromise HSE.

One of the most sensational incidents that involved DoppelPaymer occurred back in September 2020 at the University Hospital Düsseldorf in Germany. The attack is considered one of the most villainous because it is believed to have directly contributed to the death of a patient who was among the first highly publicized severe human impacts caused by a cyberattack. The attackers had exploited a vulnerability in Citrix software that the hospital had failed to patch, gaining access to the network. Once inside, they unleashed DoppelPaymer, which succeeded in encrypting data across 30 servers and crippling the hospital's IT systems. As a result, patients in urgent need of care had to be diverted to other facilities, and one critically ill patient died en-route to a hospital 20 miles away. It reiterated the urgency and need for good patch management in a timely manner, as well as good cybersecurity measures, in health care.

Another disruptive DopplePaymer operation was against Apex Laboratory, based in Farmingdale, USA. The attack involved exploitation for initial access, followed by ransomware deployment, which encrypted sensitive data. As a result of this exfiltration of PHI prior to encrypting them, a tactic these days referred to as double extortion, Apex Laboratory had to notify patients about the data breach. This approach not only disrupts operations but also blackmails victims with the release of sensitive data to the public if ransoms are not paid.

These attacks exemplify DoppelPaymer's *modus operandi* of attacking healthcare organizations, where one attack has serious consequences, thus exerting added pressure on the victim for payment. The double extortion further raises the stakes with an added data breach element leading to great reputational damage and possible legal consequences if it is found that an organization has poor security practices in place.

To conclude, these incidents show how DopplePaymer may target the HSE and points on how the threat landscape keeps evolving for healthcare service providers and underlines the need for an integrated approach toward cybersecurity. This includes: periodic vulnerability assessment, timely application of security patches, employee education regarding how to recognize phishing attacks, and development of a comprehensive incident response plan as part of mitigation strategies against such attacks.

Diving into DopplePaymer’s intricacies

Tactics, Techniques and Procedures (TTPs) employed by DopplePaymer

DoppelPaymer employs a quite complex process, beginning with infiltrating networks through deceptive spam emails that contain spear-phishing links or attachments intended to entice unsuspecting users into running malicious code disguised as a legitimate document. This code is responsible for fetching other malware with more advanced capabilities (like Emotet, Dridex and QakBot) onto the victim's system. [6]

Once these advanced malwares are installed, it communicates with its command-and-control (C&C) server to install different modules and to download and execute other malware.

The C&C server was utilized in the DoppelPaymer campaign to download and run the Dridex malware family, which is then used to download either DoppelPaymer directly or tools like PowerShell Empire, Cobalt Strike, PsExec, and Mimikatz. These tools are utilized for various purposes, including credential theft, lateral movement within the network, and execution of commands to disable security software.

Upon infiltrating the system, Dridex doesn't immediately deploy the ransomware. Instead, it attempts to move laterally within the network to identify high-value targets from which critical information can be stolen. Once a suitable target is identified, Dridex proceeds to execute its final payload, DoppelPaymer. DoppelPaymer encrypts files within the network as well as fixed and removable drives in the affected system.

Subsequently, DoppelPaymer alters user passwords, initiates a system restart into safe mode to prevent user access, and modifies the notice text displayed before the Windows login screen. The new notice text serves as DoppelPaymer's ransom note, cautioning users against resetting or shutting down the system, as well as against deleting, renaming, or moving encrypted files. The note also includes a threat to publicly share sensitive data unless the demanded ransom is paid.

Additionally, DoppelPaymer drops the Process Hacker executable, its driver, and a stager DLL. It creates another instance of itself that runs the dropped Process Hacker. Once Process Hacker is active, it loads the stager DLL using DLL Search Order Hijacking. The stager DLL remains in a listening/waiting state for a trigger from the running DoppelPaymer

process. DoppelPaymer contains a crc32 list of processes and services it terminates. If a process or service from its list is running, it triggers the Process Hacker to terminate it. [3]

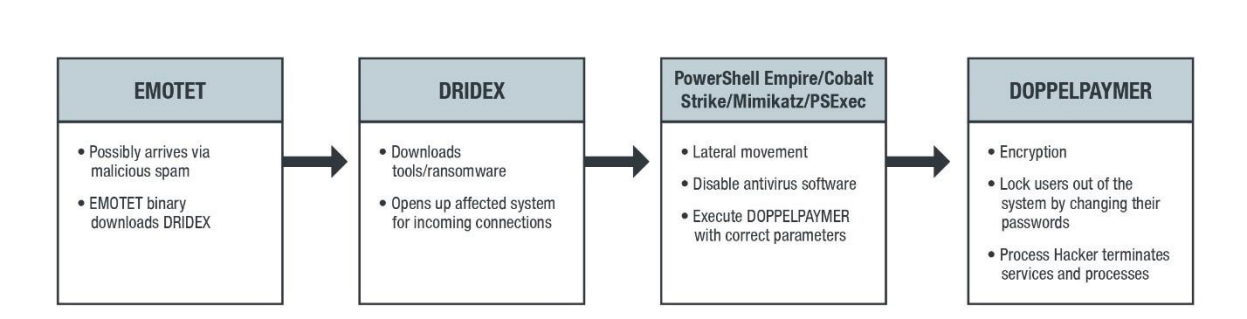


Figure 1.3: DoppelPaymer's infection routine (Original credits to Trend Micro)

Initial Access [TA0001]

Phishing *(T1566)*: DoppelPaymer may gain initial entry through targeted phishing or unsolicited emails containing harmful attachments or links. These emails are designed to look genuine and entice the victim to execute the harmful payload.

Execution [TA0002]

User Execution (T1204): If the victim opens the attachment or clicks on the link, harmful payload is executed on their device. This code serves as a loader for additional malware components needed for further network compromise.

Persistence [TA0003]

Boot or Logon Initialization Scripts (T1037): Threat actor would create system initialization services, scripts and alters them to ensure the ransomware starts upon every system reboot.

Privilege Escalation [TA0004]

Valid Accounts (T1078): Mimikatz can be used to extract credentials from system memory, enabling attackers to escalate privileges within the network.

Defense Evasion [TA0005]

Hide Artifacts (T1564): DoppelPaymer may utilize Alternate Data Streams to conceal its payload within the NTFS file system, making it challenging for antivirus solutions to detect.

Lateral Movement [TA0008]

Lateral Tool Transfer (T1507): This threat actor could use Dridex and QakBot malwares which has remote code execution capabilities, enabling attackers to execute commands on remote systems within the network, making it crucial for moving laterally across different segments of the network.

Exfiltration [TA0010]

Exfiltration over C2 channel (T1646): The critical information or data could be potentially pilfered by transmitting it through an established command and control channel. The pilfered data is concealed within the regular communication channel using the identical protocol as the C2 communications.

Impact [TA0040]

Data Encrypted for Impact (T1486): Once this threat actor has sufficiently infiltrated the network and gathered necessary credentials, it can deploy ransomware known as 'DoppelPaymer' after which it was named. This deployment often involves disabling security measures and encrypting files across the network, rendering the data and critical files of no use.

Firmware/Software features corruption (T1495): The TA would be able to erase or eliminate pre-installed data and features meant to assist in the restoration of a damaged system in order to hinder recovery by changing user passwords and accessing restricted safe mode. This action could block access to existing backups and recovery choices, which would increase the attacker's financial leverage significantly.

Mapping of DopplePaymer's TTPs to the MITRE ATT&CK Framework

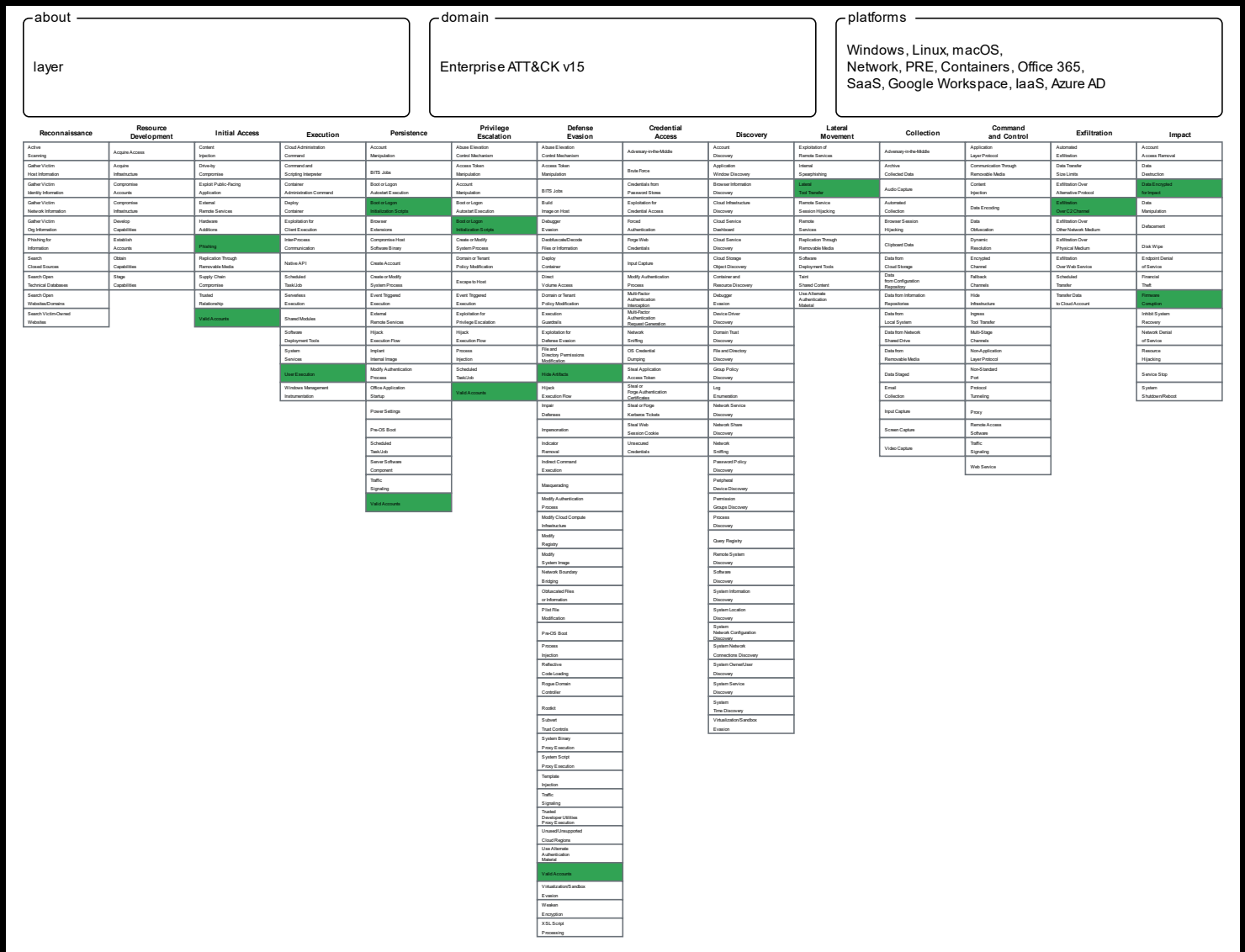
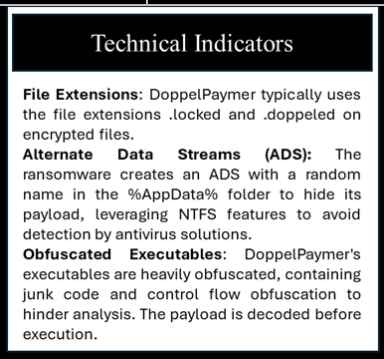


Figure 1.4: DopplePaymer's TTP mapping to the MITRE ATT&CK framework using MITRE ATT&CK navigator

Tactics	Technique	Procedure	Use case
Initial Access [TA0001]	Phishing (T1566)	Conduct reconnaissance to understand email conventions and generate target email lists. Craft deceptive emails mimicking legitimate sources, and use tools like GoPhish to send these emails, directing targets to spoofed websites that capture credentials.	DoppelPaymer actors often use spear-phishing emails with malicious attachments or links. These emails can contain Office documents with embedded macros or scripts that download and execute the ransomware payload. They may also exploit vulnerabilities in email clients or web browsers to gain initial access. **CVE-2019-19781** - A vulnerability in Citrix ADC that allows remote code execution, exploited by DoppelPaymer for initial access.
Execution [TA0002]	User Execution (T1204)	Use social engineering tactics to convince users to open malicious attachments or enable macros in documents. This can involve crafting convincing scenarios or messages that prompt the user to execute the file.	After a successful phishing attempt, DoppelPaymer relies on user interaction to execute the payload. This often involves tricking users into enabling macros in Office documents, which then run PowerShell scripts or other executables that deploy the ransomware. **CVE-2018-20250** - A vulnerability in WinRAR that allows remote code execution when processing specially crafted archives.
Persistence [TA0003]	Boot or logon initialization scripts (T1037)	Modify system startup scripts or registry keys to ensure malicious code runs at boot or logon. This can involve creating or altering scripts in common startup directories or registry entries.	DoppelPaymer may achieve persistence by modifying Windows Registry keys related to startup processes or by creating scheduled tasks using schtasks that ensure their malware runs each time the system boots or a user logs on. They might also utilize services like wscript for script execution at startup. **CVE-2022-38028** - A vulnerability allowing privilege escalation via hijacking the print spooler service execution.
Privilege Escalation [TA0004]	Valid Accounts (T1078)	Harvest credentials through phishing or keylogging, then use these credentials to access systems with higher privileges. This often involves bypassing security controls by masquerading as a legitimate user.	The group uses tools like Mimikatz to extract credentials from memory, enabling them to escalate privileges and move laterally within the network using valid accounts. They may also exploit known vulnerabilities in Windows systems (e.g., EternalBlue) to gain elevated access and move laterally across the network using compromised credentials. **CVE-2021-26857** - An insecure deserialization vulnerability used for privilege escalation in Microsoft Exchange Server.
Defense Evasion [TA0005]	Hide Artifacts (T1564)	Use techniques like modifying file attributes, encrypting payloads, or using rootkits to hide malicious files and processes from detection tools.	DoppelPaymer employs various evasion techniques such as disabling security software via Group Policy modifications, using process hollowing to inject code into legitimate processes, and leveraging obfuscation techniques to avoid detection by antivirus solutions. They might also clear event logs using wevtutil commands to erase traces of their activities. **CVE-2023-36025** - A vulnerability allowing attackers to bypass Windows Defender SmartScreen for defense evasion.
Lateral Movement [TA0008]	Lateral tool transfer (T1507)	Transfer tools or payloads across the network using protocols like SMB, FTP, or SSH. This often involves using compromised credentials to access remote systems and deploy tools for further exploitation.	DoppelPaymer actors utilize Windows administrative tools like PsExec and WMIC for lateral movement within networks. They may also use RDP with stolen credentials for remote access and deploy additional payloads via SMB shares, exploiting trust relationships between networked systems to spread the ransomware further. **CVE-2017-0144** - EternalBlue exploit used for lateral movement by exploiting SMBv1 vulnerabilities on Windows systems.
Exfiltration [TA0010]	Exfiltration Over C2 channel (T1646)	Use command and control channels to send data out of the network, often employing encryption to obfuscate the data being exfiltrated. This can involve tunneling data through common protocols like HTTP or DNS to avoid detection.	Before encrypting files, DoppelPaymer exfiltrates sensitive data using encrypted channels such as HTTPS or VPNs configured through compromised devices. This data is often sent to cloud storage services or remote servers controlled by attackers, ensuring it remains undetected by traditional monitoring solutions until ransom demands are made public. **CVE-2018-4878** - A vulnerability in Adobe Flash Player that could be leveraged for arbitrary code execution during exfiltration activities.
Impact [TA0040]	Data encrypted for impact (T1486)	Deploy ransomware or similar tools to encrypt critical data on target systems, rendering it inaccessible until a ransom is paid. This involves using strong encryption algorithms and deleting original files after encryption.	DoppelPaymer encrypts files using strong encryption algorithms like RSA-2048 combined with AES-256 for file encryption, significantly impacting business operations by locking critical data until a ransom is paid for decryption keys. They may also disable shadow copies and backup solutions using commands like vssadmin delete shadows to prevent recovery without paying the ransom. **CVE-2019-0604** - A vulnerability in SharePoint that could be exploited for arbitrary code execution leading up to ransomware deployment scenarios.
Impact [TA0040]	Firmware/Software features corruption (T1495)	Overwrite firmware components such as BIOS with corrupted versions, potentially rendering devices inoperable. This can involve exploiting vulnerabilities in firmware update processes.	Although specific firmware corruption isn't typically associated with DoppelPaymer, their impact includes severe disruption of IT operations through file encryption and potential destruction of accessible backups during the attack process. **CVE-2020-0689** - A vulnerability in Windows Secure Boot that could allow bypassing of security features leading to firmware manipulation.

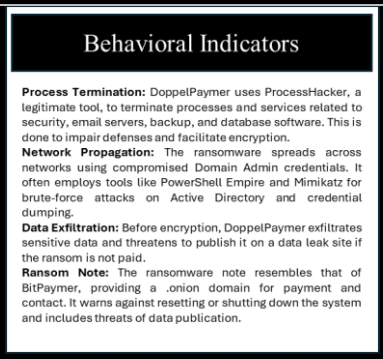
Indicators of Compromise (IOCs) leveraged by DopplePaymer

Type of IOC	Specifics / Value
HASH (SHA256)	624255fef7e958cc3de9e454d2de4ae1a914a41fedc98b2042756042f68c2b69 Ransom.Win32.DOPPELPAYMER.TGACAR
HASH (SHA256)	4c207d929a29a8c25f056df66218d9e8d732a616a3f7057645f2a0b1cb5eb52c Ransom.Win32.DOPPELPAYMER.TGACAQ
HASH (SHA256)	c66157a916c7f874bd381a775b8eede422eb59819872fdffafc5649eefa76373 Ransom.Win32.DOPPELPAYMER.TGACAP
HASH (SHA256)	f658ddcf8e87de957a81bb92d44ce02913b427e8bccbe663669ee2613d355555
Onion/Tor URL	q7wp5u55lhtuafjtsl6lkt24z4wvon2jexfzhzqqfrt3bqnpqboyqoid.onion http://doppleshare.top
HASH (MD5)	8c54bbe3f191a8627bfeeb4cb02634a9
Email	btpsupport@protonmail.com
File Path	C:\Users\gratemin\Dekstop [2] C:\Users\gratemin\Desktop\p1q135no.exe [2]
File Extension(s)	*.locked [5] .readme2unlock.txt [5] *.doppled [5]



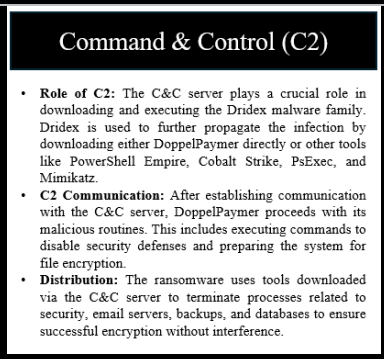
Technical Indicators

File Extensions: DoppelPaymer typically uses the file extensions .locked and .doppeled on encrypted files.
Alternate Data Streams (ADS): The ransomware creates an ADS with a random name in the %AppData% folder to hide its payload, leveraging NTFS features to avoid detection by antivirus solutions.
Obfuscated Executables: DoppelPaymer's executables are heavily obfuscated, containing junk code and control flow obfuscation to hinder analysis. The payload is decoded before execution.



Behavioral Indicators

Process Termination: DoppelPaymer uses ProcessHacker, a legitimate tool, to terminate processes and services related to security, email servers, backup, and database software. This is done to impair defenses and facilitate encryption.
Network Propagation: The ransomware spreads across networks using compromised Domain Admin credentials. It often employs tools like PowerShell Empire and Mimikatz for brute-force attacks on Active Directory and credential dumping.
Data Exfiltration: Before encryption, DoppelPaymer exfiltrates sensitive data and threatens to publish it on a data leak site if the ransom is not paid.
Ransom Note: The ransomware note resembles that of BitPaymer, providing a .onion domain for payment and contact. It warns against resetting or shutting down the system and includes threats of data publication.



Command & Control (C2)

- **Role of C2:** The C&C server plays a crucial role in downloading and executing the Dridex malware family. Dridex is used to further propagate the infection by downloading either DoppelPaymer directly or other tools like PowerShell Empire, Cobalt Strike, PsExec, and Mimikatz.
- **C2 Communication:** After establishing communication with the C&C server, DoppelPaymer proceeds with its malicious routines. This includes executing commands to disable security defenses and preparing the system for file encryption.
- **Distribution:** The ransomware uses tools downloaded via the C&C server to terminate processes related to security, email servers, backups, and databases to ensure successful encryption without interference.

Conclusion

The Conti ransomware attack, which targeted Ireland's Health Service Executive (HSE) in May 2021, had a far-reaching impact on the organization's operations. This significant event underscored the critical importance of robust cybersecurity measures in healthcare systems. By analyzing the specific tactics and entry points utilized in the Conti attack, HSE can gain valuable insights to fortify its defenses against similar threats in the future. Additionally, implementing multifaceted preventive measures, such as network segmentation, regular security audits, and employee training on identifying phishing attempts, can significantly enhance HSE's resilience against evolving ransomware threats, including the notorious DoppelPaymer ransomware.

Inference from the Conti group's attack on HSE

The recent cyber-attack on HSE by the Conti group has brought to light numerous weaknesses in the organization's cybersecurity infrastructure. Here are some important points to take away from the incident:

- Lack of Cybersecurity Readiness: The HSE demonstrated a low level of cybersecurity maturity, with ineffective monitoring and response capabilities. As a result, attackers were able to infiltrate and move laterally within the network without being detected for a significant period.
- Phishing as an Entry Point: The attack began with a phishing email that contained a malicious Excel attachment. This underscores the importance of strong email security and educating users to identify and steer clear of phishing attacks.
- Impact on Services: This attack led to a significant disruption in healthcare services, resulting in the cancellation of appointments and the need to rely on manual procedures. This highlights the essential requirement for cybersecurity to ensure operational continuity in healthcare.
- Financial Costs: The aftermath of the attack is estimated to require more than $100 million for recovery, underscoring the significant financial repercussions of insufficient cybersecurity measures.

Fortifying HSE against the DoppelPaymer threat actor

To shield against potential ransomware assaults like the ones perpetrated by DoppelPaymer, HSE has the option to implement multiple tactics:

- Defense-in-Depth Strategy: Employ a multi-layered approach to security by implementing controls across endpoints and networks, such as firewalls, intrusion detection systems, and network segmentation to prevent the spread of malware.
- Network Segmentation: Implementing network segmentation to isolate legacy systems from modern systems, reducing the risk of security breaches.
- Continuous Monitoring & Response: Set up continuous monitoring of network traffic and system logs to identify any potentially suspicious activities as soon as possible. Employ managed detection and response (MDR) tools to receive immediate alerts and enable quick reaction.
- Data Encryption: Encrypting patient data at rest and in transit to prevent unauthorized access and maintain data security.
- Patch Management: Regularly update software and systems to address known vulnerabilities that could be exploited by ransomware.

Effective recommendations & next steps for HSE

For effectively addressing the DoppelPaymer ransomware threat, HSE needs to focus on three dimensions: 1.) preparation for a breach, 2.) active response during a breach, and 3.) management of post-breach consequences.

Pre-Breach Preparation

Use an EDR Service: Implementing Endpoint Detection and Response (EDR) services can help in detecting and responding to threats in real-time. EDR solutions are crucial for monitoring endpoints for suspicious activities and providing insights into potential threats before they escalate.

Prepare an Incident Response Plan and Team: Establish a well-defined incident response plan and assemble a skilled team to handle potential breaches. This preparation ensures that the organization can quickly respond to incidents, minimizing damage and recovery time.

Purchase a Cyber Insurance Policy: Cyber insurance can provide financial protection against losses resulting from cyber incidents, including ransomware attacks. It helps cover costs associated with data recovery, legal fees, and potential ransom payments.

Active Breach Response

Disconnect or Shut Down Computing Devices: In the event of a breach, quickly disconnecting affected devices from the network can prevent the spread of ransomware and limit data exfiltration.

Contact a Trusted IR Team: Engage with a trusted incident response (IR) team to contain the breach, eradicate the malware, and restore normal operations. Professional IR teams can also assist with public relations and negotiation with attackers if necessary.

Document All Significant Events and Actions: Maintain detailed records of all events and actions taken during the breach. This documentation is essential for post-incident analysis and for legal or insurance purposes.

Post-Breach Management

Deploy EDR Services: Post-breach, ensure that EDR services are fully deployed to monitor for any lingering threats or new attacks. Continuous monitoring is vital for maintaining security posture.

Regularly Patch and Update: Keep all software and systems updated with the latest security patches to protect against known vulnerabilities that ransomware exploits.

Ensure Effective Backups Exist: Regularly back up critical data using strategies like the 3-2-1 rule—three copies of data on two different media types, with one copy offsite. Ensure backups are secure and disconnected from the network to prevent them from being compromised during an attack.

Tighten Security Configurations: Review and enhance security configurations across all systems. Implement measures such as network segmentation, firewalls, and multi-factor authentication to reduce the attack surface.

Have a Plan and Team in Place for Future Breaches: Continuously update incident response plans based on lessons learned from past breaches. Ensure that your team is trained and ready to respond to future incidents promptly.

Ongoing Cyber Awareness Training for Employees: Conduct regular cybersecurity training sessions to educate employees about recognizing phishing attempts, safe email practices, and other security protocols. Human error is often exploited in ransomware attacks.

Insure Against Future Cyber Losses: Maintain or update cyber insurance policies to ensure coverage aligns with evolving threats and organizational changes.

By implementing these strategies, HSE can significantly mitigate the risks posed by DoppelPaymer ransomware and improve their overall cybersecurity resilience.

Cyber hygiene advised for HSE

- Avoid opening emails from unknown sources and refrain from clicking on links or attachments within these messages.
- Regularly back up critical files following the 3-2-1 rule: maintain three copies of your data in two different formats, and store one copy offsite.
- Promptly update software and applications with the latest security patches to protect against vulnerabilities.
- Ensure that backups are secure and disconnected from the network after each backup session.
- Conduct regular audits of user accounts, especially those that are publicly accessible, such as Remote Monitoring and Management accounts.
- Monitor both inbound and outbound network traffic, with alerts set up to detect data exfiltration attempts.
- Strengthen account security by implementing two-factor authentication (2FA) for user logins.
- Apply the principle of least privilege to file, directory, and network share permissions to minimize access risks.

Citations & References

1. SOC Prime. (n.d.). *DoppelPaymer ransomware detection*. Retrieved from https://socprime.com/blog/doppelpaymer-ransomware-detection/
2. Acronis. (n.d.). *Threat analysis: DoppelPaymer ransomware*. Retrieved from https://www.acronis.com/en-us/blog/posts/doppelpaymer-ransomware/
3. Trend Micro. (2021). *An overview of the DoppelPaymer ransomware*. Retrieved from https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html
4. Unit 42 by Palo Alto Networks. (n.d.). *Ransomware threat assessments: A companion to the 2021 Unit 42 ransomware threat report*. Retrieved from https://unit42.paloaltonetworks.com/ransomware-threat-assessments/4/
5. CrowdStrike. (n.d.). *BitPaymer source code fork: Meet DoppelPaymer ransomware and Dridex 2.0*. Retrieved from https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
6. Proofpoint. (n.d.). *What are TTPs in cybersecurity? | Proofpoint US*. Retrieved from https://www.proofpoint.com/us/threat-reference/tactics-techniques-procedures-ttps

Appendix

i. Glossary & Definitions

Advanced Persistent Threat (APT):	A stealthy threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.
Alternate Data Streams (ADS):	A feature of the NTFS file system that allows data to be stored in hidden streams alongside a file, often used by malware to conceal its presence.
BitPaymer:	A ransomware family known for its sophisticated encryption methods and high ransom demands, from which DoppelPaymer is derived.
Command and Control (C&C) Server:	A server used by attackers to maintain communications with compromised systems within a target network.
Credential Dumping:	The process of obtaining account credentials from operating systems or software to gain unauthorized access to systems.
Data Exfiltration:	The unauthorized transfer of data from a computer or network.
DoppelPaymer:	A strain of ransomware known for targeting large organizations, particularly in healthcare, using advanced infiltration techniques and extortion methods.
Dridex:	A banking malware that facilitates credential theft and is often used as a loader for deploying ransomware like DoppelPaymer.
Encryption:	The process of converting data into a code to prevent unauthorized access. DoppelPaymer uses 2048-bit RSA and 256-bit AES encryption algorithms.
Endpoint Detection and Response (EDR):	Security solutions focused on detecting, investigating, and responding to suspicious activities on endpoints in real-time.
Indicators of Compromise (IoCs):	Pieces of forensic data that identify potential malicious activity on a system or network.
Lateral Movement:	The technique used by attackers to move through a network in search of valuable data or assets after gaining initial access.
Phishing:	A cyberattack method that uses deceptive emails or websites to trick individuals into revealing sensitive information.
ProcessHacker:	A legitimate tool used by DoppelPaymer to terminate processes related to security software during an attack.
Ransomware-as-a-Service (RaaS):	A business model where ransomware developers sell or lease their malware to affiliates who carry out attacks.
Tactics, Techniques, and Procedures (TTPs):	The behavior patterns used by threat actors during cyberattacks, encompassing their overall strategy (tactics), methods (techniques), and specific actions (procedures).