SK 쉴더스

EQST Annual Report

Security Threat Forecast Report of 2024

Contents

EQST insight

Security issues of 2023 and forecast for top five security threats of 2024

■ Review of top five security threats of 2023

In 2023, ransomware attacks continued to occur both domestically and internationally. In the case of ransomware, the main attacks exploited 0-day. Looking at overseas cases, the 'Cl0p' Ransomware Group conducted a large-scale attack by exploiting the 'MOVEit' vulnerability. In Korea, many attacks were discovered that exploited the old version of the MagicLine4NX vulnerability.

'Greatness', a 'PhaaS' service that plays a similar role as 'Caffeine' in the large-scale phishing attack environment, appeared last year. In particular, this service attracted the attention of hackers because it was easy to steal multi-factor authentication (MFA). In addition to these phishing services, the 'Qshing[1]' crime is increasing.

Moreover, ongoing threats to mobile applications have increased. In 2023, the NSO Group also attracted popular attention by distributing the new zero-click spyware.

In the IIoT (Industrial Internet of Things) field, attacks mainly exploited firewall vulnerabilities, and in the aftermath of the Israel-Palestine War, many attacks targeted major infrastructure such as energy, national defense, and communications organizations.

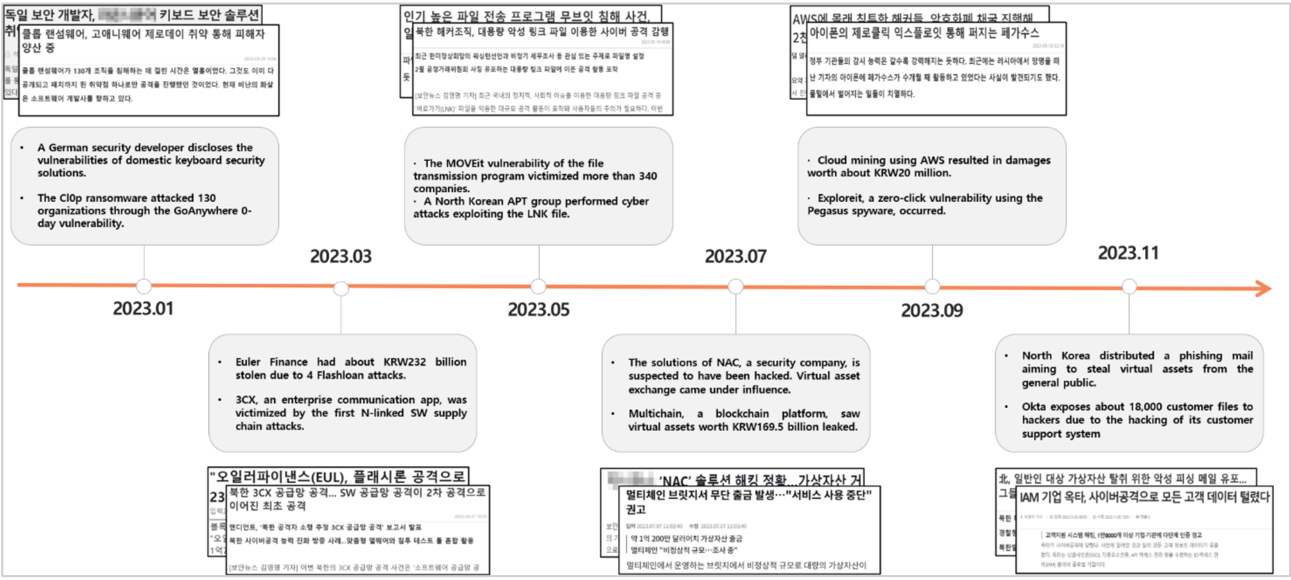
When it comes to the block chain, the scale of damage has slightly decreased in 2023 compared to last year, but large damages are still reported. Crimes exploiting the vulnerability of the cross-chain bridge were the dominant case.

SK Shieldus' white hacker group, EQST, analyzed major issues of 2023 and predicted the top five security threats of 2024.

[1] Qshing: A compound word of QR code and phishing. It is an attack technique that leads the victim to a phishing page using the attacker's QR code.

2023 security Trend review

■ Review of major cybersecurity incidents of 2023


독일 보안 개발자, [redacted] 키보드 보안 솔루션
클롭 랜섬웨어, 고애니웨어 제로데이 취약 통해 피해자 양산 중
클롭 랜섬웨어가 130개 조직을 침해하는 데 걸린 시간은 열흘이었다. 그것도 이미 다 공개되고 패치까지 된 취약점 하나로만 공격을 진행했던 것이었다. 현재 비난의 화살은 소프트웨어 개발사를 향하고 있다.
인기 높은 파일 전송 프로그램 무브잇 침해 사건,
북한 해커조직, 대용량 악성 링크 파일 이용한 사이버 공격 감행
최근 한미정상회담의 워싱턴선언과 비정기 세무조사 등 관심 있는 주제로 파일명 설정
2월 공정거래위원회 사칭 유포하는 대용량 링크 파일에 이은 공격 활동 포착
[보안뉴스 김영명 기자] 최근 국내의 정치적, 사회적 이슈를 이용한 대용량 링크 파일 공격 등 '바로가기(LNK)' 파일을 악용한 대규모 공격 활동이 포착돼 사용자들의 주의가 필요하다. 이번
AWS에 몰래 침투한 해커들, 암호화폐 채굴 진행해
아이폰의 제로클릭 익스플로잇 통해 퍼지는 페가수스
정부 기관들의 감시 능력은 갈수록 강력해지는 듯하다. 최근에는 러시아에서 망명을 떠난 기자의 아이폰에 페가수스가 수개월 째 활동하고 있었다는 사실이 발견되기도 했다. 물밑에서 벌어지는 일들이 치열하다.
2023.01
2023.03
2023.05
2023.07
2023.09
2023.11
"오일러파이낸스(EUL), 플래시론 공격으로
북한 3CX 공급망 공격... SW 공급망 공격이 2차 공격으로 이어진 최초 공격
맨디언트, '북한 공격자 소행 추정 3CX 공급망 공격' 보고서 발표
북한 사이버공격 능력 진화 방증 사례...맞춤형 멀웨어와 침투 테스트 를 혼합 활용
[보안뉴스 김영명 기자] 이번 북한의 3CX 공급망 공격 사건은 '소프트웨어 공급망 공
[redacted] 'NAC' 솔루션 해킹 정황...가상자산 거
멀티체인 브릿지서 무단 출금 발생…"서비스 사용 중단" 권고
약 1억 200만 달러어치 가상자산 출금
멀티체인 "비정상적 규모…조사 중"
멀티체인에서 운영하는 브릿지에서 비정상적 규모로 대량의 가상자산이
北, 일반인 대상 가상자산 탈취 위한 악성 피싱 메일 유포...
IAM 기업 옥타, 사이버공격으로 모든 고객 데이터 털렸다
고객지원 시스템 해킹, 1만8000개 이상 기업기관에 다단계 인증 경고

2023.01

- A German security developer discloses the vulnerabilities of domestic keyboard security solutions.
- The Cl0p ransomware attacked 130 organizations through the GoAnywhere 0-day vulnerability.

2023.03

- Euler Finance had about KRW232 billion stolen due to 4 Flashloan attacks.
- 3CX, an enterprise communication app, was victimized by the first N-linked SW supply chain attacks.

2023.05

- The MOVEit vulnerability of the file transmission program victimized more than 340 companies.
- A North Korean APT group performed cyber attacks exploiting the LNK file.

2023.07

- The solutions of NAC, a security company, is suspected to have been hacked. Virtual asset exchange came under influence.
- Multichain, a blockchain platform, saw virtual assets worth KRW169.5 billion leaked.

2023.09

- Cloud mining using AWS resulted in damages worth about KRW20 million.
- Exploreit, a zero-click vulnerability using the Pegasus spyware, occurred.

2023.11

- North Korea distributed a phishing mail aiming to steal virtual assets from the general public.
- Okta exposes about 18,000 customer files to hackers due to the hacking of its customer support system

[Major cybersecurity incidents of 2023]

In January of this year, Wladimir Palant, a German security software developer, posted an article on his blog about vulnerabilities in the Korean Internet environment, which became an issue. He disclosed the vulnerabilities of security solutions used by major banks/financial sites in Korea one by one, and among them, the vulnerability of the domestic keyboard security solution was disclosed, causing a stir. Afterwards, a large-scale security patch was implemented for related solutions.

Additionally, attacks by ransomware groups that exploited corporate solution vulnerabilities were prevalent this year. Among them, in February, there was an attack by the Cl0p Ransomware Group that exploited the 0-day vulnerability (CVE-2023-0669) of GoAnywhere, a file transmission software. The Cl0p Ransomware Group attacked more than 130 organizations and disclosed information about victimized companies on the dark web. Hatch Bank, a fintech platform, was found to have had the personal information of 139,493 customers stolen, and in addition, companies such as Hitachi Energy and Rubrik were found to have suffered damage from attacks utilizing the GoAnywhere vulnerability of the Cl0p Ransomware Group.

In March, Euler Finance, a DeFi protocol that provides Ethereum-based virtual asset secured loan service, suffered a Flash Loan attack. Euler Finance had about KRW232 billion ($197 million) of funds stolen due to this attack. Flash loan refers to an unsecured loan and it must be repaid before the transaction is completed. In a Flash Loan attack means that exploit this, a price manipulation attack is performed on exchanges using the loaned virtual assets, or the smart contract vulnerability of DeFi service is attacked to make profits, and the collateral is repaid immediately thereafter. Through this attack, the attacker stole millions of stable coins including DAI, USD coin (USDC), Staking Ethereum (StETH), and Wrapped Bitcoin (WBTC). The attacker returned more than 90% of the stolen assets to the victims, but in the process of returning them, records of some assets transferred to the Lazarus group in North Korea were discovered, suggesting a connection between the attacker and Lazarus.

In addition, it was revealed that the attack group backed by North Korea carried out a supply chain attack through DesktopApp of 3CX, an enterprise communication software. 3CX's DesktopApp can be run in Windows and MAC environments and it is used more than 600,000 customers in 190 countries around the world, and the daily number of users is known to be around 12 million. The reason why this 3CX supply chain attack is attracting attention is because it is the first case of a N-linked supply chain attack where a software supply chain attack led to another software supply chain attack. A 3CX employee downloaded X_Trader, a financial trading software, from Trading Technologies, a software provider, but the software was infected with malware. Through this malware, hackers hijacked the PC privileges of 3CX employees, exploited their credentials to connect to the 3CX system as an administrator, and then accessed the build server. Then, hackers inserted malware into 3CX's software, which was distributed in the form of an installation file through the official homepage. Based on the fact that VEILEDSIGNAL, a backdoor used by Lazarus, was discovered in X_Trader infected in the first attack, and the Gopuram malware was discovered in the second attack, i.e. the 3CX supply chain attack. Based on this, it is assumed that the mastermind behind this incident is Lazarus of North Korea.

An attack by a ransomware group that took advantage of the 0-day vulnerability of the enterprise solution continued in May. The attackers used the SQL Injection vulnerability (CVE-2023-34362) of the file transmission program MOVEit, and it was revealed that the mastermind behind the attack was the Cl0p ransomware group, which used the GoAnywhere vulnerability last February. Big global companies like the UK's BBC and British Airways, as well as the US government and public institutions, and major financial institutions around the world suffered the greatest damage. In particular, it is known that about 2,620 organizations and 77.2 million people were victimized by attacks using the MOVEit vulnerability between May and November this year.

In addition, it was discovered that APT37, a North Korean hacking organization, distributed malware RokRAT[2] through a Windows LNK file[3]. The main target of the attack was the Korean Government or related organizations, and a LNK file was used rather than the existing macro method. The attackers changed the LNK file into a PDF file and sent it to the victim by including the file in a ZIP archive along with normal files. When the victim executes the LNK file after decompressing the ZIP archive, a powershell script is executed, and this script executes another powershell script[4]. The script downloads the malicious payload from the attacker's drive, which causes RokRAT to be installed on the victim's system. APT37, which distributed the malware, is called various names, e.g., 'Geumseong 121', 'ScarCruft', and 'Red Eyes', and is carrying out attacks targeting domestic anti-North Korea organizations and national defense officials. Last March, malware was distributed using a CHM file[5] impersonating a security mail from a domestic financial company. The macro function of MS Office has been actively exploited by attackers, but since MS changed its policy in 2022 to prevent automatic execution of macros in Office document files downloaded via the Internet, attacks using macros have almost disappeared. However, caution is needed as attackers are still continuing attacks through new techniques such as LNK files.

In July, an incident occurred in which a large amount of tokens worth approximately KRW169.5 billion were withdrawn without warning from a phantom bridge operated by the block chain platform Multi-Chain. After recognizing the attack, Multi-Chain suspended service and took follow-up measures such as blacklisting wallets related to large-scale withdrawals and freezing funds. However, a few days later, it was revealed that additional virtual assets worth KRW130.9 billion were stolen. A block chain data platform, Chainalysis, said that the large-scale virtual asset leak from Multi-Chain may have been caused by external hackers who seized control of specific keys of Multi-Chain, but it is highly likely that it was an inside job or a Rug Pull[6].

[2] RokRAT: This malware can collect user information and download additional malware, and malware has a history of distribution through HWP and Word documents.

[3] LNK file: This is a file that provides a link to the original file, folder, etc. in Windows, and a click on it can call the target file.

[4] Power shell script: A command script executed in the command program powershell that is used for management and work

[5] CHM file: A help file format used in Windows that can include contents, images and scripts written in HTML

[6] Rug Pull: The act of stopping a service or project being carried out by a team or company in the virtual asset market and stealing investment funds

Also, infringement incidents targeting network access control (NAC) servers, installed at domestic virtual asset exchanges, occurred. It was confirmed that a malicious program was transmitted from the update server of the security company providing the product to the NAC policy server of some customers, and based on this, the NAC provider determined that its update server had been compromised. Two months after the incident, the company announced in an additional notice that nothing was revealed about the attacker and access path as a result of the investigation into the breach, and provided an update to the NAC product by supplementing the vulnerabilities discovered through its own investigation.

In September, a new cryptocurrency mining campaign, which exploits a lesser-known cloud service[7] provided by AWS (Amazon Web Services), was discovered. This campaign, called AMBERSQUID, is suspected to be backed by Indonesian hackers in consideration of the script or user name used in the attack. As a result of analyzing the wallet address used in the attack, it is estimated that the revenue earned by the attackers was $18,300 as of September. Caution is needed as cryptocurrency mining targeting general PCs or corporate servers is transforming into stealing cloud resources.

Additionally, a new exploit of Pegasus[8], a spyware created by Israel's NSO group, was revealed. Pegasus is a representative spyware that uses Zero-Click[9] through iOS 0-day vulnerability. The 0-day vulnerability exploited by Pegasus spyware is BLASTPASS, which was discovered in iOS 16.6 version released on July 25, 2023 by BLASTPASS. The attacker performs the attack by sending a PassKit[10] attached file to the vulnerability through iMessage. If the attack is successful, sensitive information such as users' voice information, system information, and call records may be transmitted to the attacker.

In November, it was revealed that the e-mail accounts of 1,468 Koreans were stolen due to the activities of a North Korea hacking organization Kimsuky. According to the results of the tracking and investigation of the National Office of Investigation under the National Police Agency, Kimsuky changed the IP address through 576 domestic and foreign servers and sent phishing mail impersonating government agencies and reporters. When the mail recipient accesses n attached file or clicks a URL, a malicious program that can leak internal information of the PC is installed or executed.

[7] AWS Amplify, AWS Fargate, Amazon SageMaker, etc.

[8] Pegasus: A spyware created by Israel's NSO group that exploits iPhone's security vulnerability to steal information from users' devices.

[9] Zero-Click: An attack that can access the device without the user having to interact by clicking an attached file or link.

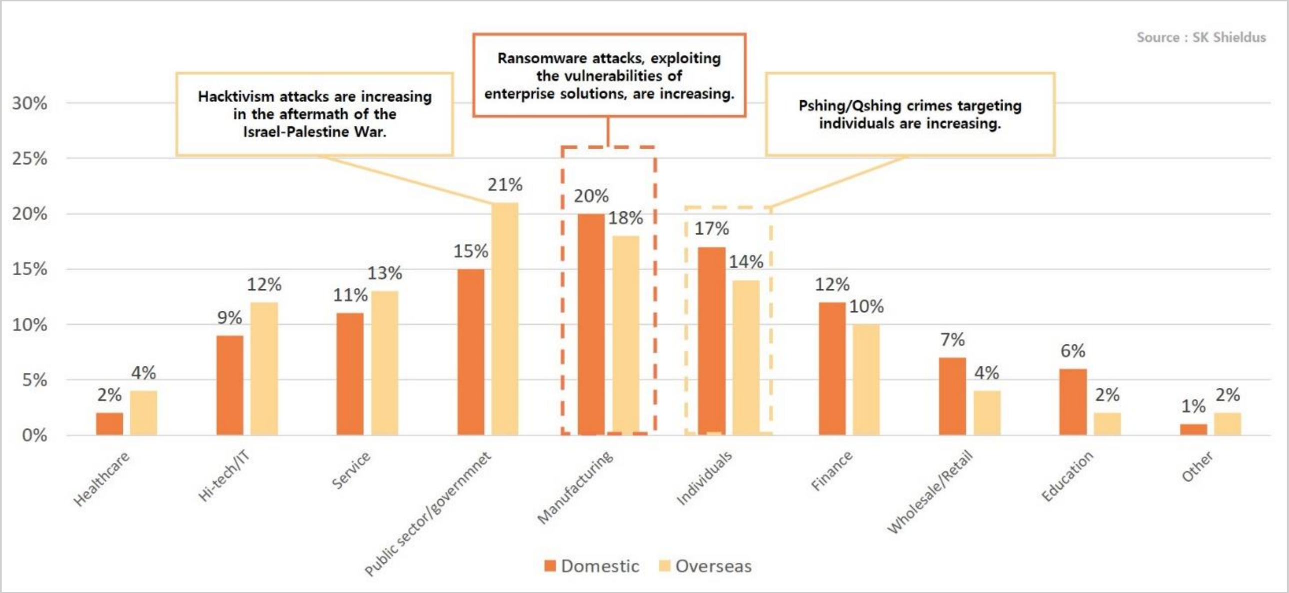
[10] PassKit: A file implemented to display the time and place on the screen or enable the push alarm function when a signature is added to the wallet of an Apple device or authentication is required.

In particular, it appears that the targets of Kimsuky's attacks have expanded to include not only public officials and experts in the fields of diplomacy and security, but also the general public. The majority of ordinary victims are users of virtual asset exchanges, and the attacker actually attempted to steal virtual assets by accessing the virtual asset exchange accounts of 19 phishing mail victims. It was also revealed that a virtual asset mining program was executed on 147 servers taken over through hacking without the administrator's knowledge.

Also, Okta, a security company, revealed that an external hacking group accessed its customer support system upload file. This system is a customer support service to resolve errors that occur while using the service provided by Okta. The files that customers upload through the system contain customers' authentication data, including session tokens and cookies. In the initial announcement of the infringement incidents, it was reported that the attacker accessed 134 customer files, but the investigation revealed that all customer data using Okta's services, i.e. Workforce Identity Cloud (WIC) and Customer Identification Solution (CIS), were stolen.

Okta, a global company in the IAM (Identity and Access Management) field that provides a login and identity management system, is becoming a major target of attackers. Last year, it was attacked by a hacking group called LAPSUS$, and there were four large-scale phishing campaigns called '0ktapus' targeting Okta credentials and authentication codes. In September of this year, social engineering attacks to steal Okta's administrator accounts became popular, and after the customer support system infringement incident in October, a third-party company related to Okta suffered a hacking attack in November, and the personal information of approximately 5,000 current and former Okta employees and family members was leaked.

Statistics on infringement incidents by industry



[Statistics on infringement incidents by industry in 2023]

Looking at the statistics on infringement incidents by industry in 2023, the largest number of incidents occurred in the domestic manufacturing sector at 20% and against individuals at 17%. Additionally, public/government accounted for 15%, finance 12%, service 11%, hi-tech/IT 11%, wholesale/retail 7%, and education 6%. Looking at overseas data, the public/government sector showed the highest figure at 21%, followed by manufacturing, individuals, and service.

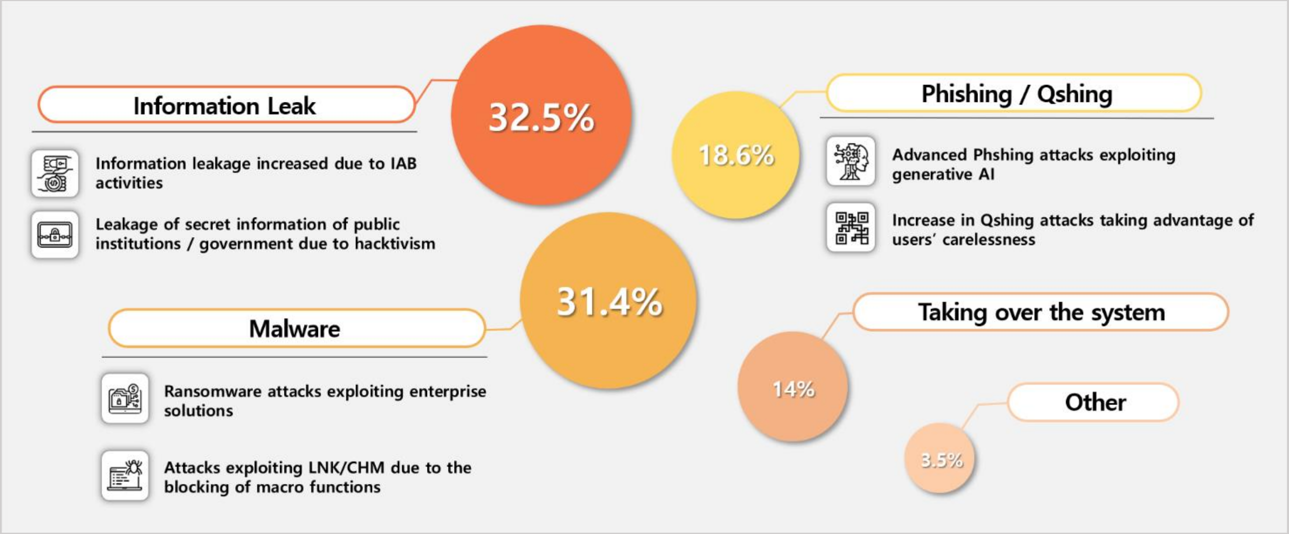
Ransomware attacks exploiting the vulnerabilities of enterprise solutions increased in the first and second half of this year. In Korea, attacks exploiting vulnerabilities in old versions of MagicLine4NX and PaperCut have increased in manufacturing and the public sector. Going overseas, ransomware attacks targeting the vulnerabilities of the MOVEit and GoAnywhere file management solutions and PaperCut, a printer management solution, resulted in data theft from numerous manufacturing companies, public sector/government, and healthcare.

Also, in the second half, the Qshing crime targeting individuals appeared, and was used in phishing attacks. In addition to Qshing attacks, smishing and e-mail phishing attacks continued, and infringement incidents targeting individuals accounted for a high proportion.

In the aftermath of the Israel-Palestine War, hacktivism[11] activities increased, leading to an increase in cyber attacks targeting the public/government sector. They account for the highest percentage.

[11] Hacktivism: A compound word of hacking and activism. It is an activity that pursues social and political goals through hacking

■ Statistics on infringement incidents by type



[Statistics on infringement incidents by type in 2023]

Looking at the statistics on the occurrence of infringement incidents by type in 2023, information leakage accounted for 32.5%, malware infection 31.4%, and phishing/scam attack 18.6%, followed by system takeovers at 14%, and other attacks at 3.5%.

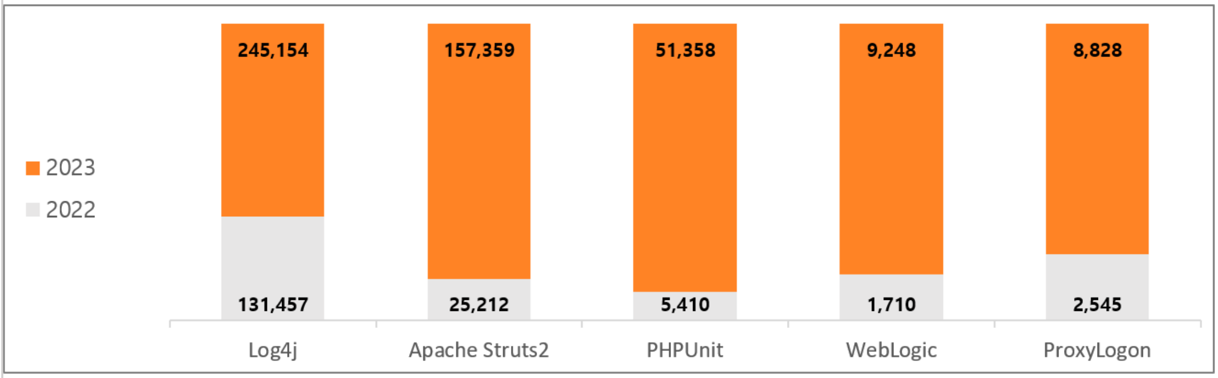
First, important information leakage accounted for the highest proportion at 32.5%. As IAB activities made it easier for attackers to find a path to access the system this year, information leakage cases increases, and confidential information leakage incidents targeting public/government organizations due to hacktivism also appear to have had a significant impact.

Second, damage caused by malware infection accounted for 31.4%. Incidents involving large-scale ransomware attacks targeting various fields by exploiting vulnerabilities in enterprise solutions, both domestically and internationally, accounted for a large portion. Looking at overseas cases, vulnerabilities such as MOVEit and GoAnywhere were exploited, and in Korea, attacks were attempted using the MagicLine4NX vulnerability. Also, in order to respond to the distribution of malware using the macro function of MS Office, MS recently applied an Office macro blocking policy, and the number of malwares in the LNK/CHM format for bypassing this has increased.

Lastly, what is noteworthy in infringement incidents due to phishing/scam is that as many AI services, including ChatGPT, an AI chatbot service, have become popular, it has become possible to create elaborate phishing mails that exploit them. Additionally, in addition to general phishing, an attack method called Qshing is increasing due to the recent increase in the use of QR codes. This is an attack technique in which an attacker attaches a manipulated QR code to the original to lead the victim to a phishing page. Individuals and companies need to be careful when the source is unclear or the QR code points to a suspicious page.

Vulnerability trends

Old vulnerabilities detected in 2022 and 2023



Source : SK Shieldus Secudium

List and cases of major vulnerabilities

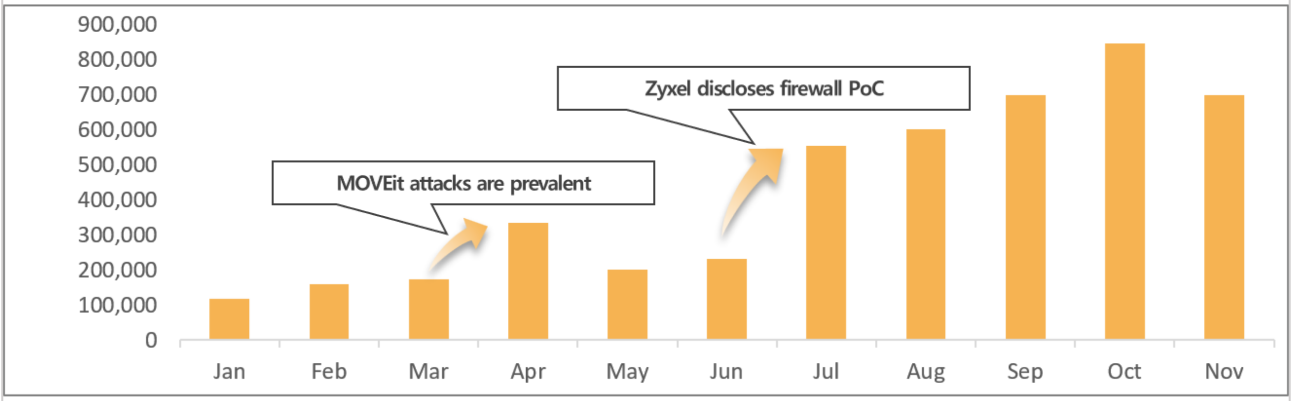
1	Log4j(CVE-2021-44228)	8220 Gang group exploited it for Coin Miner.
2	Apache Struts2(CVE-2021-31805)	A Chinese hacker organization exploited it for large-scale attacks.
3	PHPUnit(CVE-2017-22965)	Kinsing group exploited it for Coin Miner.
4	Oracle WebLogic(CVE-2021-2109)	A Chinese hacker organization exploited it for large-scale attacks.
5	ProxyLogon(CVE-2021-31805)	Tick APT group exploited it to attack East Asian countries.

[2022 and 2023 statistics on old vulnerabilities]

This year, various hacking groups are still steadily attempting attacks using old vulnerabilities. The number of attacks exploiting major vulnerabilities, such as ‘Log4j’, ‘Apache Struts2’, ‘PHPUnit’, ‘WebLogic’, and ‘ProxyLogon’, has increased overall compared to the previous year. About 240,000 ‘Log4j’ attacks, and 150,000 ‘Apache Structs2’ attacks were carried out. In particular, in the case of ‘PHPUnit’, although it was a vulnerability disclosed in 2017, about 10 times more events occurred compared to last year, showing that these old vulnerabilities are still actively used for attacks.

As a matter of fact, in the first half of this year, Chinese hacking groups Panda Intelligence Bureau (PIB), 1937cN, and Xiaoqiying carried out large-scale attacks using old vulnerabilities such as ‘Apache Struts2’ and ‘WebLogic’. In Korea, attacks were confirmed on corporate infrastructure servers, websites of public institutions, and homepages of organizations affiliated with the Ministry of Education, and in the process, there were incidents where some personal information was leaked. In addition, overseas cases that exploited ‘Log4j’ and ‘PHPUnit’ for cryptocurrency mining attacks (coin miners) have been reported, and the ‘ProxyLogon’ vulnerability targeting ‘Exchange Server’, which is used by many companies, is still used as an attack tool by the APT group. As these old vulnerabilities continue to occur, security personnel and related departments are required to pay attention to and monitor them continuously.

Monthly event detections in 2023



Source : SK Shieldus Secudium

List and cases of major vulnerabilities

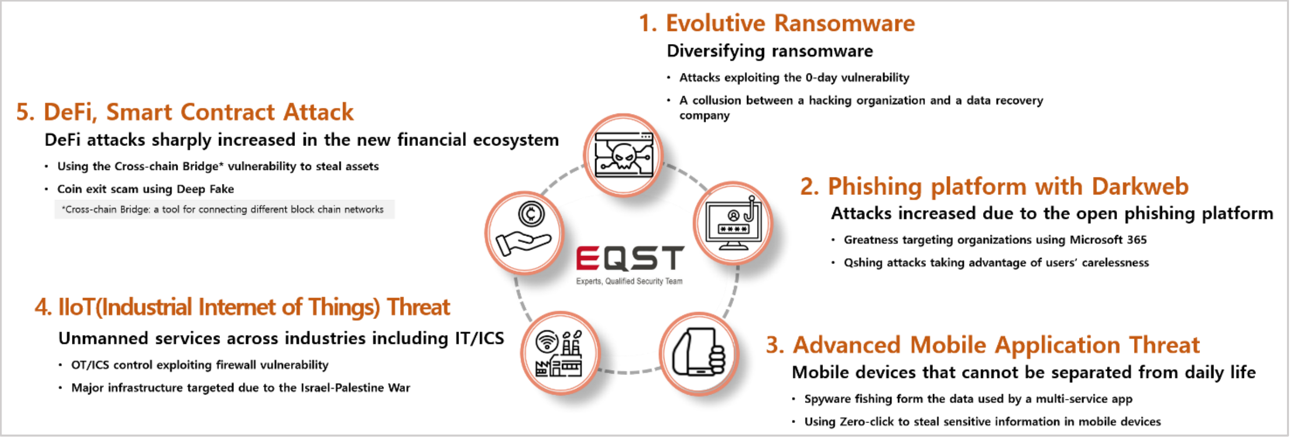
1	Zyxel OS Command Injection (CVE-2023-28771)	Exploited for attacks on key infrastructure
2	MOVEit SQL Injection (CVE-2023-34362)	Ransomware groups exploit 0-day vulnerability of enterprise solutions
3	GoAnywhere RCE (CVE-2023-0669)	
4	Papercut authentication bypass (CVE-2023-27350)	
5	Zimbra XSS (CVE-2023-37580)	Exploited for attacks on foreign government agencies

[2022 and 2023 statistics on old vulnerabilities]

This year's major new vulnerabilities, GoAnywhere (February), PaperCut (April), MOVEit (May), Zyxel (June), and Zimbra (July), were mainly discovered in the first half of the year, and as a result, many events were detected in the second half of the year. There is a spike in April and July, which is due to the influence of the MOVEit and Zyxel vulnerability. In April, the MOVEit attack using SQL Injection was prevalent, accounting for a high proportion of all events in which SQL Injection was detected. The Zyxel vulnerability, which was disclosed in June, is a firewall product-related vulnerability, and as the attack conditions are less stringent than other vulnerabilities, attacks on the overall network band have been carried out since July after the PoC was disclosed.

The vulnerability arising from the Zyxel firewall product was used to attack major infrastructure, and cases where overseas energy infrastructure was actually attacked, suffered damage, and used as a base for botnets were also reported. Attacks by ransomware groups using the 0-day vulnerability of solutions commonly used by companies, e.g., MOVEit, GoAnywhere, and PaperCut, were prevalent, and unlike existing methods, new vulnerabilities were used to inflict damage on more targets than before. There have been many cases where vulnerabilities occurring in Zimbra, a platform that provides e-mail, calendar, chat, and video services, were used to perform attacks on foreign government agencies. The 0-day vulnerability is occurring in various fields, and large-scale attacks targeting unpatched targets are carried out after the release of the PoC. So constant attention to the threat and periodic patching activities are required.

Review of security issues of 2023



1. Evolutive Ransomware

Diversifying ransomware

- Attacks exploiting the 0-day vulnerability
- A collusion between a hacking organization and a data recovery company

2. Phishing platform with Darkweb

Attacks increased due to the open phishing platform

- Greatness targeting organizations using Microsoft 365
- Qshing attacks taking advantage of users' carelessness

3. Advanced Mobile Application Threat

Mobile devices that cannot be separated from daily life

- Spyware fishing form the data used by a multi-service app
- Using Zero-click to steal sensitive information in mobile devices

4. IIoT(Industrial Internet of Things) Threat

Unmanned services across industries including IT/ICS

- OT/ICS control exploiting firewall vulnerability
- Major infrastructure targeted due to the Israel-Palestine War

5. DeFi, Smart Contract Attack

DeFi attacks sharply increased in the new financial ecosystem

- Using the Cross-chain Bridge* vulnerability to steal assets
- Coin exit scam using Deep Fake

*Cross-chain Bridge: a tool for connecting different block chain networks

[Review of security issues of 2023]

In the Evolutive Ransomware sector, the ransomware groups exploiting 0-day were active. Starting with a ransomware attack using the 'GoAnywhere' vulnerability of the 'Cl0p' Ransomware Group at the end of January 2023, a large number of activities of a ransomware group using the 'PaperCut' vulnerability were detected in April, and those using the 'MOVEit' vulnerability were detected in June. These vulnerabilities are vulnerabilities of print management software and file transmission software. In particular, the file transmission software 'MOVEit', which is widely used in overseas companies, has become the main target of ransomware groups. In addition, it has recently been confirmed that the 'Cl0p' Ransomware Group is carrying out ransomware attacks using 'SysAid' 0-day, which was discovered in November. So special caution is needed against ransomware attacks using this vulnerability.

In addition, a domestic data recovery company and a North Korea hacking organization 'Lazarus' colluded to distribute ransomware and extort money from victims. The data recovery company received the decryption key from the hacking organization in advance and promoted the decryption service. The victims who suffered ransomware damage from the hacking organization paid money to the data recovery company for decryption, and the data recovery company and the hacking organization divided the profits.

As the number of cases exploiting the 0-day vulnerability is increasing, and the attack trends are changing in a systematic/intelligent direction, individuals and companies must understand the latest trends and actively prepare preventive measures.

In the Phishing Platform with Darkweb sector, phishing attacks using 'PhaaS (Phishing-as-a-Service)' occurred. 'PhaaS' is a service-type phishing platform, which means an organized cyber crime that sells phishing kits in exchange for financial compensation. Following 'Caffeine', which was used in a large-scale phishing campaign last year, a 'PhaaS' platform called 'Greatness' targeting companies using Microsoft 365 was used this year. 'Greatness' is used for obtaining credentials and cookies to access Microsoft 365 accounts, and especially attracted attention as it can also handle accounts with multi-factor authentication (MFA) enabled. It is confirmed that this campaign mainly targeted manufacturing and medical companies located overseas, e.g., the US, the UK, and Australia.

Also, as people's ability to respond to phishing improves and the number of platforms that use QR codes, such as financial services and public bicycles, increases, 'Qshing' crimes using QR codes are increasing. Recently, cases of Qshing that induce banking deposits or target virtual currency have emerged in Korea. So special caution is needed in Korea as well.

In the Advanced Mobile Application Threat sector, a spyware attack targeting apps that provide multi-services was discovered. Due to the nature of apps that provide various services such as chatting, finance, and shopping on one platform, the various data collected and used are good prey for hackers. This year, the Chinese hacking group 'APT-41' conducted a campaign using a spyware called 'LightSpy' with the aim of stealing sensitive information on mobile devices. 'WeChat', which provides a variety of services such as Pay, SNS, and airline reservations, was one of the targets, and data used in 'WeChat', including payment data of 'WeChat Pay' and recordings of victims' conversations exploiting the audio function of 'WeChat', were targets of the attacks.

Continuing from last year, attacks using the Zero-click vulnerability occurred again this year. In April, 'QuaDream[12]' distributed the 'Reign' spyware using a Zero-click vulnerability called 'ENDOFDAYS'. This vulnerability is an exploit that occurs through the invitation function of iCloud Calendar. Although it was disclosed in 2021, it can be seen that it is still used against devices that have not been updated. Also, in September, the 'NSO' group used the 0-day vulnerability to distribute the 'Pegasus' spyware. This group carried out a Zero-click attack targeting iMessage last year using the 'FINDMYPWN', 'PWNYOURHOME', and 'LATENTIMAGE' exploits. This year, it was revealed that this group used a new exploit called 'BLASTPASS' to carry out a Zero-click attack.

[12] QuaDream: An Israeli company that sold iPhone hacking tools: it has now ceased operations.

While old Zero-click Exploits targeting vulnerable devices are used, new attacks using new Zero-click Exploits are constantly discovered. Users must continuously perform the latest security updates and pay special attention.

In the IIoT (Industrial Internet of Things) Threat sector, attacks targeting major infrastructure have become a major issue due to the Israel-Palestine War. Attackers mainly used firewall and router vulnerabilities to perform attacks, and aimed to control industrial systems by obtaining internal network access privileges. In addition, it was revealed that a hackers group used the 'Zyxel' firewall vulnerability to attack major energy infrastructure facilities in Denmark, infected them with a botnet, and then used this as a base to carry out DDoS attacks in other countries, e.g., the United States and Hong Kong. This can be seen as a case of not simply controlling a country's major infrastructure, but also carrying out additional attacks targeting other countries using that infrastructure as a base.

As the Israel-Palestine conflict broke out this year following the Russia-Ukraine war last year, cyber wars between countries are continuing. As industrial infrastructure is becoming a major target in cyber wars between countries, it seems necessary to make preparations by reviewing the security vulnerabilities of the industrial infrastructure system and continuously monitoring attacks.

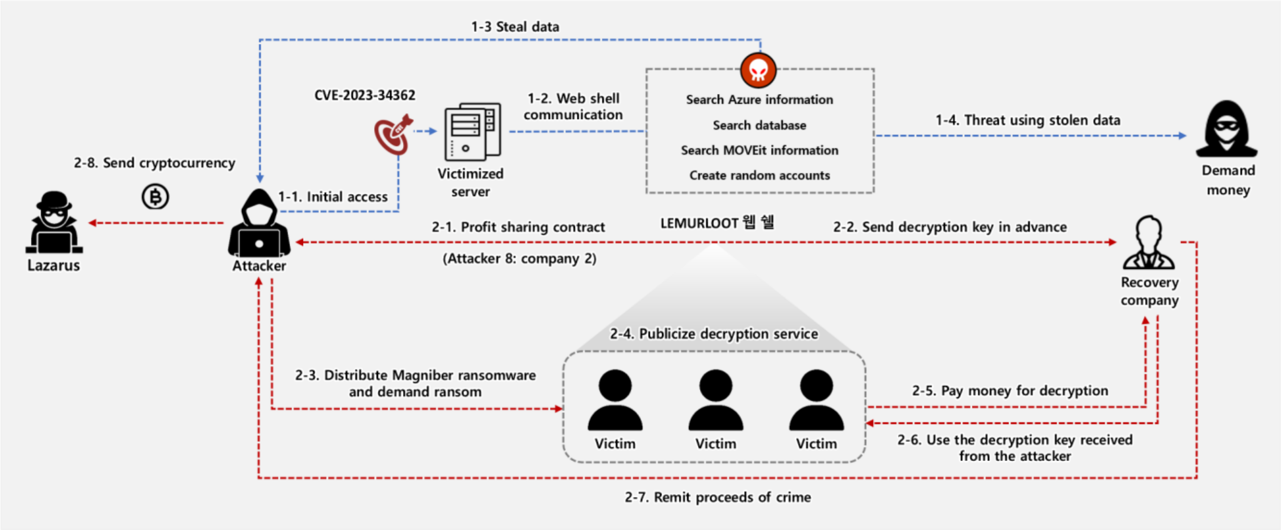
In the DeFi and Smart Contract Attacks sector, attacks targeting cryptocurrency are continuously occurring. In the first half of this year, a large-scale hacking worth $200 million occurred in the DeFi protocol 'Euler Finance'. Then, in July, a loss of approximately $125 million was incurred due to hacking of the 'multi-chain' bridge, a cross-chain bridge protocol, and in November, a loss of approximately $86.6 million was incurred due to the hacking of the 'HECO' bridge.

In addition, an 'exit scam' targeting virtual currency investors occurred. An 'exit scam' is a technique that designs a coin for the purpose of fraud, promotes the coin to induce investment, and then exchanges the coin to make a profit when the value of the coin increases due to the victims' investment. Unlike in the past when promotions were carried out by hired actors, the recent trend is such that advanced attacks are performed on investors by abusing deepfakes, which have become more sophisticated due to recent developments in AI technology.

Therefore, developers must insert an tamper-proof watermark into commercial deepfake-related models to prevent exploitation, and general users need digital literacy[13] education and enhance their security awareness to identify deepfakes.

[13] Digital Literacy: An individual's ability to find clear information from a variety of media, evaluate and combine it

■ Ransomware attack scenario


1-3 Steal data
CVE-2023-34362
1-2. Web shell communication
Search Azure information
Search database
Search MOVEit information
Create random accounts
1-4. Threat using stolen data
Demand money
2-8. Send cryptocurrency
Victimized server
1-1. Initial access
Lazarus
Attacker
2-1. Profit sharing contract
(Attacker 8: company 2)
LEMURLOOT 웹 쉘
2-2. Send decryption key in advance
Recovery company
2-4. Publicize decryption service
2-3. Distribute Magniber ransomware and demand ransom
Victim
Victim
Victim
2-5. Pay money for decryption
2-6. Use the decryption key received from the attacker
2-7. Remit proceeds of crime

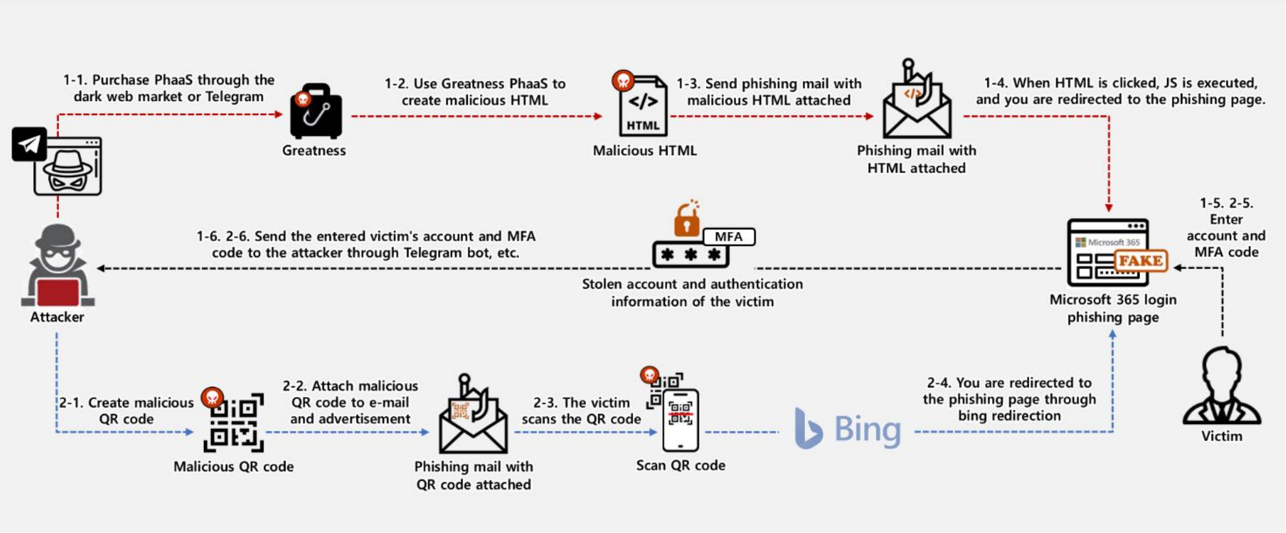
[Ransomware attack scenario]

The first scenario is an attack scenario that exploits the 'Progress MOVEit Transfer' vulnerability of 'Cl0p'. The attack was carried out after uploading a web shell named 'LEMURLOOT' to the MOVEit server through the SQL Injection vulnerability CVE-2023-34362. LEMURLOOT acts as a kind of backdoor, and was used to steal credentials including Microsoft Azure information from the victimized server and create random accounts to steal administrator privileges. After stealing key information, they attempted to blackmail victims by posting it on the dark web. A supply chain attack is possible in a relatively easy way, making it one of the large-scale attack scenarios.

The second scenario is the 'Magniber' ransomware attack scenario of the North Korean hacking organization 'Lazarus', which colluded with a domestic data recovery company. The attacker colludes with a domestic data recovery company to distribute ransomware, and the data recovery company, which has received the decryption key in advance, promotes a decryption service to victims infected with ransomware to lure victims. The recovery company performs decryption using the decryption key received from the attacker in advance and demands a decryption fee equal to the ransom amount, and divides the profits with the attacker at a ratio of 8:2. Considering that the distributed proceeds of crime were sent to Lazarus in cryptocurrency, it is presumed that it was Lazarus's doing. The crime, which occurred 730 times, resulted in proceeds of crime to the tune of approximately KRW2.6 billion, and ultimately led to the arrest of the data recovery company's CEO and employees.

Ransomware trends are continuously changing, e.g., large-scale supply chain attacks by ransomware groups and attacks exploiting vulnerabilities are increasing, and recovery companies and crime groups are colluding to infect ransomware. To prevent this, effective countermeasures must be established in line with the latest ransomware trends and attack techniques.

Phishing attack scenario


1-1. Purchase PhaaS through the dark web market or Telegram
Greatness
1-2. Use Greatness PhaaS to create malicious HTML
HTML
Malicious HTML
1-3. Send phishing mail with malicious HTML attached
Phishing mail with HTML attached
1-4. When HTML is clicked, JS is executed, and you are redirected to the phishing page.
1-5. 2-5. Enter account and MFA code
Microsoft 365
FAKE
Microsoft 365 login phishing page
1-6. 2-6. Send the entered victim's account and MFA code to the attacker through Telegram bot, etc.
MFA
Stolen account and authentication information of the victim
Attacker
2-1. Create malicious QR code
Malicious QR code
2-2. Attach malicious QR code to e-mail and advertisement
Phishing mail with QR code attached
2-3. The victim scans the QR code
Scan QR code
Bing
2-4. You are redirected to the phishing page through bing redirection
Victim

[Phishing attack scenario]

Unlike general phishing methods, cases of attacks exploiting PhaaS (Phishing-as-a-Service) and QR codes are increasing. The detailed scenario is as follows:

The first scenario is an attack method that steals the victim's account through a phishing kit. The attacker first uses 'Greatness', a PhaaS (Phishing-as-a-Service) kit purchased through the dark web or Telegram, to create malicious HTML that induces the victim's execution, such as quotes and statements, and sends them as attachments to mail. When the victim clicks on the HTML file of the phishing mail, the JS code[14] written by the attacker is executed and the victim is redirected to the fake Microsoft 365 login page, which is the phishing page.

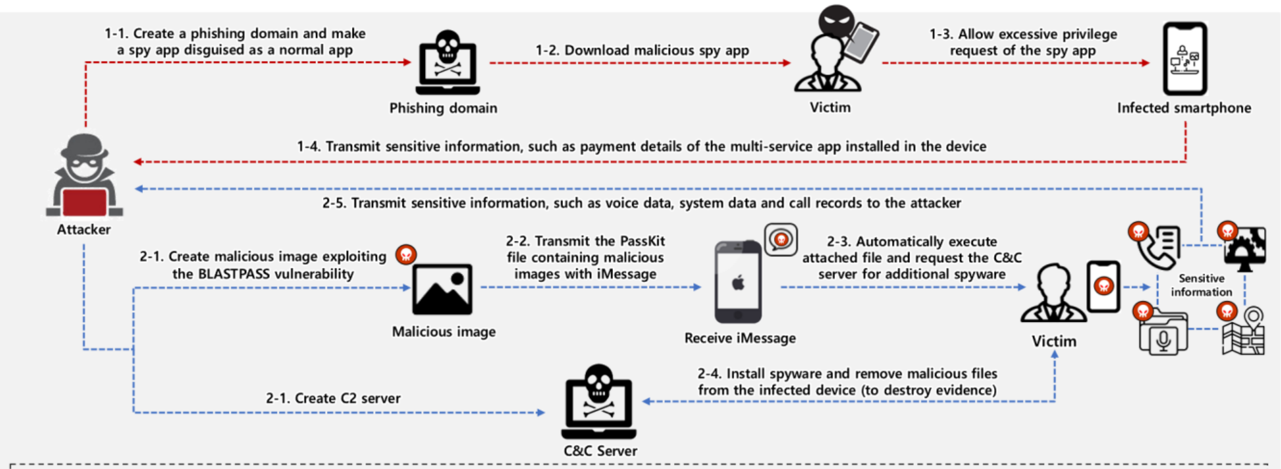
The second scenario is a phishing attack using malicious a QR code. The attacker creates a malicious QR code and sends it through mail, advertisements, etc. When the victim scans the attached QR code, he or she is connected to a phishing URL, and the site induces him or her to download a malicious app or enter personal information. This scenario exploits the Bing Redirection URL[15], and when a malicious QR code is scanned, it connects to a trusted URL bing.com/ck/a, and the victim's suspicion can be minimized.

Lastly, the attacker can steal the account and MFA code that the victim entered on the phishing page, then log in to the Microsoft 365 service and obtain the victim's privileges. Phishing attacks continue to develop by taking advantage of the victim's situation and psychology. Users should pay attention to verifying the sender's identity when viewing mail to minimize damage caused by malicious links or files.

[14] JS code: Codes written in Javascript, a programming language used to create web pages

[15] Bing Redirection URL: This is a service provided by Microsoft that allows you to create a URL that redirects to Bing to connect to a sales or affiliated page.

■ Mobile attack scenario


1-1. Create a phishing domain and make a spy app disguised as a normal app
Phishing domain
1-2. Download malicious spy app
Victim
1-3. Allow excessive privilege request of the spy app
Infected smartphone
1-4. Transmit sensitive information, such as payment details of the multi-service app installed in the device
Attacker
2-5. Transmit sensitive information, such as voice data, system data and call records to the attacker
2-1. Create malicious image exploiting the BLASTPASS vulnerability
Malicious image
2-2. Transmit the PassKit file containing malicious images with iMessage
Receive iMessage
2-3. Automatically execute attached file and request the C&C server for additional spyware
Victim
Sensitive information
2-1. Create C2 server
C&C Server
2-4. Install spyware and remove malicious files from the infected device (to destroy evidence)

- **BLASTPASS vulnerability**: a vulnerability that can exploit malicious image files without the victim's interaction
- **PassKit**: When adding a signature to the device's Wallet, or authentication is needed, this file makes it possible to display the time and place on the screen, and use the push alarm function.

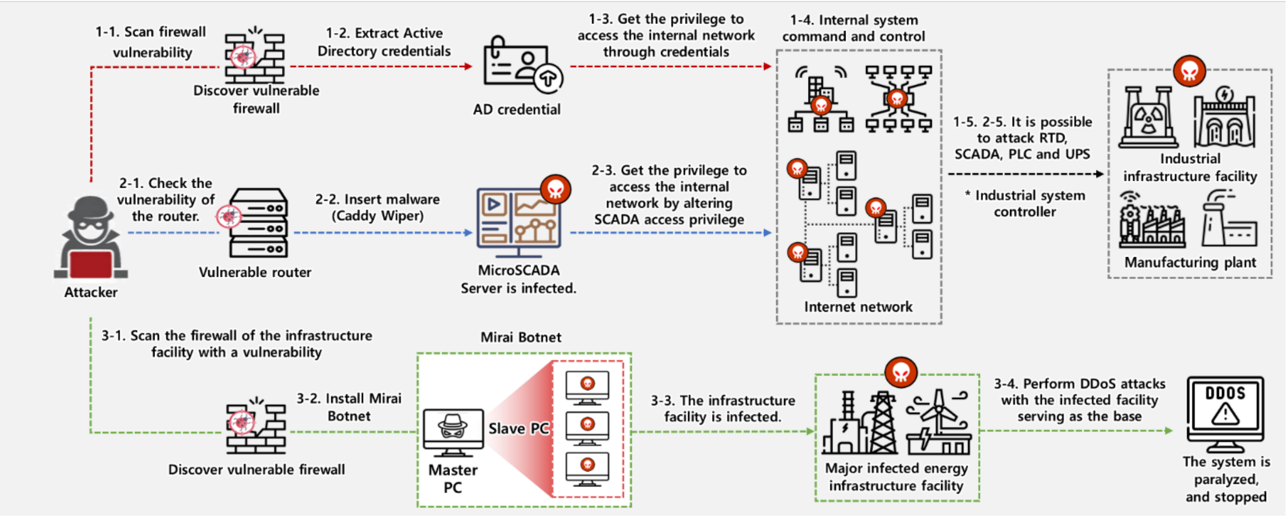
[Mobile attack scenario]

As apps supporting multiple services in one app became popular, attacks targeting them and Zero-click attacks that broke down existing response strategies became prevalent.

The first scenario is a spy app installation scenario targeting multi-service apps. The attacker confuses the victim by creating a phishing site and a spy app disguised as a normal app. When the victim downloads and runs a spy app from a phishing site, a request is forced on the victim to allow privileges outside of the required range. The smartphone infected this way steals important information such as payment details and integrated login information of apps that support multi-services from the list of apps installed on the device and transmits it to the attacker. Because it supports multiple services, the damage can increase and it is highly likely to become a target of attacks in the future. Therefore, you should be careful not to download apps from unknown sources, and be careful not to use the same account for multiple sites as this can be a threat factor.

The second scenario is the Zero-click attack scenario. The attacker creates a malicious image that can be exploited without interaction and a C&C (Control & Command) server that delivers commands to the victim. Then, the attacker includes a malicious image in the PassKit file and sends an iMessage to the victim. When the victim opens the iMessage, the PassKit file is automatically executed and the vulnerability included in the malicious image is activated. On the victim's mobile device, spyware is installed from the attacker's C&C server and malicious files are removed to destroy evidence. Therefore, it is difficult for the victim to determine whether his or her mobile device is infected. Afterwards, the attacker can continuously steal sensitive information such as the victim's voice information, system information, and call records.

■ OT/ICS scenario



1-1. Scan firewall vulnerability
Discover vulnerable firewall
1-2. Extract Active Directory credentials
AD credential
1-3. Get the privilege to access the internal network through credentials
1-4. Internal system command and control
1-5. 2-5. It is possible to attack RTD, SCADA, PLC and UPS
* Industrial system controller
Industrial infrastructure facility
Manufacturing plant
2-1. Check the vulnerability of the router.
Vulnerable router
Attacker
2-2. Insert malware (Caddy Wiper)
MicroSCADA Server is infected.
2-3. Get the privilege to access the internal network by altering SCADA access privilege
Internet network
3-1. Scan the firewall of the infrastructure facility with a vulnerability
3-2. Install Mirai Botnet
Discover vulnerable firewall
Mirai Botnet
Master PC
Slave PC
3-3. The infrastructure facility is infected.
Major infected energy infrastructure facility
3-4. Perform DDoS attacks with the infected facility serving as the base
DDOS
The system is paralyzed, and stopped

[OT/ICS attack scenario]

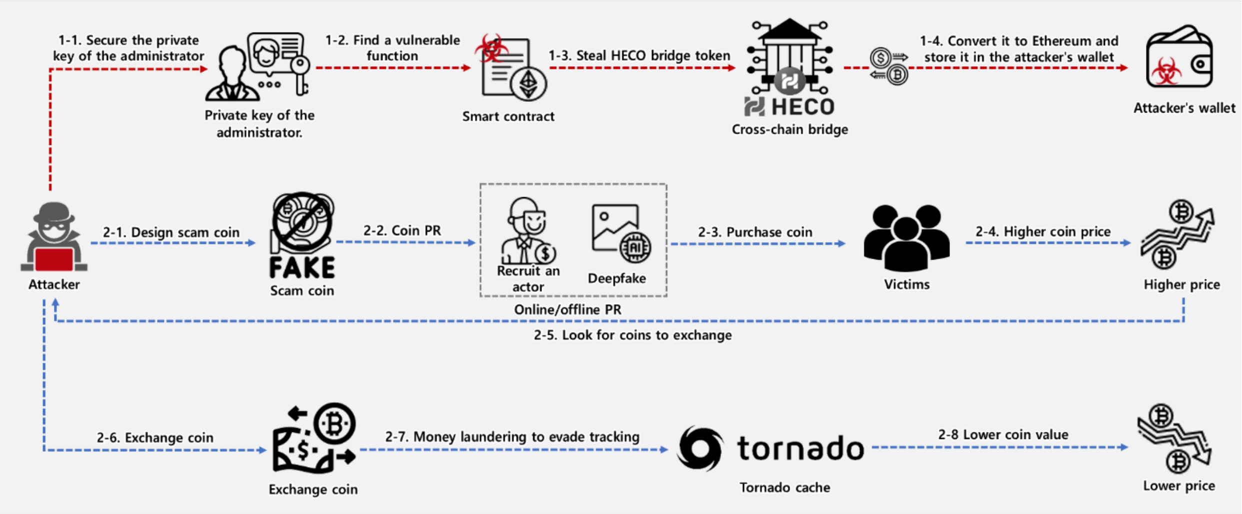
OT/ICS cyber attacks are increasing due to the digitalization of industrial facilities. The detailed scenario is as follows: The first scenario is an attack method that attacks the firewall vulnerability and takes control of the industrial system controller. The attacker gains privileges to access the internal network through AD credentials extracted through a vulnerable firewall.

The second scenario is an attack method that attacks the router vulnerability and takes control of the industrial system controller. When an attacker inserts malware called 'Caddy Wiper' into the MicroSCADA Server through the router's vulnerability, it modifies the SCADA's access privileges to obtain privileges to access the internal network. In both scenarios, you can control the internal system and issue commands through the acquired internal network access privilege. Through this, it is possible to attack controllers that control industrial systems such as RTU, SCADA, PLC, and UPS, altering data of industrial infrastructure or manufacturing plants, or causing service interruption.

The third and last scenario is an attack method that attacks the firewall vulnerability of major infrastructure and takes control of the industrial system controller. The Mirai Botnet is installed through the facility firewall vulnerability scanned by the attacker. The botnet makes it possible to use major energy infrastructure facilities infected with malicious programs as a base to perform DDoS attacks to paralyze or stop systems connected to those facilities.

If an infection occurs, it can lead to serious problems such as losses and recovery costs due to factory production interruption, safety incidents due to facility malfunctions, and decreased product reliability due to data tampering. Furthermore, it can lead to a threat to the company's stability and intellectual property. Therefore, to prepare for this, strong cyber security measures must be prepared and periodic audits are necessary.

■ Virtual asset attack scenario



[Virtual asset attack scenario]

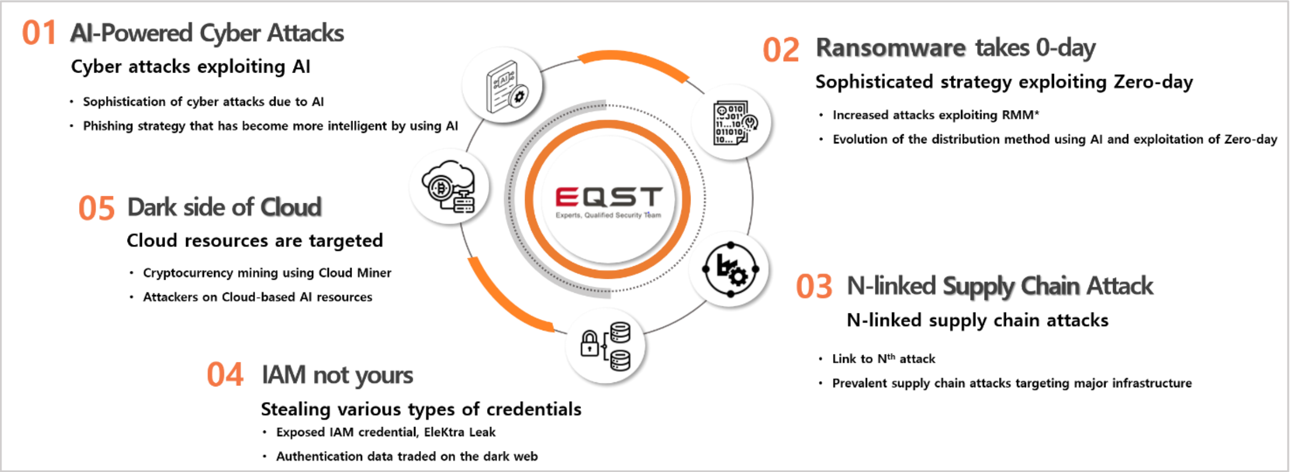
Attacks based on virtual assets are one of the areas that attackers still pay attention to because the scale of damage is large when damage occurs.

The first scenario is a scenario that causes damage by stealing the vulnerable function and private key in the HECO bridge. The attacker secures the administrator's private key through phishing, Trojan horses, etc. An attacker who obtains the administrator's private key discovers a vulnerable function in the HECO bridge's smart contract that can automatically withdraw funds with the administrator privilege. Therefore, the attacker withdraws a number of coins from the cross-chain bridge to the attacker's wallet through the administrator's private key and the vulnerable function. As the cross-chain bridge contains a mix of code areas where mistakes can occur and complex transactions, extra caution is required. You must be careful not to leak important information such as access keys or private keys.

The second scenario is an adaptation of the FSLtoken's Exit Scam scenario. The attacker creates 100 million scam coins for fraud. To sell 3 million of the 100 million coins to the victim at a high price, the attacker promotes them by using deepfake videos of certain celebrities and recruiting actors. Afterwards, when misled victims purchase scam coins on the exchange, the transaction volume increases and the price of scam coins rises. When the price of the scam coin reaches the attacker's target amount, the attacker exchanges all remaining coins into other coins. Then, in order to launder the source of the exchanged funds, the funds are laundered through Tornado Cash, one of the Crypto Mixers[16]. As a result, the price of the scam coin drops rapidly, causing financial damage to victims.

[16] Cypto Mixer: It is a device to achieve decentralization by keeping transaction details private, but it is exploited for money laundering.

Forecast for top five cyber threats in 2024



01 AI-Powered Cyber Attacks

Cyber attacks exploiting AI

- Sophistication of cyber attacks due to AI
- Phishing strategy that has become more intelligent by using AI

02 Ransomware takes 0-day

Sophisticated strategy exploiting Zero-day

- Increased attacks exploiting RMM*
- Evolution of the distribution method using AI and exploitation of Zero-day

03 N-linked Supply Chain Attack

N-linked supply chain attacks

- Link to N^th^ attack
- Prevalent supply chain attacks targeting major infrastructure

04 IAM not yours

Stealing various types of credentials

- Exposed IAM credential, EleKtra Leak
- Authentication data traded on the dark web

05 Dark side of Cloud

Cloud resources are targeted

- Cryptocurrency mining using Cloud Miner
- Attackers on Cloud-based AI resources

[Cyber threat forecast in 2024]

■ AI-Powered Cyber Attacks

- Cyber attack exploiting artificial intelligence

Recent developments in artificial intelligence (AI) technology have brought innovation to many industrial fields, but in the cyber security field, it is also exploited for various malicious purposes such as phishing and creation of malware. In particular, the LLM (Large Language Model) model, which has recently been attracting attention, is trained using a vast data set and is useful for writing sophisticated phishing mail due to its excellent characteristics in various natural language processing tasks.

As a matter of fact, 'WormGPT', a generative AI based on the LLM model created for malicious purposes, has emerged and is used for various cyber attacks. In particular, it is known that it can perform a sophisticated BEC (Business Email Compromise) attack[17] by analyzing public data and creating a persuasive malicious e-mail tailored to the recipient.

In addition, deepfake and deep voice technologies, which are so sophisticated that they are difficult to distinguish from the real thing, are exploited in numerous phishing attacks. In particular, deep voice technology has developed to the point where it is possible to replicate someone else's voice even if there is only a few seconds of voice, and cases of deep voice phishing damage are occurring frequently in Korea as well.

As AI technology develops, advanced cyber attacks using services (e.g., WormGPT) tailored to cyber attacks are expected to occur. In particular, as linguistic limitations such as grammatical errors and lack of context issues in AI-generated data are resolved, it becomes grammatically more natural. It is expected that increasingly sophisticated phishing attacks will become more prevalent.

[17] BEC attack: An attack that induces the leak of sensitive information by disguising itself as an email sent from an organization or official that the victim usually trusts.

■ Ransomware takes 0-day

- Enhancement of the strategy exploiting 0-day

Recently, the frequency of using the commercial RMM (Remote Monitoring and Management) tool is increasing for bypassing the detection of ransomware attacks and for the sake of convenience. RMM is a monitoring and management tool for remotely accessing and controlling the system, and is mainly used by companies to reduce maintenance costs and for access to resolve system problems. Although it contains a function that can be exploited for internal diffusion, it is classified as a normal activity and is not easily detected. So many ransomware groups are exploiting it.

In addition, as AI technology develops, the method of ransomware distribution is expected to change more intelligently. It is expected that the existing form of targeted phishing will evolve into phishing that exploits AI, and this will evolve into a form that will make it more difficult for users who receive mail to be suspicious, which will likely lead to an increase in ransomware attacks.

Existing ransomware groups focused on APT attacks targeting specific organizations, but recently they are shifting to large-scale attacks by exploiting the 0-day vulnerability of commercial solutions such as 'MOVEit', 'GoAnywhere', and 'PaperCut'. As these solutions are used by many companies and organizations, it is possible to use a single vulnerability to perform multiple attacks, making them targets of attackers. Large-scale attacks by ransomware groups exploiting vulnerabilities are expected to continue in 2024 as well.

■ N-linked Supply Chain Attacks

- N-linked supply chain attacks

The core risk of a supply chain attack lies in the possibility of linking it to the N^th attack. It means that simply one company or network is targeted, but the attack spreads to multiple companies that use the product of that company or are connected to its network.

These chain attacks are mainly carried out through the software supply chain or the network of the service provider or partner. The attack on the enterprise software '3CX' supply chain that occurred in April of this year can be seen as an example of the first N-linked supply chain attack that led from the first software (X_TRADER) supply chain attack to the second software (3CX) supply chain attack.

Supply chain attacks mainly target solutions used by multiple organizations, and this is very dangerous because the targeted company cannot respond immediately and they can cause a lot of damage through a single attack point.

Also, with the outbreak of the Israel-Palestine War this year following the Russia-Ukraine War last year, major infrastructure attacks through supply chain attacks are increasing. As cyber warfare between countries continues, new supply chain attacks targeting companies and major global infrastructure are expected to continue to occur.

■ IAM not yours

– Various forms of credentials are stolen.

The issue of credentials has always been an important issue every time, and credentials are stolen in various ways.

Because division of labor is the norm in most companies, account information, IAM credentials, etc. are often stored in collaboration platforms such as GitHub and GitLab. At this time, caution is required as the administrator's mistake often causes credentials to be stored in a repository[18] that is open to all users. Recently, attackers have been carrying out the 'EleKtra Leak' campaign to steal credentials by exploiting these mistakes. So special caution is required.

In addition to the developer's mistake, credentials stored on a personal PC may be leaked through phishing or malware, resulting in secondary or tertiary damage. As leaked information can be traded on the dark web and used for initial access, it is important to set up additional authentication factors in addition to basic authentication.

Even if you use the IAM platform that provides a login and identity management system, attacks targeting the vulnerability of the IAM provider, or hijacking the company's administrator account continue to occur. So there is no perfect defense.

As the business environment becomes more complex and credentials exposure paths become more diverse, cyber attacks aimed at stealing and exploiting credentials will continue in 2024 as well.

[18] Repository: A repository where developers can systematically store and work on project codes

■ Dark side of Cloud

– Targeted cloud resources

As attackers' understanding of the cloud increases, cyber attacks utilizing cloud infrastructure or platforms are increasing.

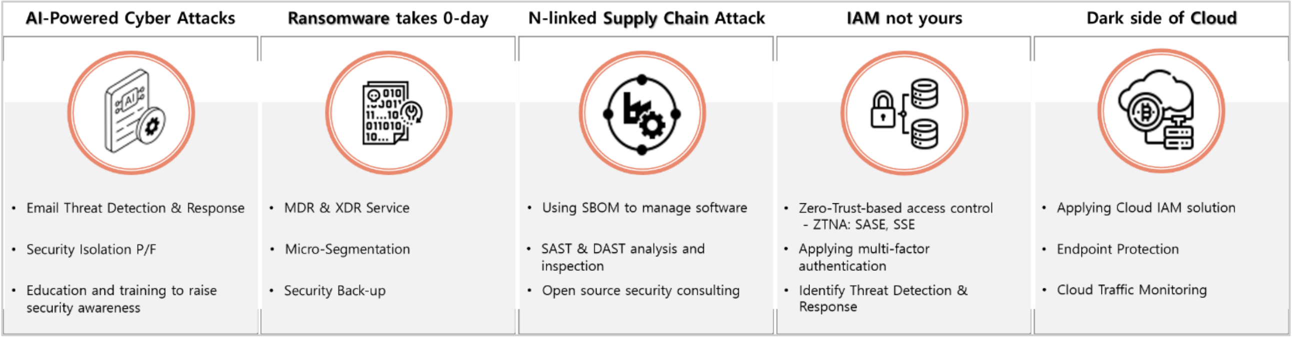
This year, many 'cloud mining' attacks that exploit cloud services to mine cryptocurrency occurred. Cloud mining is a technique for mining cryptocurrency through cloud resources. Unlike the existing mining attack that accessed the user's PC, it is currently changing to a form stealing cloud resources to perform mining attacks.

Also, when companies provide generative AI services, they are using cloud-based GPUs in order to learn vast amounts of data or efficiently manage resource costs that change rapidly in real time depending on the influx of users.

As the number of companies using the cloud environment increases and the types of resources each company uses become more diverse, it is expected that cloud resources exposed to the attack surface will continue to be exploited for intelligent attacks such as cryptocurrency mining and corporate data leaks. To respond to this, companies need to discuss advanced cloud security measures such as cloud solutions, endpoint protection, and cloud traffic monitoring.

Response strategies

■ EQST's top five threat response strategies and services



AI-Powered Cyber Attacks	Ransomware takes 0-day	N-linked Supply Chain Attack	IAM not yours	Dark side of Cloud
• Email Threat Detection & Response	• MDR & XDR Service	• Using SBOM to manage software	• Zero-Trust-based access control - ZTNA: SASE, SSE	• Applying Cloud IAM solution
• Security Isolation P/F	• Micro-Segmentation	• SAST & DAST analysis and inspection	• Applying multi-factor authentication	• Endpoint Protection
• Education and training to raise security awareness	• Security Back-up	• Open source security consulting	• Identify Threat Detection & Response	• Cloud Traffic Monitoring

[Top 5 threat response strategies]

As cyber attacks began to use AI, e.g., spear phishing, phishing attacks exploiting deepfakes/deep voices, they are becoming more sophisticated and intelligent. We must now acknowledge that cyber attacks exploiting AI are not a story in a movie, but a problem we face in reality. In order to respond to advanced phishing attacks, it is important to minimize threats by performing real-time threat monitoring and blocking malicious mail through the ETDR (Email Threat Detection & Response) solution. Additionally, if you build an e-mail isolation platform, you can create a safe environment by first isolating malicious links and contents contained in e-mails and sending only trustworthy contents to users. More than anything else, because phishing attacks are becoming more sophisticated as they take advantage of the user's situation and psychology, you must be aware that you are exposed to the risk of phishing attacks through security awareness-raising education and training, and pay attention to verifying the sender's identity.

Recently, ransomware groups are carrying out attacks using advanced strategies. In order to respond to this, we must strengthen security through the Managed Detection & Response (MDR) service, which can produce maximum effects with minimum costs as it updates IOC (Indicator of Compromise) in real time based on the combination of the XDR (Extended Detection &Response) service, which detects and analyzes threats occurring across the cloud, and the know-how of experts. Additionally, it is necessary to control and limit network access using the Micro-Segmentation technique, which segments and isolates the network when a work environment is configured. This allows security control to be implemented for each segment, and when infringement incidents occur, it does not affect other segments, thus minimizing the extent of damage. Lastly, you should protect important data by performing periodic backups on reliable systems.

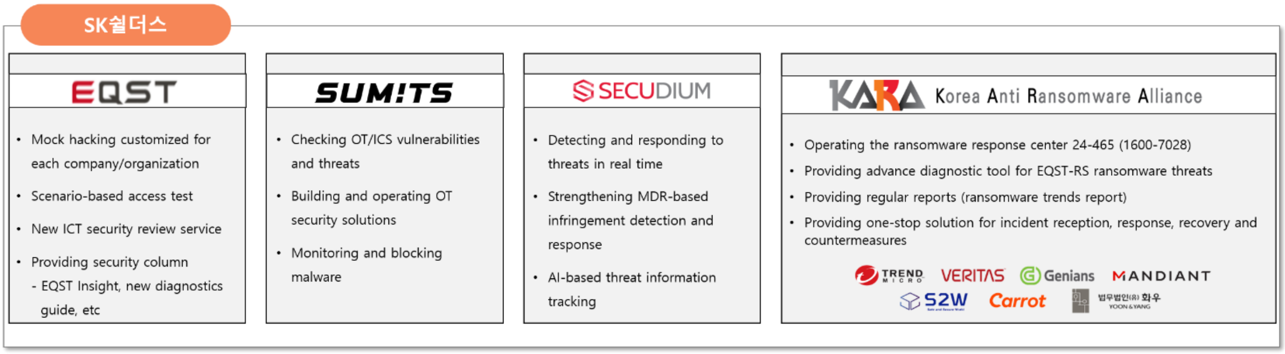
Supply chain attacks are becoming a good target for hacking groups, and are causing greater damage through Nth infections. To respond to this, you must identify the potential risks throughout the software you are using by referring to SBOM (Software Bill of Materials). SBOM refers to a list that describes detailed information about software you are using, such as versions and libraries. When a new vulnerability is disclosed, you can look at the SBOM to find and analyze files affected by the vulnerability, and take quick action. Also, periodic updates and verification of SBOM are necessary to enable correct response in real time. When developing new modules and software, you can first explore and prevent vulnerabilities that may occur during the development and operation stages through SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing). If you are using open source, security consulting must be performed to ensure safe use.

To deal with various forms of threats about theft of credentials, access control to credentials must be strengthened by establishing a Zero-Trust-based environment based on the premise of 'trusting nothing'. Unnecessary access to data and resources can be blocked by applying ZTNA (Zero-Trust Network Access), a technology that implements a Zero-Trust environment. Unlike VPN, which is designed to provide access privileges to all users across the network, ZTNA frequently requires re-authentication and does not grant privileges to unauthorized users. ZTNA can be implemented through Zero-Trust related frameworks, i.e. SASE (Secure Access Service Edge)[19] and SSE (Security Service Edge)[20]. Additionally, security must be strengthened by requiring a high level of authentication, such as multi-factor authentication, which requires two or more types of authentication when a user accesses the system. Above all, it is necessary to establish a strict security policy tailored to each corporate environment, apply segmented access control, and pay continuous attention and performing monitoring from a administrative perspective rather than simply relying on solutions.

[19] SASE (Secure Access Service Edge): It is one of the frameworks for implementing a zero trust architecture. It integrates traditional networking and cloud-native security functions.

[20] SSE (Security Service Edge): It is a component of the SASE framework. It is a definition of security policy decision and enforcement excluding WAN.

As the cloud environment becomes more common, companies are using the cloud in various ways, such as cloud-based GPUs for generative AI. Accordingly, attackers are also introducing advanced strategies tailored to the cloud environment. Previously, the main purpose was to steal data through IAM privilege theft, but it has now evolved into an attack that combines data theft and mining. In order to respond to this, security must be strengthened through access privilege management for users and resources by applying the IAM credentials solution provided by the cloud service. Also, periodic IAM credentials solution auditing is required. In addition to credentials, it is necessary to apply the Endpoint Protection function that can detect and respond to threats in real time to prepare for cases where an attacker directly attacks cloud resources. By enabling the Traffic Monitoring function, you can take prompt action when abnormal signs are detected in the cloud environment.



EQST

- Mock hacking customized for each company/organization
- Scenario-based access test
- New ICT security review service
- Providing security column
  - EQST Insight, new diagnostics guide, etc

SUMiTS

- Checking OT/ICS vulnerabilities and threats
- Building and operating OT security solutions
- Monitoring and blocking malware

SECUDIUM

- Detecting and responding to threats in real time
- Strengthening MDR-based infringement detection and response
- AI-based threat information tracking

KARA Korea Anti Ransomware Alliance

- Operating the ransomware response center 24-465 (1600-7028)
- Providing advance diagnostic tool for EQST-RS ransomware threats
- Providing regular reports (ransomware trends report)
- Providing one-stop solution for incident reception, response, recovery and countermeasures

[SK Shieldus response service]

SK Shieldus provides a variety of customized services to respond to the threats previously forecast. The white hacker group EQST performs customized mock hacking for each company/organization based on threat scenarios and diagnosis methodologies for various industries, including New ICT areas such as IoT and cloud, and provides guidance optimized for each corporate environment. In addition, to help security managers and related workers identify the latest trends and respond preemptively, it is providing various security columns containing new vulnerability analysis and technology research results free of charge through its official website.

In the OT/ICS field, where security threats are occurring continuously, it is necessary to build and operate a solution suited to the environment through customized security consulting to monitor and block threats in real time. SK Shieldus provides a threat inspection service specialized for OT/ICS using the intelligent convergence security platform SUMiTS.

In addition, the Secudium Center, our cybersecurity control center, detects security threats in real time and blocks threats in advance based on MDR, and provides detection and response services for intelligent cyber threats through AI-based tracking of threat information.

In order to quickly identify ransomware threats, it is necessary to identify the latest ransomware attack trends and quickly recognize them. SK Shieldus provides regular reports containing the latest ransomware trends and distributes 'EQST-RS', a tool that can diagnose ransomware threats in advance, for free. Individuals and companies can use this to effectively establish initial measures to respond to ransomware.

Also, in order to respond to the various changing ransomwares mentioned above, ransomware-specific services and solutions tailored to the characteristics of the company are needed. For quick response and recovery, SK Shieldus operates the Korea Anti Ransomware Alliance (KARA), a ransomware response council, and provides a one-stop integrated response process that handles all processes necessary for responding to ransomware. Additionally, SK Shieldus operates a ransomware response center (1600-7028) that can respond to ransomware 24 hours a day throughout the year.

■ Closing

Looking at cybersecurity trends in 2023, we can see that the emergence of generative AI has led to advancement and sophistication, and that the number of ransomware groups actively utilizing 0-day as well as old vulnerabilities has increased. In addition, we can see that the types of attacks have become more diverse, e.g., the N-linked supply chain attacks through enterprise solutions.

EQST is conducting research not only in the existing security field, but also in the generative AI field, which has been the biggest topic this year, and cloud. Since its establishment in 2017, EQST has been leading various activities such as 'mock hacking', 'new technology research', 'hacking program development and construction', 'ransomware response', 'new vulnerability analysis and diagnosis', and 'hacking education', and is planning to continue researches in new areas as well.

EQST

Annual Report

2023.12

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 Communication Group