Keep up with Ransomware

LockBit is back, unfinished ransomware attacks

■ Overview

In February 2024, damage cases due to ransomware attacks increased by about 40% to 418 cases compared to the previous month (299 cases). Despite the continuous arrests of attackers, cases of ransomware damage are steadily increasing. The most noteworthy issue in this situation is that the infrastructure of the ransomware as a service (RaaS[1)]) group LockBit has been reported to have been neutralized by agencies from 11 countries, including the FBI[2], NCA[3], and Europol[4], but LockBit resumed its activities by disclosing a new dark web leak site in just 5 days.

LockBit, which first appeared in 2019, is expanding its influence through continuous updates and has grown into a ransomware group that has caused the most damage since 2022. Despite its long period of activity and influence, LockBit has not been able to operate stably due to the absence of core developers, abnormal data leaks, and settlement errors between affiliates. However, it is thought of as a ransomware group that exerts global influence, and is receiving attention from several national institutions. However, on February 20, 2024, Operation Cronos[5], a coordinated effort by international law enforcement agencies, seized parts of LockBit's infrastructure, and LockBit's dark web leak site was placed under the control of a law enforcement agency until its closure.

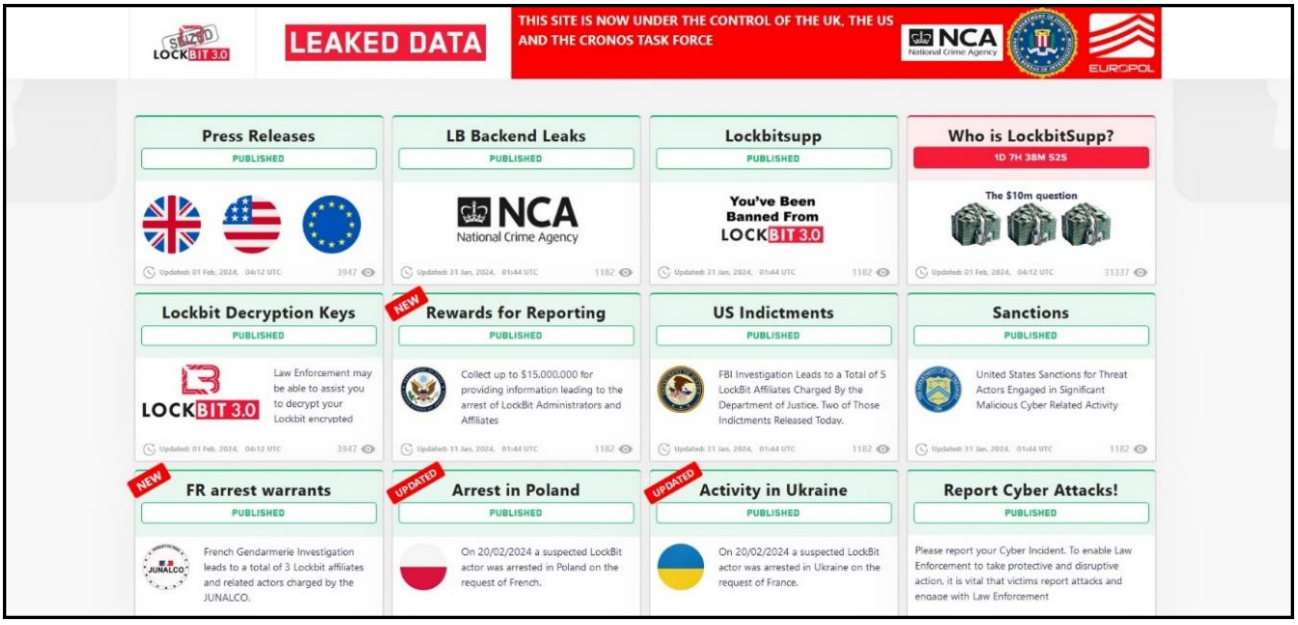
[1] RaaS (Ransomware-as-a-Service): A form in which ransomware groups provide ransomware to affiliates or attackers in exchange for compensation

[2] FBI (Federal Bureau of Investigation): A law enforcement agency within the U.S. Department of Justice

[3] NCA (National Crime Agency): The National Crime Agency, a law enforcement agency within the British Home Office

[4] Europol: A law enforcement agency of the European Union (EU)

[5] Operation Cronos: A Cyber Disruption Operation to Disrupt LockBit's Criminal Ecosystem



Source: Seized LockBit 3.0 ransomware group data leak site

LockBit officials were arrested in Poland and Ukraine by investigative agencies, and various accounts used in attacks were also suspended. In the process, information such as the source codes of the LockBit infrastructure and affiliate information, LockBit-NG-Dev (LockBit-NextGeneration-Development) ransomware, which is believed to be LockBit 4.0, its similarities to existing LockBit 3.0 and its features were disclosed.

Also, investigative agencies created and distributed decryption tools using LockBit's decryption key. Besides, LockBit disclosed to the world various analysis data related to attacks, including the infrastructure analysis of StealBit, an automated information takeover tool developed by LockBit. The information was posted for about 4 days through a dark web leak site. Afterwards, LockBit's activities seemed to be coming to an end with the closure of the dark web leak site, but it announced that it would resume activities and its activities would continue through a new dark web leak site.

Cyclops rebranding group Knight's actions are attracting attention. Knight, which was discovered in June 2023, said that it provided a builder[6], which was capable of infecting Windows, Linux, macOS, ESXi[7], and Android platforms at the time. It continued its activities steadily, distributing a lightweight version of the ransomware that only encrypts files, but suddenly disappeared in December of the same year. The data leak site that it was operating went offline on February 14, 2024.

On February 18, 2024, officials from Knight, who made a surprise appearance through the RAMP Forum[8], announced that they were selling the source codes of their ransomware. The codes they are selling are Knight 3.0 version, released in November 2023, and include an administrator panel and encryption tool within the codes. Considering that they have announced that they will sell the codes only to trusted individuals, it appears that they are temporarily suspending their activities.

Meanwhile, it was recently confirmed that new vulnerabilities in the remote desktop solution was used in a ransomware attack. The vulnerabilities are ConnectWise's ScreenConnect[9] vulnerabilities, which corresponds to CVE-2024-1708[10] and CVE-2024-1709[11]. Through these vulnerabilities, an attacker can execute arbitrary codes on the remote desktop or create and utilize an account with administrator privileges. In fact, LockBit distributed ransomware to remote locations connected to the 911 system through the CVE-2024-1709 vulnerability, and BlackCat(Alphv) is believed to have used the vulnerability to attack medical institutions. Both the BlackBasta and Bloody group also appear to have exploited the ScreenConnect vulnerabilities through initial access. Special caution is required as there are many servers where the vulnerability has not been patched.

[6] Builder: A ransomware creation tool that allows you to create ransomware with desired functions through environment settings

[7] ESXi: A UNIX-based logical platform, developed by Vmware, that can run multiple operating systems simultaneously on a host computer

[8] RAMP Forum: A Russian hacking forum that sells hacking tools or exchanges related information on the deep web and dark web

[9] ScreenConnect: Remote desktop software that allows you to remotely control your computer over the Internet or another network

[10] CVE-2024-1078: A path search vulnerability that allows an attacker to remotely execute codes in a vulnerable instance

[11] CVE-2024-1079: An authentication bypass vulnerability that allows an attacker to create a system administrator account in a vulnerable instance

■ Ransomware news

infosec

LockBit, temporarily shut down by Cronos Operation.

- Cronos operation is coordinated by national agencies from 11 countries, including the FBI, Europol, and NCA.
- The operation involved seizing critical infrastructure through PHP vulnerability (CVE-2023-3824*).
- LE shared information on the seized blog for 4 days, including decryption tools and arrests of individuals involved.
- LockBit recovered infrastructure through backup servers without PHP installation in about 5 days.
- The stolen encryption keys is 2.5% of the total, and leaked affiliates list does not include identities.

* CVE-2023-3824: RCE vulnerability through stack buffer overflow when loading PHP archive file

Law Enforcement Agency disclose information related to the Cronos operation.

- LE disclose infrastructure source code and affiliates information.
- LockBit-NG-Dev version, suspected to LockBit 4.0 based on .NET framework ransomware, discovered.
- Analyze self-developed data exfiltration automation tool, StealBit infrastructure.
- Four individuals associated with LockBit arrested in Poland and Ukraine.

Knight ransomware sold source code to individual users on the RAMP forum.

- A user named "Cyclops" posted a sales thread for the source code of Knight 3.0 version on the RAMP forum.
- Including the source code of panel and locker. Only accept offers from people with deposit or reputable people.

Ransomware groups exploited vulnerabilities in remote desktop solution, ScreenConnect.

- Path traversal and authentication bypass vulnerabilities (CVE-2024-1708, CVE-2024-1709).
- The Vulnerabilities were discovered on Feb 13, 2024 and patch released on Feb 19, 2024.
- Multiple ransomware groups such as LockBit, BlackCat(Alphv), BlackBasta, Bloody, etc. utilized vulnerabilities.

The U.S. Department of State is offering a reward of up to $15M for BlackCat(Alphv).

- Reward of up to $10M for information leading to the identification or location of any individual.
- Reward of up to $5M for information leading to the arrest and/or conviction in any country of any individual.

New ransomware group called Ransomhub, JKwerlo based on the Go-Language* appeared.

- RansomHub : Excluding CIS, Cuba, North Korea, China, Romania, and non-profit organizations from the targets.
- JKwerlo : Targeting users who use French and Spanish languages.

* Go-Language : An open-source programming language supported by Google

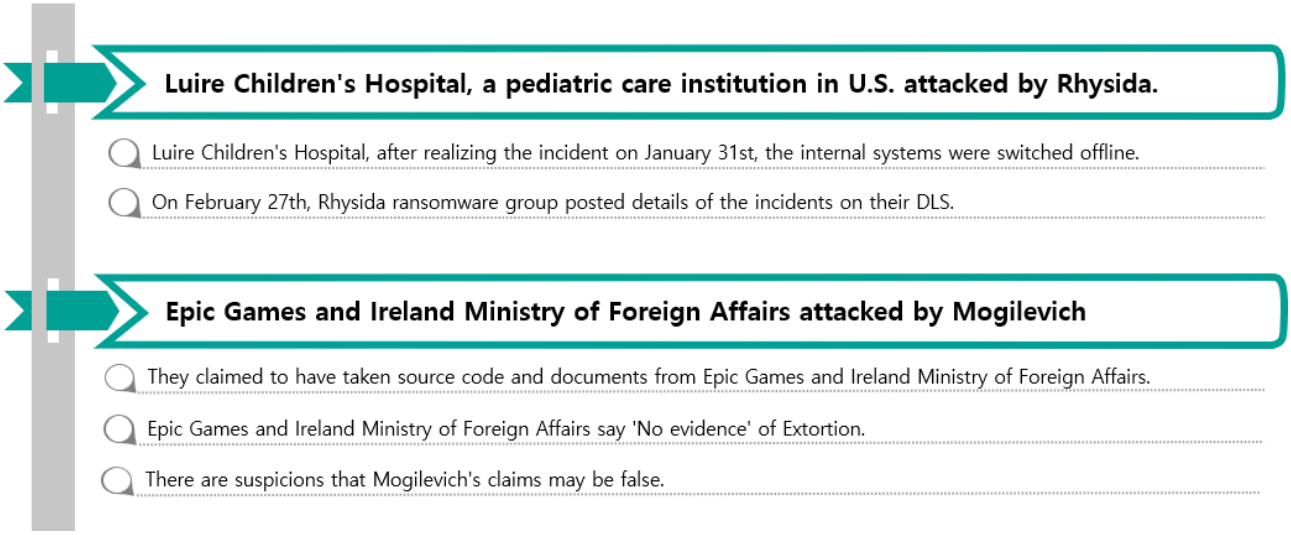


Figure 1. Ransomware trends

■ Ransomware threats

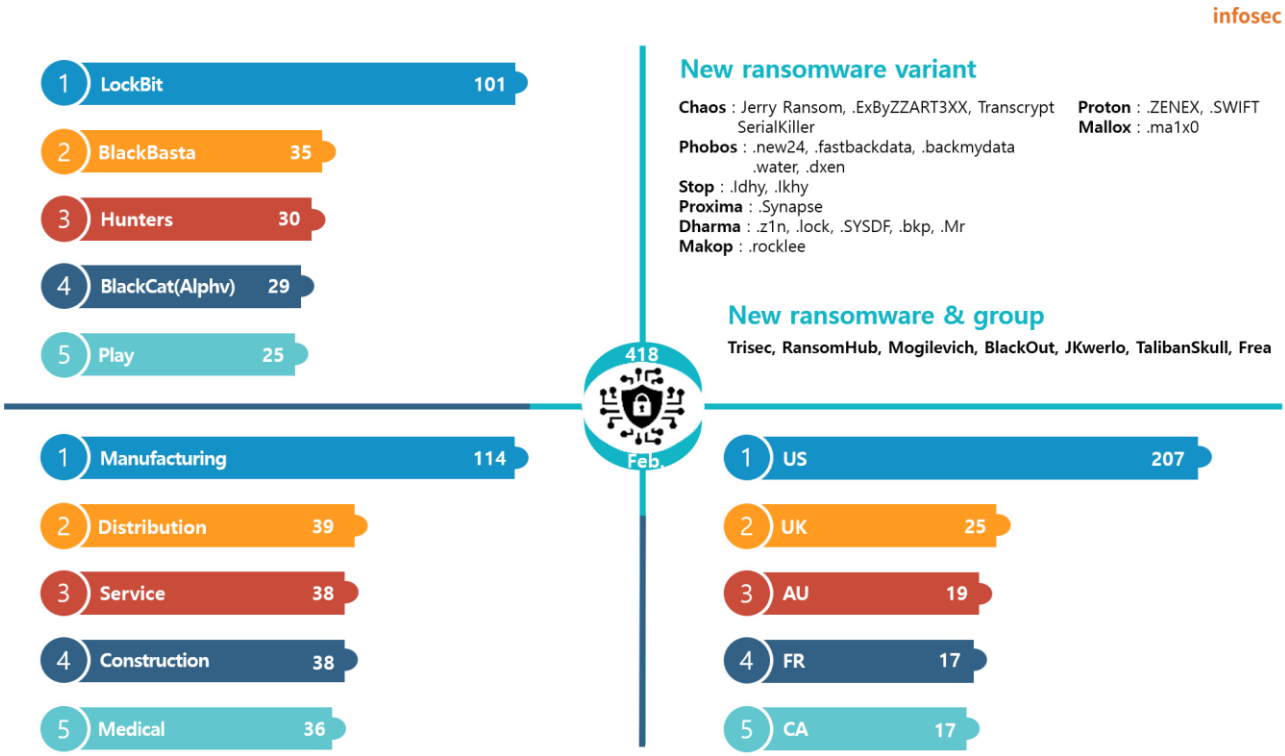


Figure 2. Ransomware threats as of February 2024

New threats

Although ransomware groups are kept in check, e.g., the LockBit group having its infrastructure seized by international organizations, and the BlackCat(Alphv) group having a bounty imposed, new ransomware groups are continuously appearing and ransomware threats are continuing.

The Trisec group uses a unique method, i.e. having the victim directly offer the initial ransom. It is somewhat different from the general method of presenting ransom to the victim. Its Telegram channel uses the Tunisian flag, and the dark web leak site contains the phrase 'Glory to Tunisia.' In addition, circumstances have been confirmed that indicate that the group is based in Tunisia, e.g., posting on a forum that it is recruiting Tunisian talent.

Ransomhub is a ransomware that can infect multiple platforms based on the Go language[12]. According to its rules announced on its dark web leak site, it does not attack CIS[13], Cuba, North Korea, China, and Rumania, and does not re-attack targets that have already been attacked. Unlike the fact that only CIS countries are usually attacked, the fact that Cuba, North Korea, China, and Rumania are included in the countries excluded from attacks can be seen as a possibility that hackers from those countries are included. Meanwhile, it usually recruits affiliates through forums.

On February 21, a new ransomware group Mogilevich appeared. It claimed to have stolen data including account information and source codes from Epic Games, an American video game distributor and software developer, as well as document data from the Irish Ministry of Foreign Affairs. However, no samples of data stolen from Epic Games and the Irish Ministry of Foreign Affairs or direct evidence of damage were confirmed. Then, on March 3, it directly disclosed the theft method and a profit of approximately KRW 160 million, proved itself to be a swindler and disappeared.

[12] Go language: An open source programming language developed by Google to increase productivity

[13] CIS (Commonwealth of Independent States): An international organization of countries that became independent after the dissolution of the Soviet Union. It includes Russia, Moldova, Belarus, Uzbekistan, Kazakhstan, etc

Top 5 ransomwares

Figure 3. Major ransomware attacks by industry/country

LockBit attracted attention by returning in just 5 days through a backup server even when its infrastructure was seized through international cooperation. LockBit announced that it plans to spread out its infrastructure to minimize problems even if the infrastructure is seized. In addition, it registered FBI in its first post on the new dark web leak site registered, and said through a text file that Operation Cronos did not cause any significant damage. Besides, LockBit was found to be using the latest vulnerability of ScreenConnect, a remote desktop solution to distribute ransomware to remote locations using the 911 system of the US.

BlackCat(Alphv) has been continuously attacking U.S. medical facilities since last December. It was confirmed that it has been attacking medical facilities in the United States using a new vulnerability of ScreenConnect since February. The FBI announced a reward of up to $15 million for information related to BlackCat(Alphv). Also, the FBI, CISA[14], and HHS[15] issued additional warnings about the BlackCat(Alphv) ransomware attacks targeting U.S. hospitals.

The Play ransomware group appeared in June 2022 and has attacked approximately 360 organizations (including major national infrastructure) to date. As a result, last December, CISA and ACSC[16] issued a joint cyber security advisory warning against Play. Recently, it announced that it attacked Welch's, an American food and beverage company, and stopped system operations, stealing the company's confidential data, customer documents, and financial information.

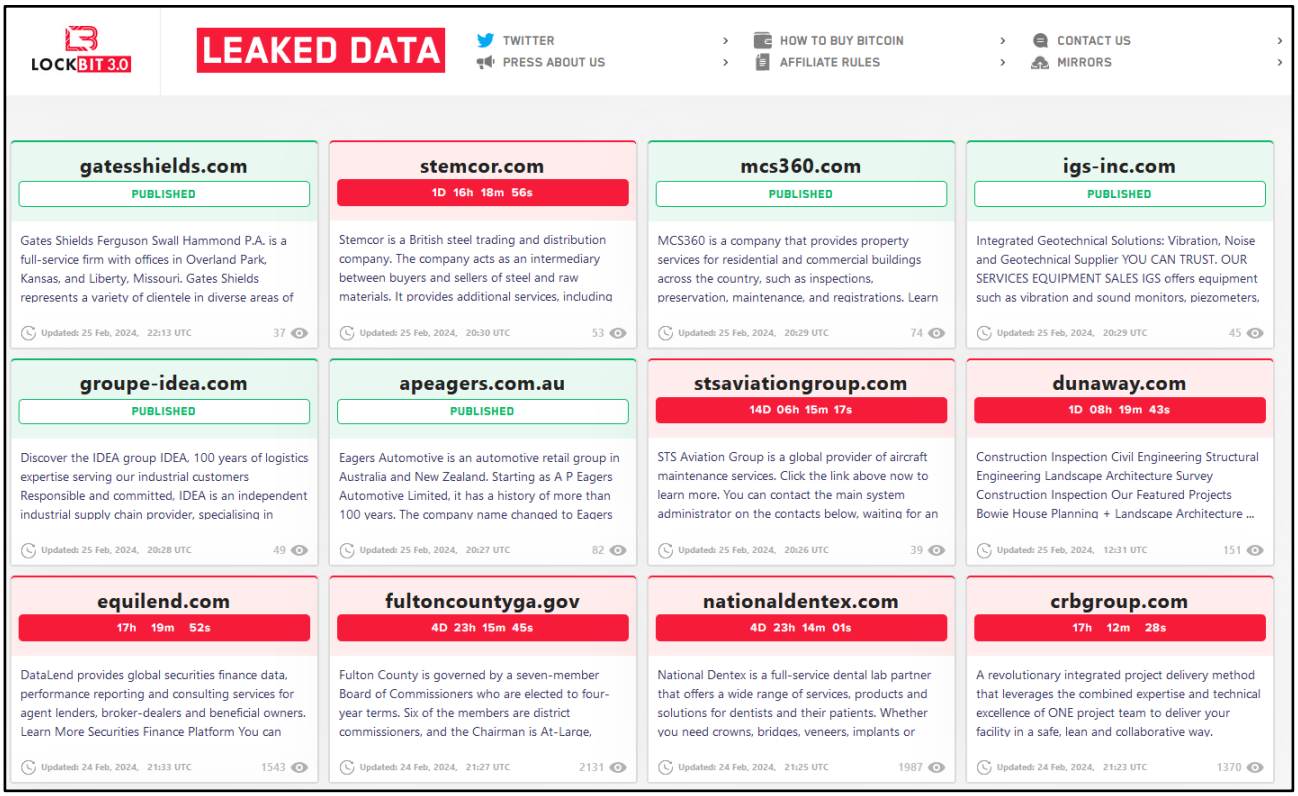
While most ransomwares carry out ransomware attacks targeting relatively vulnerable manufacturing industries, the Hunters ransomware has a relatively low manufacturing attack rate of 13% and mainly targets major institutions and distribution businesses. Additionally, the BlackBasta ransomware attacked hosting services used by many Australian companies, showing different attack patterns: Australia has been attacked most frequently among countries targeted for attacks.

[14] CISA (Cybersecurity & Infrastructure Security Agency): Cybersecurity and Infrastructure Security Agency under U.S. Department of Homeland Security

[15] HHS: United States Department of Health and Human Services

[16] ACSC (Australian Cyber Security Centre): Australian Cyber Security Center, the leading cyber security agency of the Australian government

■ Ransomware in focus

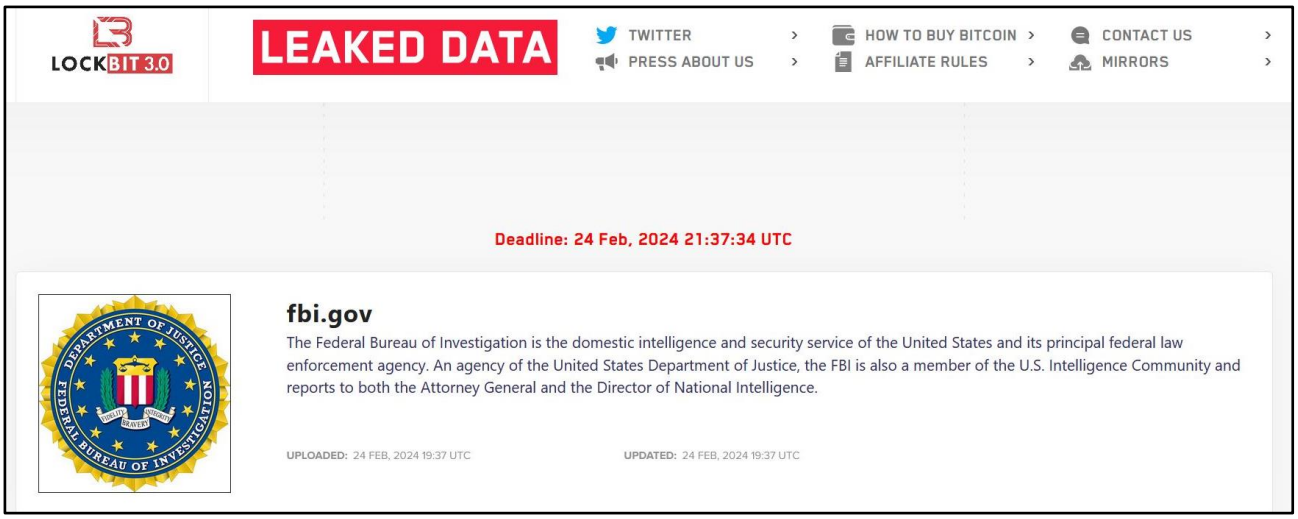


Source: LockBit 3.0 ransomware group data leak site

LockBit has been active for 4 years since September 2019, and is a RaaS-type ransomware organization that provides ransomware to multiple affiliates and receives a portion of the ransom as a fee. LockBit has continuously updated its system for systematic and effective attacks. For example, in June 2021, it updated StealBit (information theft tool) and LockBit 2.0 (Red) version (internal propagation function through group policies is added), and in June 2022, it released LockBit 3.0 (Black) version (detection avoidance technique is applied), similar to the BlackMatter ransomware. In January 2023, the LockBit Green version (Conti ransomware is reused) also appeared.

LockBit is operating very meticulously unlike a typical ransomware group. After updating the ransomware to version 3.0, it held a bug bounty[17] to prevent the release of decryption tools due to the vulnerability of the ransomware. Through this, it receives business ideas and checks whether its identity information such as IP or location information is exposed through the dark web leak site, Tox messenger[18], and Tor network[19].

On February 20, 2024, agencies from 11 countries, including the UK, FBI, and Europol, seized LockBit's dark web leak site and some data through Operation Cronos. It was announced that the criminal infrastructure, including 34 servers and 14,000 accounts used in the attacks, had been neutralized. In this process, the LockBit-NG-Dev ransomware developed in .NET[20], which can be used as LockBit 4.0 version or a new version, was discovered. In addition, they posted various information related to its activities through the seized leak site until February 25. The posted information included the StealBit infrastructure, list of affiliates, news of the arrests of officials, distribution of decryption keys and tools, news of LockBit account closure, etc.



Source: LockBit 3.0 ransomware group data leak site

[17] Bug bounty: A system that provides compensation for finding security vulnerabilities in a company's software or system

[18] Tox messenger: A messenger that provides message and user privacy protection functions

[19] Tor network: An anonymity protection network that hides your online activities

[20] .NET: Windows program development and execution environment developed by MS

Only five days after its infrastructure was seized, LockBit resumed its activities through a new dark web leak site. It recovered the dark web leak site using backed-up server data and modified the PHP vulnerability (CVE-2023-382421[21]) to a patched version.

In the new leak site, it posted the FBI first, and told stories related to Operation Cronos. It said that the stolen decryption keys were only 2.5% of the total keys, and the announced affiliate information did not contain actual identity information. It added, "There is no problem at all with LockBit's activities as the seized data is only a small portion." LockBit announced that it would further strengthen its infrastructure and operational aspects in the wake of this incident. It also delivered a message warning that other ransomware groups could be attacked through the PHP vulnerability (CVE-2023-3824).

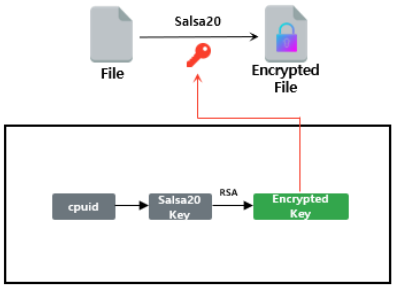
Despite several months of international cooperation between various national organizations, LockBit quickly returned and is uploading new leaked data. With this incident drawing attention to the actions of the LockBit ransomware group, we would like to take a closer look at the LockBit 3.0 ransomware. In addition, we present countermeasures against the LockBit group's strategy.

[21] CVE-2023-3824: A remote code execution vulnerability that occurs when read PHP Archive files used for distributing and installing PHP applications. It includes PHP 8.0.* versions before 8.0.30, 8.1.* versions before 8.1.22, and 8.2.* versions before 8.2.8

LockBit 3.0 Ransomeware

Encryption Key

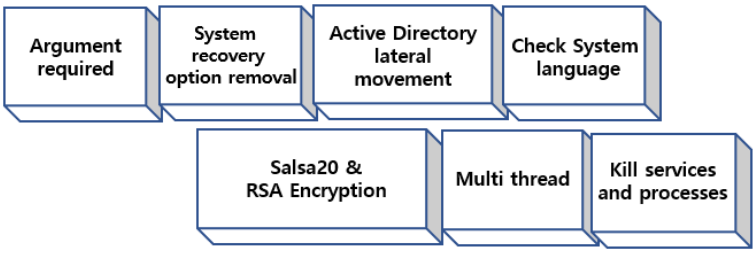
Encrypt files with the Salsa20 algorithm and protect the key with RSA



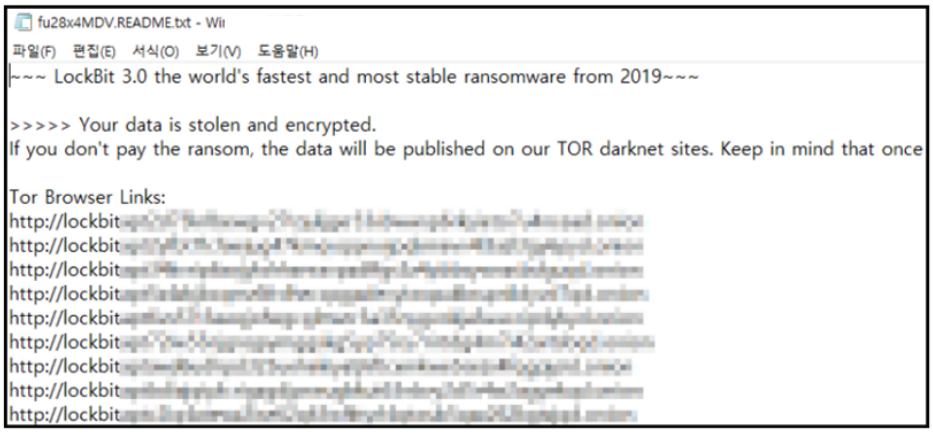
Encryption Method

For file 512KB or less: full file encryption
For file over 512KB, up to 5.5 MB : Initial 512KB encryption
For file over 5.5 MB, up to 60.5MB : encrypt every 512KB for each 5.5MB
For file over 60.5MB, up to 253MB: Encrypt 5MB, then encrypt every 512KB for each 15.5MB
For file over 253MB, up to 1GB : Encrypt 5MB, then encrypt every 1MB for each 31MB
For file over 1GB : Encrypt 15MB, then encrypt every 2.5MB for each 102.5MB

Features



Ransom Note



[A-Za-z0-9]{9}_README.txt

Extension

.[A-Za-z0-9]{9}

First 9 characters of the hash generated with RSA public key

Production Language

C/C++

Figure 4. LockBit 3.0 ransomware Outline

LockBit 3.0 ransomware strategy

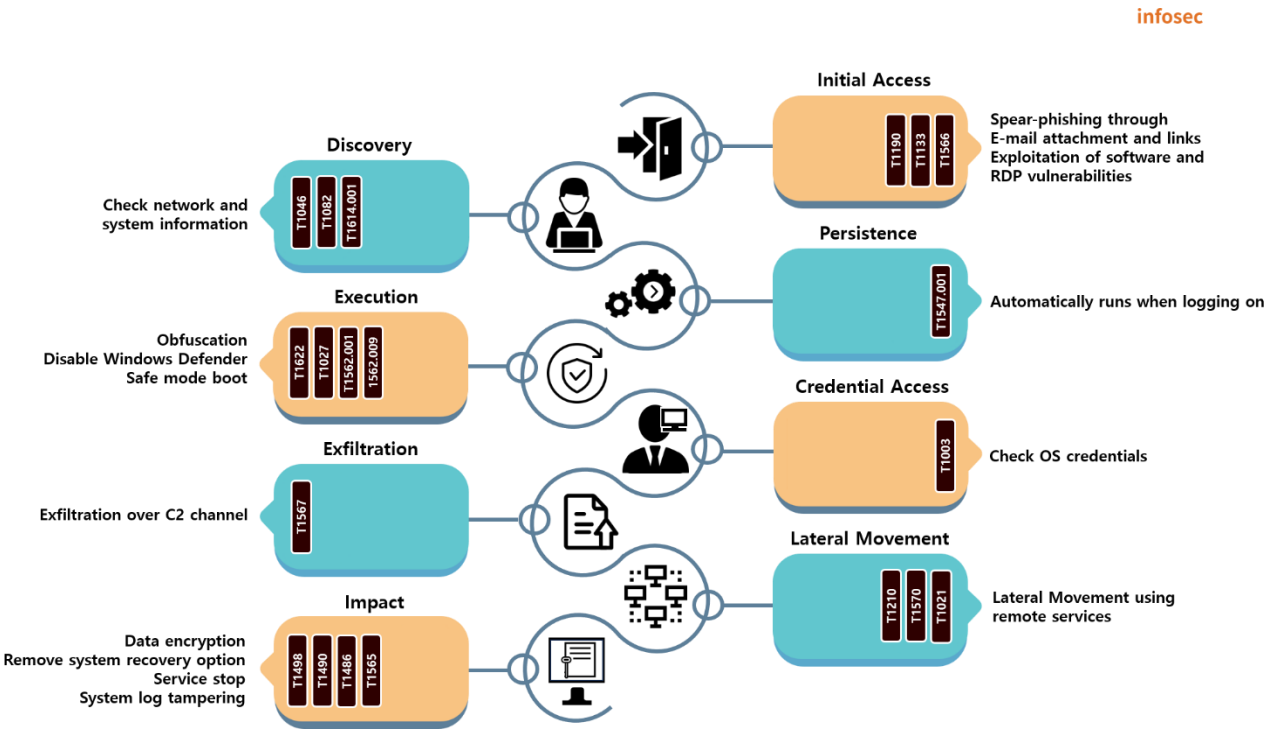


Figure 5. LockBit 3.0 ransomware attack strategy

The LockBit 3.0 ransomware uses various initial access methods for each affiliate. In some cases, initial access is attempted through vulnerable software or RDP[22] vulnerability, or by distributing an NSIS[23] exe file disguised as a Windows installation file. In Korea, an exe file disguised as a resume by changing the file icon, or a version that infects through a script included in the document, has also been discovered. As circumstances demand, there are cases where ransomware is downloaded from the C2 server[24] or compressed ransomware is used.

Additionally, tools for credential theft, system data collection, internal propagation, remote access, and data leakage are downloaded and used. In addition to malicious tools and self-made information stealing tools, normal tools that were not created for the purpose of attacking are also used for attacks.

[22] RDP (Remote Desktop Protocol): A protocol that allows you to remotely control another computer

[23] NSIS (Nullsoft Scriptable Install System): Script-based installation system for Windows

[24] C2 server (Command & Control server): A set of tools and techniques that allow an attacker to maintain communication with a device that has initially been successfully accessed and pass commands and control

File name	Description
Chocolatey	Command line-based package manager for Windows software
Rclone	An external storage management and upload/download program
WinSCP	A Windows program that can transfer or manage files between a computer and a server
PsExec	A tool that can run random processes on the local/remote system.
StealBit	A self-developed information theft automation tool
Mimikatz	A tool to extract sensitive information such as passwords and credentials from the memory of the Windows system

Table 1. Tools used by LockBit 3.0

The LockBit ransomware can perform various functions by checking command execution parameters and provides functions for the convenience and efficiency of attacks. In particular, file encryption will proceed only after the key required to execute the ransomware is entered.

According to the leaked LockBit 3.0 builder, there is a function that encodes and protects part of the ransomware to prevent analysts from easily analyzing the ransomware. In the case of a protected file, if a 32-byte-long key is not entered with the -pass argument, the file will not be decoded and functions such as file encryption and internal propagation will not be executed, and will be terminated.

Argument	Description
-path {path}	Encrypt only the specified path
-pass {32Bytes key}	Enter the key necessary for executing the ransomware
-safe	Encrypt files after booting in safe mode
-wall	Change desktop and print the ransom note
-gspd	Modify group policies and propagate them internally
-psex	Use managed sharing for internal propagation
-gdel	Delete group policy changes
-del	Self-delete after execution

Table 2. LockBit 3.0 ransomware arguments

Administrator privileges are required to access system components such as file encryption or registry manipulation, but after forcibly accessing system components by bypassing UAC[25], the privileges of a process with administrator privileges are duplicated and used. After privilege escalation, end running processes and services related to security and backup, and delete VSC[26] to prevent the victim from arbitrarily recovering. Then, access drives and network resources to collect targets and encrypt files.

To spread ransomware, the PsExec tool is used to remotely execute commands or the group policy is modified to infect AD'[27]s domain server. LockBit 3.0 must be executed together with the -psex or -gspd argument for internal propagation to occur.

In addition to managing system components for file encryption and internal propagation as described above, LockBit penetrates by changing various elements. It replaces the desktop and encrypted file icons with self-created image files, and registers ransomware as a startup program. When the user boots the system, ransomware is automatically executed. In addition, it overwrites event log[28] data through a character string hardcoded into the ransomware, disables the event log, deletes attack traces of the LockBit ransomware to avoid tracking, and hinders detection and analysis to make it difficult to identify the attack vector.

[25] UAC (User Account Control): A security mechanism that checks whether operations that can affect the system are permitted

[26] VSC (Volume Shadow Copy): A function to create a point-in-time backup copy of a file or volume on the Windows system

[27] AD (Active Directory): A Windows-based centralized management service that can manage resources and permissions within an organization

[28] Event log: Data that records important information such as system performance, errors, warnings, and operational information

How to respond to the LockBit 3.0 ransomware

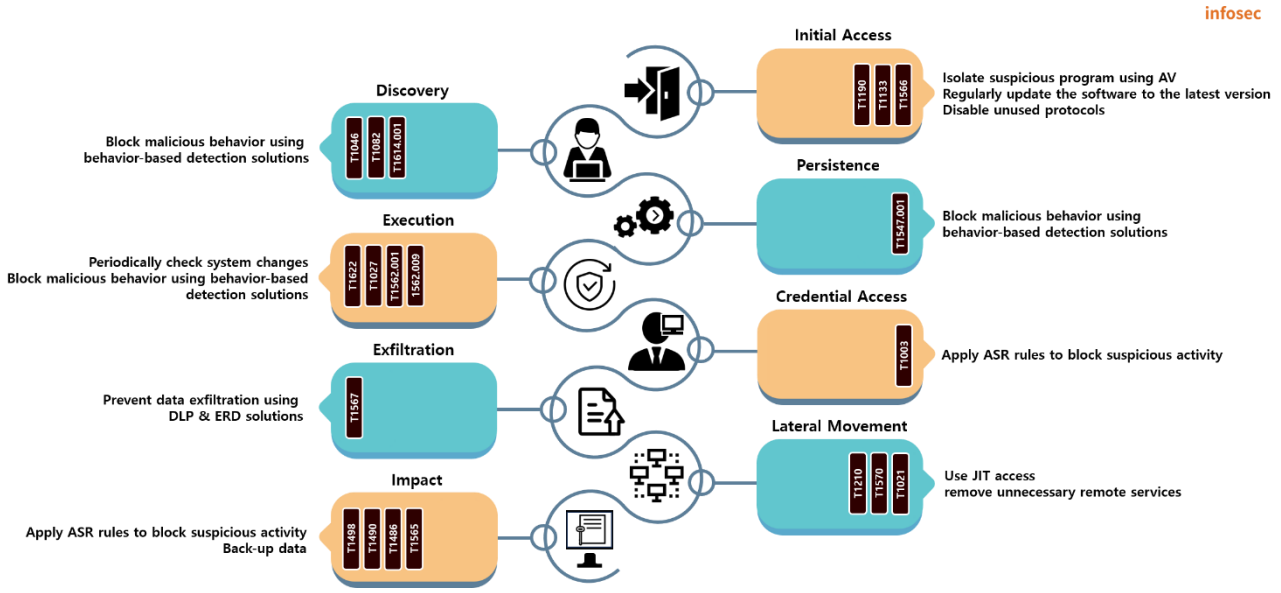


Figure 6. How to respond to the LockBit 3.0 ransomware

LockBit induces the execution of ransomware through an email attachment. The attached file is a file containing a malicious script or an exe file disguised as a document icon. In Korea, it has been distributed under the disguise of a resume or e-mail impersonating copyright violation. Therefore, be careful not to execute attached files or links from e-mails whose sources are unknown, and use anti-virus to prevent programs or scripts from being executed. Also, it can be distributed directly using software vulnerability or protocol vulnerability. Accordingly, you should periodically update your software or operating system to a non-vulnerable version and disable unused protocols to prevent infection.

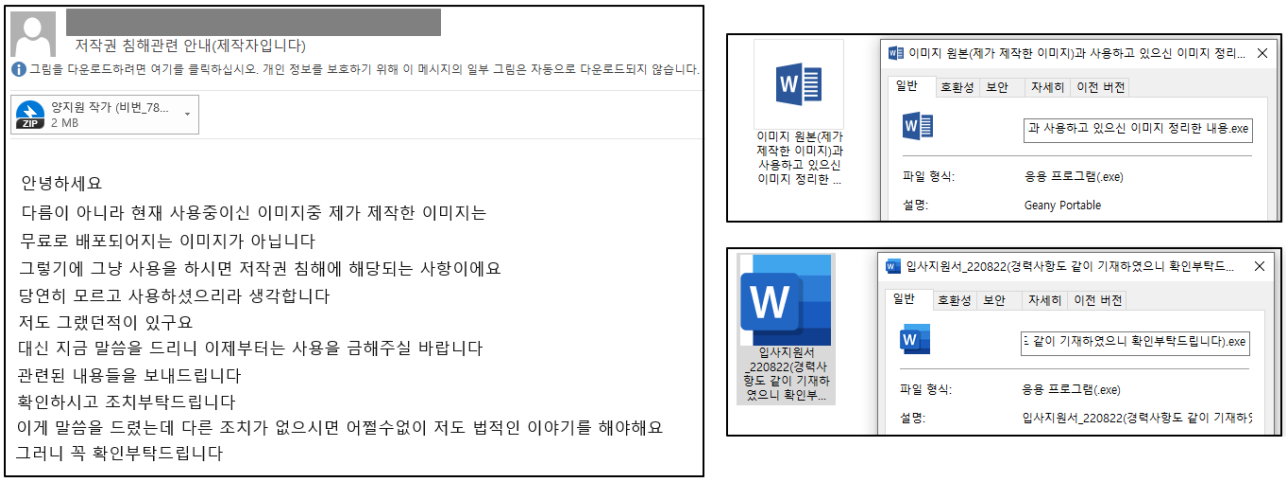


Figure 7. E-mail and malicious files LockBit 3.0 distributed in Korea

CVE	Description	Affected version	Patch version
CVE-2018-13379	When using SSL VPN[29] in Fortinet's secure OS FortiOS, vulnerability in exploring the file path where system files can be downloaded	5.4.6 ~ 5.4.12 5.6.3 ~ 5.6.7 6.0.0 ~ 6.0.4	5.6.8 and higher 6.0.5 and higher
CVE-2020-0796	Remote code execution vulnerability that occurs in SMB 3.1.1, a resource sharing protocol used by Windows	Windows 10 & Server 2016 (build 1903, 1909)	KB4551762 update
CVE-2021-44228	Remote code execution vulnerability discovered in Log4j, a JAVA-based open source logging library	2.0-beta9 ~ 2.15.0 (excluding 2.12.2, 2.12.3, and 2.3.1)	2.12.2, 2.12.3, 2.3.1, 2.16.0 and higher
CVE-2021-22986	Remote code execution vulnerability occurring on BIG-IP and BIG-IQ, what are F5's application distribution network equipment	16.0.*, 15.1.*, 14.1.*, 13.1.*, and 12.1.* before the patch version	16.0.1.1 and higher 15.1.2.1 and higher 14.1.4 and higher 13.1.3.6 and higher 12.1.5.3 and higher
CVE-2021-26855 **CVE-2021-26857** **CVE-2021-26858** **CVE-2021-27065**	Remote code execution vulnerability occurring in Exchange Server, MS's email server	Exchange Server 2013, 2016, 2019	KB5000871 update
CVE-2021-36942	Vulnerability in Windows Server that can allow an unauthenticated attacker to be authenticated for another server through the domain controller	2008 r2 sp1, 2016, 2008 sp2, 2012, 2012 r2, 2020 h2, 2004, and 2019	KB5005076 or KB5005106 update
CVE-2022-3653	Heap buffer overflow vulnerability occurring in the Vulkan graphics engine of the Chrome browser	Lower than 107.0.5304.62	107.0.5304.62 and higher
CVE-2022-36537	Vulnerability that occurs in the open source JAVA framework Zk Framework, which allows access to sensitive information by manipulating POST requests	9.6.1, 9.6.0.1, 9.0.1.2, and 8.6.4.1	9.6.2 and higher
CVE-2023-0669	Vulnerability that allows remote code execution in Forta's security management file transfer software	7.1.1 and lower	7.1.2 and higher
CVE-2023-20269	Vulnerability that can obtain credentials due to the remote access VPN vulnerability of the Integrated security platform Cisco ASA and next-generation threat	9.19.1.18 and lower	9.20 and higher
CVE-2023-27350 **CVE-2023-27351**	Vulnerability that allows remote code execution after accessing the server as an administrator by bypassing user credentials in the print management software	15.0.0 ~ 20.1.7, 21.0.0 ~ 21.2.11, 22.0.0 ~ 22.0.9	20.1.7 and higher 21.2.11 and higher 22.0.9 and higher
CVE-2023-4966	Information leak vulnerability occurring in networking products, i.e. NetScaler ADC and NetScaler Gateway	14.1*, 13.1*, 13.0* before the patch version	14.1-8.50 and higher 13.1-49.15 and higher 13.0-92.19 and higher
CVE-2024-1709	Vulnerability of ScreenConnect, i.e. an authentication bypass vulnerability, that can create a system administrator account on a remote desktop	23.9.7 or lower	23.9.8 and higher

Table 3. Software vulnerability exploited by LockBit 3.0

[29] VPN (Virtual Private Network): A virtual network used to protect personal information and bypass regional restrictions

After initial access, to avoid detection and ensure continuity, manipulate the registry, or terminate the Anti-Virus service, and boot in safe mode. To prevent exploitation of these system functions, it is recommended to use a behavior-based detection solution.

To spread ransomware, modify group policies or execute commands remotely. To prevent this, use the JIT Access[30] method to grant use permissions at a set time based on the principle of least privilege. In addition, you should check for anything suspicious, e.g., checking the list of services and group policies registered in AD through continuous monitoring.

It is also necessary to prepare for data takeover, deletion of backup data, and file encryption. It is possible to use the DLP[31] solution or EDR[32] solution to prevent data leakage. Also, regular backups must be created and managed for file recovery, and since there are cases where data on the NAS[33] and backup storage are deleted, it is recommended to manage the data through vaulting backup[34] in separate networks or storages.

[30] JIT Access (Just-in-Time Access): An approach in which permissions granted to access an application or system are provided only for a predetermined period of time

[31] DLP (Data Loss Prevention): A data leak prevention solution that monitors the flow of data and monitors/blocks important information leaks

[32] EDR (Endpoint Detection and Response): A solution that prevents the spread of damage by detecting, analyzing, and responding to malicious actions occurring on terminals such as computers, mobile devices, and servers in real time

[33] NAS (Network Attached Storage): A storage device connected to a network that allows multiple users to share and access data

[34] Vaulting backup: A method of storing backed-up data separately at a certain distance away

Indicator Of Compromise

Lockbit 3.0 : SHA256

5c9b94f7aed569bb91c77cb0bf8a4f0c13145f8ac35bccc961c973720e46cc62
a4219b77de0ee4c2e17011b95acc69432bcb1a8dc4eb761027b9c997144a76dd
cafaaadd3747dfec3df88a34fea56695a0b5b03b27091b770075a72b03d2d105
917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
535e0dbd97cb9ea66f375400b550dd3bcad0788a89fb46996a651053a2df07c3

임서은.docx (Dropper) : SHA256

1f0617725b2a0b0c3bb1067f0b77da049da0545710d9743813969b3bbcc563f4

저작권 침해관련 안내(제작자입니다).eml : SHA256

4ade4f6ed21b33f627fcc704db4cbfb3dd807516c1e6fc52ae6edb8a66bc80a5

File Name

임서은.docx
sed.exe
저작권 침해관련 안내(제작자입니다).eml
입사지원서_220822(경력사항도 같이 기재하였으니 확인부탁드립니다).exe
이미지 원본(제가 제작한 이미지)과 사용하고 있으신 이미지 정리한 내용.exe

■ Reference site

URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

URL : https://www.boannews.com/media/view.asp?idx=126668&page=1&kind=1

URL : https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/b/LockBit-attempts-to-stay-afloat-with-a-new-version/technical-appendix-LockBit-ng-dev-analysis.pdf

URL : https://www.state.gov/reward-offers-for-information-on-LockBit-leaders-and-designating-affiliates/

URL : https://www.nomoreransom.org/en/decryption-tools.html

URL : https://home.treasury.gov/news/press-releases/jy2114

URL : https://www.secureworks.com/blog/LockBit-in-action

URL : https://seed.kisa.or.kr/kisa/Board/167/detailView.do

URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

URL : https://asec.ahnlab.com/ko/31620/

URL : https://nvd.nist.gov/vuln/detail/CVE-2022-36537

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-20269

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-27350

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-27351

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-4966

URL : https://nvd.nist.gov/vuln/detail/CVE-2024-1709

URL : https://nvd.nist.gov/vuln/detail/CVE-2021-26855

URL : https://nvd.nist.gov/vuln/detail/CVE-2023-0669

URL : https://nvd.nist.gov/vuln/detail/CVE-2018-13379

URL : https://nvd.nist.gov/vuln/detail/CVE-2020-0796

URL : https://nvd.nist.gov/vuln/detail/CVE-2021-22986

URL : https://nvd.nist.gov/vuln/detail/CVE-2021-36942

URL : https://nvd.nist.gov/vuln/detail/CVE-2022-3653