Keep up with Ransomware

Continuing BlackSuit ransomware threats

■ Overview

In December 2023, the number of damage cases caused by ransomware attacks decreased by about 15% to 420 compared to the previous month(497 cases). Many ransomware issues occurred this month too, and one of the most notable issues was that the ransomware infrastructure of BlackCat(Alphv), a representative RaaS(Ransomware-as-a-Service) group, was largely neutralized by FBI's international cooperation. BlackCat(Alphv) is a ransomware group that is gaining worldwide notoriety, and its predecessor is Darkside, which attacked the Colonial Pipeline in the past. They have been stealing data from more than 1,000 companies and organizations, and the criminal proceeds extorted from victims amount to $300 million(approximately KRW395 billion).

Through this international cooperation, the FBI shut down some of BlackCat(Alphv)'s networks and dark websites and secured the **ransomware decryption key** they mainly use. As a result, the over 400 schools and hospitals damaged by BlackCat(Alphv) attacks could restore the infrastructure damaged by the ransomware without having to pay the recovery amount of about $68 million (approximately KRW88.6 billion). However, BlackCat(Alphv) claimed that this was a simple hosting issue and re-opened the dark web leak site, and posted a notice to its affiliates authorizing them to carry out attacks targeting sensitive infrastructure such as hospitals and nuclear power plants. Afterwards, the FBI again confiscated the leaked site, but they are continuing to open leak sites through other domains and write posts saying that they carrying out attacks against multiple targets.

While BlackCat(Alphv) was having difficulties, it was confirmed that another major ransomware group, LockBit, proposed to join as an affiliate of BlackCat(Alphv). In fact, data related to the German Energy Agency, which was posted as an example of an attack by BlackCat(Alphv), was registered on LockBit's dark website. The BlackCat(Alphv) group wrote a post on the Cross-Site Scripting(XSS) Forum[1] mentioning a recent incident and expressing gratitude for LockBit. LockBit also mentioned the need to form a cartel and said that messages of support and cooperation are needed.

Recently, due to the cooperation of global law enforcement agencies, many ransomware groups are pressured into extinction. This situation is raising the alarm of major ransomware groups. If a ransomware cartel is formed now, tactical and strategic changes may occur, and threats may increase rapidly as a result. In order to prevent and respond to this problem, a preemptive and integrated response is needed.

Movements to foster cooperative relationships are also confirmed in other ransomware groups. Recently, it was confirmed that the BianLian, White Rabbit, and Mario ransomware group jointly carried out a BEC(Business Email Compromise)[2] attack targeting financial institutions in the APAC(Asia-Pacific) region by hacking the business accounts of specific maritime logistics companies and distributing malicious emails. At the same time, they attempted to hack the Microsoft Exchange server through a password Brute Force Attack[3] by exploiting IPs from China, Taiwan, Thailand, Korea, and India. This resulted in damage such as ransomware infection and data theft, and victimized companies suffered from threatening emails and phone calls demanding money.

[1] XSS Forum: a dark web forum where hacking tools are sold or related information is exchanged.

[2] BEC: an attacker posing as a trustworthy person and requesting money or confidential information via e-mail.

[3] Brute Force Attack: a technique that cracks a password by trying all possible combinations.

Cooperation between ransomware groups is expected to increase further in the future. This is because international investigative agencies, including the FBI, are moving to directly strike attackers' bases, going beyond existing relaxed responses such as IP blocking. Also, as the importance of IAB(Initial Access Broker)[4] is emphasized, the number of ransomware groups collaborating with them is increasing, and it is expected that they will cooperate with each other as their attack strategies and infrastructure overlap.

In addition, it was confirmed that a ransomware group, rebranded from Royal to BlackSuit, attacked domestic company A. As the data posted by BlackSuit on the dark web leak site also includes customers' personal information, users of the service may be exposed to additional crimes such as phishing and smishing. So caution is required. In fact, it was confirmed that some victims whose personal information was exposed received phishing texts mentioning the leak incident and offering to give stocks as an apology. If you receive such a phishing text, you should report it to the investigative agency or delete it to prevent secondary damage. If you can't be sure, you should be careful, e.g., you should contact relevant agencies. Including the company in question, BlackSuit posted leaked data from five domestic and foreign companies related to construction, education, and distribution in December alone.

[4] IAB: an individual or group that sells initial access paths

Ransomware news

infosec

China arrested four attackers who exploited ChatGPT for ransomware attacks.

○ They were arrested for developing ransomware through ChatGPT.

○ They demanded 20,000 Tether (about KRW26.4 million) as ransom after carrying out a ransomware attack on Chinese company A.

○ The arrested attackers used ChatGPT in the process of developing and optimizing the ransomware.

FBI shut down the BlackCat(Alphv) dark web leak site.

○ BlackCat(Alphv) extorted $300 million (KRW395 billion) in ransom from more than 1,000 organizations over the years.

○ The FBI secured a decryption tool, and provided free decryption service for over 400 organizations.

○ BlackCat(Alphv) scuffled with the investigative agency, and the leak site was shut down and restored repeatedly.

A decryption tool was developed through the defect of the BlackBasta ransomware.

○ Germany's SRLabs released a decryption tool helpful in recovering from damage due to the BlackBasta ransomware..

○ BlackBasta became aware of the defect, and distributed a newly modified ransomware.

The dark web leak sire of SiegedSec, a hactivist group, was shut down.

○ The dark web leak site of SiegedSec, a pro-Russian hactivist group that started working in February 2022, was shut down.

○ SiegedSec has been active, e.g., affiliation with other hactivist groups like GhostSec.

DragonForce attacked 21 organizations including the Australian branch of Yakult.

○ On December 20, DragonForce said on its leak site that it attacked the Australian branch of Yakult, and leaked 95GB of data.

○ This group was first discovered in December, and its association with DragonForce Malaysia, a hacktivist group, has not been confirmed.

○ In addition, it performed attacks against various industries including manufacturing, construction and distribution.

Werewolves performed attacks against various industries, and claimed that it infringed on 23 organizations.

○ Werewolves, first discovered in December, is operating a surface website in Russian.

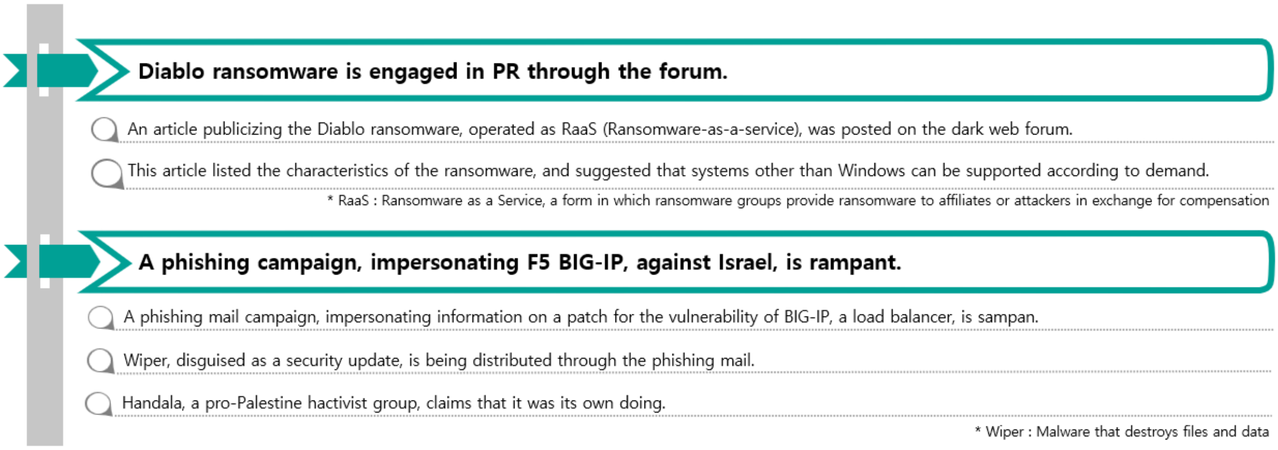
○ It is operating its own bug bounty, and claims that its mission is to strengthen the cybersecurity of all companies around the world.

* Surface web : A general website that can be found using a search engine

A new ransomware group, which succeeded to RansomedVC, appeared.

○ Raznatovic, first discovered in December, is thought to have purchased the infrastructure of RansomedVC.

○ It uploaded posts about 5 organizations on a dark web leak site, but it is inaccessible now.



Diablo ransomware is engaged in PR through the forum.

- An article publicizing the Diablo ransomware, operated as RaaS (Ransomware-as-a-service), was posted on the dark web forum.
- This article listed the characteristics of the ransomware, and suggested that systems other than Windows can be supported according to demand.

* RaaS : Ransomware as a Service, a form in which ransomware groups provide ransomware to affiliates or attackers in exchange for compensation

A phishing campaign, impersonating F5 BIG-IP, against Israel, is rampant.

- A phishing mail campaign, impersonating information on a patch for the vulnerability of BIG-IP, a load balancer, is sampan.
- Wiper, disguised as a security update, is being distributed through the phishing mail.
- Handala, a pro-Palestine hactivist group, claims that it was its own doing.

* Wiper : Malware that destroys files and data

Figure 1. Ransomware trends

Ransomware threats

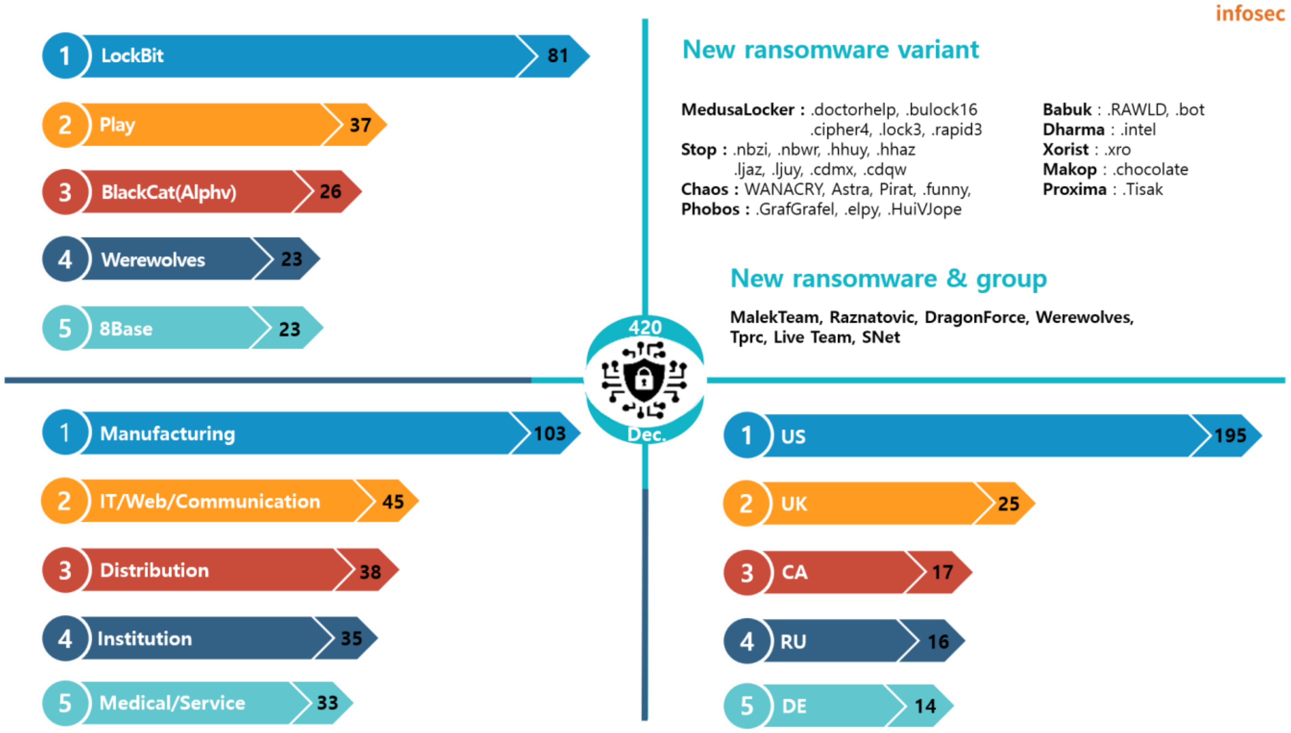


Figure 2. Ransomware threats as of December 2023

New threats

Ransomware groups newly discovered in December include Malek Team, Raznatovic, DragonForce, and Werewolves. Malek Team operates a surface website and Telegram channel and introduces itself as a multinational team in the cyber hacking field. They posted that they had carried out attacks on five organizations, including hospitals and manufacturers in Israel, and some of the posts were confirmed to contain leaked data.

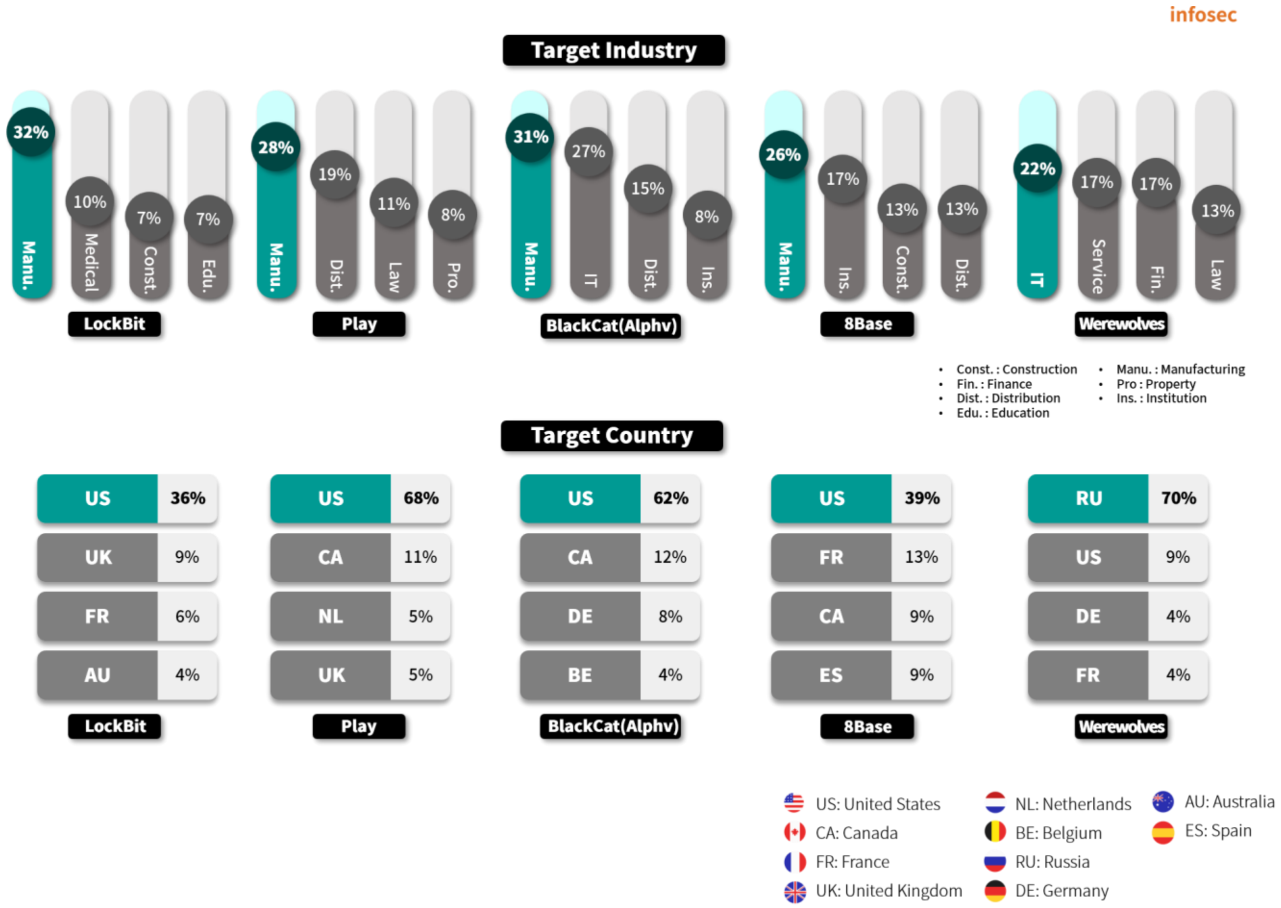
Raznatovic is a group that succeeds to RansomedVC. RansomedVC is a ransomware group that began its activities last October and attracted attention by claiming to have hacked Sony. They have a history of securing more than 200 members in the first week of activity. However, when pressure from investigative agencies began, six people were arrested after suddenly posting on the forum that they were selling various kinds of infrastructure, including ransomware builders, and disappeared due to reasons such as hiring young and inexperienced affiliates. Then, seeing that a group introducing itself as ‘Ransomed.VC aka Raznatovic’ began its activities, it is presumed that Raznatovic purchased the infrastructure.

The Werewolves group has been making unusual moves since its appearance. On the surface website operated by this group, an article claiming to have stolen data from as many as 23 organizations and some leaked data were posted. Also, the site holds its own bug bounty[5] and states that it will pay a bounty of up to $1 million (approximately KRW1.32 billion) to anyone who reports website vulnerability, software vulnerability, Tor browser vulnerability, etc.

The Astra ransomware, a variant of the Chaos ransomware, was also discovered. Chaos was first discovered in June 2021, released several versions, and released a builder on the dark web hacking forum, enabling an unspecified number of people to mass-produce variants that exploited it. Then, ransomware with various names such as Yashma and Onyx emerged based on Chaos and caused a lot of damage. The recently discovered Astra ransomware is also based on Chaos. Because the file is encrypted with AES and the key is protected with RSA, decryption is difficult. So efforts must be made to prevent infection.

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

Top 5 ransomwares



LockBit		Play		BlackCat(Alphv)		8Base		Werewolves	
US	36%	US	68%	US	62%	US	39%	RU	70%
UK	9%	CA	11%	CA	12%	FR	13%	US	9%
FR	6%	NL	5%	DE	8%	CA	9%	DE	4%
AU	4%	UK	5%	BE	4%	ES	9%	FR	4%

Figure 3. Major ransomware attacks by industry/country

The ransomware group that caused the most damage in December is LockBit. LockBit claimed to have carried out an attack on Dena, the German energy agency, and also posted a message threatening to leak data if the company did not agree to negotiations by December 26. Dena acknowledged that there was a cyber attack, but did not specify whether the attack was caused by ransomware. Additionally, LockBit took advantage of the shutdown of BlackCat(Alphv) to propose collaboration to developers and affiliates of BlackCat(Alphv). In fact, it appears that there are affiliates who have transferred as Dena data from the existing BlackCat(Alphv) site was also posted on the LockBit leak site.

The Play Ransomware Group attacked about 300 organizations around the world between June and October 2022. As the attacks involved major national infrastructure, it is known as a group with considerable influence. As a result, the FBI recently issued a joint cyber security advisory warning against Play along with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Australian Cybersecurity Center (ACSC).

BlackCat(Alphv) is repeatedly closing and restoring its infrastructure due to the cooperation of international investigative agencies. They declared that they would restore the infrastructure and retaliate against the FBI even though the FBI had shut down the infrastructure. Also, at the XSS Forum, BlackCat(Alphv) and Lockbit exchanged conversations about forming a ransomware cartel, which could lead to a cooperative relationship in the future, and there is also a possibility of going through the same rebranding process as before to divert the attention of investigative agencies.

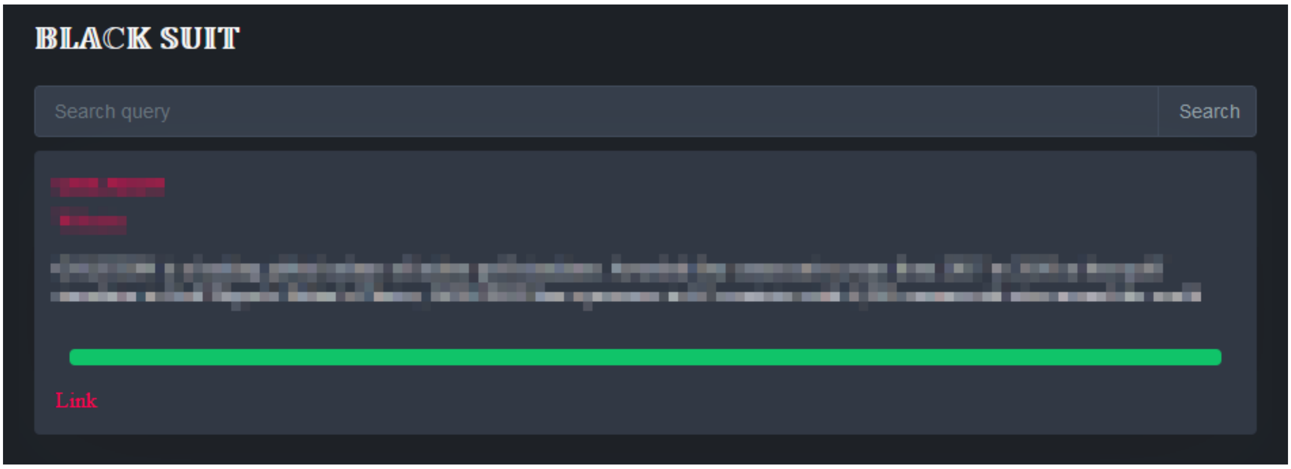
The 8base Ransomware Group has been steadily active since opening a dark web leak site in May 2023. They are carrying out attacks using variants of Phobos ransomware. In particular, it spreads ransomware through SmokeLoader[6]or infects systems by including obfuscated ransomware in the loader itself. As SmokeLoader is distributed mainly through phishing emails, it is recommended to prevent infection by avoiding downloading attached files from e-mails from unknown sources.

Werewolves is a ransomware group newly discovered in December. They are carrying out attacks against vulnerable public services using LockBit 3.0 ransomware and leaked Conti hacking tools. As a result, 23 organizations suffered damage as hundreds of terabytes of data was stolen. Among them, 16 companies were victimized by attacks performed against Russia. In addition, a connection with LockBit is suspected, e.g. the use of LockBit 3.0 and six cases overlapping with the victimized organizations posted by LockBit.

[6] SmokeLoader: malware used to download other malware to an infected system

■ Focus of ransomware

Outline of the BlackSuit ransomware

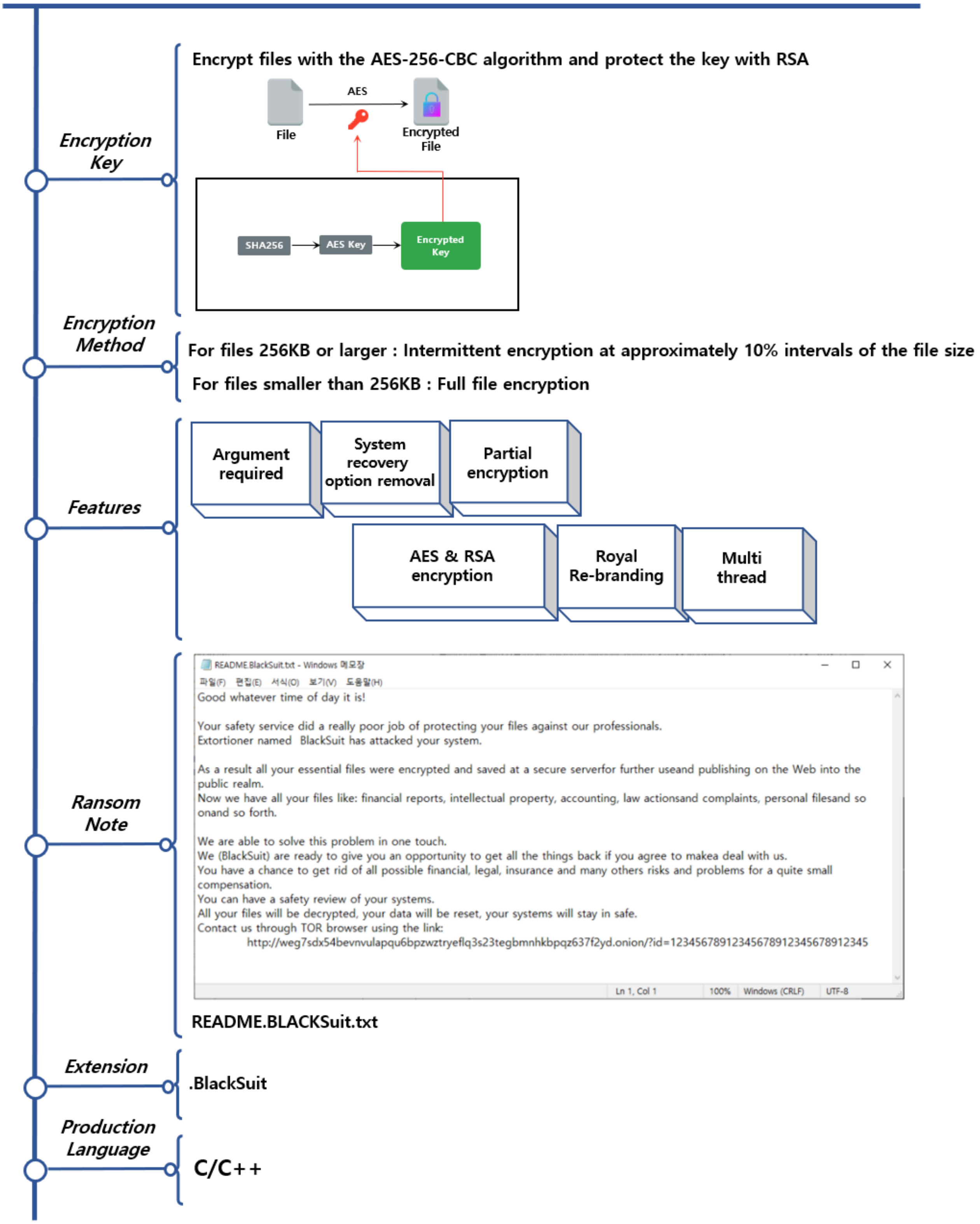


Source: BlackSuit ransomware group's dark web leak site

BlackSuit appeared in May 2023 and is a ransomware group rebranded from Royal. They attack both Windows and Linux and use a double extortion method, i.e. demanding ransom and threatening to leak data at the same time.

Royal, the predecessor of BlackSuit, is a ransomware group derived after the disbandment of the Conti ransomware, which ended its activities in June 2022. Since its emergence, it has been revealed that it has demanded an amount equivalent to $275 million (approximately KRW362.7 billion) through threats against more than 350 organizations, and the number of organizations whose data was posted on the dark web leak site alone exceeds 200 companies. Royal, which had shown such significant influence, was quiet starting around July as pressure from investigative agencies intensified after attacking the county of Dallas, USA in May 2023, and eventually disappeared in October, and was completely rebranded as BlackSuit.

BlackSuit is spread through phishing email attachments, Torrent website, malicious advertisements, etc., and an incident recently occurred in which leaked data from domestic company A was made public. Company A notified customers of the damage three weeks after the ransomware attack occurred and revealed that some customers' personal information had been leaked. Additionally, after the ransomware attack, some users suffered damage, e.g., receiving phishing text messages impersonating Company A. As personal information leaked in this way can cause secondary damage such as phishing or smishing, special caution is required.



Encryption Key

Encrypt files with the AES-256-CBC algorithm and protect the key with RSA

Encryption Method

For files 256KB or larger : Intermittent encryption at approximately 10% intervals of the file size

For files smaller than 256KB : Full file encryption

Features

Argument required

System recovery option removal

Partial encryption

AES & RSA encryption

Royal Re-branding

Multi thread

Ransom Note

README.BlackSuit.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8

Good whatever time of day it is!

Your safety service did a really poor job of protecting your files against our professionals.
Extortioner named BlackSuit has attacked your system.

As a result all your essential files were encrypted and saved at a secure serverfor further useand publishing on the Web into the public realm.
Now we have all your files like: financial reports, intellectual property, accounting, law actionsand complaints, personal filesand so onand so forth.

We are able to solve this problem in one touch.
We (BlackSuit) are ready to give you an opportunity to get all the things back if you agree to makea deal with us.
You have a chance to get rid of all possible financial, legal, insurance and many others risks and problems for a quite small compensation.
You can have a safety review of your systems.
All your files will be decrypted, your data will be reset, your systems will stay in safe.
Contact us through TOR browser using the link:
http://weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd.onion/?id=12345678912345678912345678912345

README.BLACKSuit.txt

Extension

.BlackSuit

Production Language

C/C++

Figure 4. BlackSuit ransomware Outline

BlackSuit ransomware strategies

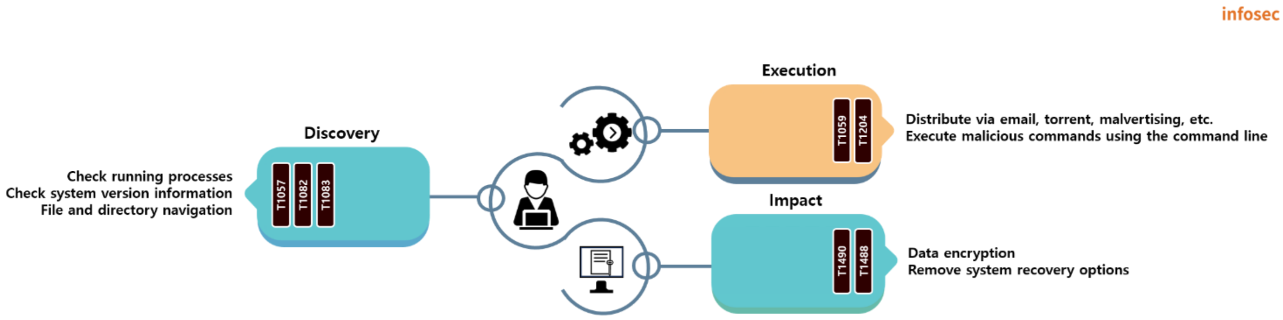

infosec
Execution
Distribute via email, torrent, malvertising, etc.
Execute malicious commands using the command line
T1059
T1204
Discovery
Check running processes
Check system version information
File and directory navigation
T1057
T1082
T1083
Impact
Data encryption
Remove system recovery options
T1490
T1488

Figure 5. BlackSuit ransomware attack strategies

The BlackSuit ransomware carries out attacks that attach ransomware to an attached file or attaches a document file containing a macro that causes ransomware to be executed, causing infection without the user's knowledge when the file is executed. In addition, you need to pay attention because when you click on a malicious advertisement, you are automatically redirected to a site where ransomware is installed, or it may be installed through malware in the form of a downloader.

The ransomware appears to have been designed for the attacker's convenience by passing various arguments, and is designed so that if a certain argument is not delivered, encryption does not proceed and the process is terminated immediately. It is believed to aim at the effect of bypassing detection and interfering with analysis.

Argument	Description
-p {target path}	Encrypt only the contents of the specified path
-name {32byte string}	Unique ID: if not delivered, the process terminates.
-percent {0~100}	Specify encryption strength
-list {text files}	A text file in which the object to be encrypted is written
-delete	Self-deletion
-network	Encrypt network shared resources
-local	Encrypt local system
-disablesafeboot	Disable safe boot
-noprotect	Disable mutex creation

Table 1. BlackSuit ransomware arguments

Among BlackSuit's arguments, the ones worth noting are −name and −percent. When ransomware is executed through a macro or script, the 32−byte string delivered with the −name argument is used as the victim's unique ID and is also written in the ransom note. If the argument is not delivered, the process is terminated, and as the argument value is simply used as a value to identify the victim, the ransomware can be executed if only a 32−byte string is delivered.

The encryption strength can be specified through the argument delivered along with the －percent argument. BlackSuit, which adopted an intermittent encryption method for files over 256KB, assumes by default that 100 has been delivered if the －percent argument is not delivered, and performs intermittent encryption in units of approximately 10% of the file size.

$$\boxed{N = \left(\frac{X}{10}\right) \text{x} \left(\frac{\textbf{Original File Size}}{\textbf{100}}\right)}$$

[Formula for calculating the encryption strength of BlackSuit]

- N： number of bytes to be used for intermittent encryption
- X： the value of the factor passed with the －percent argument.
- The calculated N is finally lowered to a multiple of 16.

BlackSuit deletes VSC(Volume Shadow Copy)[7] without the victim's knowledge using the Quiet option by executing a command at the command line, preventing the user from arbitrarily recovering it. Through this, it boots in the safe mode and removes the safeboot option to prevent the victim from using the recovery option. This ransomware is a 32−bit program, but even in the case of 64−bit programs, it shows a high level of circumspection by executing 64−bit commands as well to prevent recovery through VSC. After these commands are executed, the computer is immediately rebooted, leaving the user helpless to ransomware without being able to take any action.

[7] VSC： a function to create and maintain backup copies of files or folders on Windows systems

How to respond to the BlackSuit ransomware

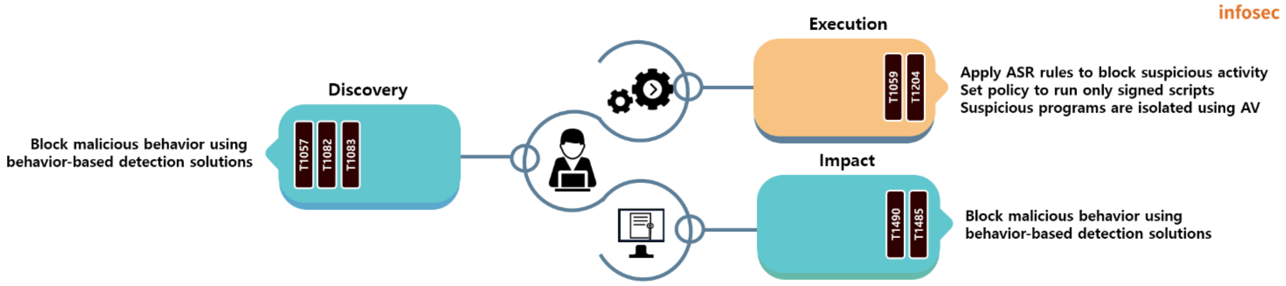

infosec
Discovery
Block malicious behavior using behavior-based detection solutions
T1057
T1082
T1083
Execution
T1059
T1204
Apply ASR rules to block suspicious activity
Set policy to run only signed scripts
Suspicious programs are isolated using AV
Impact
T1490
T1485
Block malicious behavior using behavior-based detection solutions

Figure 6. How to respond to the BlackSuit ransomware

As most of the behavior of the BlackSuit ransomware exploit basic system functions, it may be difficult to accurately distinguish them from signature-based security solutions. To solve this problem, if you use a security solution that detects based on behavior or enable the ASR (Attack Surface Reduction)[8] rules, you can block abnormal parts of the basic system functions.

In these cases, more efforts must be made to prevent ransomware infection in advance. Since infection can occur through various paths, organizations need to use various methods, e.g., providing training to raise security awareness among members.

In particular, you must be careful when downloading or opening attachments to e-mails from unknown sources, downloading or updating from places other than the application's official website, or clicking on advertising banners on vulnerable websites. If individuals or organizations recommend that people should refrain from such actions in order to increase security awareness, the possibility of ransomware infection can be minimized.

[8] ASR: a technique to block malware attack paths

Indicator Of Compromise

BlackSuit : SHA256

90ae0c693f6ffd6dc5bb2d5a5ef078629c3d77f874b2d2ebd9e109d8ca049f2c

1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e

449df90b819d01d290d218929bd33ee24941b3e6c00cdedc0e6f2714aea8460b

feced22ef920c40e032e12b9eb315591a7b6adcd371453c7d2fa08e2c8972aac

File Name

sys32.exe

■ Reference site

URL: https://www.bleepingcomputer.com/news/security/fbi-alphv-ransomware-raked-in-300-million-from-over-1-000-victims/

URL: https://www.bleepingcomputer.com/news/security/how-the-fbi-seized-blackcat-alphv-ransomwares-servers/

URL: https://techcrunch.com/2023/11/15/cisa-fbi-royal-ransomware-blacksuit-sanctions/

URL: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/

URL: https://www.resecurity.com/blog/article/Exposing-Cyber-Extortion-Trinity-BianLian-White-Rabbit-Mario-Ransomware-Gangs-Spotted-Joint-Campaign

URL: https://thecyberexpress.com/werewolves-ransomware-group/

URL: https://www.scmp.com/tech/tech-trends/article/3246612/chatgpt-aided-ransomware-china-results-four-arrests-ai-raises-cybersecurity-concerns

URL: https://www.bleepingcomputer.com/news/security/fake-f5-big-ip-zero-day-warning-emails-push-data-wipers/