Keep up with Ransomware

Knight ransomware threat targeting various platforms

■ Overview

In September 2023, the number of damage cases due to ransomware attacks increased by 23.7% from the previous month(401 cases) to 496 cases. This is related to the increase in damage cases caused by the LockBit Ransomware Group, as well as the robust activities of the recently discovered ransomware groups Cactus, Ransomed, and LostTrust. These ransomware issues are occurring one after another and the threat continues.

Recently, when the LockBit ransomware was blocked in a LockBit affiliate's attack campaign, a case of system infection using 3AM, a new Rust[1]-based ransomware, was discovered. 3AM is a ransomware that became a hot topic after it was used by a LockBit affiliate, although its relationship with other ransomware groups has not yet been revealed. This attack appears to be a strategy to increase the success rate of ransomware infection by selectively using the LockBit and 3AM ransomware.

Also, an attack case was confirmed in which the LockBit and Akira Ransomware Group exploited the CVE-2023-20269[2] vulnerability of Cisco's network security solutions, ASA (Adaptive Security Appliance) and FTD (Firepower Threat Defense). Recently, attackers have tended to use a strategy of attacking multiple companies by exploiting a single vulnerability.

[1] Rust: It is a type of programming language that malware producers use for its advantages such as fast encryption speed and bypass of analysis and detection.

[2] CVE-2023-20269: vulnerability A vulnerability that accesses the ASA and FTD software without authorization.

In addition, the LockBit Ransomware Group secured 800GB of data from a large domestic company, posted sample data such as agreements, a list of stolen data, and capacity, and posted a threat to disclose all data after 7 days. The data was found to have been leaked from a Chinese factory in charge of photovoltaic business, and the victimized company refused to negotiate with the LockBit Ransomware Group. Accordingly, the LockBit Ransomware Group posted approximately 100 GB of compressed files and data list, including work-related documents, picture files, and database-related files. Recently, cases of ransomware infections and double extortion have been occurring one after another among domestic companies. So caution is needed.

BianLian is a ransomware group that has been steadily active, and recently caused public anger due to an incident in which it anonymously posted stolen data and then quietly deleted it. The posts were anonymous, e.g. '**** **e ******e* ***e*********', but the description that the victim is the world's leading non-profit organization, employing approximately 25,000 people and operating in 116 countries, and the company employs around 25,000 people and operates in 116 countries, and the masked text revealed that it was 'Save The Children International', a non-profit charity organization. When this fact became known, criticism arose in various communities with a concerned reaction. In response, the BianLian Ransomware Group tried to settle the dust by quietly deleting the post the next day.

The movements of a new ransomware group called LostTrust are also unusual. The LostTrust Ransomware Group newly emerged after posting a total of 53 damage cases on a dark web leak site. It was confirmed that the ransomware they are using has codes similar to those of the SFile ransomware, raising suspicions that the source code has been borrowed or rebranded. Meanwhile, their leak site design and group introduction appear similar to those of the MetaEncryptor Ransomware Group. This is one of the strategies to promote through imitation, and the newly discovered CryptBB Ransomware Group is also beginning its activities by simply imitating the 8base Ransomware Group.

The Knight Ransomware Group is a rebranded group of the Cyclops Ransomware Group. It provides a builder that can infect Windows, Linux, macOS, ESXi[3] and Android platforms, and has reportedly been developing it for about 3 years. To facilitate attacks by its affiliates, the Knight Ransomware Group provides a full version that includes encryption and infostealer and a lightweight ransomware that only encrypts files. Additionally, they are actively attempting to gain access through phishing, SPAM, and social engineering attack to secure many affiliates. The Knight Ransomware Group has recently been confirmed to be conducting a SPAM campaign in Italy and is using a strategy of inducing users to run exec files disguised as document files.

Meanwhile, it was claimed that the Knight ransomware is related to the LockBit and Babuk ransomware, and actual analysis results confirmed that the encryption logic has similar codes. It is often found that ransomware groups have similarities in codes or TTP (Tactics Techniques and Procedures)[4], which is an evidence that ransomware is produced with reference to leaked codes or that information exchange and collaboration is taking place between ransomware groups.

Attackers from Vidar and RedLine, influential infostealer, began distributing ransomware in the same way they distributed infostealer. They seem to have used a strategy of expanding the scope of attacks by utilizing existing resources without the need to develop or apply a new strategy or technology from scratch using the same distribution channels. It was confirmed that the ransomware used at this time was the Knight ransomware. As many attacker groups reuse TTP and use it with only partial modifications, analysis from the attacker's point of view is becoming more important for effective response.

[3] ESXi: virtualization OS developed by VMware

[4] TTP: A method for expressing the attacker's strategies, tactics, and procedures

Recently, ransomware groups have been carrying out attacks using a variety of initial access methods, including attacks that exploit vulnerabilities, phishing, SPAM, and social engineering attack. Both access by exploiting vulnerabilities discovered through professional knowledge and conflicting strategies using social engineering attack, which are relatively easy, are being discovered. This strategy can be attributed to a difference in technology between large attack groups such as LockBit and BlackCat and new/small-scale ransomware affiliates, but it is worth noting that ransomware groups do not easily change their initially designed strategies. Therefore, in order to effectively block ransomware, it is necessary to take proactive and preemptive measures by establishing appropriate response steps suited to the corporate environment and understanding the strategies and tactics of ransomware groups in advance.

■ Ransomware news

infosec

LockBit steals UK ministry of Defense data through manufacturer attack

- LockBit, UK Ministry of Defense data breach
- Leaked data includes information from several important defense facilities
- Manufacturer Zaun claims it suffered damage, but no key data was damaged
- Concerns are growing about supply chain attacks, with Departments refusing to comment on the incident

Ransomed attacks Airbus, world's largest aircraft manufacturer

- Airbus supplier information leaked to dark web under investigation
- Hackers hack into Turkish airline employee accounts to access network
- Airbus has been attacked by Chinese hackers before

BianLian steals 7TB of data through Save the Children attack

- BianLian steals approximately 7TB of data through Save the Children attack
- Criticism continues as it can affect countless children

11 TrickBot and Conti members sanctioned

- TrickBot and Conti organizations stole $180 million globally, and Conti organization collapsed
- Sanctions have banned all financial transactions and have affected organizations

LockBit and Akira attack Cisco VPN vulnerability exploit

- Cisco warns that VPN service vulnerabilities are being exploited by LockBit and Akira
- The vulnerability allows attackers to perform Brute Force Attacks for initial access
- MFA(Multi Factor Authentication) measures are required to prevent damage

* MFA: Account authentication by requiring the user to provide additional information other than a password

Cuba spreads new malware that is difficult to detect

- Cuba equips new malware with anti-virus detection avoidance feature through use of encrypted data
- Cuba uses homegrown tools for its attacks and is continuously improving them

3AM emerges as an alternative to LockBit

- 3AM written in Rust, was distributed after an attack through LockBit failed
- As it is used by LockBit's affiliates, it is likely to secure reliability from other attackers

BlackCat(Alphv) attacks Azure Storage with Sphynx variant

- Exploiting stolen Microsoft accounts during Azure Cloud Storage encryption via Sphynx variant
- Encrypt approximately 40 Azure Storage accounts by modifying security policies
- BlackCat(Alphv) continues to improve its strategy and conduct attacks targeting businesses around the world

* Azure Storage: Cloud-based data storage and management service

IAB hijacks accounts through Microsoft Teams phishing

- One of the IAB groups providing the initial access vector is carrying out phishing attacks via Microsoft Teams
- MS rolls out updates to better identify and alert external users in Teams to help defend against such attacks

Vidar and RedLine turn to ransomware

- Vidar and RedLine group turn to distributing ransomware
- Users should avoid unverified sources when downloading files and enhance system security

Ransomed, Cyberattack on Japanese Manufacturing and Telecom Giants

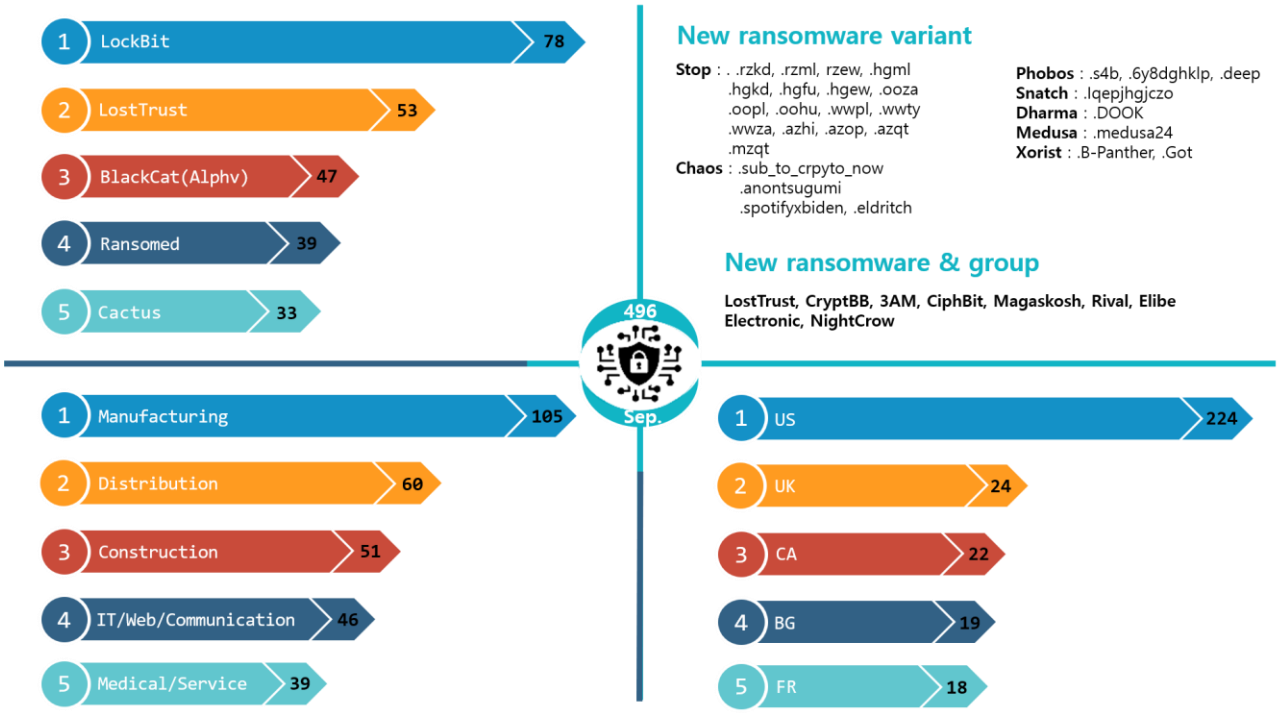
- Japanese manufacturer Sony attempted to blackmail money after the attack, but the negotiations failed and the leaked data was posted
- After attacking Japan's major corporation, NTT DoCoMo, and demand of $1,015,000 for decryption was made

Rhysida, Attack on Kuwait's Ministry of Finance

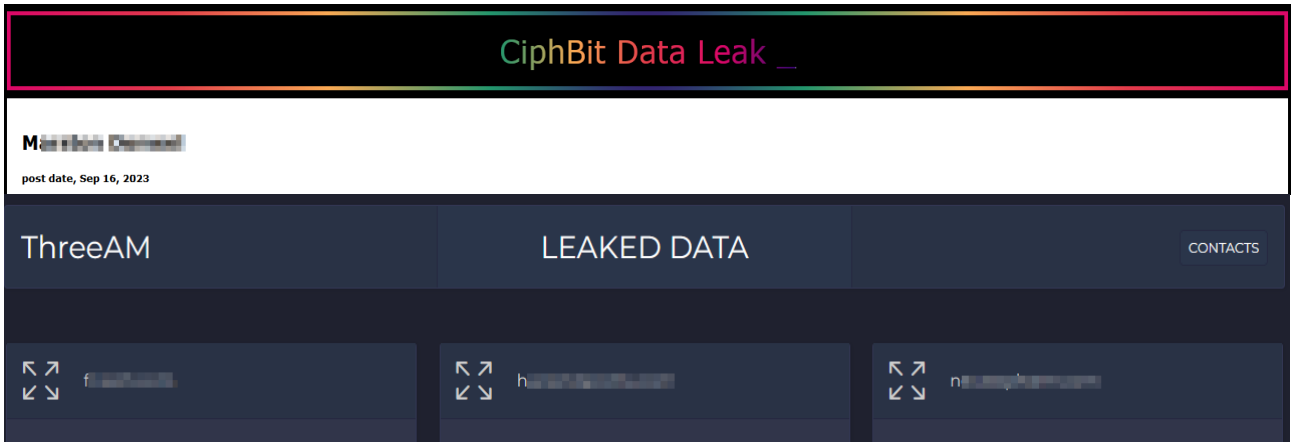
- Some Finance Ministry systems blocked due to ransomware attack
- The government's finance systems are isolated, ensuring that the salary transfer process remains unaffected

■ Ransomware threats

infosec



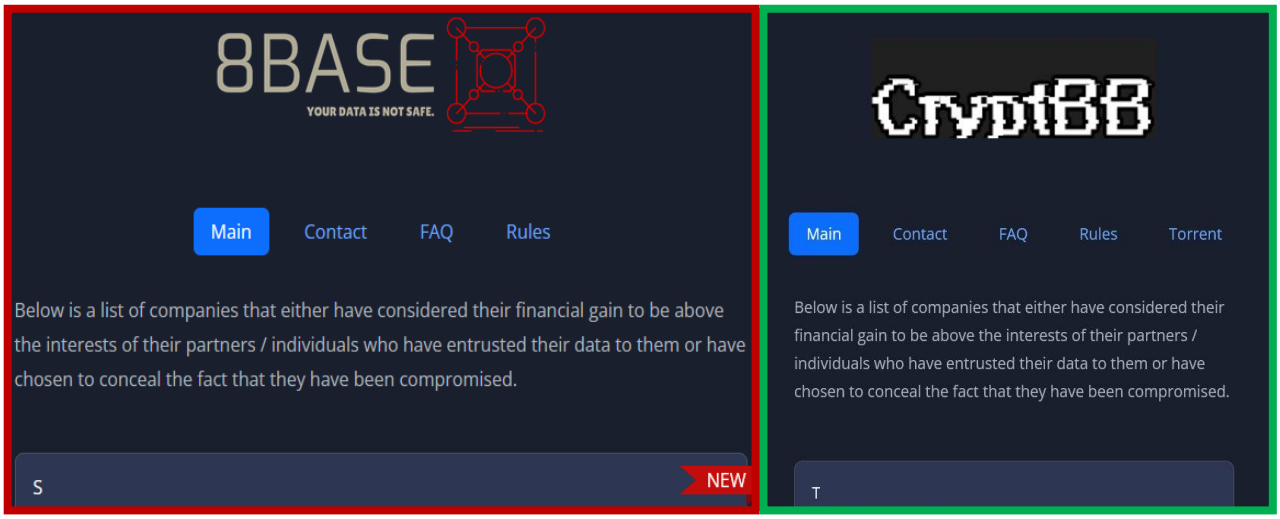
New threats



*Source: images of the CiphBit and 3AM ransomware group sites

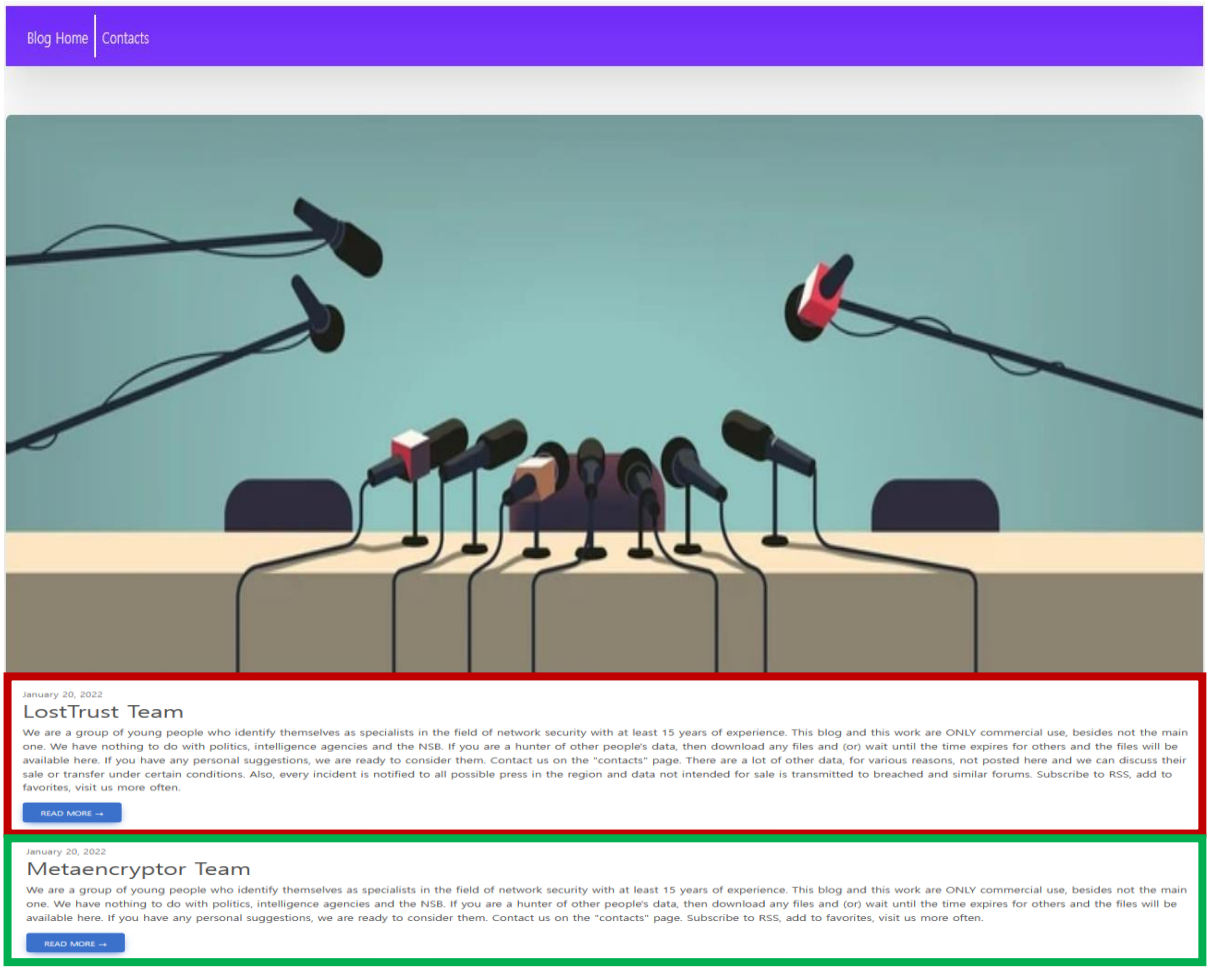
Recently, new and variant ransomwares and related groups seem to be engaged in unusual activities. It was confirmed that the newly discovered 3AM ransomware was used as an alternative when a LockBit affiliate was blocked by the security system during an attack. The relationship between 3AM and existing ransomware sample groups has not been confirmed. The 3AM ransomware is written in the Rust language and provides options such as partial encryption, local/network drive encryption, and access keys written in the ransom note.

As soon as the CiphBit group appeared, it disclosed data on eight damaged companies. Their strategy for distributing ransomware was to impersonate the Bulgarian police. Although all distribution channels have not been confirmed, most of them are spread through phishing emails. So it is important not to click on attachments or links from emails of questionable sources. In order to prevent damage, you must be aware that investigative agencies do not request individuals to visit their office via e-mail.



*Source: images of the 8base and CryptBB ransomware group sites

The CryptBB Ransomware Group, newly discovered in September, appears quite similar to the 8base Ransomware Group. The CryptBB group posted some of the same dark web leak site design and damage targets as the 8base group. However, their group site only contains some data already posted by the 8base group and is not continuously updated. So it appears to be an imitation of the 8base group. As if to support this, 8Base claimed that it had no connection with the CryptBB group and was merely imitating them.



*Source: images of the LostTrust and MetaEncryptor ransomware group sites

Similarly, there are cases of the MetaEncryptor group discovered last August and the LostTrust ransomware group discovered last September. The two ransomware groups use the same dark web leak site design and similar introductory texts. However, unlike the CryptBB and 8base group cases described above, the posted damage targets all show different characteristics (12 cases in the MetaEncryptor group, and 53 cases in the LostTrust group). Like this, imitation between ransomware groups is becoming more frequent. This can be seen as one of the strategies to gain promotional effects or show off their threats.

Top 5 Ransomwares

The LockBit Ransomware Group has been active this month as well as last month, creating many damage cases. Recently, the LockBit Ransomware Group had an incident where many affiliates left or expressed dissatisfaction due to an operational issue. As if to say that it had overcome this and show off the same influence as before, it recorded 78 cases of damage this month, following 122 cases last month.

Recently, the LockBit Ransomware Group has been continuously carrying out ransomware attacks to access target networks and spread the ransomware by exploiting RMM (Remote Monitoring and Management), a commercial remote monitoring and management tool, as part of a large-scale attack. In particular, they are using strategies to avoid detection by using legitimate software. So caution is required. In addition, as they are carrying out attacks by exploiting the RMM tool, efforts should be made to ensure personal and organizational security, e.g. setting up multi-factor authentication and paying attention to phishing.

As mentioned earlier, the newly discovered LostTrust Ransomware Group has the same dark web leak site design and uses phrases similar to those used by the MetaEncryptor group. So there is a possibility of connection or imitation. However, there is no apparent information yet regarding imitation and connection between these groups and other groups. However, as a result of analyzing the LostTrust ransomware, codes similar to those of the SFile ransomware discovered in 2020 were confirmed. So it is possible that the source codes were borrowed or rebranded. The LostTrust Ransomware Group posted a total of 53 cases of damage in September, and it is confirmed that this group has caused a significant number of damages comparable to those caused by the LockBit ransomware.

The BlackCat(Alphv) Group continues to carry out attacks against various targets such as media, resorts, and Azure Storage. They have ransomware variants that can carry out attacks targeting various environments, including Windows, Linux, and ESXi. In addition, they continue to conduct attacks exploiting RMM, vulnerabilities, etc. So they can be said to be quite a threatening group.

The Ransomed Group discovered last August is also attempting attacks targeting companies in various fields. Although it was discovered in August, it was confirmed to have as many as 77 affiliates. In particular, they claim that in addition to cybercrime activities, they own several legitimate businesses and operate by laundering money extorted through cybercrime to finance their businesses.

The Cactus Ransomware Group was first discovered last March, but has been engaging in various activities since July by opening a dark web leak site. They use self-encryption of the binary to avoid detection, and it is confirmed that they mainly use the initial access method that exploits VPN vulnerabilities. They are carrying out ransomware attacks across industries such as manufacturing, distribution, and construction, mainly in English-speaking countries like the United States and the United Kingdom, and are using a strategy of threatening by posting stolen data on a leak site before encrypting files.

■ Focus of Ransomware

Overview of the Knight ransomware

*Source: image of the Knight Ransomware Group site

Knight is a ransomware group rebranded by Cyclops which was discovered around June 2023. The previously discovered Cyclops ransomware was developed in the Go language, a non-mainstream language, but the Knight ransomware was designed to infect Windows, Linux, macOS, ESXi, and Android platforms by providing various builders for each platform. Ransomware attacks are also carried out in various ways. Full-version ransomwares, which include encryption or infostealer, and lightweight versions that only encrypt files are being distributed. Recently, a SPAM campaign attack disguised as a Tripadvisor complaint was also confirmed, and in this campaign, an attack was attempted in the form of .xll[5], an add-in file for Microsoft Excel.

The Knight Ransomware Group consists of four hackers from Russia and Europe. The Knight ransomware, provided as RaaS (Ransomware-as-a-Service), is confirmed to have been prepared for a long time. They have built an easy-to-use interface for affiliates who receive the service, and provide services to use various methods and platforms for attacks, such as lightweight versions and full versions. In particular, in case of infection with a full-version infostealer, the stolen data and personal information can be used for secondary attacks, and the leaked information can be used for double extortion. So caution is required.

[5] xll: A DLL file written in the C language family. An add-in file that allows custom functions or other functions to be developed in Microsoft Excel and used in Excel.

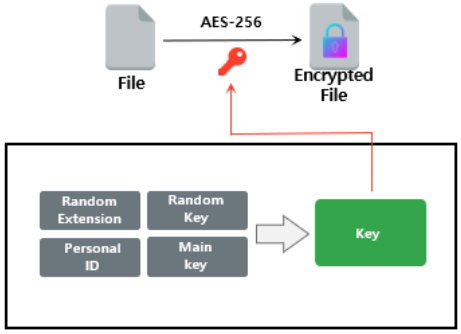
The Knight Ransomware Group provides differentiated and advanced functions in addition to the functions provided by Ransomware-as-a-Service. They actively reflect and support the needs of affiliates through a simple and automated payment system for paying decryption costs, independent dark web chatting for each affiliate and individual wallet addresses for each victim, and customized support. It suggests that the Knight Ransomware Group possesses considerable technological power, and it is a function differentiated from other RaaS. Emphasizing this differentiation, Knight Ransomware Group continues active promotion and activities to increase the number of affiliates.

The Knight ransomware uses a random extension or 'knight_l' depending on the version, and is characterized by intermittent encryption of files when the file size is large and use of a different key for each file, making decryption difficult. Also, for execution, it is necessary to create and then execute shell codes through an access-key or binary provided by the server, making it difficult to analyze arbitrarily. The encryption key generation process requires a combination of random extension + unique ID of the victim + main key + random key. Since it is very difficult to identify and decrypt randomly generated elements, it seems that several defense mechanisms are installed to prevent the ransomware from being arbitrarily decrypted. Meanwhile, the encryption logic using ChaCha20 + AES256 is similar to the logic of LockBit and Babuk. So it is suspected that there is a connection with them.

Knight Ransomware

Encryption Key

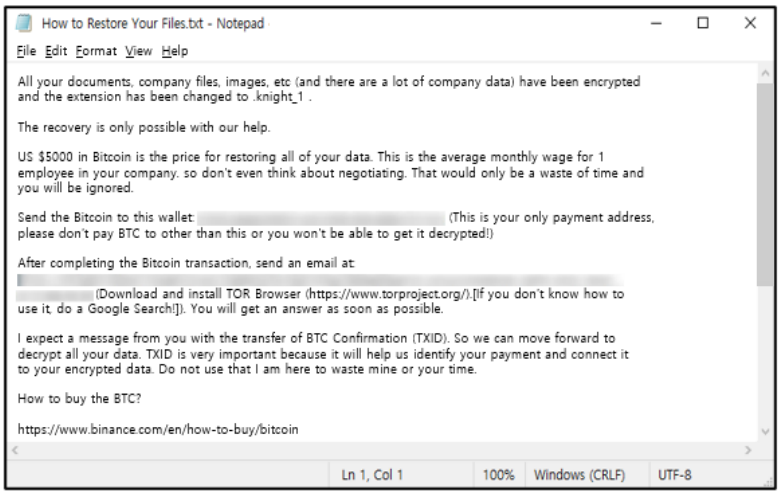
Encrypt files with AES-256 and encrypt their keys with ChaCha20



Characteristics

- RaaS
- DLL Side-Loading
- Partial Encryption
- AES-256 & ChaCha20 Encryption
- Anti-VM & Anti-Sandbox
- Terminate Service and Process

Ransom Note



How To Restore Your Files.txt

Changed Extension

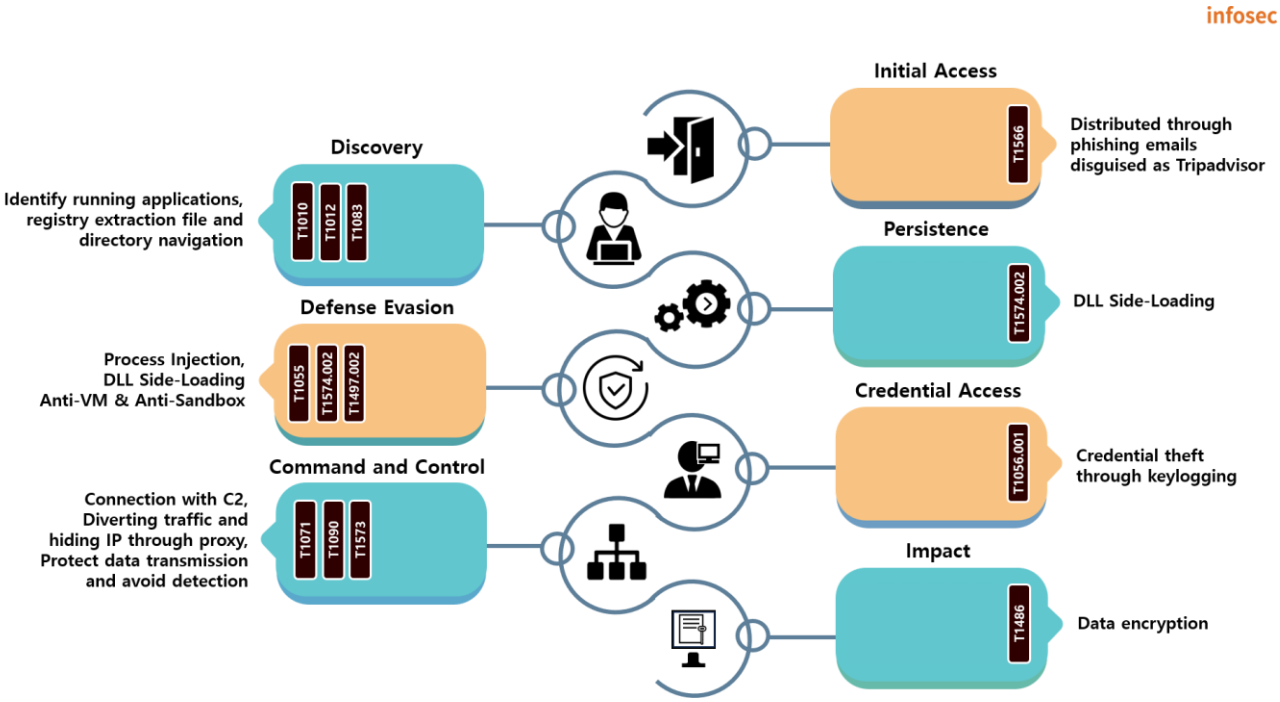
Random generation

knight_l

Production Language

C++

Knight ransomware strategies



The Knight ransomware targets various platforms such as Windows, Linux, macOS, ESXi, and Android. This ransomware has recently been distributed through phishing e-mails disguised as Tripadvisor's complaint page. Shell codes, which are initially executed through the page connected to the phishing e-mail, are downloaded and executed after injection[6] into the normal process after two decryptions. Detection avoidance technologies include DLL Side-Loading[7], Anti-VM[8] and Anti-Sandbox[9] techniques, and this ransomware obfuscates files and information required for execution.

The Knight ransomware also uses key logging[10] to intercept user input to steal personal information. In addition, it collects various kinds of information by searching the system, network, software, files and directories for additional actions, and is also equipped with a function to take screenshots and collect clipboard data to collect important data.

[6] Injection: a technique for inserting and executing a malicious DLL into a normal program

[7] DLL Side-Loading: an attack technique that loads and executes a malicious DLL instead of a normal DLL used in the program

[8] Anti-VM: a technique for bypassing analysis by verifying that it is running on a virtual machine

[9] Anti-Sandbox: a technique for bypassing analysis by verifying that it is running in a sandbox

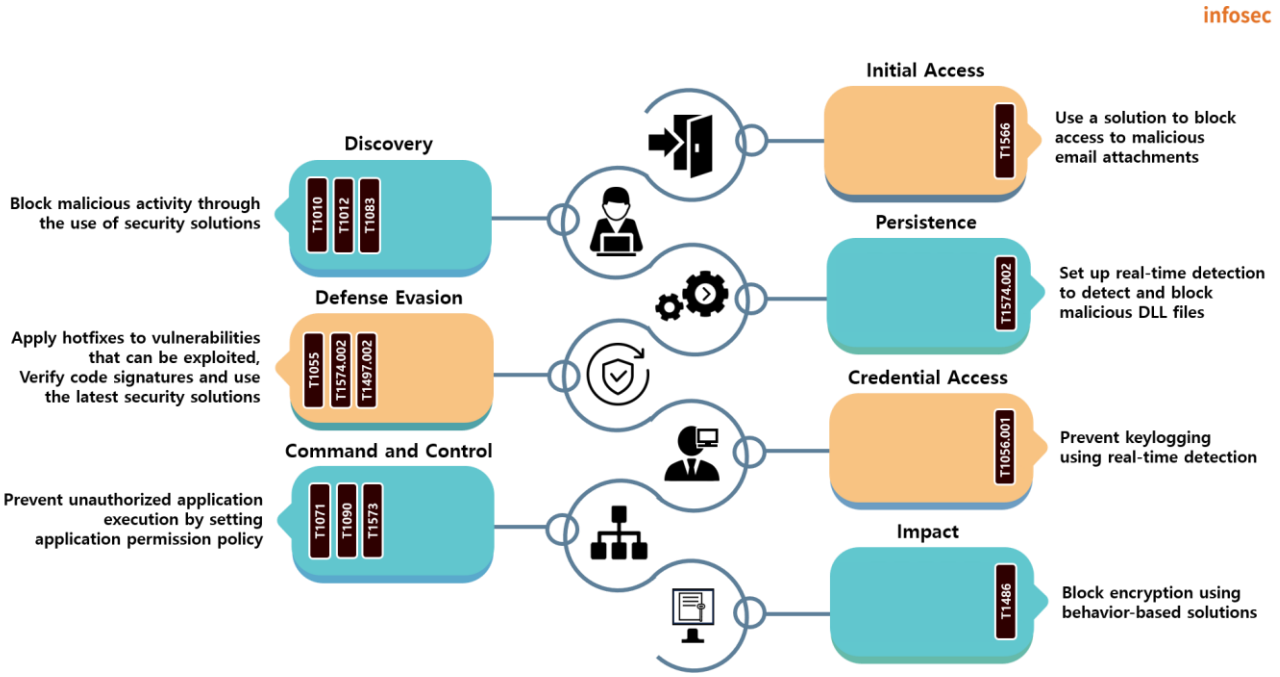
[10] Key logging: a technique for recording the keys the user types on the keyboard

In particular, the Knight ransomware is capable of encrypting local drives and network files through SMB (Server Message Block)[11]. What is noteworthy here is that a normal ransomware performs the data backup disabling function to prevent recovery, but quite unusually, this function has not been confirmed in the Knight ransomware. So partial recovery may be possible in some cases.

The Knight ransomware uses a double extortion strategy, i.e. it not only encrypts files, but also leaks data before encrypting files through a full-version infostealer. Infostealer provides various options, such as the maximum size of the file to be stolen, the option to send split data, the path to be stolen, and the extension.

[11] SMB: a Windows OS protocol designed to share resources existing on a network

Countermeasures to the Knight ransomware



As the Knight ransomware performs malicious actions by exploiting basic system functions, countermeasures are limited. First, the Knight ransomware is spread through a phishing e-mail campaign. So be careful not to execute attachments or links in e-mails from unknown sources. In order to respond more actively, it is necessary to use a system that blocks malicious e-mails and apply Contents Disarm & Reconstruction (CDR) solution.

Second, the Knight ransomware operates secretly within the system and performs registry manipulation and searches on various system elements to avoid detection. Their typical method is to escalate privileges and encrypt files through DLL Side-Loading and Process Injection. To prevent exploitation of these legitimate system functions, ransomware must be blocked through the use of a real-time security solution that detects malicious behavior. Also, since network encryption is performed through SMB during the internal diffusion process, preemptive preventive measures by blocking SMB ports are necessary.

Lastly, regular updates are required to update the system and apply security patches, and threats must be detected through monitoring to detect log events and abnormal signs. Depending on the environment, it may be difficult to apply all defensive measures, but it is necessary to establish a process that suits the corporate environment and establish a plan to block and mitigate ransomware step by step.

Indicator Of Compromise

Knight : SHA256

5ACE35ADEB360B9E165E7C55065D12F192A3EC0CA601DD73B332BD8CD68D51FE

75E227A3A41DC1C2D4384E877D88F9A06437A49F2C71F8EFA7E2CC60BAB6CC4A

4F1E46AC9E46F019D3BE3173F0541F5ED07BDE6389180CD7E8255D35B49F812E

DCD45491DD78122EFEDE7AE460A4D3E0B20AEB13965A8EB14EEF862FBCE66366

262618E0D48DB5B244759E07787DDE11736555AC0BD3C64FEE2556DA50DEA02

9123E42CDD3421E8F276AC711988FB8A8929172FA76674EC4DE230E6D528D09A

File Name

TripAdvisor Complaint - Possible Suspension.exe
TC4ShellHost.64.exe
TripAdvisor_Complaint-Possible-Suspension.xll
TripAdvisor-Complaint-Avywfp.PDF.htm

■ Reference sites

URL: https://cert-agid.gov.it/news/il-ransomware-knight-distribuito-in-italia-tramite-falsa-fattura/

URL: https://gridinsoft.com/blogs/qakbot-hacked-removed-from-700k-machines/

URL: https://www.mirror.co.uk/news/uk-news/russia-linked-hackers-hit-uk-30850139

URL: https://thecyberexpress.com/cactus-ransomware-group-major-corporations/

URL: https://www.bleepingcomputer.com/news/security/cisco-warns-of-vpn-zero-day-exploited-by-ransomware-gangs/

URL: https://www.bleepingcomputer.com/news/security/us-and-uk-sanction-11-trickbot-and-conti-cybercrime-gang-members/

URL: https://www.scmagazine.com/brief/save-the-children-suspected-to-be-compromised-by-bianlian-ransomware

URL: https://www.bleepingcomputer.com/news/security/hackers-use-new-3am-ransomware-to-save-failed-lockbit-attack/

URL: https://www.infosecurity-magazine.com/news/cuba-ransomware-undetectable/

URL: https://www.bleepingcomputer.com/news/security/ransomware-access-broker-steals-accounts-via-microsoft-teams-phishing/

URL: https://www.trendmicro.com/en_us/research/23/i/redline-vidar-first-abuses-ev-certificates.html?&web_view=true

URL: https://www.teiss.co.uk/news/news-scroller/airbus-investigating-major-cyber-attack-claimed-by-the-ransomed-hacker-group-12856

URL: https://cybersecuritynews.com/ransomed-vc-japanese-giants/

URL: https://securityaffairs.com/151501/cyber-crime/rhysida-ransomware-kuwait-ministry-of-finance.html