TLP: GREEN

Threat Trend Report on Region-Specific Ransomware

Ransomware Active in South Korea, Taiwan, China, and Chile

V1.0

AhnLab Security Emergency Response Center (ASEC)

Feb. 14, 2023

AhnLab

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

The version information of this report is as follows:

Version	Date	Details
1.0	2023-02-14	First version

Contents

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Localized Ransomware Attacks

1) Background

Currently, ransomware creators include individuals, cyber criminal gangs and state-supported groups. Out of these individuals and groups, cyber criminal gangs are the most proactive in ransomware development, while individuals and state-supported groups are less so. Privately developed ransomware is most often for research purposes with the intention of destroying data. Some state-sponsored threat groups also develop ransomware. The purpose of these cases is not for financial gain either but for data destruction, and Wipers, which do not allow recovery, are created disguised as ransomware.

Some ransomware gangs do not attack medical institutes or social infrastructures. This could be due to social criticism and to avoid drawing attention from legal authorities. To avoid the surveillance of regional law enforcement, these threat actors also design ransomware to not function in systems in specific regions.

As the ransomware industry grew, cyber criminal gangs could not undertake all the tasks by themselves. So, they operate via Ransomware-as-a-Service (RaaS) and invite affiliates to distribute the ransomware. These affiliated organizations are called initial access brokers (IABs), and they are responsible for infecting systems with ransomware.

Ransomware is the most popular and profitable method for cyber criminal gangs. To maximize their profits, people involved often attempt attacks tailored to local environments. These organizations also tend to spread ransomware in familiar areas. The language, programs, and cultures differ by location, so this process often requires attack methods suitable for specific regions. Also, there are ransomware gangs that started their activities locally. These organizations first conduct activities in regions familiar to themselves before branching out to other locations.

Currently, there are signs of localized ransomware attacks in some areas, but it cannot yet be said that localized ransomware attacks are the mainstream.

2) Localization Strategies for Each Stage

Threat actors usually apply their localization strategies to the 'initial infiltration' and the last 'security product incapacitation' stages.

Attacks using emails are the most common. Early ransomware attacked with emails written in English, but upon receipt of English emails, users from non-English speaking countries would not read them and instead mark them as spam or simply delete them. Due to such language barriers, threat actors wrote emails using machine translation, but due to the limits of machine translation performance, the content was crude and no serious harm could be inflicted. Afterward, with the joining of a member who speaks the target language, the emails become natural and sophisticated.

Targeted ransomware mostly attacks corporations, and it infiltrates by exploiting predictable RDP passwords, mail servers, DB servers, or VPN server vulnerabilities. There are also cases of infiltration through vulnerabilities of management software used in particular regions, servers of external affiliates, or servers open for access from these partners. After infiltrating into the internal system, other systems in the network are overtaken one by one through lateral movement. The process up to this point is similar to that of typical APT attacks, but unlike data breaches, the target system must be infected with ransomware. Some ransomware infects only servers, while others attack user systems as well. To distribute the ransomware, IIS web services are installed or file distribution features of asset management programs are used.

The final hurdle for threat actors is endpoint security products such as anti-malware or EDR products. Different security products are widely used in different regions. For the ransomware to run successfully, threat actors must evade detection from, or disable endpoint security products. The easiest method is to uninstall the security products. An investigation into the ransomware reported by the attacked companies often reveals that they are already being detected in anti-malware products. In some cases, threat actors bypassed making changes to evade the detection of security products and instead uninstalled anti-malware products entirely. There are also cases where real-time protection features are turned off or the ransomware file is added to the whitelist to avoid detection.

When the threat actor is unable to change the security product settings, they may run the ransomware through other methods. In the case of one victim, the threat actor attempted to execute the ransomware 3 times. The first two attempts were detected and blocked by an

anti-malware product, but instead of giving up, the threat actor evaded detection by encrypting the ransomware, creating a loader, and executing it in the memory.

Cases of Region-Specific Ransomware

According to Dragos, there are ransomware strains that are active in specific regions.[1] Below is a map of ransomware active in each region based on multiple sources.

Figure 1. Locally active ransomware

Name	Region	Details
ARCrypter (ChileLocker)	Chile	Currently expanded to Canada and China
ColdLock	Taiwan	Attacked many Taiwanese organizations in 2020
Cheers	Japan	
Gwisin	Korea	
Lorenz	US	
Masscan	Korea	
Sparta Blog	Spain	
Stormous	Vietnam	

Table 1. Locally active ransomware

[1] https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q3-2022/

Cases of localized activities aside from regional activities of general ransomware organizations are as follows.

1) Republic of Korea

The timeline of major ransomware in Korea is as follows.

Year	Ransomware	Details
2015	CryptoLocker	First large-scale infection
2016	VenusLocker	Attack using perfectly fluent Korean emails
2017	Magniber	Active only in early Korean Windows
2018	GandCrab	Korean GandCrab distribution group
2019	Clop	Targeted ransomware attacks
2021	Gwisin	Discovery of ransomware active only in Korea
2022	Masscan	Discovery of ransomware active only in Korea

Table 2. Major ransomware active in Korea

There was no massive damage from ransomware attacks in Korea until 2015. The first official attack case was the CryptoLocker infection in 2015 that occurred through a famous IT website.[2]

In December 2016, VenusLocker attacks involving emails written in Korean were identified.[3] The threat actor group is called Venus IAB, and they distribute ransomware in Korea. Emails in past ransomware attacks used broken Korean written via machine translation, but the Korean used by Venus IAB was highly natural and contained slang or even profanities used by actual Koreans. It is thus likely that there is a Korean or someone fluent in Korean in the group. Many users had their systems infected after opening attachments to emails written in perfect Korean.

They are called the VenusLocker group because they distributed VenusLocker in their early

[2] https://www.boannews.com/media/view.asp?idx=46010&page=1&kind=1

[3] https://asec.ahnlab.com/ko/1054/ (This report supports Korean only for now.) - ASEC Analysis Team

days, but they also used other ransomware such as AutoCryptor, GandCrab, BlueCrab (Sodinokibi), Nemty, Makop, and LockBit, and even installed CoinMiners. While the types of ransomware changed, the string VenusLocker_korean could be found in the LNK file attached to emails. Moreover, the name of the folder used by user 'l' was 'Yangjinee' in Korean. Yangjinee (pallas's rosefinch) is the name of a bird.

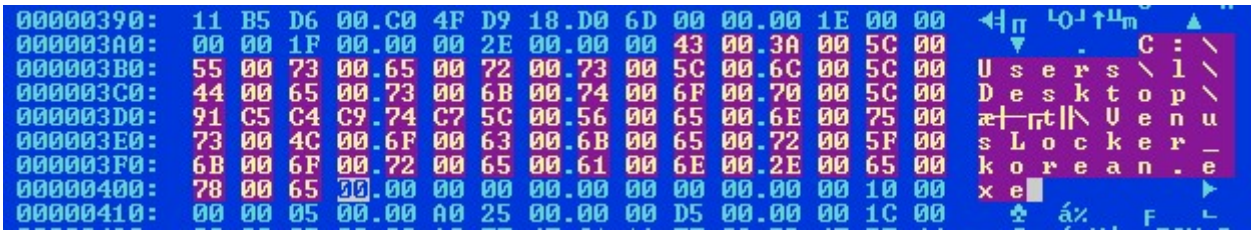

Figure 2. Strings within the LNK file that signify the creator is the same

The font used in the bait document is 'SimSun', a Chinese font not usually used by Koreans.

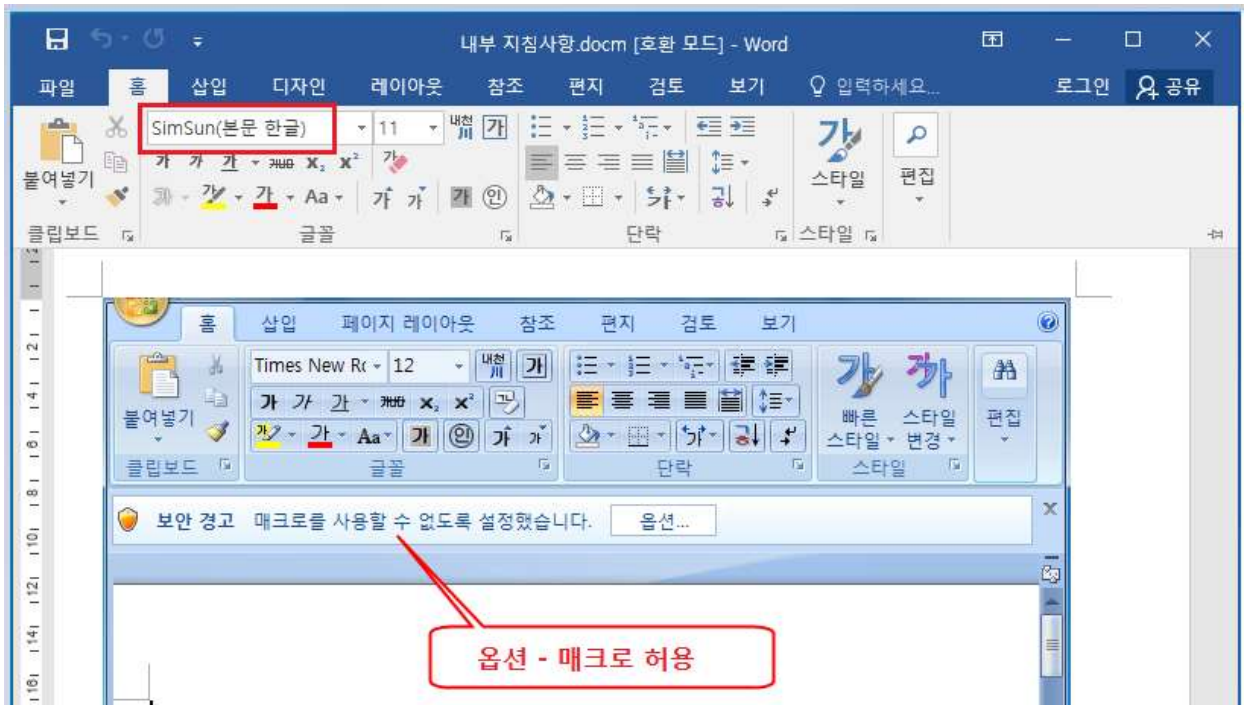

Figure 3. Bait document using the SimSun font

From this, we assume that the writer of the bait document is Chinese or a person fluent in Chinese.

Magniber ransomware was first identified in October 2017. This ransomware targets Korea, and some variants are only active in Korean Windows and Korean IP addresses.

```
179  if ( GetSystemDefaultUILanguage() != 1042 )   // Korean ?
180    DeleteItSelf_4075A0();
```

Figure 4. Magniber ransomware checking for the use of Korean

Infection of Magniber was conducted in a fileless format for some time and had to be detected via behavior-based detection by anti-malware products. Recently, various file extensions are being used. The ransomware is still active, and there have been reports of its infection in January 2023 in Europe, which shows they are expanding their boundaries to other countries.[4]

GandCrab ransomware was first found in Korea in February 2018. At first, it attacked using emails in broken Korean generated via machine translation. Eventually, their emails were written in fluent Korean. At the time, it was thought that a Korean or a fluent Korean speaker was participating, but as this is run as Ransomware-as-a-Service (RaaS), there is a high possibility that the writer is a local partner. There are cases where only users in Korea are infected through IP checks done before infection. If they are IAB, they could have made a contract to attack only Korean regions. About a year and a half of attack and defense progressed between AhnLab analysts and GandCrab creators until GandCrab ceased their activities in 2019.[5]

It seems that there are multiple GandCrab ransomware distributors in Korea. In February 2021, a Korean in their 20s was apprehended for distributing the GandCrab ransomware. He is said to have sent over 6,000 emails impersonating the police in February 2019. The ransomware developer received BitCoins, and the distributor obtained 7% of the profit through a broker. The total profit amounted to KRW 12 million, which is a lower figure than expected.

In 2019, targeted ransomware such as Clop started to surface, attacking corporations. Many of them suffered damage, and ransomware was no longer a personal problem but a corporate problem.

Gwisin ransomware is active in Korea, and the name 'Gwisin' is a transliteration of the Korean word for 'ghost'. From this fact alone, it is likely that a person who is familiar with the Korean culture and fluent in Korean was behind the Gwisin attacks.

[4] https://twitter.com/AvastThreatLabs/status/1613248553626787842

[5] https://asec.ahnlab.com/ko/1281/ (This report supports Korean only for now.) - ASEC Analysis Team

Figure 5. Gwisin ransomware

Gwisin ransomware was first found in September 2021. It was covered from time to time on the news until the spring of 2022 and no public information was released until July 2022. The affected company was included in the ransom note and a client alerted their security provider, but because they wished to conceal their infection, there was limited information shared even between Korean security providers for some time. There are Windows and Linux versions of Gwisin. The Windows version is distributed in MSI file format and the actual ransomware is encrypted within the Binary.helper file. Additional arguments are required for the Windows version to run. Having only the executable file and not knowing the additional arguments, analysts may find the file suspicious but unable to find out precisely what behaviors it performs. However, the Linux version encrypts files without additional arguments. The ransom note contains the name of the affected company and the analysis details after the data breach occurred. This tells us that the threat actors are fluent in Korean and familiar with the security situation in Korea.

Masscan ransomware became known in the summer of 2022 through an attack on a certain service, but it had been active in Korea since April 2022. The threat actors target vulnerable DB servers, and according to KISA, 64% of the reported ransomware attacks on DB servers until September 2022 were Masscan attacks. A configuration file is needed for the ransomware to run correctly. Unfortunately, the configuration file has not currently been procured and its specific content is unknown. After file encryption, the .Masscan file extension was added to the files, and the shared network folder was also encrypted. The Financial Security Institute released a Threat Analysis Report in December 2022.[6] According to the

[6] https://www.fsec.or.kr/bbs/detail?menuNo=244&bbsNo=11174

institute, there have been circumstances of suspected Masscan ransomware infection in the US, Vietnam, and the Czech Republic.

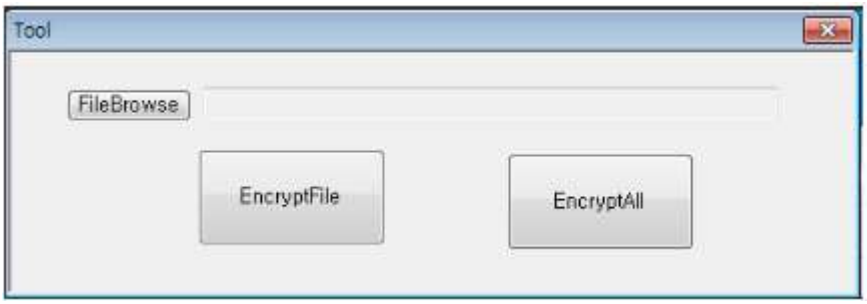

Figure 6. Masscan ransomware execution

State-sponsored threat groups that are active in Korea are also creating ransomware. In June 2021, Kaspersky revealed that the Andariel group used ransomware in their attacks in 2020,[7] and through the published IOC, AhnLab found a client report of a variant in September 2020. While no actual damage was done, it was not strange to find that they used ransomware in their attacks because the Andariel group attacked multiple Korean corporations with their wiper. In July 2022, it was announced that the Maui ransomware was attacking medical institutions in the US[8], and Kaspersky revealed that the Maui ransomware had connections with the Andariel group.[9] It has not been confirmed whether or not the Maui ransomware had been active in Korea.

The Kimsuky group started its activities in Korea, but now they target victims worldwide. In December 2022, the Korean police published the results of investigations on the Kimsuky group that had been conducted in May 2022. A notable point in this report is that 13 shopping mall company servers used in the C2 server were encrypted before a demand for a cryptocurrency ransom was made.[10] The amount was several million Korean won and this led to a hypothesis that it could be an individual aiming to earn pocket money. Further observation will reveal whether these ransomware infection cases are activities of the Kimsuky group as an organization or a personal stride by one of its members.

[7] https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

[8] https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

[9] https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/

[10] https://www.youtube.com/watch?v=vVC067aGEkk

There is also ransomware that has not been categorized yet. It cannot be determined if it is an unreported or unidentified variant. The case could not be attributed to a party, but a search query using the email address in a ransom note matches the information on MedusaLocker.[11] This ransomware was thought to be a MedusaLocker variant, but there was no file hash information provided. The information was then compared to information on MedusaLocker from other security providers, but the code cannot be seen as that of MedusaLocker. There is a possibility that MedusaLocker has since seen a great change to its code, or that the ransomware distributor distributed another ransomware with the same email address.

There had been a case in Korea where a computer repair company infected its client computers with ransomware.[12] Remote control malware was installed in the computers of clients who requested data recovery, and when the ransomware was executed and clients placed recovery orders, they received the fee. The operators extorted about KRW 360 million from 40 victims.

There are ransomware negotiation services in Korea. When infected with ransomware, people generally search for ransomware recovery on web portals. A search query for ransomware recovery on the most commonly used web portal in Korea returns ads that claim to be data recovery services but are in fact companies that negotiate with ransomware gangs. When a ransomware incident occurs, corporations contact negotiation services and security providers. Negotiators earn a higher profit than security providers through the process of reaching a discount on the ransom requested by the threat actor and receiving a portion in return. Although a lower ransom can be paid through the effort of these services, some suspect their connections to the ransomware gangs.

2) Taiwan

More than 10 different Taiwanese organizations were subject to attacks from the ColdLock ransomware in May 2020.[13] This includes a targeted attack on CPC (Taiwan Chinese Petroleum Corporation), the largest national gas company in Taiwan.

---

[11] https://www.cisa.gov/uscert/ncas/alerts/aa22-181a

[12] https://therecord.media/south-korean-police-arrest-computer-repairmen-who-made-and-distributed-ransomware/

[13] https://www.trendmicro.com/en_us/research/20/e/targeted-ransomware-attack-hits-taiwanese-organizations.html

According to a Taiwanese security company,[14] the threat actor gained initial access privilege on the targets before April 26, after which backdoors were installed and ransomware was distributed across the entire system between May 1 and May 3 when most employees were off work.

On May 15, the Ministry of Justice Investigation Bureau released a relevant investigation report.[15]

Figure 7. Investigation results

Security researchers expect the ultimate goal of this attack to be political motives rather than financial gain.

3) China

There have been reported cases of ransomware active in China that was created there or exploited vulnerabilities of Chinese software.

On December 5, 2018, there was a large-scale infection of ransomware in China where after file encryption, 110 yuan (about KRW 20,000) was demanded over WeChat.[16] Thankfully, the

[14] https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5

[15] https://www.mjib.gov.tw/news/Details/1/607

[16] https://www.bleepingcomputer.com/news/security/ransomware-infects-100k-pcs-in-china-demands-wechat-payment/

incident was rudimentary and a recovery program was able to be made. The suspect was identified as well, and Chinese law enforcement apprehended ransomware developer Luo Moumou.[17]

The Tellyouthepass ransomware is said to have infected systems by exploiting the zero-day vulnerability of Chanjet T+, corporate management software.[18]

Recently, Russian ransomware gangs have been advertising in Chinese, showing attempts to recruit Chinese members.[19]

4) Chile

On August 25, 2022, Chile's Computer Security Incident Response Team (CSIRT) announced that the computer systems of a Chilean government organization became a target of a ransomware attack.[20]

This involved ransomware that had not been reported before. It became known as Chile Locker as it was first found in Chile, and it is also called Arcrypter.

Its specific attack methods are not yet known, and reports of its detection were also raised in China and Canada.[21]

Prospects of Region-Specific Ransomware

[17] https://www.bleepingcomputer.com/news/security/chinese-police-arrest-dev-behind-unnamed1989-wechat-ransomware/

[18] https://www.antiy.cn/research/notice&report/research_report/20220830.html

[19] https://resecurity.com/blog/article/nevada-ransomware-waiting-for-the-next-dark-web-jackpot

[20] https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-incidente-en-servicio-publico/

[21] https://blogs.blackberry.com/en/2022/11/arcrypter-ransomware-expands-its-operations-from-latin-america-to-the-world

There are both possibilities of increase and a temporary phenomenon when discussing prospects of region-specific ransomware.

The possibility of the localization of ransomware intensifying is based on the fact that ransomware is one of the most profitable means for cyber criminal gangs. Local crime organizations can also partake in ransomware gangs. As local crime organizations cannot first start their activities globally, there is a higher possibility that they will commence their activities in familiar regions or neighboring countries. Even if many ransomware gangs run as RaaS, local IABs can continue to exist and partially be active in specific regions, attempting to adapt to the concerned environment.

A negative view is that ransomware localization is a temporary phenomenon and cyber crime gangs will want to be active in various regions. Activities in locations where the ransomware developer lives can draw attention from law enforcement, so these developers may target other countries. Aside from this fact, ransomware known to be active only in certain regions can actually be active in other areas, and region-specific ransomware may be a minority.

More case studies from a wider scope of areas are needed for details on region-specific ransomware.

AhnLab Response Overview

The aliases and the engine version information of AhnLab products are shown below. Even if the activities of this threat group have been identified recently, AhnLab products may have already diagnosed related malware in the past. While ASEC is tracking the activities of this threat group and responding to related malware, there can be variants that have not been identified and thus are not detected.

Ransomware/Win.Agent.C4556366 (2021.07.18.00)
Ransomware/Win.Encrypt.C5211137 (2022.07.19.02)
Ransomware/Win.Encrypt.C5212584 (2022.07.22.02)
Ransomware/Win.Gwisin.C52149645 (2022.07.27.03)
Trojan/Win.Agent.C4700357 (2021.10.15.00)
Trojan/Win32.ColdLock.R335649 (2020.05.08.08)
Trojan/Win32.MSILKrypt.C4096440 (2020.05.14.06)

Conclusion

Ransomware is evolving to RaaS and targeted attacks. This report stemmed from the question of whether ransomware is becoming localized following the emergence of ransomware that are active only in certain regions.

Cases in Korea show that local IABs and local ransomware are active simultaneously. There are also other ransomware strains that are difficult to be classified into existing categories, but this could be due to misjudgment from insufficient information.

Endpoint security products are the last line of defense. Knowing this, threat actors uninstall these products or turn their real-time protection features off. Thus, users must set limited permissions regarding changing anti-malware settings, and endpoint security products with abnormal settings must be detected by central management products. Unfortunately, threat actors complete their job in just a few hours, and admins may not catch their acts in time.

To prevent damage from ransomware, companies must track attack routes precisely to stop repeated attacks. However, many corporations choose to resolve the issues by paying a negotiation agency instead of implementing fundamental measures. These corporations are at risk of not only ransomware but also other types of attacks.

While there are cases where detailed information is not publicly available, users must pay attention to ransomware cases that occur in each country. Information on attack vectors, ransomware gangs, and their ransomware must be shared because locally active ransomware gangs may branch out to neighboring regions.

Indicators of Compromise (IOC)

A portion of the following IOC quotes other analysis reports, and there are some unverified cases because samples could not be obtained. Updates may occur without prior notice when new information is found.

File Paths and Names

The file paths and names used by the threat group are as follows. File names of some malware or tools may be the same as those of normal files.

Binary.helper DeEnCrypt.exe javaw.exe main.dll Read.exe scar.exe svhost.exe Update.exe window.exe windows.exe windows_x32.exe Winlo.exe

File Hashes (MD5)

The MD5 of the related files are as follows. However, sensitive samples may have been excluded.

ColdLock 28991de4ef6d97b324503991adb6bc0b 0998f695ddd72f1ed0f8937929f1afdd Gwisin 13eef02d5e5f5543e83ad8c8a8c8ff9a 1c9458b64ff31fed8f7c1f403d5e797a 26f663daa327e9f720177d01a83b05b5 58ea26d1faa6231118bcde64734c7f22 995ab4d1736df696563f9c377e51c60c Masscan

566c0616437be7bbd5ce6781981cf5e5
95bf1f7f6997d46f569f521f776b3ff7
9760a6cbb9612ce56b7a2480ec999f7a
d055658ed50601a747d0970ed1db6242
dd5494973313e3ece576a41933a512bf
ea6f19b477aef535dd52132e795b4b40
f4d74e57fafd190e32264ba66f372194

Tellyouthepass

7b2680c6bdf2a1ab1a59c29f7219730a
26c2df81a69afc059736d815ea136bde
c31c7a4e3ec51053ab508fbed3bb8308

References

[1] Trend Report on Ransomware (https://atip.ahnlab.com/ti/contents/issue-report/trend?i=248edf72-0064-4815-97c9-36892b728609) (This report supports Korean only for now.) - ASEC Analysis Team
[2] CHA Minseok, 'Localization of Ransomware, New Change or Temporary Phenomenon?' (https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_2_3_jacky_en.pdf)
[3] TellYouThePass Ransomware (https://atip.ahnlab.com/ti/contents/asec-notes?i=39ef28c9-4e1a-428b-a64b-bda8e22f2ee1) (This report supports Korean only for now.) - ASEC Analysis Team

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
www.ahnlab.com
www.asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency Response Center(ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab