

Localization of Ransomware, New Change or Temporary Phenomenon?

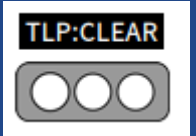
- Characteristics and Techniques of Active Ransomware Gangs in Korea

CHA Minseok (Jacky Cha, 車珉錫)

Senior Principal Threat Intelligence Researcher

Threat Intelligence Team | ASEC

JSAC 2023 (January 26, 2023)



More security,
More freedom

:~\$whoami

- CHA Minseok (Jacky Cha, 車珉錫)
 - Senior Principal Threat Intelligence Researcher at AhnLab
 - Joined AhnLab in 1997 (25+ years of experience in Anti-Virus technologies)
 - ICT Cyber Expert Group in Korea, Former AVAR (Association of Anti-Virus Asia Researchers) Director, Former WildList Reporter
 - Speaker at AVAR, AVTOKYO, CARO Workshop, CODE BLUE, HITB GSEC Commsec, JSAC, SECUINSIDE and Virus Bulletin
 - Enjoys old video games (Apple][, Atari 8 bit, Commodore 64, MSX, MS-DOS) and old Anime

Table of Contents

- 1 Recent Ransomware Trends**
- 2 Localization of Ransomware?**
- 3 Case Study: Republic of Korea**
- 4 Characteristics of Targeted Ransomware (in Korea)**
- 5 Outlook of Ransomware Localization**
- 6 Conclusion**

1

Recent Ransomware Trends

Ransomware

- Ransomware
 - Greatest concern for customers
 - RaaS (Ransomware as a Service)
 - Targeted attack
 - Recovery Tool: Securing ransomware bug and key

Royal Mail hit by Russia-linked ransomware attack

🕒 12 January

[ASIA](#) [Privacy & Security](#)

Osaka hospital hit by ransomware: report

It is now the fourth known cyberattack on a Japanese hospital this year.

By [Adam Ang](#) | November 02, 2022 | 04:34 AM



Photo by Markus Spiske/Pexels

On the morning of 31 October, Osaka General Medical Center in the city of Osaka, Japan reported a system outage caused by a ransomware attack on its EMR system.

Following the attack, the 865-bed hospital immediately postponed non-emergency outpatient services and turned to manual operations using paper records, according to a [news report](#) by public broadcaster NHK. The incident has affected around 1,000 patients, another [news report](#) noted.

* Source: <https://www.bbc.com/news/business-64244121>, <https://www.healthcareitnews.com/news/asia/osaka-hospital-hit-ransomware-report>

Recent Ransomware Trends

- Characteristics of Recent Ransomware
 - Target : Individuals or companies (Targeted attack)
 - RaaS (Ransomware as a Service) : Emergence of local partners. Localized attack attempts
 - Certain targets excluded from attacks (Medical Institution, Critical Infrastructure) – Some Ransomware Gangs

Ransomware gang apologizes, gives SickKids hospital free decryptor

By **Lawrence Abrams**

 January 1, 2023  02:00 PM  7

* Source: <https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-gives-sickkids-hospital-free-decryptor/>

- Attack Vectors : Email, Server Vulnerability -> Distributed using company environment (Management Software)
- Emergence of Wipers disguised as ransomware
- Ransomware development by nationally supported Threat Actors
- Localization?

2

Localization of Ransomware?

Localization of Ransomware

- Localization of Ransomware
 - Due to the differences in language, culture, environment, and habits, threat actors use various methods of attacks according to region and language
 - Language : attacks used emails written in local language
 - Not active in certain regions in order to avoid being tracked by the legal authorities in those areas
 - Add Local Program Extension (local word processor), Bypass Local AntiMalware (Exclude specific Path, Bait Files)
 - Ransomware active in certain regions discovered (Korea, Taiwan)

APT & Targeted Attacks

Targeted Ransomware Attack Hits Taiwan Organizations

A new targeted attack has infected several organizations in Taiwan with a new ransomware family, which we have dubbed ColdLock. This attack is potentially destructive as the ransomware appears to target databases and email servers for encryption.

By: Trend Micro
May 06, 2020

* Source: https://www.trendmicro.com/en_us/research/20/e/targeted-ransomware-attack-hits-taiwanese-organizations.html

Regionally Active Ransomware

- Region-specific active ransomware
 - ARCrypter (ChileLocker): Chile -> Canada, China
 - Cheers: Japan
 - Gwisin, Masscan: South Korea
 - Lorenz: US
 - Stormous: Vietnam
 - Sparta Blog: Spain
 - ColdLock: Taiwan

Ransomware Victimology Trends

During Q3 of 2022, Dragos continued to observe trends in the victimology of ransomware groups. This does not, however, determine the permanent focus of these groups, as victimology can change over time. Three more ransomware groups were observed targeting industrial sectors and regions of the world in this last quarter than in Q2 of 2022. Based on our analysis of the Q3 2022 timeframe, Dragos observed that:

- Ragnar Locker has been targeting mainly the Energy sector.
- ClOp Leaks has been targeting only Water and Wastewater sector.
- KARAKURT has targeted only manufacturing in Q3, while in Q2, it only targeted transportation entities.
- Lockbit 3.0 is the only group that targeted chemicals, drilling, industrial supplies, and interior design.
- Stormous has only targeted Vietnam.
- Lorenz has only targeted the United States.
- Sparta blog has only targeted Spain.
- Black Basta and Hive targeted the transportation sector.

* Source: <https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q3-2022/>

Regionally Active Ransomware

- Regionally active ransomware

-



* Source: https://www.traveltip.org/countries_visited.php

3

Case Study: Republic of Korea

Ransomware Timeline in Korea

- Timeline

- 2010: Ransomware infection through a certain messenger program -> Financial sector infected
- 2011: Discovery of Korean version of Ransomware using translator
- 2015: Cryptolocker infection through a famous IT website -> First large-scale damage
- 2016: VenusLocker ransomware attacks with emails written in Korean discovered -> Serious damage
- 2017: A web hosting company suffers damage from Erebus ransomware
- 2017: Magniber ransomware targeting Korean users discovered
- 2018: Emergence of the GandCrab ransomware which targeted Korea
- 2019: Companies attacked by Clop ransomware
- 2019: Smaller companies attacked with files such as fake job applications
- 2021: New Emergence of ransomware only active in Korea

Ransomware Attack Timeline

- Ransomware attack cases (2021-2022)

Date	Ransomware
Nov 2021	Hive
Feb 2022	Hive
Apr 2022	Gwisin
July 2022	Masscan
July 2022	Gwisin
July 2022	LockBit 3.0
July 2022	Bluecrab (Sodinokibi)
July 2022	BitLocker
July 2022	Hive
July 2022	Masscan
Aug 2022	BitLocker
Dec 2022	Cuba

Attackers - Venus IAB (Initial Access Brokers)

- Venus IAB

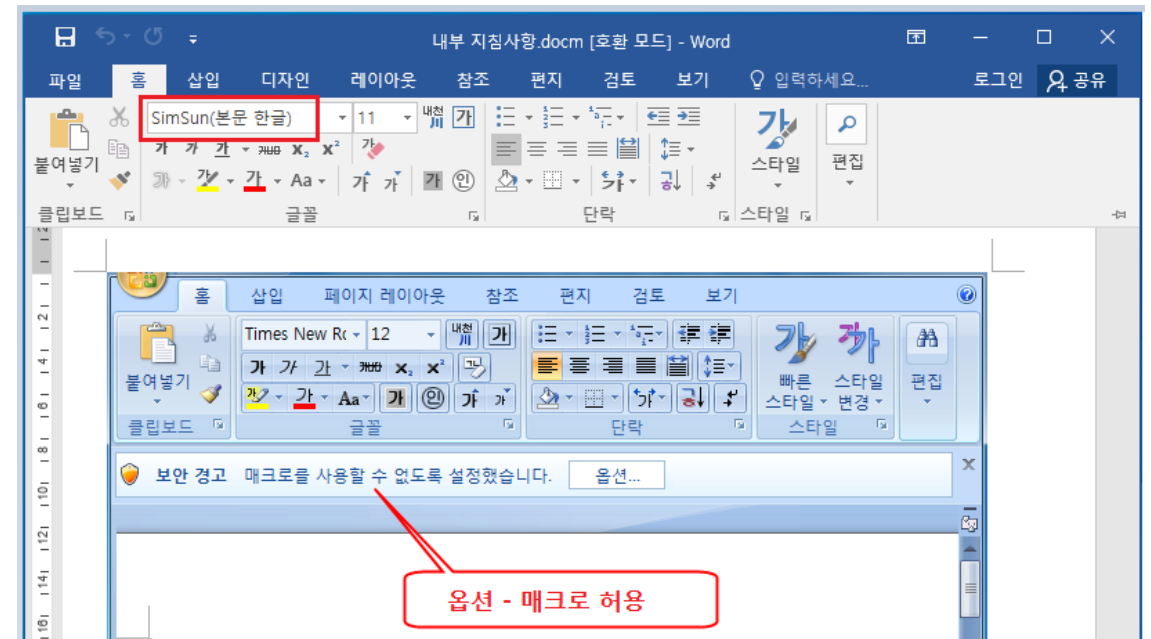
- First emerged in late 2016
- Fluent Korean (everyday expressions, profanities, etc.): Native Korean or fluent Korean speaker
- Attacks involved emails disguised as internal guidelines, lawsuits, training schedules, traffic fines, copyright infringements, job recruitment ads, etc.
- Used a compressed file extension (EGG) that is used in Korea
- Utilized various ransomware: VenusLocker -> Auto Cryptor -> GandCrab -> Sodinokibi -> Nemty -> Makop -> LockBit 3.0
- Distributed CoinMiner

- Questionable points

- String within LNK file: VenusLocker_Korean.exe

```
00000390: 11 B5 D6 00 C0 4F D9 18 D0 6D 00 00 00 1E 00 00  U s e r s \ l
000003A0: 00 00 1F 00 00 00 2E 00 00 00 43 00 3A 00 5C 00  D e s k t o p \
000003B0: 55 00 73 00 65 00 72 00 73 00 5C 00 6C 00 5C 00  æ t r \ V e n u
000003C0: 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00  s L o c k e r
000003D0: 91 C5 C4 C9 74 C7 5C 00 56 00 65 00 6E 00 75 00  k o r e a n . e
000003E0: 73 00 4C 00 6F 00 63 00 6B 00 65 00 72 00 5F 00  x e
000003F0: 6B 00 6F 00 72 00 65 00 61 00 6E 00 2E 00 65 00
00000400: 78 00 65 00 00 00 00 00 00 00 00 00 00 10 00
00000410: 00 00 05 00 00 A0 25 00 00 00 D5 00 00 00 1C 00
```

- SimSun (Chinese Font): ????



Attackers - Magniber Ransomware

- Magniber Ransomware

- First discovered in Oct 2017
- Targeting Korea? Some variants only active on Korean Windows and Korean IP addresses

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

- Distributed using typosquatting
- Fileless format -> Distributed with file extensions such as MSI, CPL, JSE, JS, WSF, etc.
- Attacked Japan and Taiwan. Hit France, Germany, Italy in 2023

Posted on December 15, 2022




Caution! Magniber Ransomware Restarts Its Propagation on December 9th With COVID-19 Related Filenames

On December 9th, 2022, the ASEC analysis team discovered that Magniber Ransomware is being distributed again. During the peak of the COVID-19 outbreak, Magniber was found being distributed with COVID-19 related filenames alongside the previous security update related filenames.



Avast Threat Labs
@AvastThreatLabs

...

Several waves of [#MagniBer](#) [#ransomware](#) attacks have hit FR , IT  and DE  in the past hours with roughly 20K protected users. The attackers used [#malvertising](#), leading to downloading a ZIP file with a fake MSI installer that appears to be an important security update.

Attackers - GandCrab (Bluecrab) IAB

- GandCrab Ransomware IAB
 - Discovered in Korea in February 2018
 - Initially, attacks were done through machine-translated emails with broken Korean
 - Added the HWP (Hancom Word Processor) file extension as an encryption target
 - Speculated to be a local partner
 - Cases where only users in Korea were infected through IP scans
- GandCrab Ransomware distributor apprehended
 - In February 2021, the suspect that impersonated the police and distributed GandCrab Ransomware was apprehended
 - In February 2019, 6,486 emails claiming to be from the police were sent
 - Received by the developer -> 7% of the profit sent to the distributor via a broker -> 12 million won (1,265,000 Yen) profit



* Source: <https://www.korea.kr/news/pressReleaseView.do?newsId=156440086>

Attackers - Gwisin Ransomware

- Gwisin Ransomware

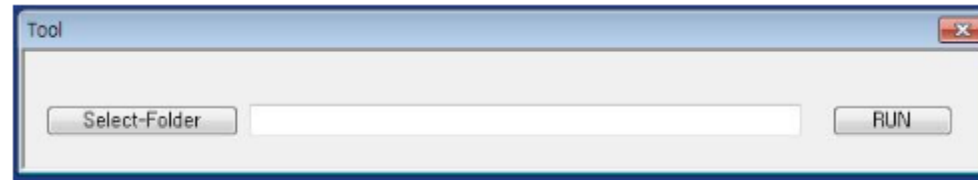
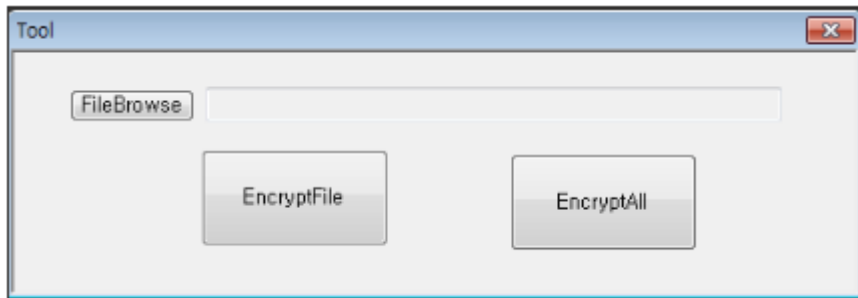
- Taking its name from '귀신'(鬼神, kwisin), a Korean term for 'Ghost' or 'Spirit'



- After first being discovered in Sept 2021, it was only covered on the news until the spring of 2022 before relevant information was released in July 2022
- Windows and Linux versions
- Targeted ransomware that includes the victim in the ransom note -> Limits information sharing among security companies
- The Windows version is distributed as an MSI file while the actual ransomware is an encrypted Binary.helper file
- The Windows version requires additional values such as SERIAL, LICENSE, SMM and ORG to be executed -> Cannot be executed only with samples
- After leaking information, related details are included in the ransom note -> Speculated to be a fluent Korean speaker

Attackers - Masscan Ransomware

- Masscan Ransomware
 - First discovered in Apr 2022
 - According to KISA, Masscan took up 64% of the 58 reported ransomware that targeted database servers until Sept 2022
 - Circumstantial cases in the US, Vietnam, and Czech Republic
 - Attacks vulnerable DB servers
 - Encryptor and decryptor are the same files



- Has a configuration file (not retained)
- Masscan extension added after file encryption
- Encrypts the shared network folder
- Operation MaRS: Masscan Ransomware Threat Analysis Report

Attackers - Unclassified Ransomware

- Unreported variants? Unconfirmed variants?
- Ransomware difficult to attribute
 - Email address within the ransom note -> Same information as MedusaLocker -> The malware is not MedusaLocker but another ransomware

If you can not use the above link, use the email:

karloskolorado@tutanota.com

bugervongir@outlook.com

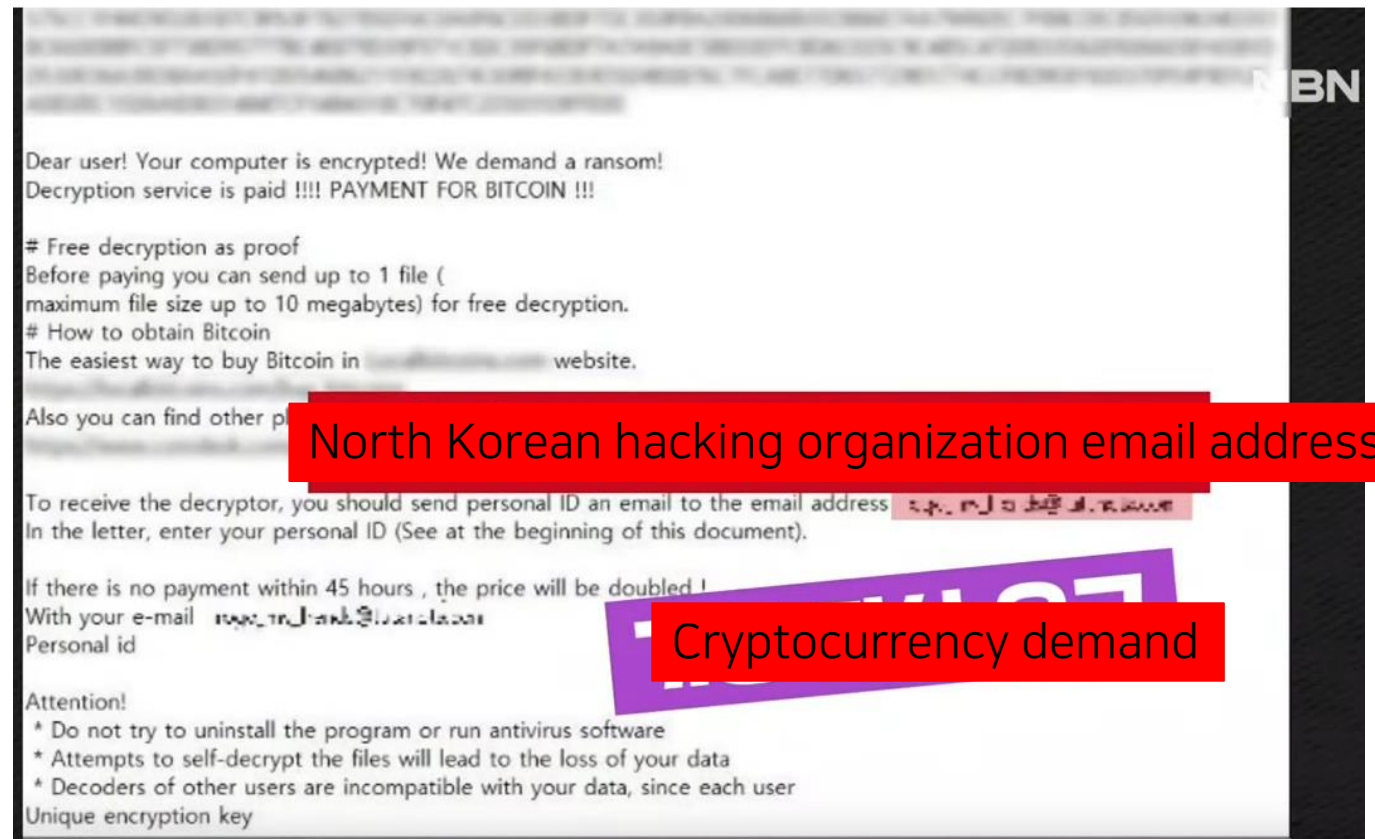
rapid@aaathats3as[.]com	korona@bestkoronavirus[.]com
rescuer@tutanota[.]com	lockPerfection@gmail[.]com
ithelp01@decorous[.]cyou	lockperfection@gmail[.]com
ithelp01@wholeness[.]business	mulierfagus@rdhos[.]com
ithelp02@decorous[.]cyou	[rescuer]@cock[.]li
ithelp02@wholness[.]business	107btc@protonmail[.]com
ithelpresotre@outlook[.]com	33btc@protonmail[.]com
cmd@jitjat[.]org	777decoder777@protonmail[.]com
coronaviryz@gmail[.]com	777decoder777@tfwno[.]gf
dec_helper@dremno[.]com	andrewmiller-1974@protonmail[.]com
dec_helper@excic[.]com	angelomartin-1980@protonmail[.]com
dec_restore@prontonmail[.]com	ballioverus@quocor[.]com
dec_restore1@outlook[.]com	beacon@jitjat[.]org
bitcoin@sitesouheat[.]com	beacon@msgsafe[.]jio
briansalgado@protonmail[.]com	best666decoder@tutanota[.]com
bugervongir@outlook[.]com	bitcoin@mobtouches[.]com

* Source: <https://www.cisa.gov/uscert/ncas/alerts/aa22-181a>

- Similar ransomware but with a different ransom note -> Order-made ransomware?
- Ransomware creation service?
 - Multiple similar ransomware with different ransom notes exist

Attackers – Government-Sponsored Threat Actor

- Andariel Group
 - Kaspersky revealed that the Andariel Group performed attacks using ransomware
 - Sample received from the customer in Sept 2020 (Actual damages were unconfirmed)
 - In July 2022, a Maui Ransomware attack was reported in the US
 - No cases of Maui Ransomware activities confirmed in Korea
- Kimsuky Group
 - The Korean police force presented its investigation results in Dec 2022
 - Encrypted 13 shopping mall company servers before requesting cryptocurrency
 - Individuals trying to earn pocket money?



* Source: <https://www.youtube.com/watch?v=vVC067aGEkk>

Attackers – Computer Repair

- Computer repairmen who made and distributed ransomware
 - 9 people were charged for infecting clients with ransomware after being requested for services such as data recovery
 - Remote control malware installed on the computers of about 20 companies during on-site repairs -> Ransomware infection -> Recovery request
 - Appropriated about 360 million won (37,900,000 Yen) from 40 victims

Catalin Cimpanu

June 16, 2021

Cybercrime

News



South Korean police arrest computer repairmen who made and distributed ransomware

South Korean authorities have filed charges today against nine employees of a local computer repair company for creating and installing ransomware on their customers' computers.

The scheme netted the suspects more than 360 million won (\$321,000) in ransomware payments from 40 companies they serviced throughout 2020 and 2021.

Not all of the company's employees were involved in the scheme, but only nine employees from the company's Seoul offices.

* Source: <https://therecord.media/south-korean-police-arrest-computer-repairmen-who-made-and-distributed-ransomware/>

Negotiation Agencies

- Ransomware negotiation agencies
 - Search for "Ransomware Recovery" on Korean portal websites returns ads for negotiation agencies
 - Negotiation services and Forensics: Negotiation agencies make more profit

파워링크 '랜섬웨어복구' 관련 광고입니다. ⓘ



랜섬웨어복구정직한복구 · 정직한 서비스 정직한 비용!
[광고] j... .me/
랜섬웨어복구 전문 복구회사,후불제,전국서비스가능,세금계산서가능,기업전담팀운영
랜섬웨어복구 10,000원부터
하드웨어AS 10,000원부터
소프트웨어AS 5,000원부터



2년 소비자만족1위 !
[광고] j... .kr
데이터복구,데이터복구, 랜섬웨어복구, 15분 긴급방문, 출장비무료, 소비자만족1위
전담엔지니어, 출장비무료



한국데이터복구: ... · 랜섬웨어 복구 전문팀운영중
[광고]co.kr
랜섬웨어복구 전문기업. 24시간상담. 확장자 변경 랜섬웨어복구, 꼭 읽어보세요! 긴급 , 랜섬
웨어복구 관련 사기업체주의
이벤트 24시간상담. 무료원격진단

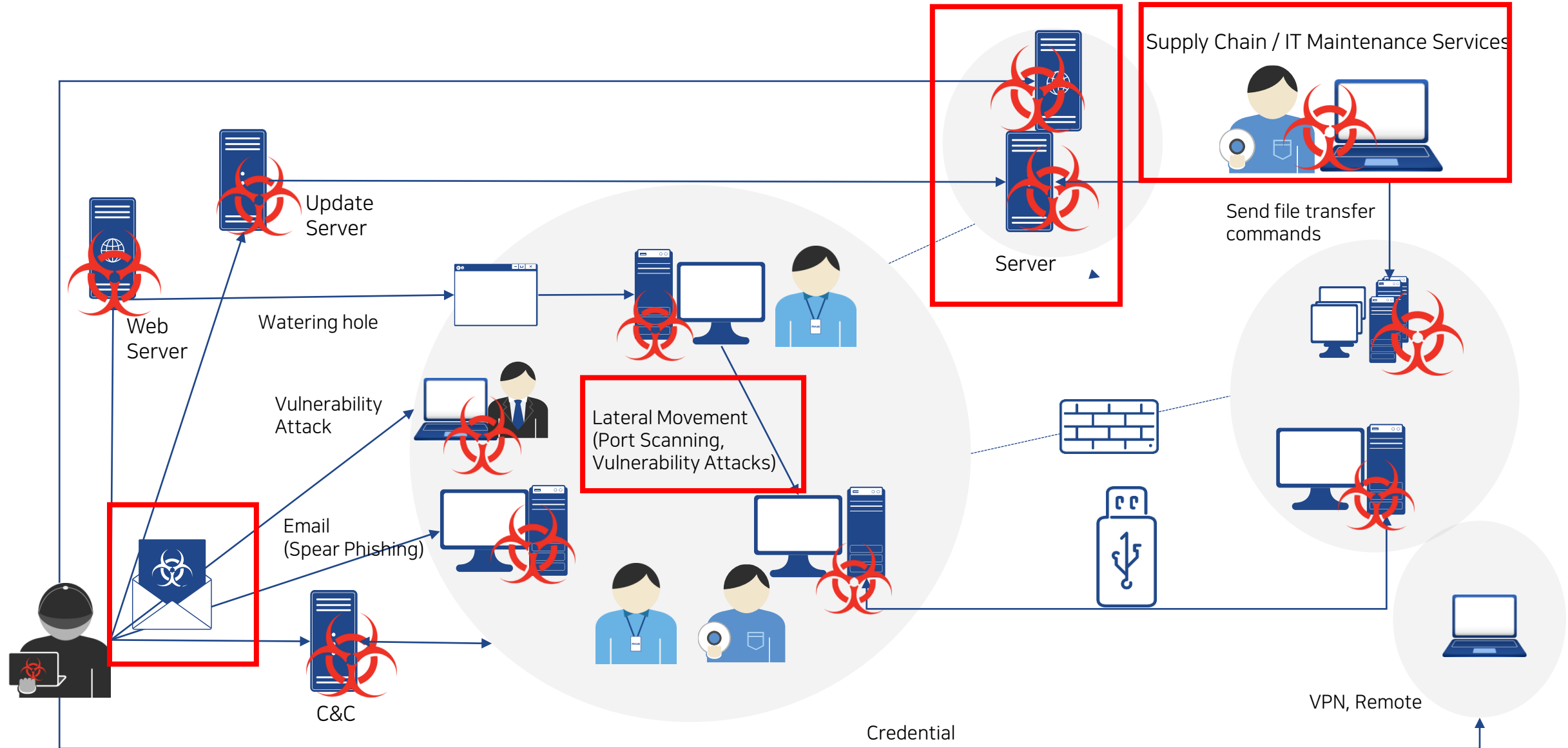
Ransomware recovery ads

(negotiate with ransomware creators)

4

Characteristics of Targeted Ransomware (in Korea)

Corporation Attack Vectors



Bypass AntiMalware

- Disablement and evasion of Endpoint Security Product
 - Attempts to uninstall
 - Prompts users to uninstall
 - Turns off Real Time Protection
 - Adds to Whitelist
 - Uses loaders
- Case of evasion using loaders
 - First Attempt : Blocked by AntiMalware Real Time Protection
 - Second Attempt : Blocked by AntiMalware Behavior-based Protection
 - Third Attempt : Loaded and executed the encrypted ransomware memory using a loader -> Success

5

Outlook of Ransomware Localization

Outlook

- Ransomware Localization (Pros)
 - Participation in ransomware from criminal organizations in each country
 - Ransomware created not only for financial gains but also for political gains
- Ransomware Localization (Cons)
 - Temporary phenomenon: Desire activity in various regions
 - Possibility of ransomware being active in other countries but undetected
- Outlook
 - Local ransomware gangs can spread to nearby countries -> High possibility of becoming active in specific languages, cultures, and regions
 - Local research: language, IT environment, security products, backups ...

6

Conclusion

Conclusion

- Changes in ransomware
 - RaaS, Targeted Attack
- Ransomware localization
 - Emergence of ransomware active in certain regions
- Cases in the Republic of Korea
 - Local ransomware and IAB activities
 - Types that cannot be classified into existing ransomware categories (Insufficient information?)
- Endpoint Security
 - Limit user permissions to change settings
 - Faulty endpoint security product identification needed
- Interest in cases from other countries
 - Attackers sometimes start in one region and expand to neighboring countries
 - Information sharing regarding attack vectors, threat actors, and ransomware needed

Thank you for your attention!

CHA Minseok (Jacky)

- minseok.cha@ahnlab.com
- mstoned7@gmail.com
-  [@mstoned7](https://twitter.com/mstoned7)



Reference

- Gwisin Ransomware Targeting Korean Companies (<https://asec.ahnlab.com/en/37483/>)
- TTPs #8 Operation GWISIN - Analysis on Fully Customized Ransomware Attack Strategies
(https://www.boho.or.kr/krcert/publicationView.do?bulletin_writing_sequence=66955)
- Masscan Ransomware Threat Analysis (<https://www.fsec.or.kr/bbs/detail?menuNo=1006&bbsNo=11181>)

More security, More freedom

AhnLab