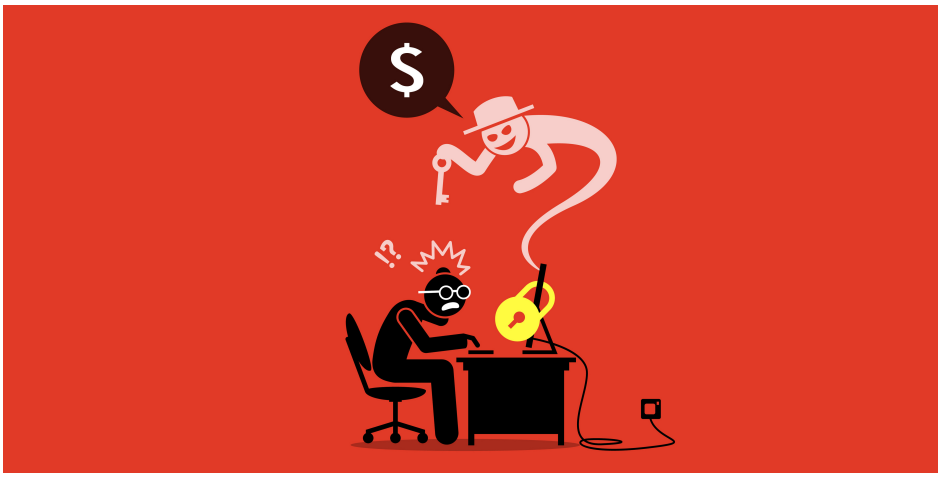
GwisinLocker ransomware targets South Korean industrial and pharma firms

Threat Research
| August 4, 2022

Joseph Edwards, Senior Malware Researcher at ReversingLabs



Taking its name from “Gwisin,” a Korean term for “ghost” or “spirit,” GwisinLocker is a new ransomware family that targets South Korean industrial and pharmaceutical companies.

Executive Summary

ReversingLabs researchers discovered a new ransomware family targeting Linux-based systems. The malware, dubbed GwisinLocker was detected in successful campaigns targeting South Korean industrial and pharmaceutical firms. The malware is notable for being a new malware variant produced by a previously little known threat actor, dubbed “Gwisin” (귀신) — a Korean word meaning ‘ghost’ or ‘spirit’ — and targeting systems running the open source Linux operating system. The ransomware is deployed following a substantial network compromise and data exfiltration.

Analysis

Background

On July 19th in the course of threat hunting, ReversingLabs researchers discovered an undetected Linux ransomware sample which bore the markers of a Gwisin campaign. We have chosen to name this malware GwisinLocker.Linux for clarity, as versions of the malware affecting Windows systems have also been identified.

Gwisin is a ransomware group targeting South Korean industrial and pharmaceutical companies. The name "Gwisin” (귀신) refers to the Korean term for a ghost or spirit. The Gwisin group was first referenced in a report on new ransomware actors in Q3 2021, but have maintained a relatively low profile. To date, there has not been a public technical analysis of the group’s ransomware. This blog post will attempt to describe the new threat based on samples obtained in the wild and analyzed by ReversingLabs, as well as published reports describing attacks associated with the malware.

Configuration

The GwisinLocker.Linux samples can be run with the following options (descriptions were removed by the malware authors, but inferred from analysis):

```
Usage: Usage
-h, --help    show this help message and exit
Options
-p, --vp=<str> Comma-separated list of paths to encrypt
-m, --vm=<int> Kills VM processes if 1; Stops services and processes if 2
-s, --vs=<int> Seconds to sleep before execution
-z, --sf=<int> Skip encrypting ESXi-related files (those excluded in the configuration)
-d, --sd=<int> Self-delete after completion
```

-y, --pd=<str> Writes the specified text to a file of the same name
-t, --tb=<int> Enters loop if Unix time is < 4 hours since epoch

Operation

First, the malware redirects the standard input, standard output and standard error file descriptors to /dev/null to avoid outputting debug or error strings. Both the 32-bit and 64-bit samples used the file /tmp/.66486f04-bf24-4f5e-ae16-0af0fdb3d8fe as a mutex, writing a lock to the file. If GwisinLocker reads a lock set on this file, it exits immediately.

Next, the GwisinLocker.Linux ransomware decrypts its configuration data. GwisinLocker.Linux's configuration is embedded in the malware, encrypted with a hard-coded RC4 key. The JSON configuration was the same in both samples and includes a list of excluded and targeted files.

The following directories are excluded from encryption to prevent Linux operating system crashes:

"bin","boot","dev","etc","lib","lib64","proc","run","sbin","srv","sys","tmp","usr","var","bootbank","mbr","tardisks","tardisks.noauto","vmimages"

These services and related processes are killed before encryption (if the --vm=2 option is set) to ensure open file handles are closed:

"apache","httpd","nginx","oracle","mysql","mariadb","postgres","mongod","elasticsearch","jenkins","gitlab","docker","svnserve","yona","zabbix"

The following filenames are excluded from encryption (if the --sf option is set), as they are important for VMWare ESXI operations. Perhaps the threat actors intended to maintain access to ESXi virtual machines. The ransom notes are also excluded.

"imgdb.tgz","onetime.tgz","state.tgz","useropts.gz","jumpstrt.gz","imgpayld.tgz","features.gz","!!!_HOW_TO_UNLOCK_MCRGNX_FILES_!!!.T

These directories were specifically targeted by Gwisin to encrypt operational data:

"/Information/Database/","/Information/korea_data/","/Information/","/Infra/","/var/www/","/var/opt/","/var/lib/mysql/","/var/lib/postgresql/","/var/lc server/","/usr/local/"

Once the command-line arguments are parsed, GwisinLocker enumerates the number of processors and creates up to 100 threads. The directories to be encrypted are specified with the --vp option, or by default include the list of directories in the configuration.

If the --vm=1 option is supplied, the ransomware executes the following commands to shut down VMWare ESXi machines before encryption:

esxcli --formatter=csv --format-param=fields=="DisplayName,WorldID" vm process list

esxcli vm process kill --type=force --world-id="[ESXi] Shutting down - %s"

Impact

Files encrypted in this GwisinLocker campaign carry the extension .mcrgnx, and the file's corresponding key is stored (encrypted) in a separate 256-byte file with the extension .mcrgnx0. GwisinLocker employs AES to encrypt victim files, hiding the key to prevent convenient decryption. In addition, compromised endpoints are renamed 'GWISIN Ghost,' according to published reports.

Encryption

GwisinLocker combines AES symmetric-key encryption with SHA256 hashing, generating a unique key for each file. The following steps occur when a file is encrypted:

1.
    1. 1. Initialize RSA context from embedded public key
    2. 2. Generate random AES key and IV:
    - Initialize new SHA256 context
    - Read 32 bytes from /dev/urandom, hash with SHA256 context
    - Utilize SHA256 digest as a key to initialize AES context and generate AES key
    - Repeat steps 1-3 with 16 new bytes from /dev/urandom to generate an Initialization Vector
    1. 3. Rename the target file to **[targetfile].mcrgnx**
    2.
        4. Encrypt and store the AES key in the file **[targetfile].mcrgnx0**:
    - Initialize new SHA256 context
    - Read 32 bytes from /dev/urandom, hash with SHA256 context
    - Utilize SHA256 digest as a key to initialize AES context and generate AES key 2
    - Encrypt AES key from Part 1 with AES key 2
    - Encrypt the resulting buffer with RSA context
    - Write encrypted key to **[targetfile].mcrgnx0**
    1. 5. Lastly, encrypt **[targetfile].mcrgnx** with the unencrypted AES key and IV generated in step 1.

2. Targets

According to published reports in South Korean media, the Gwisin threat actors focus exclusively on South Korean firms. The group attacked large domestic pharmaceutical companies in 2022. In those incidents, it often launched attacks on public holidays and during the early morning hours (Korean time) - looking to take advantage of periods in which staffing and monitoring within target environments were relaxed.

In communications with its victims, the Gwisin group claim to have deep knowledge of their network and claim that they exfiltrated data with which to extort the company. Ransom notes associated with GwisinLocker.Linux contain detailed internal information from the compromised environment. Encrypted files use file extensions customized to use the name of the victim company.

Ransom Note

According to published reports, GwisinLocker.Linux ransom notes are text format files written in English and created in the same target folder as encrypted files. The name of the ransom note is typically "!!!_HOW_TO_UNLOCK_******_FILES_!!!.TXT." The note includes contact information, along with a list of data and intellectual property stolen from within the company.

Though the ransom notes are written in English, they contain references that make clear the intended targets are South Korean firms. That includes the use of Hangul (Korean language script) characters and explicit warnings to victims not to contact a range of South Korean law enforcement or government agencies including the Korean police, the National Intelligence Service, and KISA.

Sample Ransom Note

The following is a (redacted) copy of a GwisinLocker ransom note.

Hello [REDACTED],
You have been visited by GWISIN.
We have exfiltrated a lot of sensitive data from your networks,
including, but not limited to:

I. Production applications, source (Git/SVN), files and DBs
[1] [REDACTED] (all regions) + [REDACTED] and other internal platforms

By combining lab [REDACTED] data and the primary big customer platform
[REDACTED], it is easy to identify customer projects, credentials and data.
Despite ISO27001 and ISMS-P with a good PIMS strategy, you have failed to protect customer data across all services.
Your privacy policy assures customers their data security and privacy is top priority, reality seems very different.
We wonder what your customers will have to say about that?

[2] [REDACTED] and general DTC related data

Once again failing to protect very sensitive data and communications of your customers.

[3] Infrastructure and sequencing pipeline data / scripts

Everything from documentation to project specs to produced VCFs and PDF reports post-analysis were collected.
More importantly, a full deep dive of your network infrastructure documentation and access.
The only way to kick us out is to buy all new hardware, including network equipment (UTM / switches) and sequencing / data storage systems.
Someone could have quietly modified your [REDACTED] pipeline instead of contacting you, causing you much bigger issues (legal, financial and otherwise).
Can you really trust your results, if you can't trust your input data and processing pipelines?

II. Internal Data & Communications

[1] ERP/CRM Systems (NEOE, Dynamics)
[2] Active Directory dump with credential history (NTDS + passive credential collection)
[3] DO GW with DB (your groupware contains a lot of data)
[4] Exchange email communications (PST) of targeted important employees in various roles
[5] Financial / Accounting / Research / IT / Customer / Etc. documents

- A lot of documents and other files were collected from SHARE/NEWSHARE machines among other servers
- Your DLP and monitoring was rendered effectively useless and could not stop us, neither could your security team and defensive products

We have also encrypted critical Windows and Linux servers.
We recommend that you do NOT restart servers or recovery may be slower.
The good news for you is that we can:

- Decrypt all files with extension ".mcrgnx" very quickly
- Delete all sensitive data we have exfiltrated, instead of selling it
- Help you improve your security
- Disappear and not be your problem anymore

All you have to do is follow the instructions:
1.) Download Tor Browser: https[://]www[.]torproject.org/download/
2.) Go to our website:
http[://]gwisin:fa5d9dfc@gwisin4yznpdtzq424i3la6oqy5evublod4zbhddzuxcnr34kgfokwad[.]onion
3.) Login with username: mcrgnx, password: [REDACTED]
4.) Change password (one time setup)
5.) Setup end-to-end message encryption password
6.) Read the full instructions on the website and contact us using the message system provided there

[WARNING - #1]
If you are having trouble reaching our website, attempt closing and re-opening the Tor browser.
If you are still unable to reach our website, create a DNS TXT record @ mcrgnx.[REDACTED].com containing a hex-encoded email address and we will contact you.
However, eventually we will need to communicate using our website to preserve the privacy of all parties involved.

[WARNING - #2]
Do NOT contact law enforcement (such as NPA, KISA or SMPA) or threat intelligence organizations as they may prevent you from recovering quickly.
They can't really help you and they don't care if your business is destroyed in the process.
Contact us within 72 working hours, so we can negotiate in good faith and resolve this quickly.

Campaign Markers

Indicators of Compromise

The following are indicators of compromise (IOCs) assembled from GwisinLocker.Linux samples used in the wild.

Filesystem

The following hashes and strings correspond to files associated with active GwisinLocker.Linux variants and attacks.

SHA1 Hash (Filename)	Description
(/tmp/.66486f04-bf24-4f5e-ae16-0af0fdb3d8fe)	Mutex
(!!!_HOW_TO_UNLOCK_MCRGNX_FILES_!!!.TXT)	Ransom Note
ce6036db4fee35138709f14f5cc118abf53db112	GwisinLocker Ransomware (32-bit ELF)
e85b47fdb409d4b3f7097b946205523930e0c4ab	GwisinLocker Ransomware (64-bit ELF)

Processes

The following processes are associated with active GwisinLocker.Linux variants.

esxcli --formatter=csv --format-param=fields=="DisplayName,WorldID" vm process list

esxcli vm process kill --type=force --world-id="[ESXi] Shutting down - %s"

Payment

GwisinLocker.Linux victims are required to log into a portal operated by the group and establish private communications channels for completing ransom payments. As a result, little is known about the payment method used and/or cryptocurrency wallets associated with the group.

Significance

GwisinLocker.Linux is notable for being a new ransomware variant from a heretofore little-known threat actor. The malware's exclusive focus on prominent South Korean firms and references to South Korean law enforcement entities as well as the use of Korean (Hangul) script in ransom notes suggest the threat actor is familiar with both South Korean language and culture. That could suggest that Gwisin group is a North Korea based threat actor, given that nation's aggressive use of offensive hacking, including the use of ransomware, to target South Korean government agencies and private sector firms.

The group's apparent ability to compromise and maintain persistent access to victim environments prior to deploying the GwisinLocker.Linux ransomware, as well as the group's use of double extortion attacks involving the theft of sensitive data suggest that Gwisin possesses sophisticated offensive cyber capabilities. South Korean firms in sectors targeted by Gwisin including heavy industry and pharmaceuticals should be particularly alert for attacks and indicators of compromise. However, the risk posed by Gwisin likely extends to South Korean firms in other sectors, as well.

Conclusions

GwisinLocker is a significant new ransomware family that has been used in attacks on prominent South Korean industrial and pharmaceutical firms. Our analysis of a variant of GwisinLocker that targets Linux-based systems reveals a sophisticated piece of malware with features specially designed to manage Linux hosts and operate and interact with VMWare ESXI virtual machines.

Analysis and public reporting of the larger GwisinLocker campaign suggests the ransomware is in the hands of sophisticated threat actors who gain access to- and control over target environments prior to the deployment of the ransomware. That includes identifying and stealing sensitive data for use in so-called "double extortion" campaigns. Details in samples of the group's ransom notes suggest a familiarity with the Korean language as well as South Korean government and law enforcement. This has led to speculation that Gwisin may be a North Korean-linked advanced persistent threat (APT) group.

This threat should be of particular concern to industrial and pharmaceutical companies in South Korea, which account for the bulk of Gwisin's victims to date. However, it is reasonable to assume that this threat actor may expand its campaigns to organizations in other sectors, or even outside of South Korea.

Firms concerned with GwisinLocker should review the Indicators of Compromise in this report and make those available to internal- or external threat hunting teams.