Gwisin Ransomware Targeting Korean Companies

asec.ahnlab.com/en/37483

August 3, 2022

The cases of Gwisin ransomware attacking Korean companies are recently on the rise. It is being distributed to target specific companies. It is similar to Magniber in that it operates in the MSI installer form. Yet unlike Magniber which targets random individuals, Gwisin does not perform malicious behaviors on its own, requiring a special value for the execution argument. The value is used as key information to run the DLL file included in the MSI.

As such, the file alone does not perform ransomware activities on security products of various sandbox environments, making it difficult to detect Gwisin. The ransomware's internal DLL operates by being injected into a normal Windows process. The process is different for each infected company.

The following shows the characteristics of Gwisin that have been identified so far.

(1) Distributed in an MSI installer file form
(2) Uses the argument value used to run MSI to run internal DLL
(3) Performs ransomware behaviors by being injected into a Windows system process
(4) Contains the information of the infected company inside the DLL (displayed in the ransom note)
(5) Supports a feature to encrypt files in safe mode

When the MSI file is run, it calls the export function update() of the internal ransomware DLL. The function checks the execution argument. If it is abnormal, the function will not operate.

```
MsiGetPropertyA(a1, "SERIAL", v158, &v132);
v20 = v175;
MsiGetPropertyA(a1, "LICENSE", v159, &v133);
MsiGetPropertyA(a1, "VERSION", v160, &v134);
MsiGetPropertyA(a1, "ORG", v161, &v135);
MsiGetPropertyA(a1, "SMM", v162, &v136);
MsiGetPropertyA(a1, "SLP", String, &v137);
MsiGetPropertyA(a1, "TBT", v164, &v138);
MsiGetPropertyA(a1, "TZC", v165, &v139);
for ( j = 128i64; j; --j )
{
  *(_DWORD *)v20 = 0;
  v20 += 4;
}
v140 = 512;
MsiGetPropertyA(a1, "OriginalDatabase", v175, &v140);
```

Figure 1. Routine for checking argument upon running MSI

At the moment of the encryption process, the ransomware is executed with the following arguments (some parts of the arguments are hidden).

> msiexec /qn /i C:\ProgramData*****.msi SERIAL=463f********7ce7 LICENSE=7f21********5071 SMM=0 ORG=***

Among arguments that are needed to run Gwisin, SMM can have a value of 0 or 1. Normally, the routine for encrypting files is processed if the value is 0. If SMM is 1, the ransomware is installed to operate on safe mode. It first copies itself to a certain path of ProgramData and is registered as a service. It then uses bcdedit to set the boot option as safe mode. The computer is forcibly rebooted after 5 seconds. After the system is rebooted in safe mode, the registered service starts encrypting files.

Service Name	Command
a35f23725b5feab2	> msiexec /qn /i C:\ProgramData*****.msi SERIAL=463f********7ce7 LICENSE=7f21********5071 SMM=0 ORG=***

Registered service

When the process for verifying the argument ends, the ransomware decrypts the internal shellcode using the arguments. It then runs a normal program “certreq.exe” to inject the decrypted shellcode. The injected shellcode ultimately decrypts Gwisin to run it in the memory (besides “certreq.exe”, various normal Window processes are used to run the ransomware).

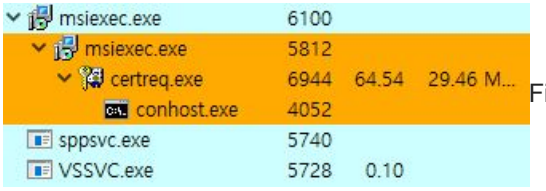


Figure 2. Process tree of Gwisin

After encrypting files, the ransomware changes the extension name to the name of the targeted company.

Figure 3. Encrypted files

The folder chosen to be encrypted contains a ransom note. The name of the note also contains the extension string such as “!!!_HOW_TO_UNLOCK_******_FILES_!!!.TXT“. The note file shows a list of stolen information and contacts.

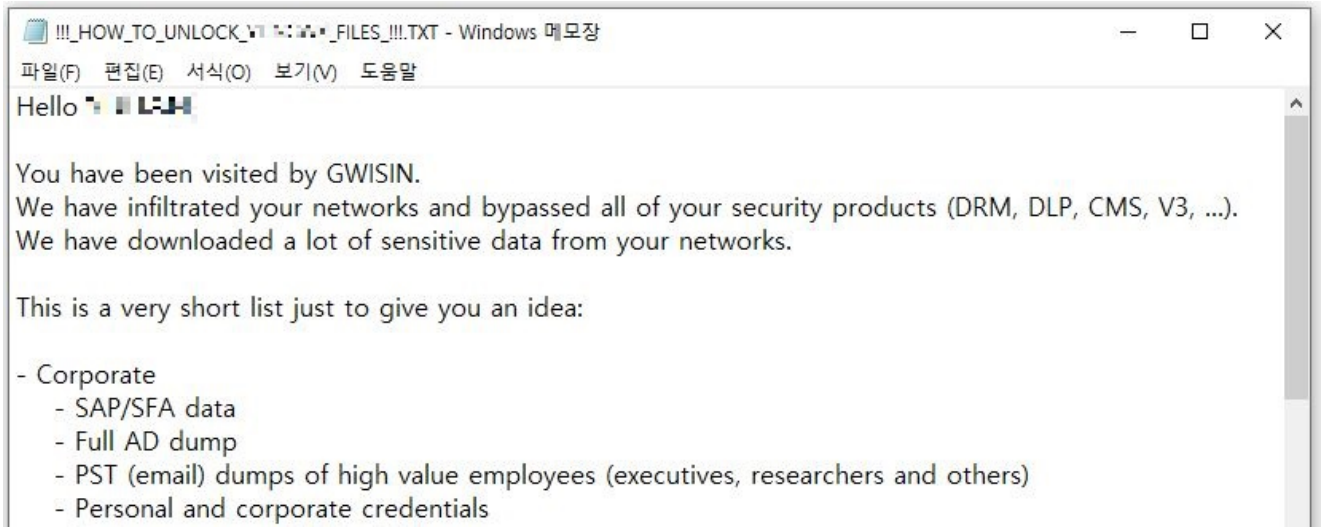
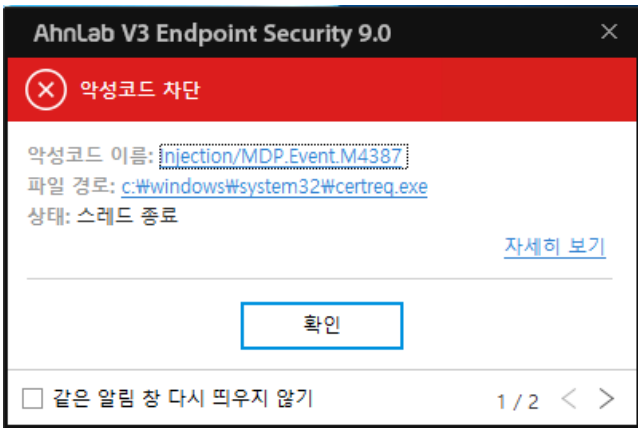


Figure 4. Ransom note of Gwisin

Figure 5. Desktop after being infected

The Gwisin cases show that the anti-malware products are neutralized before the infection process begins. As V3 products block Gwisin ransomware using such a method in the injection process through behavior-based detection, it is necessary to enable the 'Behavior-based Detection' option.

Because the ransomware is installed and executed in various systems after dominating the internal system, companies must analyze how the infection happened in the first place. If the cause of the infection cannot be analyzed after a breach had occurred, another ransomware may infect the system in the future and cause a similar incident.



[File Detection]
– Ransomware/Win.Gwisin.C5214965 (2022.07.27.03)

[Behavior Detection]
– Injection/MDP.Event.M4387 (2022.07.28.00)

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:APT, Gwisin, Ransomware