vb2023 LONDON

4 - 6 October, 2023 / London, United Kingdom

MAY THE SHADOW FORCE BE WITH MAGGIE – SHADOW FORCE GROUP CHARACTERISTICS AND RELATIONSHIP TO MAGGIE

Minseok Cha, Junseok Kim & Jaejin Lee

AhnLab, Republic of Korea

minseok.cha@ahnlab.com
junseok.kim@ahnlab.com
jaejin.lee02@ahnlab.com

ABSTRACT

The Shadow Force Group is an alleged Chinese-speaking threat actor that has been active since 2014, primarily in South Korea. This threat actor has been active for 10 years, but is not well known. In 2019, when we came across related malware while tracking the activity of another threat actor, only one public analysis report was available. After *AhnLab* published an analysis report in early 2020, it seemed to be forgotten as no further activity was identified, but after KRCert disclosed Shadow Force Group's activity in 2022, further investigation revealed consistent activity.

The Shadow Force Group targets *Windows* server systems and uses a variety of malware and tools after initial infiltration. Some of the files are signed with compromised digital certificates. The group also manipulates PE files to load malicious DLL files. Some malware or tools have had the same file name for years.

In October 2022, *DCSO CyTec* and *SentinelOne* published an analysis of the malware Maggie. High infection rates were found in the APAC region, including South Korea, and they raised the possibility that the Maggie malware is associated with the Shadow Force Group.

In this presentation, we will demonstrate our tracking of the Shadow Force Group, its assumed attack vector, and the malware and tools they have used in recent years. We will also reveal the connection between the Shadow Force Group and Maggie malware, as well as additional malware associated with Maggie.

We hope that this presentation will help researchers learn more about this threat group, and discover whether this threat actor is active only in South Korea or also in other countries.

INTRODUCTION

The Shadow Force group is a threat group that has been active in Korea since 2013. Maggie, a malware that first became known in 2022, was being distributed in the Asia-Pacific region and its connection to the Shadow Force group was suspected, but there was not enough conclusive evidence to confirm the connection. This document covers the major malware employed by the Shadow Force group along with the types of Maggie malware and also provides a summary of the relationship between the Shadow Force group and Maggie.

SHADOW FORCE GROUP

As a threat group that has been active since 2013, Shadow Force mainly targets Korean corporations and organizations. *Trend Micro* published the first analysis report on Shadow Force [1] in September 2015, in which it stated that a Korean media-related company had been attacked. In April 2020, *AhnLab* published an analysis report on Operation Shadow Force [2]. It was introduced as a single campaign as there was the possibility of it being the activity of an existing threat group. However, three years after the release of the report no relevant threat group information has been found outside of Korea, and it thus seems to be a group active in Korea. In July 2022, KRCert published the details of its analysis of the Shadow Force group's additional breach [3]. In October 2022, *AhnLab* announced that the PE-modifying iatinfect.exe file is continuously being detected [4]. There are continued reports of file modification using iatinfect.exe, while the usage rate of the backdoor used in the past has decreased. Instead, there have been cases where other backdoors such as Viticdoor were used, and since December 2021, cryptocurrency miners have been being installed alongside them.

This group usually uses tools that are in Chinese and leave the name of the developer, such as Melody, Syrinx and WinEggDrop, in the malware. The group has also developed various tools, such as a file property changer and process viewer, that are used in hacking. The threat actor has been using the same file name and similar malware and tools since 2014, making it easier to identify.

The group shows different characteristics compared to those of threat groups suspected of being state-sponsored, one example being the fact that the former leave their nicknames within the malware. The installation of coin miners leads us to believe that Shadow Force is closer to a cybercrime organization, but it is not known why the group is mainly active in Korea.

Attack targets and actual cases

AhnLab received over 40 reports of infection cases, where many Korean corporations and organizations had been attacked. Most are deemed to be SQL servers, and because infection does not affect the system's operations, some victims may not be aware of the infection. As of 2014, the group has been employing a method of modifying a file that's trusted by the user, such as a management program, and manipulating the malware to be loaded when this trusted file is run to make it more difficult to detect. The KRCert report also mentions a case where the targeted company's system had been infiltrated by the threat actor for years before the company became aware of the infection.

Attack vectors

The exact attack vectors of Shadow Force are not known. It could be by internal infiltration through email, but considering that most of the targeted systems are *Windows Server*, and that there is a case where other malware was downloaded through sqlserver.exe (an executable file for normal SQL servers), there is a high possibility that the malware infiltrated via vulnerable SQL servers.

Htran (usually aio.exe or aiom.exe) is a tool that provides various features for hacking, such as uploading, downloading and executing files; creating and deleting accounts; deleting logs; hiding processes; registering services; logging off; port mapping; and terminating and rebooting the system. There was a history that showed that aio.exe was downloaded from sqlservr.exe, which is an SQL-related file. This could mean that the threat actor first took control of the SQL server and then downloaded the aio.exe file.

Pemodifier, downloaded through aio.exe with the file name iatinfect.exe or iat.exe, modifies *Windows* executable files. It usually modifies files that are trusted or frequently executed by the user, and when the user launches the modified file, malware such as Shadow Force is simultaneously loaded. The Pemodifier file (iatinfect.exe) was first discovered in September 2014, which is around the same time as the Wgdrop malware was changed to a DLL-type. The threat actor had been using the EXE-type of Wgdrop, and after the spring of 2014, the strategy developed into modifying normal EXE files to run DLL-type malware.

Certain systems install additional programs such as a keylogger and screen recorder. The method of data leakage remains unknown.

Leaked and forged certificates

The threat actor stole or forged legitimate certificates to sign the malware, and it is deemed that a certificate key obtained through hacking was used in the malware.

The attacker mostly counterfeited and stole the certificates of Korean companies. The threat actor used the *CyberLink* certificate in 2012, the *A'digm* certificate in 2012 to 2013, *EZNIX* in 2014, *4NB* in 2017, and the *blueside* certificate in 2018 to 2020. In particular, another *blueside* certificate key (serial number: 6613fd5935f1bb8f1d355c28f920b028) was leaked in November 2018.

Certificate	Serial number	Country	Period	Method	Status
4NB	483f0bf7a6d84c6cf429d4eb4988e686	Korea	2017	Presumed to be forged	?
A'digm	456e967a815aa5cbb99fb86aca8f7f69	Korea	2012–2013	Stolen (key leakage presumed)	Revoked
blueside	706ac96953034b9d9926d4cc1d3248b3, 6613fd5935f1bb8f1d355c28f920b028	Korea	2018–2020	Stolen (key leakage presumed)	Valid
CyberLink	1d226108cbb0eb7b504697bdfec66a8b	Taiwan	2012	Presumed to be forged	Revoked
EZNIX	73e78017a7bf71b6762a603dc41fb6b5	Korea	2014	Stolen (key leakage presumed)	Valid

Table 1: Certificates.

Major malware

The major malware used by this threat group are shown in Table 2, and Figure 1 (see following page) shows a timeline of their usage.

Name	Type	Description
Loader	Loader	Loads malware
Dnsdoo	Backdoor	
Wgdrop	Backdoor	Initial backdoor
Shadow Force	Backdoor	Late-stage backdoor
Viticdoor	Backdoor	Loads a normal vtcp.dll file

Table 2: Types of malware.

Refer to the Operation Shadow Force report for more details on the malware.

32 variants of Wgdrop were found between March 2013 and December 2015. Decrypting the password reveals the string 'Dynamic W32TimeF Mode VC Socks5 Proxy V1.23 Build 11/16/2012 By Melody!'.

Between September 2014 and March 2020, the threat actor used the Shadow Force malware instead of Wgdrop. Unlike Wgdrop, the Shadow Force malware does not have an encrypted string, but rather the string 'Welcome To Shadow Force' is visible in plain text, as shown in Figure 2.

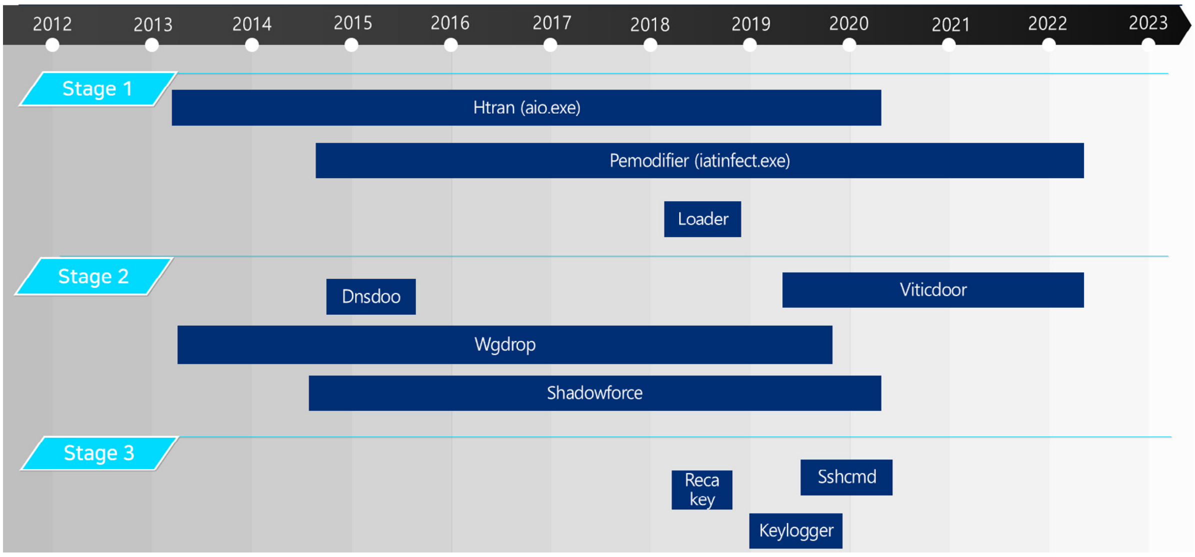
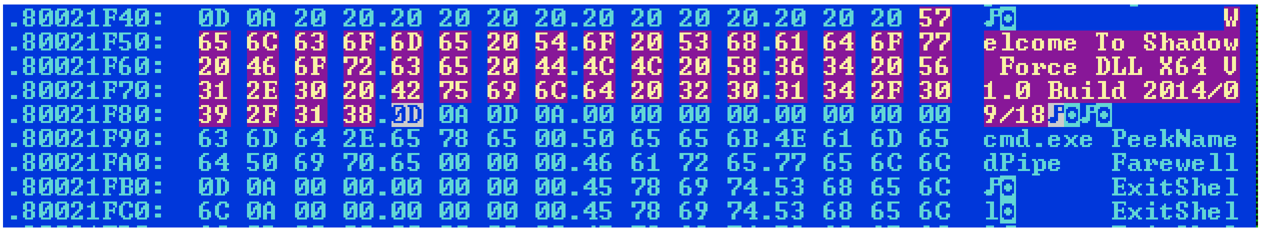


Figure 1: Major malware and tools.



```
.80021F40:  0D 0A 20 20.20 20 20 20.20 20 20 20.20 20 20 57  ♪◙                W
.80021F50:  65 6C 63 6F.6D 65 20 54.6F 20 53 68.61 64 6F 77  elcome To Shadow
.80021F60:  20 46 6F 72.63 65 20 44.4C 4C 20 58.36 34 20 56   Force DLL X64 V
.80021F70:  31 2E 30 20.42 75 69 6C.64 20 32 30.31 34 2F 30  1.0 Build 2014/0
.80021F80:  39 2F 31 38.0D 0A 0D 0A.00 00 00 00.00 00 00 00  9/18♪◙♪◙
.80021F90:  63 6D 64 2E.65 78 65 00.50 65 65 6B.4E 61 6D 65  cmd.exe PeekName
.80021FA0:  64 50 69 70.65 00 00 00.46 61 72 65.77 65 6C 6C  dPipe   Farewell
.80021FB0:  0D 0A 00 00.00 00 00 00.45 78 69 74.53 68 65 6C  ♪◙      ExitShel
.80021FC0:  6C 0A 00 00.00 00 00 00.45 78 69 74.53 68 65 6C  l◙      ExitShel
```

Figure 2: Shadow Force-specific string.

Viticdoor began to be used in March 2019 [5]. Vtcp.exe (sha2 : b4381e7c793148e3c365f11a734dbe1fe0c4e51141293b9ac4a18ad7279e8def) creates a normal vtcp.dll file after being executed and can be used as a backdoor by executing a reverse shell (cmd.exe), offering features such as uploading, downloading, executing and deleting files. Viticdoor loads vtcp.dll to upload and download files, so some variants store the vtcp.dll file in their resources. Vtcp.dll is a normal file created in China, and some of these files were signed with stolen legitimate certificates.

The version identified in 2021 includes new commands such as FastDownload, FastUpload, RamDownload and RamUpload, and the version discovered in 2022 (sha2 : 9925e66536b7838c0275882a33f2447e8b911444f71eaee5f3344750950d7d52) no longer offers the port-listening feature.

Major tools

The major tools used by this threat group are shown in Table 3.

Name	Type	Description
Htran	Tool	Hacking tool
Fileaccess.exe	Tool	Manages file permissions
Pemodifier	Tool	Modifies PE files and patches them to load a specific DLL file
Recakey	Keylogger	Screen recording and keylogging
Keylogger	Keylogger	Saves user key input
SSHCMD	Keylogger and screen recorder	Records the screen and saves user key input

Table 3: Types of tools.

Htran (aio.exe)

Htran is a hacking tool that offers various features needed for hacking and was mainly used by the threat actor to download other malware. It was first discovered in March 2013 and the file names were all aio.exe.

When the aio.exe file found in 2014 is executed, it prints the string ‘Mini Version Without Scan Feature V1.0 Build 11/11/2013’. It offers features such as deleting logs, FTP, finding user passwords and executing services and drivers.

Aio.exe, detected in 2014 in a system that fell victim to an infiltration incident, is a modified version of a hacking tool created in 2008. It has not been determined whether the hacking tool created in 2008 (sha2: 2f52c398c47b4eff7c0432a240 c3e6c566095a6006665428d1de3cb77cc43afe) is a tool created by the same author or whether it is a modified version of a tool whose source code was made public. A similar program was also used in a hacking incident in Korea in 2018, but a different threat actor is judged to have launched this attack. For this reason, this tool is presumed to be one used by multiple hacking groups.

Pemodifier (iatinfect.exe)

Pemodifier is a tool that modifies a designated EXE file to load a specific DLL file. A total of 34 variants were found between September 2014 and February 2022, and in over 30 variants, the file name iatinfect.exe was used.

The name of the creator is WinEggDrop, who is known to have also created other malware, but the name of another creator, Syrinx, can also be found within the file. There is a high possibility that the overall tool was developed by WinEggDrop and the PE file infection feature by Syrinx.

The iatinfect.exe file has 32-bit and 64-bit versions. The initial version displays 'PE File infector V1.0' and 'By WinEggDrop'.

The variants found after April 2020 all have the file name iatinfect.exe but do not display the program information.

The file patched with iatinfect.exe has the string 'Syrinx's Victim' added within the file header.

SSHCMD

SSHCMD, identified in November 2019, provides features such as acquiring the system information and process lists as well as executing files. Upon execution, the string 'SyrinxOS Operating System [Version 1.0] (C) Copyright 1998-2016 SyrinxOS Team.' is displayed.

Coin mining

In some systems infiltrated by the Shadow Force group in 2022, crypto (virtual currency) miners were also found. Over 30 similar miners were found, but only five samples were found alongside malware such as iatinfect.exe and ntuser.dat, the characteristic file names used by the Shadow Force group. They require configuration files such as wbdbase.plk and .xmrig.json for execution, and further analysis was not possible as only the executable file was collected.

MAGGIE MALWARE

In October 2022, *DCSO CyTec* released information [6] on the Maggie malware [7], which was targeting *Microsoft SQL* (hereinafter referred to as *MS SQL*) servers. A few days later, *SentinelOne* released additional information [8] on Maggie and malware signed with the *DEEPSoft* certificate.

Maggie was developed in Extended Stored Procedure (ESP) format, supported by *MS SQL* servers [9], and after loading the malware on the target server through ESP, the threat actor is able to control the malware through SQL queries.

Attack targets and actual cases

The specific infection route of the Maggie malware has not yet been identified, but infection through vulnerable account passwords is suspected.

According to the *DCSO CyTec* blog post, over 250 servers infected with Maggie have been identified, with many of the infections occurring in the Asia-Pacific region in countries such as Korea, India, Vietnam, China and Taiwan. According to the *SentinelOne* blog, Maggie was mostly found in communications and IT service providers in the Middle East and Asia.

Based on the shared IOCs, *AhnLab* detected over 100 variants and 540 cases of infection through *AhnLab Smart Defense* (*ASD*). However, the attack targets could not be specified.

Leaked certificates

Since 16 April 2022, the malware has been signed with the certificate of *DEEPSoft*, a Korean software development company.

There is a high possibility that the certificate was stolen from *DEEPSoft* software signed with this certificate. Currently, the certificate is no longer valid.

Amongst the files signed with the *DEEPSoft* certificate, there were pieces of malware that create mini process dumps, keyloggers and screen recorders, and malware for leaking information saved in web browsers. Out of the IOCs provided by *SentinelOne*, some samples could not be procured, and including the IOCs provided by *SentinelOne*, *AhnLab* identified a total of 17 pieces of malware signed with the *DEEPSoft* certificate up to 13 April 2023 [10].

Major malware

The major malware used by this threat group are as follows.

Name	Type	Description
Maggie	Backdoor	Includes the string 'MSSQL Procedure'
Maggie (MSSQL Hook Procedure)	Backdoor	Similar to Maggie and includes the string 'MSSQL Hook Procedure'. Some features are called from an external DLL file
MaggieScan	Scanner	Scans for vulnerable MS SQL servers

Table 4: Types of malware.

Maggie

Based on the shared IOCs, *AhnLab* identified additional variants of Maggie which had the following changes:

- The initial version identified in March 2020 (sha2: 0787fdde0c10a42b67251283d41b49c7c2b6e37966d321d335527e2bd3f1b76b) contains the string 'SQL Extended Procedure X64 V1.0 Build 11/09/2019 By WinEggDrop'. The malware is deemed to have been created around November 2019.
- The variant found in April 2020 (sha2: 2916f44601b04047eddd74c1e70b51f77fa19b20fbfd9499723e82e2470fb650) had its string changed to 'MSSQL Procedure 04/01/2020'.
- The variant found in January 2021 (sha2: be8ace42c5edcc0086d10e8bd1ceee2fb731d032692edc5c07259138571435a3) had the file name changed to ntuser.dat. Ntuser.dat is the most frequently used file name out of the Maggie variants. The string containing malware-related information was removed, and the Export function is sqlext.
- For variants after March 2021, Maggie is used for the Export function (sha2: 3187d7ac0dfbc72c43940d1b4de60b213552912672589eb2d1ea7fd0ca16b14e). Names other than Maggie have been used for the Export function, but the name Maggie was most frequently used, giving the malware its name.
- Maggie variants after March 2022 include more commands, being improved to support about 50 commands. The input command processing method is also different from the 2020–2021 versions.
- The variants detected between May and July 2022 (sha2 : f29a311d62c54bbb01f675db9864f4ab0b3483e6cfdd15a745d4943029dcdf14) are signed with a certificate from *DEEPSoft*, a Korean software development company.
- The variant found after November 2022 (sha2: 4ce0221aab3b978d761279a410b5b0fe58f43fd8b3bbf5908338dc1f7d34ff3f) uses ntuser.dat for the file name again, and the certificate signature was removed.
- The variant of Maggie created in March 2023 was found in Korea and Japan [11]. This variant uses 'syrinx' for the Export function name and includes the string 'MSSQL Procedure Syrinx 02/23/2023'.
- The initial version found in 2021 supported about 20 commands, but the variant found in 2022 supported about 50 commands, and the 2023 version supports even more commands, with 57 in total. As the developer of Maggie is continuously adding features, it will likely support even more commands in the future.

  Major commands include system information collection, including checking whether or not the system is a virtual environment, management of files and directories (obtaining file lists, executing and deleting files, changing file properties, and creating file paths), downloading files, SQL scanning, and function hooking.

Maggie (MSSQL Hook Procedure)

Some variants after February 2022 contain the string 'MSSQL Hook Procedure' (sha2 : 6a25c62503243b65ffff466a791f3fde9cd8b0ab125b2405880003ac7d7cd13a).

There are no significant differences between this and Maggie; the Export function name is sql_hook and some features require the FindOsInfo function and external files (Osinfo.dll).

MaggieScan (MSSQL Procedure Scan)

MaggieScan is a program that finds vulnerable *MS SQL* servers and characteristically contains the string 'MSSQL Procedure Scan'.

It was first identified in January 2022 (sha2: 2143e901e649cc028b3c14c046060082467df047847f4a8bc0144408bbc24b04) and a total of four variants were discovered up to April 2023.

ATTRIBUTION

Upon analysing related malware, the creator names Melody, Syrinx and WinEggDrop are seen repeatedly. Whether the authors are multiple individuals or a single person, whether they only develop malware or also take part in hacking, we cannot confirm. In particular, some tools created by WinEggDrop are available on the internet for anyone to use.

A summary of the attributions made through the information we have about the malware, its certificate, and developer(s) is as follows:

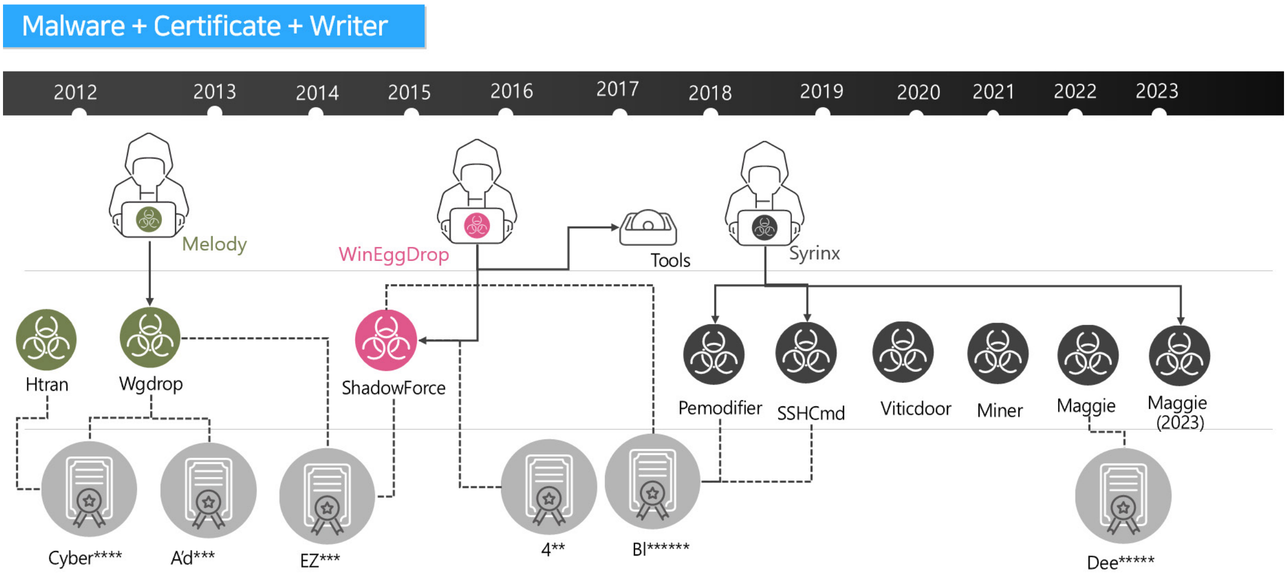


Figure 3: Attribution.

Various pieces of malware are signed with an identical digital certificate. We cannot make the assumption that a single group has conducted all the actions solely from the fact that multiple malware are signed with an identical certificate. However, the threat actor behind Operation Shadow Force downloads files using aio.exe and uses the file iatinfect.exe to patch system files to load a DLL, and also uses a similar backdoor. The traces of these files from the infected system are important pieces of evidence.

The threat actor periodically changes the malware but retains the attack method of downloading malware through aio.exe and modifying normal files through iatinfect.exe.

The suspicion of the Shadow Force group being the creator of Maggie was present from the initial analysis. However, because WinEggDrop is the creator of many pieces of malware and tools, it is difficult to determine whether Shadow Force is behind Maggie based on this evidence alone.

While tracking additional Maggie variants, *AhnLab* found the following connections to the Shadow Force group:

- The Shadow Force group usually attacked *MS SQL* servers and the Maggie malware also targets *MS SQL* servers. However, while both are predicted to use brute force attacks or exploit vulnerabilities, their exact route of infection has not yet been identified.
- Developer nicknames such as WinEggDrop and Syrinx found in malware and tools used by the Shadow Force group are present within the Maggie malware. As tools developed by WinEggDrop are being used by multiple threat groups, it is difficult to conclude that this is from the same group, but the Maggie variant identified in January 2023 contains 'Syrinx', another Shadow Force developer name.
- The file names used by Maggie are linkinfo.dll and ntuser.dat, the same file names as used by Shadow Force.
- Some malware and tools are signed with a certificate from *DEEPSoft*, a Korean company. The linkinfo.dll file detected in October 2022 is a screen capture program with the same file name and similar code as the file the Shadow Force group used to attack a Korean government organization in 2021.
- The Pemodifier file (iatinfect.exe), a program used by the Shadow Force group, was found in a portion of the systems infected with Maggie.

Based on such evidence, *AhnLab* has concluded that there is a high possibility that the Shadow Force group or one of their subsidiary groups is behind the Maggie malware. For a more definite conclusion, an investigation of the Shadow Force group and systems infected with Maggie is needed.

CONCLUSION

Traces of a new threat group that has been active in Korea for a long time were found while tracking the activities of another threat group. Fortunately, this threat actor has used a similar attack method and tools with the same file name for years, and overall, has not changed its habits.

Since the Shadow Force group attacked various Korean industries and government organizations, it was suspected of being a state-sponsored threat group that aims to steal information, but given that its developers leave their nicknames within their malware and that they installed coin miners in their recent activities, there is a high possibility that this group is a cybercrime organization motivated by financial gains. However, there is little coverage of this threat group from security corporations and organizations, so there is still an insufficient amount of relevant information.

Until now, the Shadow Force group's activities have mostly been detected in Korea and there are no relevant external reports; but according to our investigation, there are a small number of infection reports being filed from areas other than Korea, so it is deemed that the group is expanding its field of activities.

After its first discovery in 2021, new Maggie variants and related malware are continuously being found. Ever since the information on the Maggie malware was first released, many security companies suspected its relationship with the Shadow Force group based on *AhnLab*'s report, but there was a lack of evidence to support this. We have tracked Maggie and found additional variants as well as additional grounds to support its link to the Shadow Force group. The infection route of Maggie has not yet been identified, so when a system is found to have been infected with the Maggie malware it is important for operators to contact a security company to uncover the remaining secrets of the Maggie malware through additional analysis including forensics.

There are still unanswered questions regarding the Shadow Force group and the Maggie malware. The malware's initial infiltration method and method of information leakage are still unconfirmed. Luckily, there are many cases where the Shadow Force group and the Maggie malware use the same file names, rendering tracking relatively easy.

Based on the IOCs information provided here, we would like to cooperate with other security companies and have the remaining questions answered.

REFERENCES

[1] Trend Micro. Shadow Force Technical Brief. September 2015. http://documents.trendmicro.com/assets/pdf/shadow-force-technical-brief.pdf.

[2] AhnLab. Operation Shadow Force: Hidden Behind Legitimate Digital Certificates for Seven Years. April 2020. https://download.ahnlab.com/global/brochure/[Analysis_Report]Operation_Shadow_Force.pdf.

[3] KISA. TTPs#7 Internal network migration strategy analysis using SMB Admin Share. July 2022. https://boho.or.kr/data/reportView.do?bulletin_writing_sequence=66830.

[4] https://atip.ahnlab.com/ti/contents/asec-notes?i=226d5bfe-4a8e-4a3f-8f52-af7dce7508ea.

[5] https://atip.ahnlab.com/ti/contents/asec-notes?i=a78a218a-fcf4-4ed6-bcac-feea0fb825fb.

[6] DCSO CyTec Blog. MSSQL, meet Maggie. 4 October 2022. https://medium.com/@DCSO_CyTec/mssql-meet-maggie-898773df3b01.

[7] DCSO CyTec Blog. Tracking down Maggie. 11 October 2022. https://medium.com/@DCSO_CyTec/tracking-down-maggie-4d889872513d.

[8] Chen, J. WIP19 Espionage | New Chinese APT Targets IT Service Providers and Telcos With Signed Malware. SentinelOne. 12 October 2022. https://www.sentinelone.com/labs/wip19-espionage-new-chinese-apt-targets-it-service-providers-and-telcos-with-signed-malware/.

[9] Microsoft. SQL Server. How Extended Stored Procedures Work. https://learn.microsoft.com/en-us/sql/relational-databases/extended-stored-procedures-programming/how-extended-stored-procedures-work?view=sql-server-ver16.

[10] https://atip.ahnlab.com/ti/contents/asec-notes?i=1a72378c-81fa-46d1-8b6e-ef3b14cdc016.

[11] https://atip.ahnlab.com/ti/contents/asec-notes?i=f8e8e762-784d-4687-aaf1-8cd74c57783a.

[12] Johann Aydinbas. Private Communication, 2022.