2020. 04. 07

Analysis Report

Operation Shadow Force

Hidden Behind Legitimate Digital Certificates for Seven Years

AhnLab Security Emergency-response Center (ASEC)

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | www.ahnlab.com |

Table of Content

Executive Summary ... 3

Introduction: Operation Shadow Force ... 3

Details on Operation Shadow Force Attack Stage ... 4

Tracking Down Operation Shadow Force ... 6

Activities Exploiting Fake or Exposed Certificates ... 7

Analysis of Malware and Hacking Tools ... 8

Relationship Analysis ... 8

Signs of Infection ... 9

Conclusion ... 10

Executive Summary

The journey to track down Shadow Force first begin in January 2020, when a Japanese Press, Asahi Shimbun, reported about a massive cyberattack against Mitsubishi Electric. Mitsubishi Electric is a Japanese multinational electronics and electrical equipment manufacturing company that manages major Japanese defense industries and social infrastructures. Asahi Shimbun revealed that four threat groups were involved in this cyber attack: Aurora Panda, Emdivi, Tick, and BlackTech.

This led ASEC (AhnLab Security Emergency-response Center) to initiate a research about Aurora Panda, a group not yet well-known in South Korea. ASEC made unexpected discoveries while tracing a threat group allegedly involved with Aurora Panda. It was a string named “Welcome to Shadow Force,” which gave away the clue. This analysis report will introduce how AhnLab uncovered Operation Shadow Force.

All cyberattacks against Korean companies and organizations using Shadow Force malware and Wgdrop malware are classified as Operation Shadow Force. The activities were dubbed as Operation Shadow Force primarily because it used Shadow Force malware. Operation Shadow Force’s first cyber attack was discovered in March 2013 and has been active for the last seven years. However, considering the period of development, there is also a high possibility that the group was active even before 2012. It has not been confirmed whether the attacker behind Operation Shadow Force is associated with any known group.

Introduction: Operation Shadow Force

Details regarding Operation Shadow Force attack methods remain unconfirmed. The attackers could have used emails as a medium to infiltrate the system. However, it is likely that a vulnerable SQL server was exploited for the attacks since Windows Server was mostly targeted, and other malware was downloaded onto sqlserver.exe, a normal SQL server executable file, it is likely that a vulnerable SQL server was exploited for the attacks.

Operation Shadow Force used the fact that the mastermind behind the operation was little-known to the public for the past seven years. Since 2014, the attacker has been using the method of modifying trusted files, such as error handling programs and disk management programs, to automatically load the malware when executed. Because these programs are often connected to the network and classified as trusted programs, user suspicion was avoided even if it showed a rather abnormal behavior. The attacker evaded detection by signing the digital certificate with a normal certificate key that had already been leaked. Security programs classify files signed with normal digital certificates as trusted programs, therefore all abnormal behaviors are neglected.

In September 2014, Pemodifier (iatinfect.exe) file was first discovered. This was around the same time Wgdrop malware had changed into DLL type. The creator had been using Wgdrop in the EXE type. But after Spring 2014, the strategy had advanced into modifying normal EXE file to run DLL type malware.

There are many cases in which the malware creator’s name exists on the malware, such as Melody, Syrinx, and WinEggDrop. The creators developed various hacking tools, such as file property changer and process viewer, to carry out attacks.

Fortunately, the connections between the attackerswere quickly made as they used the same technique and file post-2014.

Details on Operation Shadow Force Attack Stage

The group behind Operation Shadow Force has been active for seven years since 2013, yet the number of reported incidents was extremely low. Some were totally clueless that they had been compromised.

Confirmed cases of the attacks are as follow:

Date	Target	Description
September 2014	IT Management	Attacks using Htran (d014027b15e3f5099676e423131ef805), Pemodifier (9e0859b29641c9300058a2686daa1b06), Wgdrop (1fd5d459f198bda20399f0e76ce64f8e) and more
January 2015	Medical	VAN management program patched and Wgdrop type B executed (e4b0d1942064d644e7bd65fca8508c21)
May 2015	News Media	Shadow Force variant discovered (5408579f20d1dc533857cbbc114323d3)
July 2015	Distribution	Shadow Force (07a390809ba4f8e4d0b213e9f9a88252) and Pemodifier (e52dddabd40783032e85fe1076db2c6c) discovered
August 2015	Food Service	Wgdrop type A (f57e577822b6aaac5b9dfd9e464d4694) and Wgdrop B executed by modifying the system management program (9fe571b36f14e23269095164398 1011c)
March 2019	Government Organization	Shadow Force variant reported

Table 1. Operation Shadow Force Incident Report

The targeted system was mostly Windows Server, and the attacker infiltrated the system through an unknown route. Although the infiltration route remains unknown, it was revealed that many malware were downloaded via the aio.exe file. The system history revealed that aio.exe was downloaded from sqlservr.exe, which is a SQL-related file. This could indicate that the attacker first took control of the SQL server, then downloaded the aio.exe file.

The attack starts with the attacker first downloading the malware via Htran (aio.exe) file then modifying a regular program with Pemodifier (iatinfect.exe) to run a specific DLL file. Modified EXE file is executed along with the malicious DLL, such as Shadow Force. Some systems install additional programs such as keylogger and screen recorder to carry out other malicious activities.

Approximately 98 malware were used for Operation Shadow Force from 2013 to March 2020.

Figure 1 shows the number of malware discovered each year. Note that the time of discovery may not coincide with the time the malware was used in attacks.

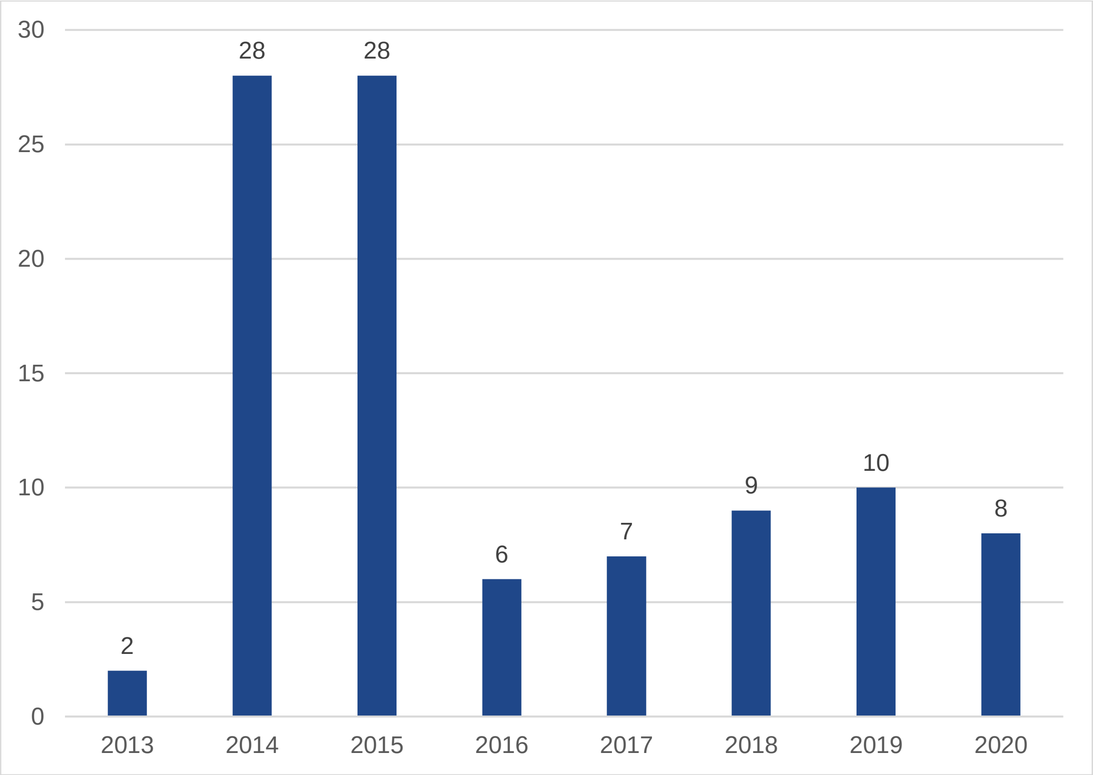

Figure 1. Number of Malware Discovered Being Used for Operation Shadow Force

Out of the 98 malware discovered, 32 malware were classified as Wgdrop variants and 23 were classified as Shadow Force variants.

The attacker primarily used Shadow Force variants after 2014, resulting in an increase in the number of Shadow Force variants being found, hence the name.

According to the analysis the attacker utilized a total of 34 hacking tools during the attacks.

Tracking Down Operation Shadow Force

Operation Shadow Force was first discovered while AhnLab was researching an unrelated topic. In January 2020, the Japanese press reported the hacking of Mitsubishi Electric.[1] According to the Japanese press, 4 groups, including Aurora Panda (APT17), Emdivi, Tick, and BlackTech, have been attempting to carry out various attacks since 2013.[2]

AhnLab released several analysis reports regarding the attack on Japan Pension Service led by Emdivi[3] and Tick group's activities in Korea.[4] However, Aurora Panda and BlackTech were groups with little publicity in Korea. AhnLab decided to track down Aurora Panda group to reveals their activities in Korea. Note that information on malware used during the Mitsubishi Electric attack remains unknown.

Since many security providers released analysis reports on Aurora Panda, the Indicator of Compromise (IOC) were found. However, Aurora Panda activities in Korea were not tracable using the existing IOC. Just when AhnLab was about to put an end to the investigation, new discoveries revealed that a Zoxpng variant, which is known to be related to Aurora Panda, had signed a digital certificate belonging to a Korean company.[5] As there is a possibility that other malware signed with 4N* certificate could exist, AhnLab then quickly proceeded to track the file signed with 4N* certificate to find any suspicious files.

At the time of analysis in January 2020, there were a total of 672 files signed with 4N* certificate. Few suspicious files were investigated, but most files were found to be normal. However, from a file (md5: 6f0e62b15efd2b2468ef37c138eb189a) collected in November 2017, a suspicious string named, "Welcome To Shadow Force" was found.

This file contained a different certificate serial number, unlike malware signed with an existing 4N* certificate (serial number: 483f0bf7a6d84c6cf429d4eb4988e686). The certificate information was also uncertain, which increased the possibility of the file being an abnormal certificate. But overall, the discovery of Shadow Force was a significant lead. An analysis report released by Trend Micro in 2015 was referred to for more relevant information.[6]

One Shadow Force variant was discovered using a forged 4N* certificate. After carefully examining the samples collected by AhnLab, 23 Shadow Force variants were discovered. Report from Trend Micro was about a variant that attacked Korean companies in 2015, but the relevant hash information was not released, making it impossible to confirm the malware identity. However, AhnLab could conjecture through the file name that it is a sample similar to the one retrieved in 2015. The variant was first discovered in September 2014, and by checking if the client receipt is existent in the file found, a variant was confirmed to be the file (md5: fcd695fa1cd04b23697b2e4fdd2d557b), which Korean government organization reported in March 2019. There was also a file (md5: a952b2cd5661c94ed7f13a88f8c41ee7), which remained active till early 2020 without being reported once.

[1] https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html

[2] https://www.asahi.com/articles/photo/AS20200121004397.html

[3] https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?cmd=scrap&seq=23821&menu_dist=2

[4] https://asec.ahnlab.com/1216

[5] https://www.novetta.com/wp-content/uploads/2014/11/ZoxPNG.pdf

[6] https://blog.trendmicro.com/trendlabs-security-intelligence/shadow-force-uses-dll-hijacking-targets-south-korean-company/

Activities Exploiting Fake or Exposed Certificates

The attacker of Operation Shadow Force exploited a legitimate digital certificate, either already exposed or through hacking activities, to sign the malware.

The attacker used CyberLink certificate in 2012, A'd*** certificate in 2012-2013, EZ*** in 2014, 4N* in 2017, and blue**** certificate in 2018-2020.

Certificate	Certificate Key	Country	Period	(Possible) Method	Status
4N*	483f0bf7a6d84c6cf429d4eb4988e686	ROK	2017	Using Fake Certificates	Unknown
A'd***	456e967a815aa5cbb99fb86aca8f7f69	ROK	2012 ~ 2013	Exploiting Exposed Certificates	Revoked
Blue****	706ac96953034b9d9926d4cc1d3248b3	ROK	2018 ~ 2020	Exploiting Exposed Certificates	Valid
CyberLink	1d226108cbb0eb7b504697bdfec66a8b	Taiwan	2012	Using Fake Certificates	Revoked
EZ***	73e78017a7bf71b6762a603dc41fb6b5	ROK	2014	Exploiting Exposed Certificates	Valid
P*****a	39880be01fe37120ad98698509663f92	ROK	2018	Using Fake Certificates	Unknown

Table 2. Activities Exploiting Fake or Exposed Certificates

The attacker mostly exploited stolen certificates from Korean companies for the attack. However, this does not prove anything. To confirm the connection between this activity and the group behind Operation Shadow Force, we must also look into the attack methods.

Analysis of Malware and Hacking Tools

Figure 2 shows the main malware used for Operation Shadow Force.

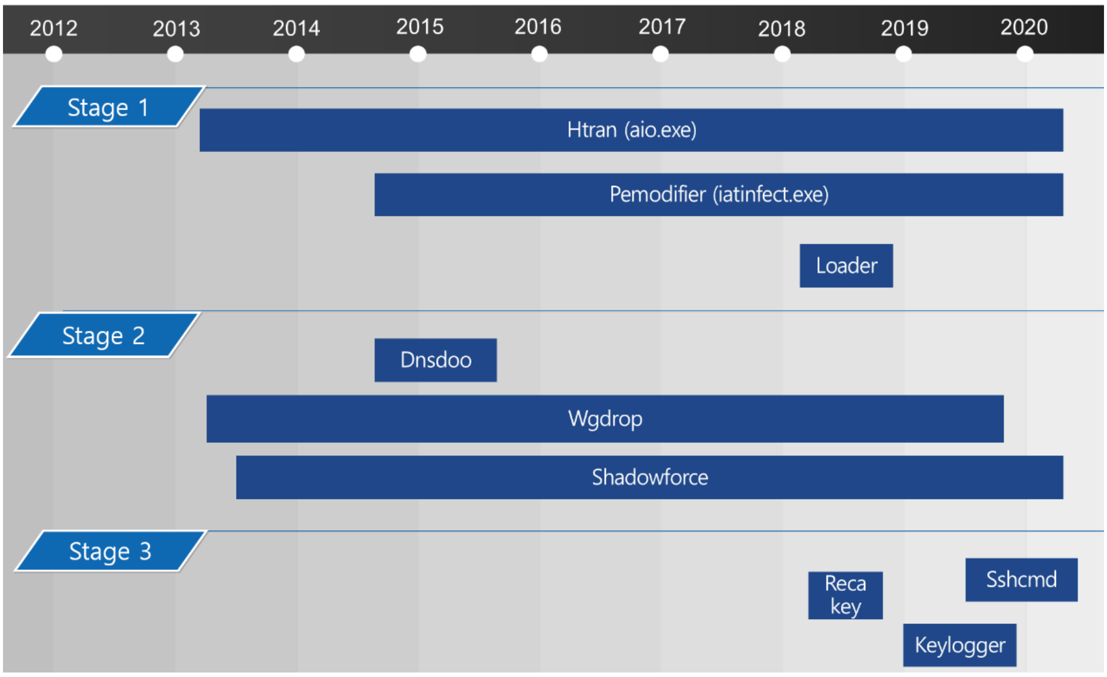

Figure 2. Malware Used for Operation Shadow Force

According to the analysis of the attack stages, the attacker used Htran(aio.exe), Pemodifier, Loader in stage 1, DNsdoo, Wgdrop, Shadowforce in stage 2, and Recakey, Keylogger, SSHCMD in stage 3. There are many more hacking tools used for the attacks than what is shown in Figure 2.

Relationship Analysis

While analyzing related malware, three creators, including Melody, Syrinx, and WinEggDrop, constantly appeared. According to Trend Micro report, WinEggDrop is the name of a person born in China in 1982. Whether the creators are multiple people or a single person or if they only develop the malware or also partake in the hacking, remains unknown. Some of the tools developed by WinEggDrop is available online for anyone to download and utilize.

The relationship between the malware, certificates, and creators are shown in Figure 3.

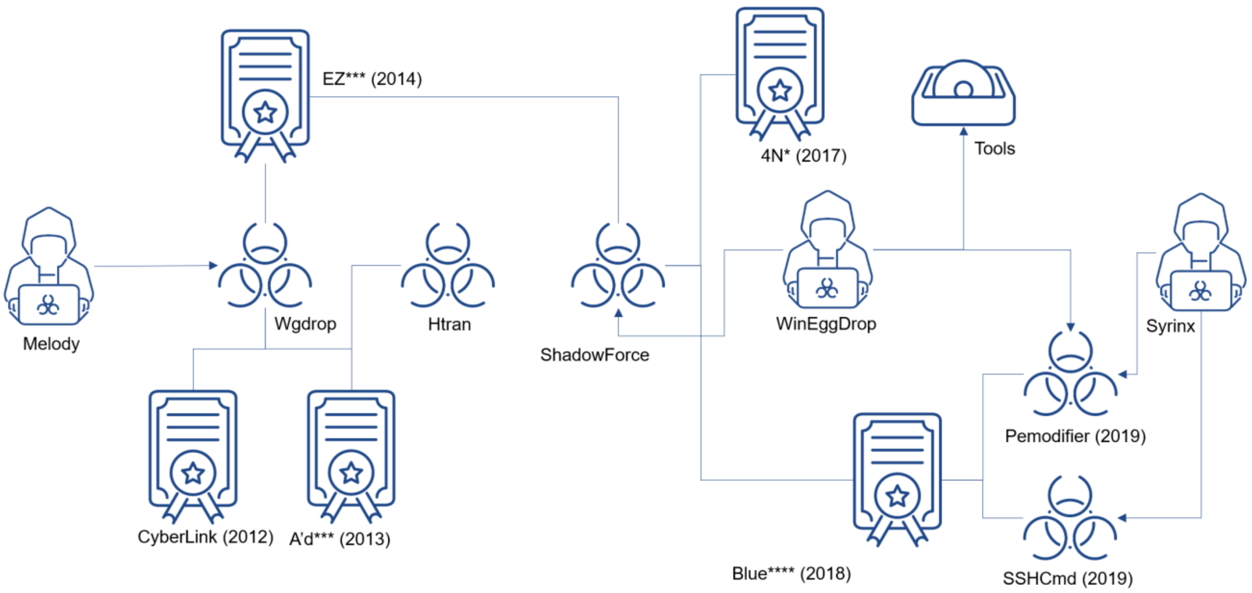

Figure 3. Relationship Between the Malware, Certificates, and Creators

Various malware were signed with an identical digital certificate. However, assuming that a single group conducted all the attacks cannot be made just from the fact that various malware are signed with an identical certificate. The attacker behind Operation Shadow Force downloaded files through aio.exe file, loaded DLL by patching system files through iatinfect.exe, and used a similar backdoor. The traces of these files from the infected system are significant findings.

The attacker periodically changes the malware being used for the attack. However, the attacker does not change the attack method of downloading malware through aio.exe file and modifying legitimate files through iatinfect.exe file.

Signs of Infection

Attacker downloads files in the system using aio.exe, and modify files through iatinfect.exe. Therefore, if either aio.exe or iatinfect.exe file is found, it implies that the group had already attacked the system.

Since the attackers are using the technique of patching normal programs and loading the malware, files signed with certificates become modified, resulting in an invalid certificate. If the digital signature information of the program is no longer valid or a string named, “Syrinx’s Victim,” exists in the EXE file, it implies that the file may have already been modified.

Also, if command-line programs developed by Melody, Syrinx, and WinEggDrop is found or RAR 3.80 exists on the console program, there is a possibility that it was Operation Shadow Force.

Conclusion

It was a total coincidence and a bit of pure luck that AhnLab was able to track down Operation Shadow while tracing a whole different topic. AhnLab was analyzing activities about a threat group that had attacked Mitsubishi Electric.

AhnLab aimed to find if the same hacking group was also active in Korea, and as a result, AhnLab managed to find the traces of the group that has been secretly active in Korea for seven years. The fact that this group remain under the covers for such a long period of time while carrying out malicious activities was remarkable. At the same time, concerns increased regarding the possibility of other threat groups being secretly active in Korea.

Fortunately, the attacker used very similar attack methods and hacking tools utilizing the same files for quite some time. This made it easy for AhnLab to track down relevant activities. After analyzing the similar malware and attack methods, AhnLab dubbed the attacks aginst Korean companies as “Operation Shadow Force.”

However, many aspects still need answers. After much research, it is still unknown whether Operation Shadow Force and Aurora Panda (APT17) have any connections. ZoxPNG malware and Operation Shadow Force cannot be assumed to have any links just with a single identical certificate with a different serial number.

AhnLab released this analysis report in hopes of helping Korean companies to detect Operation Shadow Force early on in the attack by using the signs of infection stated above.