

TLP: GREEN

Shadow Force Group's Viticdoor and CoinMiner

2020 - 2022 Threat Trend of Shadow Force Group

V1.0

AhnLab Security Emergency response Center (ASEC)

Mar. 27, 2023

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	Documents that can only be accessed by the recipient or the recipient department Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	Can be copied and distributed within the recipient organization (company) of reports Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

This report is a work of authorship protected by the Copyright Act. Unauthorized copying or reproduction for profit is strictly prohibited under any circumstances.

Seek permission from AhnLab in advance if you wish to use a part or all of the report.

If you reprint or reproduce the material without the permission of the organization mentioned above, you may be held accountable for criminal or civil liabilities.

The version information of this report is as follows:

Version	Date	Details
1.0	2023-03-27	First version

Contents

Activities of Shadow Force Group in 2020 - 2022.....	5
1) Introduction	5
2) Attack Targets and Actual Cases.....	6
Discovery of Additional Malware Signed with Game Developer Company B's Certificate	8
Viticdoor.....	9
Activities for Financial Gain Through Coin Mining.....	14
Conclusion	16
AhnLab Response Overview.....	17
Indicators Of Compromise (IOC)	17
File Paths and Names	17
File Hashes (MD5).....	18
Related Domains, URLs, and IP Addresses	19
MITRE ATT&CK.....	20
References	24



CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Activities of Shadow Force Group in 2020 - 2022

1) Introduction

The Shadow Force group is a threat group that has been active since 2013, targeting corporations and organizations in South Korea. Trend Micro revealed the first analysis report¹ in September 2015, where it stated that a Korean media-related company had been attacked. In March 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 activities of an existing threat group. However, no relevant threat group information has been found for over three years since the release of the analysis report, and it thus seems to be a group active in Korea. In July 2022, KRCert published the details of their analysis of the Shadow Force group's additional breach through their report "Analysis of Lateral Movement Strategies Using TTPs#7 SMB Admin Share".³ In October 2022, AhnLab announced that the PE-modifying iatinfected.exe file is continuously being detected.⁴

This report covers the changes made to existing malware and new malware discovered through tracking recent activities of the Shadow Force group. There are continued reports of file modification using iatinfected.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 were being installed alongside them. The threat actor has been using the same file name and similar malware and tools since 2014, making it easier to identify them.

¹ <http://documents.trendmicro.com/assets/pdf/shadow-force-technical-brief.pdf>

² [https://download.ahnlab.com/global/brochure/\[Analysis_Report\]Operation_Shadow_Force\(1\).pdf](https://download.ahnlab.com/global/brochure/[Analysis_Report]Operation_Shadow_Force(1).pdf)

³ <https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000127&searchWrd=&menuNo=205021&pageIndex=2&categoryCode=&nttId=66830> (This report supports Korean only for now)

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

2) Attack Targets and Actual Cases

Cases of attack identified by AhnLab between 2020 and 2022 are as follows.

Date	Attack Target	Details
Sep. 2020	Korean political organization	Only Linkinfo.dll reported (md5: 1e7bc7c9856a3020325527fd108b50e3)
Feb. 2021	Korean government organization	Only Linkinfo.dll reported (md5: 91d0af0a1219e00a5eb77b4e560a3cde)
Mar. 2021	Korean food	Viticdoor discovered
Sep. 2021	Korean IT service	Viticdoor discovered
Dec. 2022	Korean communications	Viticdoor discovered
Dec. 2022	Korean outsourcing	Viticdoor discovered

Table 1. Major attack cases

While not many case reports have been filed to AhnLab, there are over 40 cases of infection where the targeted company has not been identified. Most are deemed to be servers, and many victims were unaware of the breach because it did not affect the system's operations. The KRCert report also mentions a case where the targeted company's system had been overtaken by the threat actor for years until the company became aware of the infection after it had been contacted.

Some of the infected IPs were web servers that could be accessed externally and had vulnerabilities.



Figure 1. Accessing the infected IP

Discovery of Additional Malware Signed with Game Developer Company B's Certificate

The Shadow Force group has been signing malware files with the certificate of Korean game developer company B since April 2018. In February 2023, AhnLab investigated files signed with this certificate in 2021 and onwards and found Viticdoor and remote execution tools.⁵ However, the date of the signatures was in 2019, and it is presumed that malware used in the past were being discovered recently.

The malware and tools signed with the aforementioned certificate that have not been documented are as follows.

When vtcp.exe (md5: b4021d49e0478ac6436a22498e699976) is executed, it creates a normal vtcp.dll file, which can be used as a backdoor to upload, execute, delete files, and execute reverse shells (cmd.exe).

remoteexec.exe (md5: c9f17ac6aec437b2e9c1e79ed67646dd) is a remote execution tool created by WinEggDrop from the Shadow Force group.

```
c:\work>remoteexec.exe
Remote Exec V1.0 By WinEggDrop Built 02/18/2019
[!] WARNING: Not Running As Local SYSTEM. Not All Tokens Will Be Available.
```

Figure 2. Execution of remoteexec.exe

⁵ <https://atip.ahnlab.com/ti/contents/asec-notes?i=ee7d08fd-3990-4052-a427-907297ec7427>

Viticdoor

AhnLab named vtcp.exe as Viticdoor, and further investigation confirmed that a similar malware has been in use since March 2019.⁶

File names of Viticdoor include LZ4VTCPNormal.exe, mvp.exe, and vtcp.exe, and some are packed. Files are about 32 - 200 KB in size, and some packed files exceed 10 MB.

Viticdoor is disguised as Microsoft's "Dynamic Virtual Channel" file.

⁶ <https://atip.ahnlab.com/ti/contents/asec-notes?i=a78a218a-fcf4-4ed6-bcac-fee0fb825fb>

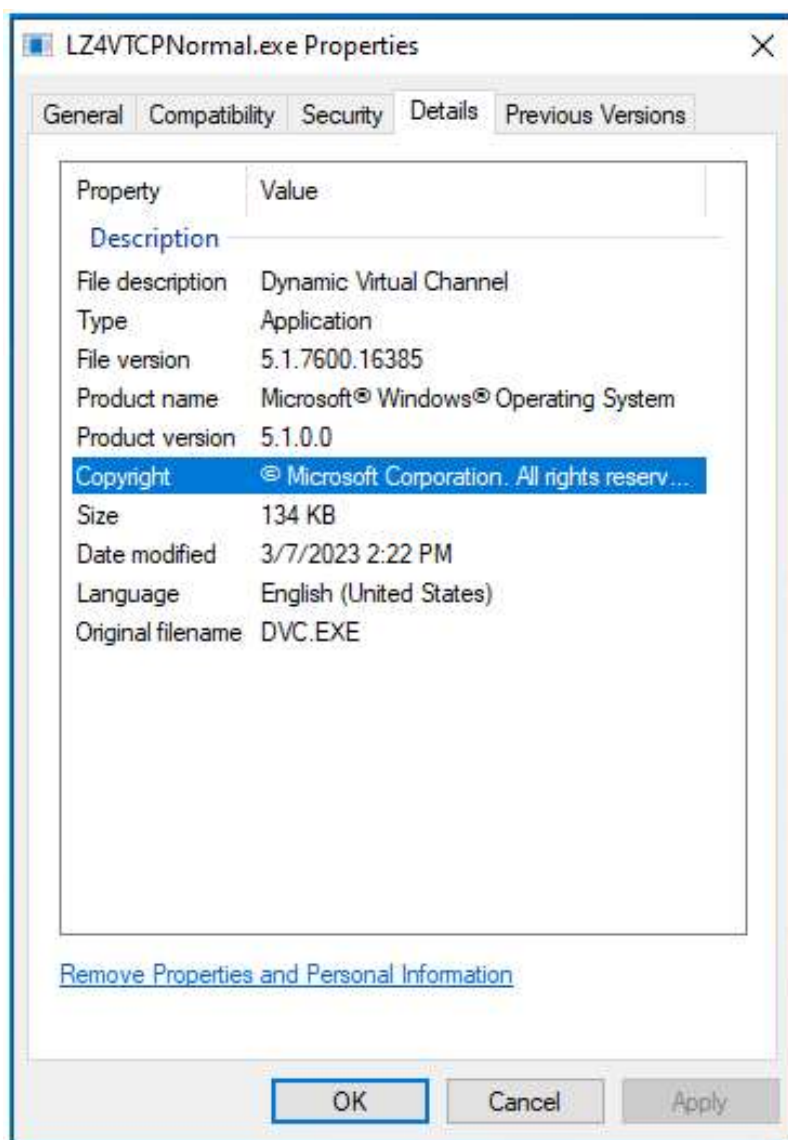


Figure 3. Disguised as a Microsoft file

Viticdoor loads vtcp.dll to upload and download files, allowing some variants to save the vtcp.dll file in the resource area.

vtcp.dll is a normal file created in China. AhnLab only detects files that are modified in ways such as being signed with stolen certificates.

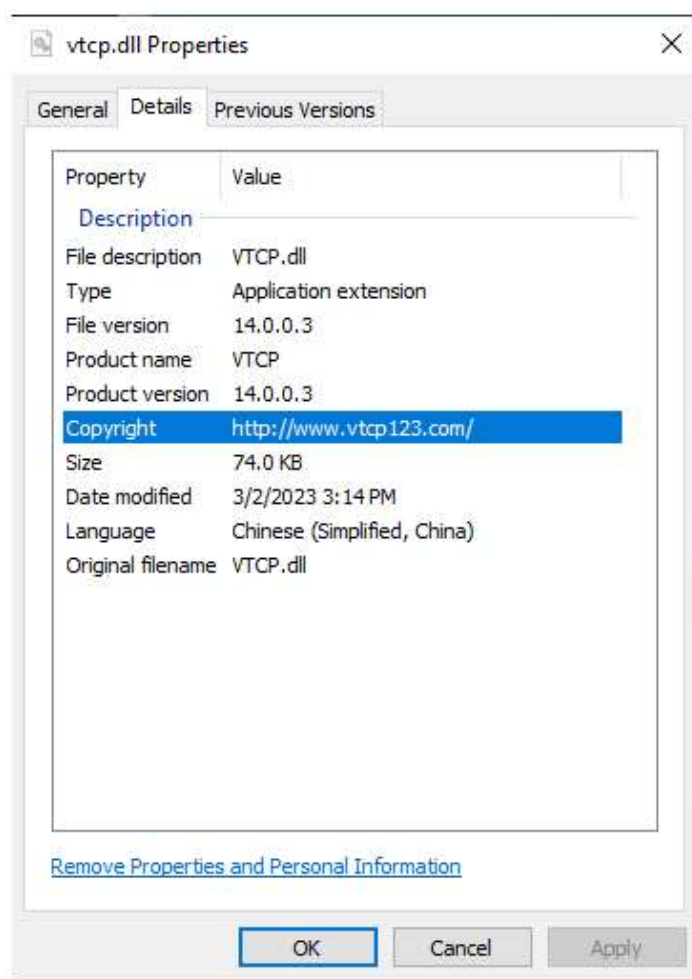


Figure 4. vtcp.dll properties

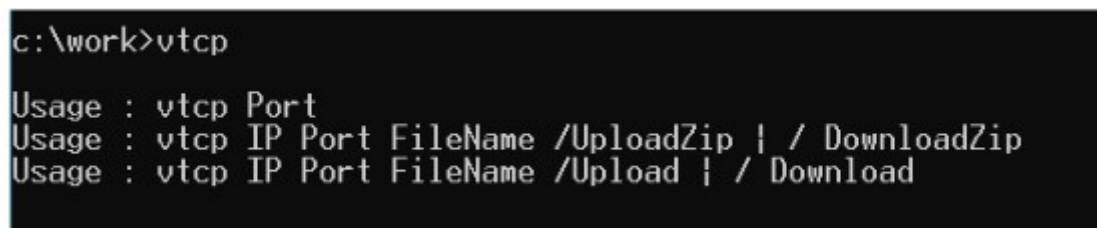
The table below shows the changes the file went through up to December 2022 since the discovery of its first version in March 2019.

First Detected	Details
Mar. 2019	Initial version. Supports commands including listening on specific ports, reverse shells, uploading, downloading, and deleting files
Mar. 2020	Packed version discovered
Jan. 2022	Supports uploading and downloading of additional files
Dec. 2022	Port listening feature removed

Table 2. Evolution of Viticdoor

Some versions after March 2020 are packed, and the size of these files often exceed 10 MB.

When Viticdoor is executed without an argument, a manual is displayed.



```
c:\work>vtcp
Usage : vtcp Port
Usage : vtcp IP Port FileName /UploadZip | / DownloadZip
Usage : vtcp IP Port FileName /Upload | / Download
```

Figure 5. Execution screen of vtcp.exe

In some variants, the actual option command and the description given on the screen differ.

```

47     argva = (char *)argv[3];
48     if ( strcmpi(argv[4], aU) && strcmpi(argv[4], aD) )// /U, /D
49     {
50         if ( strcmpi(argv[4], asc_4182F4) )// /L
51         {
52             if ( strcmpi(argv[4], aUz) && strcmpi(argv[4], aDz) )// /UZ /DZ
53             {
54                 if ( strcmpi(argv[4], aE) ) // /E
55                 {
56                     if ( strcmpi(argv[4], aDelete) )// /Delete
57                     {
58                         if ( !strcmpi(argv[4], aR) )// /R
59                         {
58                             ReverseShell_40CA60(v6, v7, (int)argva);
59                         }
59                     }
58                 }
57             }
56         }
55     }
54     }
53     }
52     }
51     }
50     }
49     }
48     }
47     }

```

Figure 6. Options that differ from the execution screen

The version found in 2021 was added with commands such as FastDownload, FastUpload, RamDownload, and RamUpload.

```

52     case 2:
53         v5 = atoi(argv[1]);
54         Listening_40C7EB(v5);
55         break;
56     case 3:
57         if ( !strcmpi(argv[2], aUnzip) )           // /UnZip
58             sub_408C44((HANDLE)argv[1], 0);
59         break;
60     case 5:
61         v6 = argv;
62         NumberOfBytesRead = (char *)argv[1];
63         argca = (void *)atoi(argv[2]);
64         argva = (char *)argv[3];
65         if ( strcmpi(v6[4], aUpload)              // /Upload
66             && strcmpi(v6[4], aRamupload)          // /RamUpload
67             && strcmpi(v6[4], aFastupload)         // /FastUpload
68             && strcmpi(v6[4], aDownload)           // /Download
69             && strcmpi(v6[4], aRamdownload)        // /RamDownload
70             && strcmpi(v6[4], aFastdownload) )     // /FastDownload
71         {
72             if ( strcmpi(v6[4], aList) )
73             {
74                 if ( strcmpi(v6[4], aUploadzip_0) && strcmpi(v6[4], aDownloadzip_1) )// /DownloadZip
75                 {
76                     if ( strcmpi(v6[4], aExecute_0) ) // /Execute
77                     {
78                         if ( strcmpi(v6[4], aDelete) ) // /Delete
79                         {
80                             if ( strcmpi(v6[4], aRshell_0) )// RShell
81                             {
82                                 if ( strcmpi(v6[4], aLz4upload) && strcmpi(v6[4], aLz4download) )// /LZ4Upload
83                                 {
84                                     if ( strcmpi(v6[4], aAesupload) && strcmpi(v6[4], aAesdownload) )// /AESUpload
85                                     {
86                                         if ( strcmpi(v6[4], aNormaldel_0) )// /NormalDel
87                                         {
88                                             if ( !strcmpi(v6[4], aEcho) )// /Echo
89                                             {
90                                                 v7 = (char *)v6[1];
91                                                 argvc = atoi(v6[2]);
92                                                 v8 = atoi(v6[3]);
93                                                 Echo_4044EC(v7, argvc, v8);

```

Figure 7. 2021 version

The version discovered in 2022 (md5: d7824290ee4e4bd98453e0530005b678) has the port listening feature removed.

```

c:\work>vtcp
Usage : vtcp IP Port FileName /UploadZip | / DownloadZip
Usage : vtcp IP Port FileName <SaveName> /Upload | / Download

```

Figure 8. 2022 version of Viticdoor

Activities for Financial Gain Through Coin Mining

CoinMiners that mine crypto (virtual) currency have also been found in systems infiltrated by the Shadow Force group. Over 30 similar CoinMiners were discovered, and out of these, five samples were found alongside malware with file names unique to the Shadow Force group: iatinfect.exe and ntuser.dat.






2022-11-07 13:25:21	 xpadsi.exe	Trojan/Win64.Miner
2022-11-07 13:22:00	 iatinfect.exe	Trojan/Win.ShadowForce
2022-11-07 12:54:54	 invoke-smbclient.ps1	Trojan/PowerShell.SMBClient.S1594
2022-11-07 12:48:42	 ntuser.dat	ASD.Prevention
2022-11-07 12:48:42	 jp.exe	Trojan/Win.ShadowForce

Figure 9. Files collected from systems attacked by the Shadow Force group

A notable point about these CoinMiners is that they are signed with invalid Microsoft certificates.

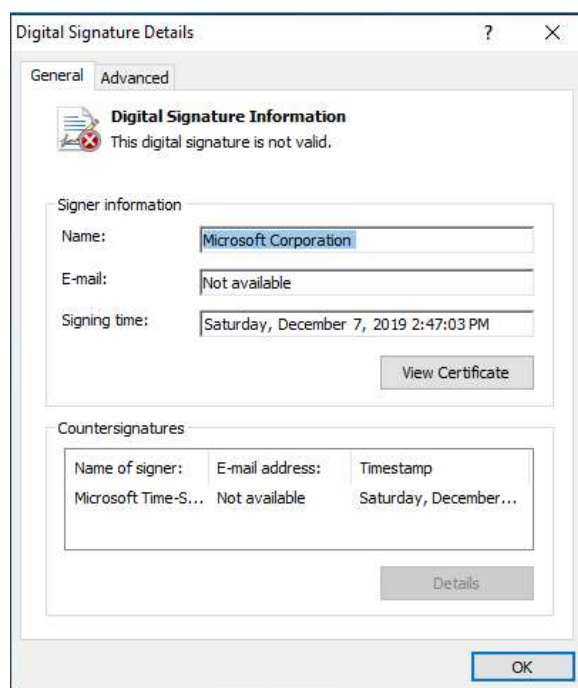


Figure 10. Disguised signatures using Microsoft certificates

Configuration files such as wdbase.plk and .xmrig.json are required for execution. Only the executable files were collected and additional analysis was not possible.

Conclusion

As the Shadow Force group attacked various Korean industries and government organizations, they were presumed to be a state-sponsored threat group with the goal of information theft. However, seeing from the fact that they leave their nickname in the malware and that they install CoinMiners in recent attack campaigns, there is a high possibility that this group is a cybercrime organization motivated by financial gains. However, coverage of this threat group by security companies or organizations is low, and there is still an insufficient amount of relevant information.

Currently, their activities have mainly been detected in Korea, and there are no related external reports. However, according to AhnLab's research results, there were small numbers of pertinent infections in areas other than Korea, suggesting that this group is expanding their region of activity.

The Shadow Force group is presumed to target Windows servers, and their specific attack methods have not yet become known. Fortunately, the Shadow Force group often uses the same file names, and thus breach incidents can be detected with only the file names. When a system is suspected of being breached by the Shadow Force group, security managers are advised to contact AhnLab for investigation of the suspected infiltration.

AhnLab Response Overview

The aliases and the engine version information of AhnLab products are shown below. Even if the activities of this threat group have been identified recently, AhnLab products may have already diagnosed the related malware in the past. While ASEC is tracking the activities of this threat group and responding to related malware, there can be variants that have not been identified and thus are not detected.

Backdoor/Win.Viticdoor.C1828479 (2023.03.17.00)
Backdoor/Win.Viticdoor.C5338464 (2023.03.22.03)
Backdoor/Win.Viticdoor.C5354013 (2023.03.17.00)
Backdoor/Win.Viticdoor.C5392852 (2023.03.10.00)
Backdoor/Win.Viticdoor.R561352 (2023.03.09.03)
Backdoor/Win.Viticdoor.R561356 (2023.03.09.03)
Backdoor/Win.Viticdoor.R561357 (2023.03.09.03)
Backdoor/Win.Viticdoor.R561358 (2023.03.10.00)
Backdoor/Win.Viticdoor.R561489 (2023.03.10.03)
Backdoor/Win.Viticdoor.R561494 (2023.03.17.00)
CoinMiner/Win.ShadowForce.R544353 (2022.12.22.00)
Trojan/Win64.Miner.R358817 (2020.12.19.00)

Indicators Of Compromise (IOC)

A portion of the following IOC quotes other analysis reports, and there are some unverified cases because samples could not be obtained. Updates may occur without prior notice when new information is found.

File Paths and Names

The file paths and names used by the threat group are as follows. File names of some malware or tools may be the same as those of normal files.

iexplor.exe lz4vtcp1436.exe

```
LZ4VTCPNormal.exe  
mvp.exe  
SecurityHealthSystray.exe  
vtcp.exe  
vtcps.exe  
WsatConfig.exe  
xemingliu.ttf
```

File Hashes (MD5)

The MD5 of the related files are as follows. However, sensitive samples may have been excluded.

```
. Miner  
5bfc7795c4e7bfff983854d09586d821  
1924edba0f1b9d45889c17f926b2782c  
e9dad7bdac452217c5a79a2daae905b  
19f842085bc90ff54af2db6b3d12299f  
b1389a13c326d716807a7dd4f1ed818a  
  
. Viticdoor  
288d40766729019ceea6630344c19743  
49306e932018bf72abe717e6050c1953  
26dfb0aea560069b9c31315e8fce5f5f  
b336a3713b8a06dbcf1cc3a6034d855  
75e13b8fbccc8574f86bbeed602bc0ee  
f8235c51e43c388ee85dc53bacac0e4b  
43495da1f2b19554c7be584e04b85eaa  
ed8042c000e107e32c82d3c6a7d697cf  
f7ea2db9149e0d61abc408b2aaa577b1  
fb7a84c3d0effba662a1a8297e7674d9  
b67d0d7ed3408fa10c3ed1ad966fcafa  
5001281b792a9b1801e93e411b9401c7  
7b264a9f2704f2d449ead768949da56e  
bc80aab531616d76055e8d2b5d131f8b  
1681ff45501e752c386e9663441e5ba5  
4f86621b9852147cbd197966a11b4ba6  
5d5fcf23c96cd29f1025a1da7eee20db  
824dfc97525b3ab7d64c0f50e42bf3ca  
69d616d91ae3df371d38805f2ae34c8b  
849307e4bb42f3e0f6a337b043ac4f71  
59bba020254967c42888e75dedf96210
```

```
0e1d438f5bf7317981239d240123ac35  
aab7a109a2bd7d887f37b9afcf39cad1  
7162118a94e6794762f48f541e2e2220  
2c14f38b1d2561901a62893bd0ca3ab3  
ac7000dc5c699716550cca026a957b69  
b4021d49e0478ac6436a22498e699976  
bdadd1bf32c686f926dd38e9ba6f1984  
9bec8f22ad907060046c2f4592da3b42  
d7824290ee4e4bd98453e0530005b678  
657f7854f500af0f622afa8faa7fefe3  
c78a2a7bf2fa8f18e17d189c1a4f47f9
```

Related Domains, URLs, and IP Addresses

The download and C2 addresses used are as follows. http was changed to hxxp, and sensitive information may have been excluded.

```
151.106.25.243:80  
178,128,242,134:443  
103.253.75.186:443
```

MITRE ATT&CK

The MITRE ATT&CK information on this security attack is as follows. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is the classification of the tactics and techniques of malicious behaviors presented by the threat actor. Relevant information can be found on <https://attack.mitre.org/>.

The MITRE ATT&CK ID corresponding to this threat group quotes from another analysis report and has additional details confirmed by AhnLab.

Tactic	ID	Description
Reconnaissance (TA0043)		
Resource Development (TA0042)	T1583.001 Acquire Infrastructure: Domain	
	T1583.004 Acquire Infrastructure: Server	
	T1587.001 Develop Capabilities: Malware	
	T1587.001 Obtain Capabilities	
Initial Access (TA0001)		

Execution (TA0002)	T1569.002 System Services: Service Execution	
	T1059.003 Command and Scripting Interpreter: Windows Command Shell	
Persistence (TA0003)	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	
	T1546.008 Event Triggered Execution: Accessibility Features	
	T1543.003 Create or Modify System Process: Windows Service	
	T1554 Compromise Client Software Binary	
	T1078.001 Valid Accounts – Default Accounts	
Privilege Escalation (TA0004)		

Defense Evasion (TA0005)	T1140 Deobfuscate/Decode Files or Information	
	T1036.001 Masquerading: Invalid Code Signature	
	T1553.002 Subvert Trust Controls: Code Signing	
	T1036.004 Masquerading: Masquerade Task or Service	
	T1574 Hijack Execution Flow: DLL Side-Loading	
Credential Access (TA0006)	T1056.001 Input Capture: Keylogging	
	T1003.001 OS Credential Dumping – LSASS memory	
	T1110 Brute Force	
Discovery (TA0007)	T1057 Process Discovery	
	T1087.001 Account Discovery: Local Account	
	T1082 System Information Discovery	

Lateral Movement (TA0008)	T1021.002 Remote Services: SMB/Windows Admin Shares	
Collection (TA0009)	T1056.001 Input Capture: Keylogging	
	T1115 Clipboard Data	
	T1113 Screen Capture	
Command and Control (TA0011)	T1219 Remote Access Software	
	T1571 Non-Standard Port	
	T1105 Ingress Tool Transfer	
Exfiltration (TA0010)		

Impact (TA0040)	T1565.001 Data Manipulation: Stored Data Manipulation	

Table 3. MITRE ATT&CK

References

- [1] Variant of Shadow Force Group's iatinfected.exe Found (<https://atip.ahnlab.com/ti/contents/asec-notes?i=226d5bfe-4a8e-4a3f-8f52-af7dce7508ea>)
- [2] Threat Trend Report on Shadow Force Threat Group (<https://atip.ahnlab.com/ti/contents/issue-report/trend?i=4476ca85-7fa6-4586-8b2d-800e9edabcf4>) (This report supports Korean only for now.)
- [3] Shadow Force Group's Viticdoor Malware Discovered (<https://atip.ahnlab.com/ti/contents/asec-notes?i=a78a218a-fcf4-4ed6-bcac-fee0fb825fb>)

More security, More freedom

AhnLab, Inc.

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

Tel : +82 31 722 8000 | Fax : +82 31 722 8901

<https://www.ahnlab.com>

<https://asec.ahnlab.com/en>

© AhnLab, Inc. All rights reserved.

About ASEC

AhnLab Security Emergency response (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.