TLP: AMBER

Threat Trend Report on LuoYu Group

Analysis on WinDealer Malware

V1.0

AhnLab Security Emergency Response Center (ASEC)

Aug. 10, 2022

AhnLab

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.

The version information of this report is as follows:

Version	Date	Details
1.0	2022-08-10	First version

Contents

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.

LuoYu Group

1) Introduction

LuoYu is a threat group deemed to be from China who started their activities in 2014, targeting dissidents in China. The WinDealer malware used by the LuoYu group was first detected in 2008, so they may have been active for a longer period of time than we know. In January 2021, a Taiwanese security company named TeamT5 first introduced this malware at the Japan Security Analyst Conference (JSAC) in 2021, and [1]in January 2022, announced additional activities by the LuoYu group in JSAC 2022[2].

This group mainly uses Demsty (ReverseWindow, Sysetmd), SpyDealer, and WinDealer. Demsty is a malware with Android, Linux, macOS, and Windows versions, and SpyDealer is an Android malware. It is said that WinDealer intercepted auto-update features of Chinese software to infect user systems.[3] WinDealer was first introduced in October 2021 by Japan Computer Emergency Response Team Coordination Center (JPCERT/CC),[4] and in June 2022, additional information on WinDealer was disclosed by Kaspersky and BlackBerry.[5]

2) Attack Targets and Actual Cases

According to TeamT5, LuoYu attacks dissidents in China, and their activities have also been reported in Japan, Korea, Taiwan, Germany, Austria, United States, Czech Republic, Russia, and India. It is recorded that diplomatic organizations, academics, and corporations in national defense, logistics and communications were targeted.

---

[1] https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf

[2] https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_7_leon-niwa-ishimaru_en.pdf

[3] https://securelist.com/windealer-dealing-on-the-side/105946

[4] https://blogs.jpcert.or.jp/en/2021/10/windealer.html

[5] https://blogs.blackberry.com/en/2022/06/threat-thursday-china-based-apt-plays-auto-updater-card-to-deliver-windealer-malware

Below are cases of attacks collected through published analysis reports and information from AhnLab.

Date	Target	Details
2015 - 2017	China	Malicious Android app
April 2017	Taiwan, Korea, Japan	Attacks using the Demsty macOS version
June 2017	A university in Hong Kong	Details unknown
2019	Chinese news users	Demsty malware distributed through a Chinese news website in the US
May 2019	An IT company in China	Details unknown
September 2019	Presumed to be Korean regional governments, public corporations, and public organizations	WinDealer infection
May 2021	Chinese branches of Japanese corporations	Details unknown
August 2021	Chinese bank users	Details unknown
September 2021	Chinese branches of Japanese corporations	Details unknown

Table 1. Major attack cases

Since 2015, Chinese people with anti-establishment dispositions were under surveillance, and in 2017, the macOS version of Demsty attacked corporations in Taiwan, Korea, and Japan.

While it has been said that Demsty has been distributed on Chinese news websites in the US in 2019, but the corresponding IOC has not been disclosed.

In September 2019, AhnLab detected a case of infection of a WinDealer variant (md5: 46b9ec9af427869467cc3dbffae30086) in Korea. Whilst the specific attack target has not been identified, there is a high possibility that the target is either a Korean regional government, public company, or public organization.

3) Attack Method (Attack Vectors)

LuoYu's attack methods can largely be categorized into download, watering hole, and Man-On-The-Side attacks.

It is known to have been distributed in 2019 disguised as a normal Android app by hacking a Chinese news website in the US.
The Man-On-The-Side attack method, which intercepts update requests by certain programs and infects the requesting system with malware, [6]is behind the cases of malware infection. When the Chinese file ogametool.exe runs an update, malware is downloaded instead of the normal file. Relevant details were found on Chinese online forums.[7]

Man-On-The-Side Attack: Instead of taking complete control over a network node like the (Man-In-The-Middle) attack, the threat actor regularly accesses the communications channel to read the traffic and insert new messages. However, it does not allow the modification or deletion of packets in transmission between server and client. The threat actor must have perfect timing in order to make sure that their response to the victim's request arrives before the legal response. According to the document exposed by Edward Snowden in 2013, this term was used to describe malware infection by the NSA (National Security Agency).

4) Major Malware

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

[6] https://en.wikipedia.org/wiki/Man-on-the-side_attack

[7] https://bbs.kafan.cn/thread-2157062-1-1.html

Name	Type	Details
Demsty (ReverseWindow, Sysetmd)	Info-leakage	Supports various platforms (Android, Linux, macOS, Windows)
SpyDealer	Backdoor, Info-leakage	Android app
WinDealer	Backdoor, Info-leakage	Infection through Chinese software updates (Man-On-The-Side attack)

Table 2. Types of Malware

(1) Demsty (ReverseWindow, Sysetmd)

Demsty, also known as ReverseWindow and Sysetmd, has Android, Linux, macOS, and Windows versions. The IOC has not been released by TeamT5, so the exact sample could not be examined, but we found analysis information for a seemingly related malware.[8]

According to TeamT5, the following pieces of information are collected.

. Host name
. OS version
. User name
. MAC address
. CPU information
. RAM capacity
. Actual IP
. Hard drive volume names (Windows only)
. External storage files (Windows only)

(2) WinDealer

[8] https://vms.drweb.com/virus/?_is=1&i=15299312&lng=en

WinDealer is known to have first been found in 2008 and has DLL and EXE file versions. AhnLab only inspected the versions distributed after 2017, and these DLL files acted as the dropper and contains the following unique strings.

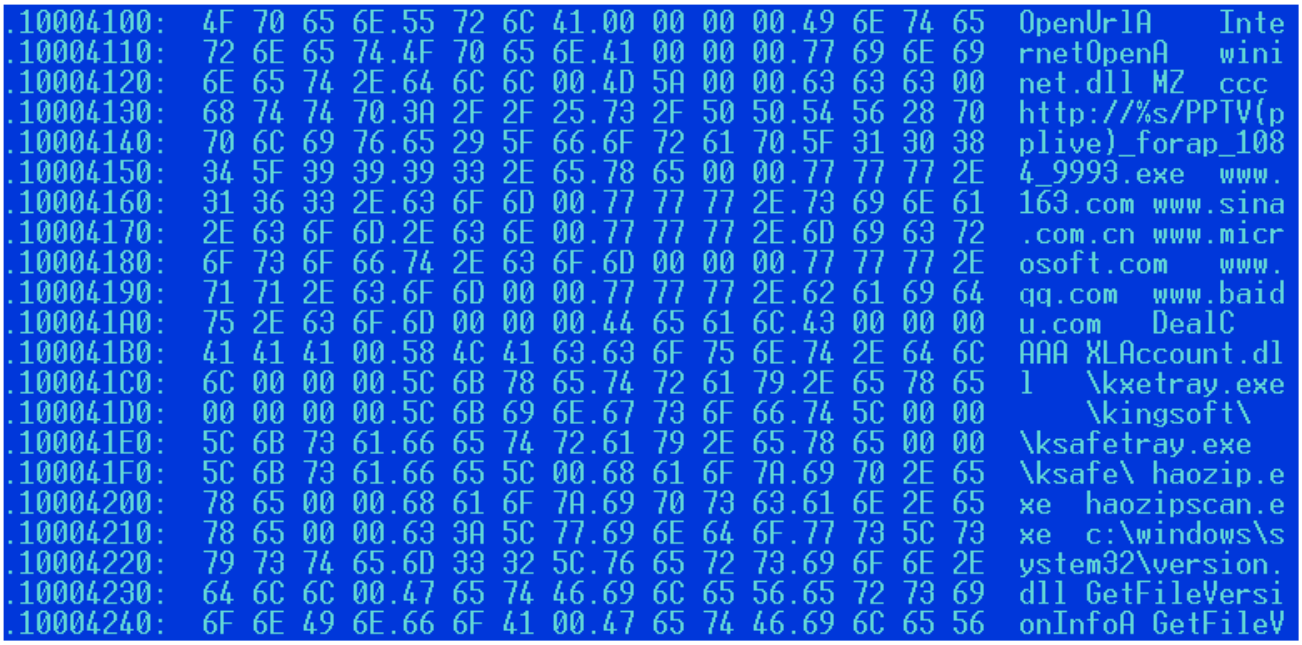

Figure 1. WinDealer-specific strings

The DLL file contains the actual backdoor file in its resources and creates the file xlaccount.dll among others. An arbitrary value is added according to the time each file is created, so each file hash is different. AhnLab has identified over 4,000 files from 11 variants.

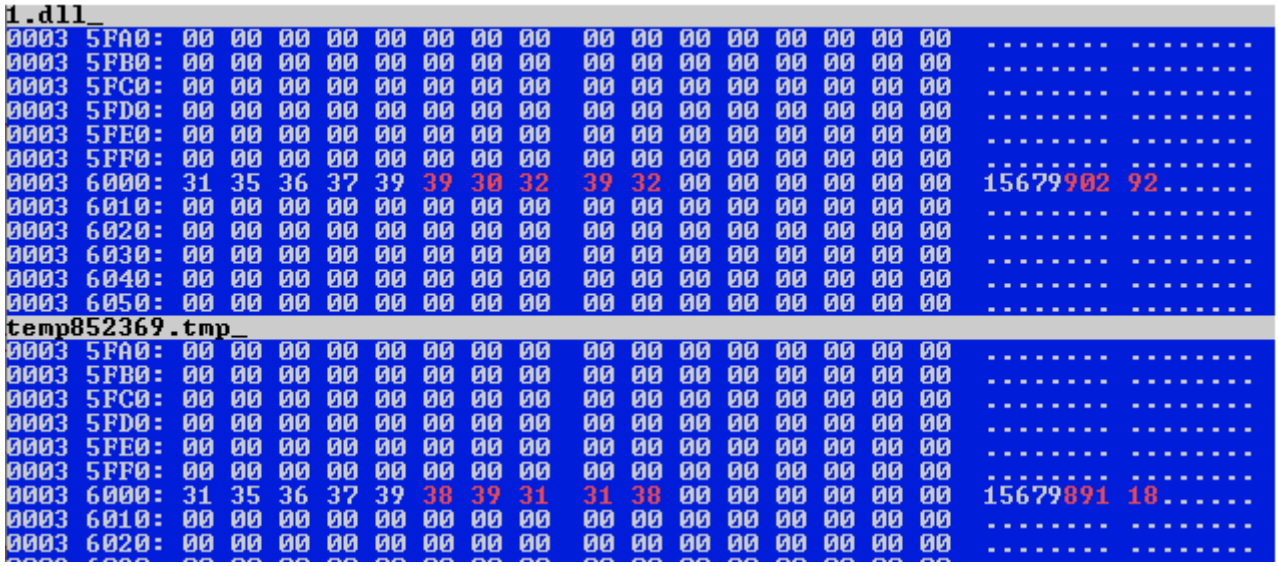

Figure 2. Comparison of DLL files with arbitrary values added

After February 2021, an EXE file version was found with the following structure.

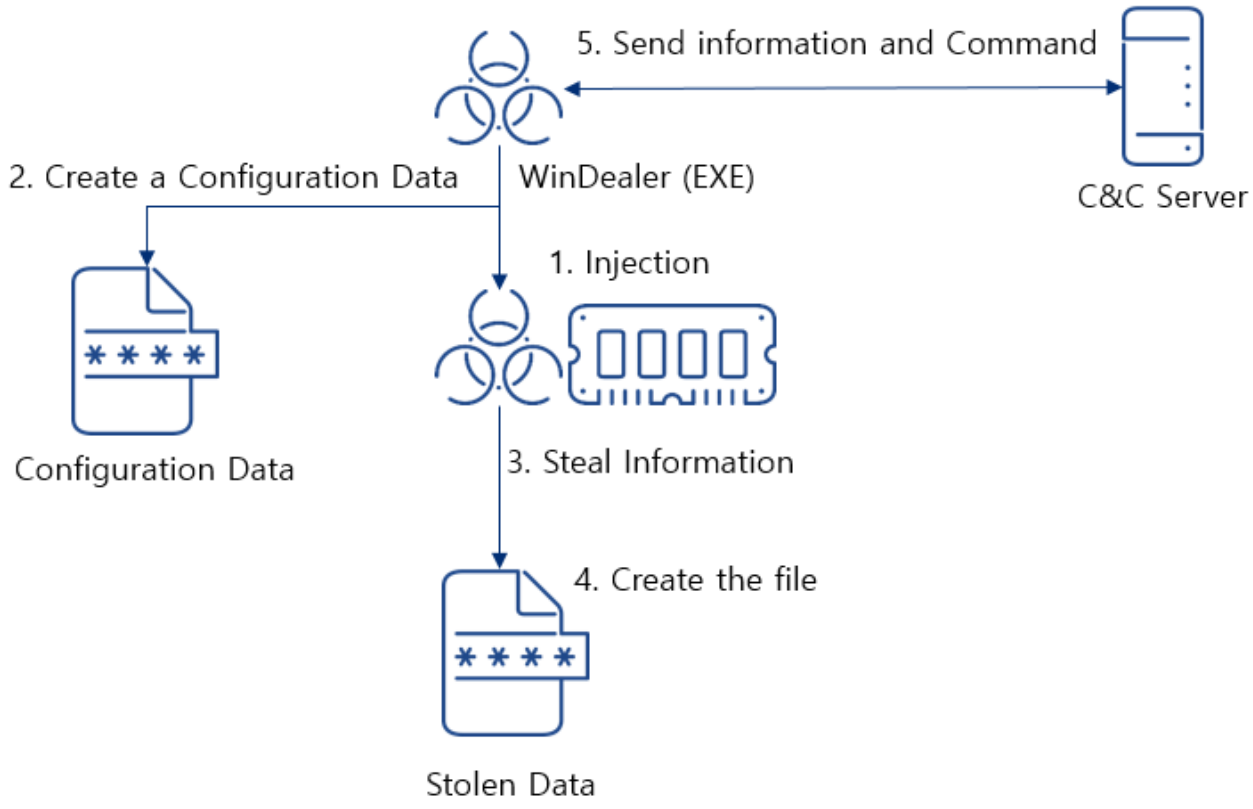

Figure 3. EXE file configuration

When the malware is executed, it is injected into a process (no. 1) and creates a configuration file (no. 2) before executing the information-collecting malware in the memory area (no. 3). Then, system information is collected and saved in a file (no. 4), and this in turn is sent to the C2 server (no. 5).

Some droppers include the version information inside the excluded WinDealer malware.

```
.1002C610:  0D 0A 0D 0A.00 00 00 00.25 30 32 64.25 30 32 64   ♪◙♪◙    %02d%02d
.1002C620:  25 30 32 64.00 00 00 00.25 30 34 64.25 30 32 64   %02d    %04d%02d
.1002C630:  25 30 32 64.00 00 00 00.31 36 2E 31.38 2E 31 30   %02d    16.18.10
.1002C640:  33 30 00 00.01 00 00 00.0D 0A 0D 0A.00 00 00 00   30 ○    ♪◙♪◙
.1002C650:  55 6E 6B 6E.6F 77 6E 20.43 50 55 20.74 79 70 65   Unknown CPU type
```

Figure 4. WinDealer version information

The version information is formatted as 'Malware Version.Year.Month and Date'. For example, 16.18.1030 represents the main version (16) of the malware, which is a version from October 30th, 2018.

Confirmed version information at this point is as follows.

Version	File Length	Details
16.18.1030	208,896 bytes, 219,136 bytes	DLL file
17.19.0505	227,328 bytes	DLL file
18.19.0628	231,424 bytes, 241,664 bytes	DLL file
18.20.1225	368,640 bytes	EXE file, Main md5: ef25d934d12684b371a17c76daf3662c

Table 3. Malware by version

The main features are as follows.

. File and file system control: Reading, writing, and deleting files, listing directory, gaining disk information
. Information collection: Collecting hardware details, network configuration and/or keyboard layout, listing running processes, installed applications and configuration files of popular messaging apps (Skype, QQ, WeChat, and Wangwang)
. Downloading and uploading of arbitrary files
. Execution of arbitrary commands;
. Total system search for text files and Microsoft Word documents
. Screenshot capture;
. Network scanning with ping scans
. Backdoor maintenance: Setting or removing persistence, updating configurations

Instead of the precise C2 address, the malware attempts to connect to an arbitrary IP address from a predefined range of 111.120.0.0 – 111.123.255.255 and 113.62.0.0 - 113.63.255.255, making it difficult to find the C2 server. The ports used are either TCP 55556 or UDP 6999.

AhnLab Response Overview

The alias 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 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.WINDEALER.C4733794
Backdoor/Win.WINDEALER.C5156829
Downloader/Win.Generic.R437183
Malware/Win.Reputation.C4393369
Malware/Win32.Generic.C2398745
Malware/Win32.Generic.C2673516

Conclusion

Although LuoYu is not well-known, it is one of the older threat groups, being in action since 2014. Whilst they mainly target anti-establishment personnel of China, cases of their attacks have been reported in many countries. They use not only malware for Windows, but also for macOS and Linux. Their Man-On-The-Side attack leaves the potential for systems to be infected with malware through update processes for normal software. They are a threat group that is less notorious in comparison to their period in action, but nonetheless, caution is advised.

IOC (Indicators Of Compromise)

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.

NewsClientPlugin.exe
RuntimeBroker.exe
version.dll
winversion.dll
xlaccount.dll

File Hashes (MD5)

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

03a884859153e2784df4ebaac2d43f2a
0a7b55f69c312b8882fde291ce071e2a
0c8663bf912ef4d69a1473597925feeb
1bd4911ea9eba86f7745f2c1a45bc01b
1cde670ddf77f6f7b7a46553ed6e4aca
2135f9ce5477f3044e0ee522095d094a
25736f8facf2c8951da448033d2f93fd
2ceaf88707af1cb5adf138ee40ca69d9
387b7fee503bf6be4c768c4c897c2e02
46b9ec9af427869467cc3dbffae30086
46c1b81d2cc911a9dd1923b74f434d59
5191cef6303b4c0b4e69e842a24e72f2
5a2a8d1a90f2768d2c90faca7d08c216
5a7a90ceb6e7137c753d8de226fc7947
6102f77c85541d00b4c3bc95f100febc
679863157ff2968151346f85624f00b1
69084f89edded0a8560b803b6db6f8c8
7148c44dc587a0d06c2219ba7678dafd
73695fc3868f541995b3d1cc4dfc1350
76ba5272a17fdab7521ea21a57d23591
7a2656a6b3fc11a2c145fe6be409a8fb
827802b305c1ee0644f844150e7c8dde
8410893f1f88c5d9ab327bc139ff295d
8645ed20381ca90c272d7e0729241aff
8a9fb104a5baa12631607942d8066f19
8d10474edfa235a944c8e5873d96c386
946a99f36a46d335dec080d9a4371940
97791e6752f673e1e70f8499e69ad732
9cedddc5785ae6a1086127bc9f827a86
9cfc6f26dfacdcaa1fb16e9e74fb77d2
a8de1713f3a6e5655959d84280fdc153

ab0e2ca694b07e049b4740ef270ef17b
b1d713a8f8935e3115ff62bf784db5ea
c425df2a5590fad136df54683139f8bc
cc7207f09a6fe41c71626ad4d3f127ce
cd9988a37e32de5241062aeec10f9c08
d45e50d0cc6c1342e40ea254edae091a
d76edec5e00e629bb1fafa599daa0d77
e01b393e8897ed116ba9e0e87a4b1da1
eb8bd1594a656877312dff766fd9f104
ec98666733b32d486857f17f2ff387a7
ef25d934d12684b371a17c76daf3662c
ef25d934d12684b371a17c76daf3662c
f0a5447d5e1138162de144cf15b2746e
f68b68cd999a53a5afef91d0298b63cd
f93d0c0f6c73c13eedbb86950df88d4d
faa8eaed63c4e9f212ef81e2365dd9e8
fafa0d93fcffbca0b5ff2f38086b3da0

Related Domains, URLs, and IP Addresses

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

There is no particular C2 server for this malware, but instead, it attempts to connect to a certain IP range. Ports are either TCP 55556 or UDP 6999.

111.120.0.0 – 111.123.255.255
113.62.0.0 - 113.63.255.255

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 tactics and techniques of the 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)		
Initial Access (TA0001)	Drive-by Compromise (T1189)	
	Trusted Relationship (T1199)	
Execution (TA0002)	Command and Scripting Interpreter: Windows Command Shell (T1059.003)	Cmd.exe to be connected via pipe
Persistence (TA0003)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)	Load a malicious DLL using a normal EXE file
	Hijack Execution Flow: DLL Side-Loading (T1574.002)	

Privilege Escalation (TA0004)		
Defense Evasion (TA0005)	Obfuscated Files or Information (T1027)	
	Obfuscated Files or Information: Software Packing (T1027.002)	
	Modify Registry (T1112)	
	Deobfuscate/Decode Files or Information (T1140)	
Credential Access (TA0006)		
Discovery (TA0007)	File and Directory Discovery (T1083)	
	Process Discovery (T1057)	
	Query Registry (T1012)	
	System Network Configuration Discovery (T1016)	
	System Network Configuration Discovery: Internet Connection Discovery (T1016.001)	
	System Network Connections Discovery	

	(T1049)	
	Process Discovery (T1057)	
	System Information Discovery (T1082)	
	File and Directory Discovery (T1083)	
	Peripheral Device Discovery (T1120)	
	Software Discovery (T1518)	
Lateral Movement (TA0008)		
Collection (TA0009)	Screen Capture (T1113)	Screen capture
Command and Control (TA0011)	Ingress Tool Transfer (T1105)	
	Dynamic Resolution (T1568)	
	Encrypted Channel: Symmetric Cryptography (T1573.001)	
	Encrypted Channel: Asymmetric Cryptography (T1573.002)	

Exfiltration (TA0010)	Exfiltration Over C2 Channel (T1041)	
Impact (TA0040)		

Table 4. MITRE ATT&CK

References

[1] LuoYu - The eavesdropper sneaking in multiple platforms (https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf)
[2] Malware WinDealer used by LuoYu Attack Group (https://blogs.jpcert.or.jp/en/2021/10/windealer.html)
[3] LuoYu: Continuous Espionage Activities Targeting Japan with the new version of WinDealer in 2021 (https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_7_leon-niwa-ishimaru_en.pdf)
[4] WinDealer dealing on the side (https://securelist.com/windealer-dealing-on-the-side/105946)
[5] Threat Thursday: China-Based APT Plays Auto-Updater Card to Deliver WinDealer Malware (https://blogs.blackberry.com/en/2022/06/threat-thursday-china-based-apt-plays-auto-updater-card-to-deliver-windealer-malware)

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
www.ahnlab.com
www.asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency Response Center(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. The 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.

AhnLab