Account Credential-Stealing Malware Detected by AhnLab MDS (Web Browsers, Email, FTP) - ASEC

By ATCP

Published: 2024-01-23 · Archived: 2026-04-05 16:00:33 UTC

For convenience, users frequently use automatic login feature provided by programs like web browsers, email clients, and FTP clients. This allows programs to store user account credentials in their settings data. Therefore, despite being a convenient feature, this poses a security risk because threat actors are then able to leak the users' account credentials easily.

If malware or threat actors gain control of an infected system, they can employ various tools to extract users' account credentials. Additionally, there are specifically designed Infostealers crafted for the sole purpose of extorting account credentials. If the malware is already known, anti-malware software installed on the endpoint can effectively respond to it. However, in order to handle unknown malware, AhnLab Malware Defense System (MDS) is necessary.

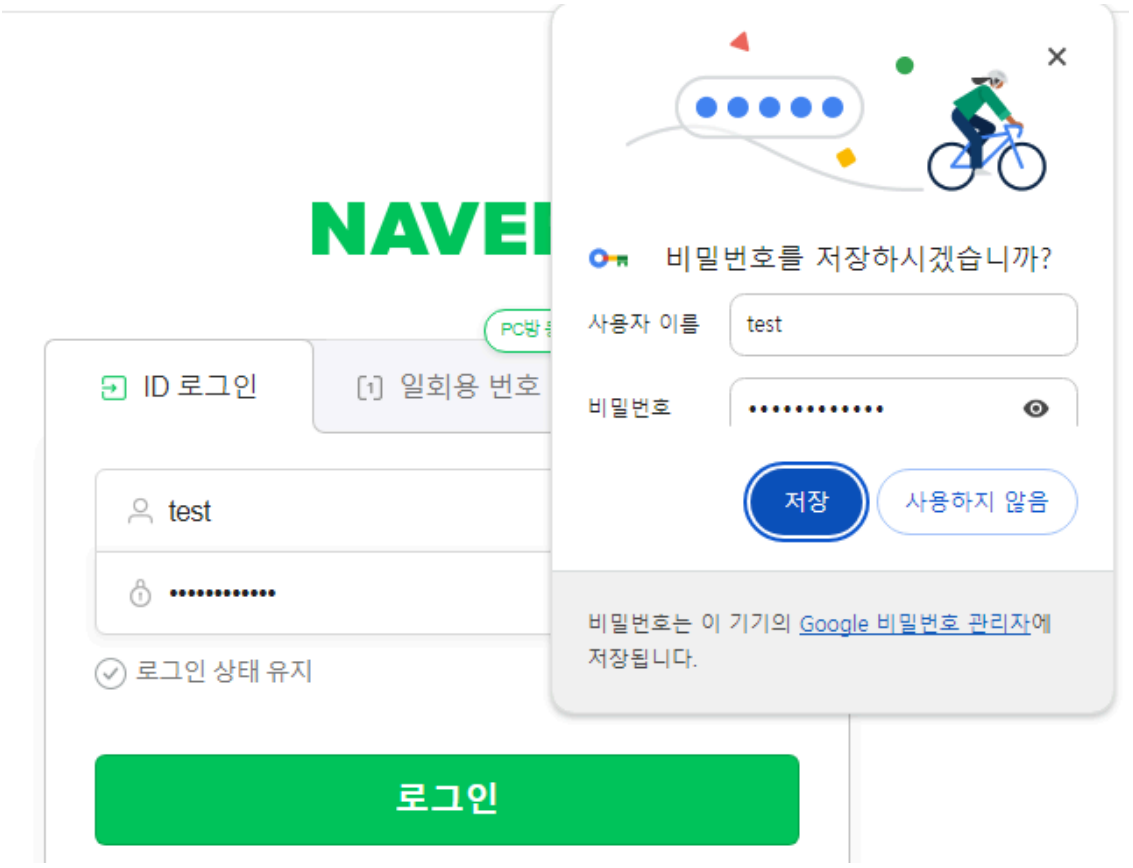
AhnLab MDS is a sandbox-based file analysis solution that executes files in a virtual environment to analyze their behavior. Since even new files exhibit known malicious behaviors, AhnLab MDS can effectively detect them. AhnLab MDS comes equipped with an assortment of analysis engines that are utilized to analyze file behavior or the files themselves, enabling an accurate detection of advanced threats.

1. Overview

Web browsers are one of the most commonly and frequently used programs by PC users. This not only includes personal users but also employees who are performing corporate tasks. Web browsers are utilized for accessing web services, including search functions and email communication. Furthermore, various other tasks such as document work can be done through web browsers if the necessary web interface is provided.

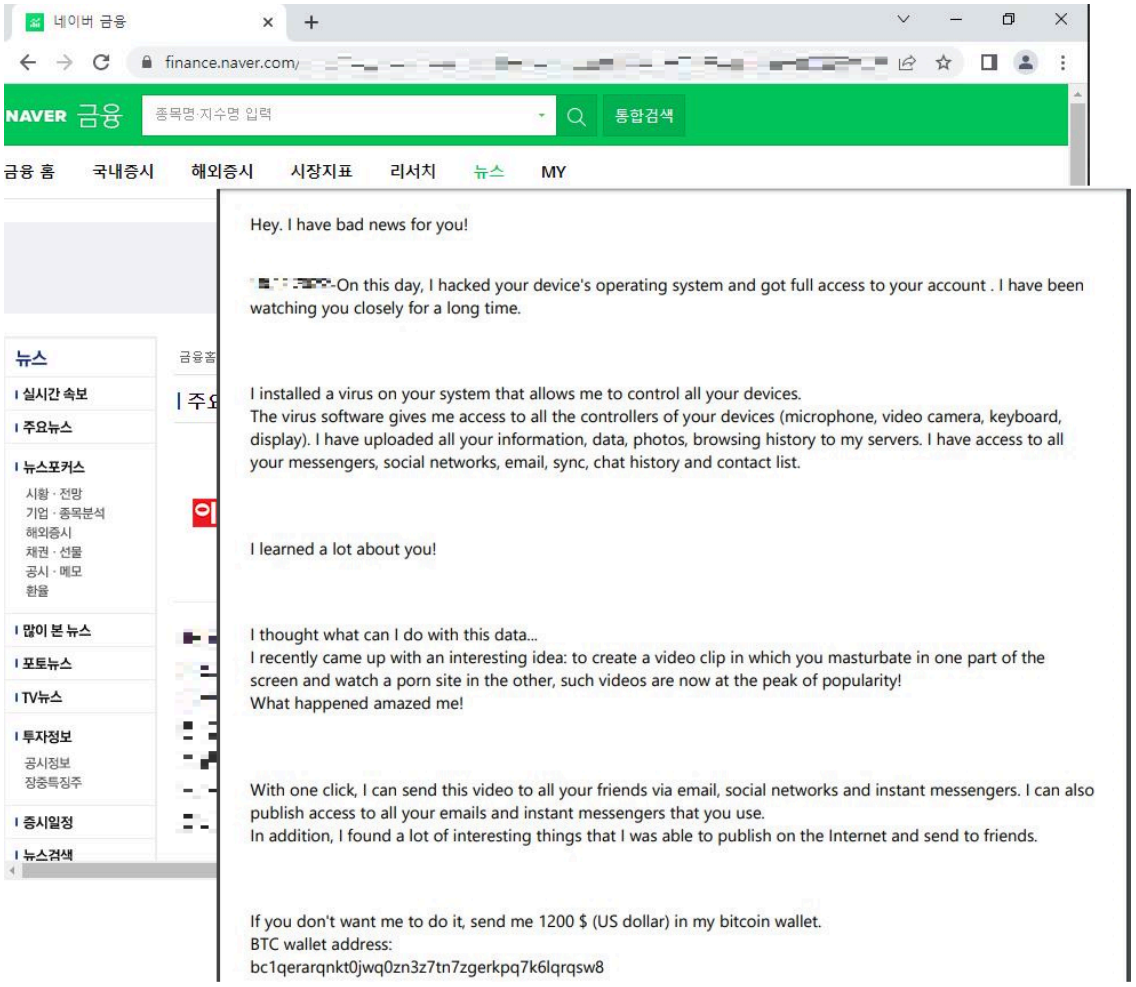
As for emails, although they can be checked through web browsers, employees often prefer to install and use dedicated email clients such as Microsoft Outlook and Mozilla Thunderbird on their PCs. Although cloud services have become more popular for sharing files in recent years, there are still many cases where FTP is used.

The commonality among these programs is that users log in to access services with their own accounts. While users can log in each time they start their computers, most applications, including web browsers, support automatic login. This means that once logged in, the account credentials are stored in each application's settings data, allowing seamless usage without the need for repeated logins.



However, such convenience comes with risks. If a threat actor gains control of a user's system or if malware is installed on the system, this stored account information can be easily stolen. Typically, users only use a few accounts for various services, so even if a small number of logged-in account credentials are stolen, various user information can fall into the hands of the threat actor.

It is worth noting that if an email address is used to log in, the email address itself is also exposed to the threat actor. This threat actor can then leverage this information to send threatening emails. Below is an example of a threatening email sent by a threat actor to an email address collected from a system that was infected with an Infostealer. Along with a captured screenshot and gathered information, the email threatens to produce explicit content using the collected information and send it to acquaintances via email and social media. The email also instructs the recipient to send $1,200 to the threat actor's Bitcoin wallet address if the recipient does not wish for this to happen.



2. Known Malware Cases

Infostealer is a type of information-stealing malware with the goal of stealing user information, such as the account credentials and history saved in applications like web browsers and email clients. Threat actors often employ techniques like packing and obfuscation before distributing their malware to bypass file detection by anti-malware software. However, even if their outer appearances are changed, the behaviors of malware include known malicious activities – these activities can be detected by AhnLab MDS.

Here, we compiled cases of AhnLab MDS being used to detect the information exfiltration behavior of major Infostealers widely used in attacks.

A. AgentTesla

AgentTesla is an Infostealer that is primarily distributed via spam emails. This malware targets and collects information from a variety of applications, including most web browsers, email/FTP clients, and VNC programs. The collected information is then sent to a C&C server through SMTP, FTP, or the Telegram API **[1]**.

Among the various information exfiltration behaviors, this section outlines instances where AhnLab MDS detected the theft of user account credentials stored in web browsers and VNC by the AgentTesla Infostealer.

웹 브라우저 계정정보 접근 행위를 탐지했습니다. 웹 브라우저에 저장된 계정정보를 탈취할 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오.

[파일 정보]
경로: C:₩Users₩TVM₩AppData₩Roaming₩OPERA SOFTWARE₩OPERA STABLE

프로세스가 웹 브라우저의 계정 정보 파일에 접근하는 행위를 탐지했습니다.

[파일 정보]
● Login Data
MD5:
전자 서명: 없음
경로: C:₩Users₩TVM₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩Login Data

웹 브라우저 계정정보 접근 행위를 탐지했습니다. 웹 브라우저에 저장된 계정정보를 탈취할 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오.

[파일 정보]
경로: C:₩Users₩TVM₩AppData₩Roaming₩Mozilla₩Firefox₩PROFILES.INI

Thunderbird 이메일 계정 정보에 접근하는 행위를 탐지했습니다. 이메일에 저장된 계정 정보를 탈취하려는 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오.

[파일 정보]
경로: C:₩Users₩TVM₩AppData₩Roaming₩Thunderbird₩PROFILES.INI

의심스러운 프로세스가 계정 정보가 저장된 파일에 접근하는 행위를 탐지했습니다. 악성코드 실행으로 인한 위협이 존재할 가능성이 높으므로 시스템 전체에 대해 악성코드 검사를 실행하십시오.

[레지스트리 정보]
키: HKCU₩Software₩TigerVNC₩Server

[레지스트리 정보]
키: HKLM₩SOFTWARE₩RealVNC₩vncserver

[레지스트리 정보]
키: HKCU₩Software₩ORL₩WinVNC3

B. Lokibot

Similar to AgentTesla, Lokibot is an Infostealer that targets a wide range of applications to steal account credentials, including web browsers, email/FTP clients, file/password management programs, and terminal emulators [2].

Among the various information exfiltration behaviors, this section outlines instances where AhnLab MDS detected the theft of user account credentials stored in email and FTP clients by the Lokibot Infostealer.

FTP 계정정보 접근 행위를 탐지했습니다. FTP에 저장된 계정정보를 탈취할 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오.

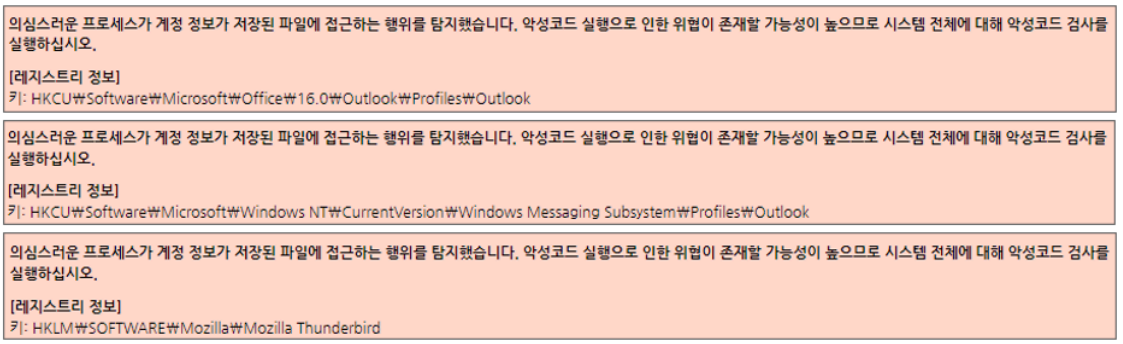
[파일 정보]
● recentservers.xml
MD5:
전자 서명: 없음
경로: C:₩Users₩TVM₩AppData₩Roaming₩FileZilla₩recentservers.xml

의심스러운 프로세스가 계정 정보가 저장된 파일에 접근하는 행위를 탐지했습니다. 악성코드 실행으로 인한 위협이 존재할 가능성이 높으므로 시스템 전체에 대해 악성코드 검사를 실행하십시오.

[레지스트리 정보]
키: HKCU₩Software₩Far2₩Plugins₩FTP₩Hosts

의심스러운 프로세스가 계정 정보가 저장된 파일에 접근하는 행위를 탐지했습니다. 악성코드 실행으로 인한 위협이 존재할 가능성이 높으므로 시스템 전체에 대해 악성코드 검사를 실행하십시오.

[레지스트리 정보]
키: HKCU₩Software₩NCH Software₩ClassicFTP₩FTPAccounts



3. Cases of APT Attacks

Up to this point, we have discussed well-known malware that are distributed indiscriminately to the public. However, stealing user account credentials is a crucial step in the attack process that can provide threat actors with significant advantages. For example, even if the target is an ordinary user, threat actors can leverage stolen credentials to obtain more information later. For corporate users, stolen credentials can be used not only to infect systems but also to move laterally within the organization's internal network and seize control.

Therefore, obtaining credentials is an essential step even for APT attack groups. It is important to note that due to the nature of APT attackers, they often create their own malware instead of using well-known ones. However, even if they create new malware, the behavior of stealing information is often similar to that of known malware.

AhnLab MDS executes and analyzes file behaviors in a virtual environment. Therefore, unlike other anti-malware software, it is able to detect and respond to information theft performed by unknown malware even when the appearance of the file cannot be diagnosed. Here, we cover cases where AhnLab MDS was used to detect various information-stealing malware used by APT groups to acquire user account credentials in the past.

A. Andariel

The Andariel threat group primarily targets South Korean corporations and institutions and is known to collaborate with or operate as a subsidiary organization of the Lazarus threat group. The group was first identified targeting South Korean entities in 2008, with major targets including national defense, political organizations, shipbuilding, energy, telecommunications, and other security-related entities. Additionally, universities, transportation, ICT companies, and various other corporations and agencies located in South Korea have also been targeted.

The Andariel threat group mainly utilizes spear phishing attacks, watering hole attacks, and supply chain attacks during the initial access process. There are also cases where the group exploits centralized management solutions during the malware installation process **[3]**. This post will cover the Infostealer that was installed in the past by the Andariel group using TigerRAT.

TigerRAT is a backdoor, so it does not have extensive features related to information theft. In order to gather additional information, the group used malware similar to other Infostealers to steal user account credentials stored in web browsers and Outlook clients. This malware is capable of stealing user account credentials from Chrome, Firefox, Internet Explorer, Opera, and Naver Whale web browsers, as well as the Outlook client. It then outputs them as command line outputs.

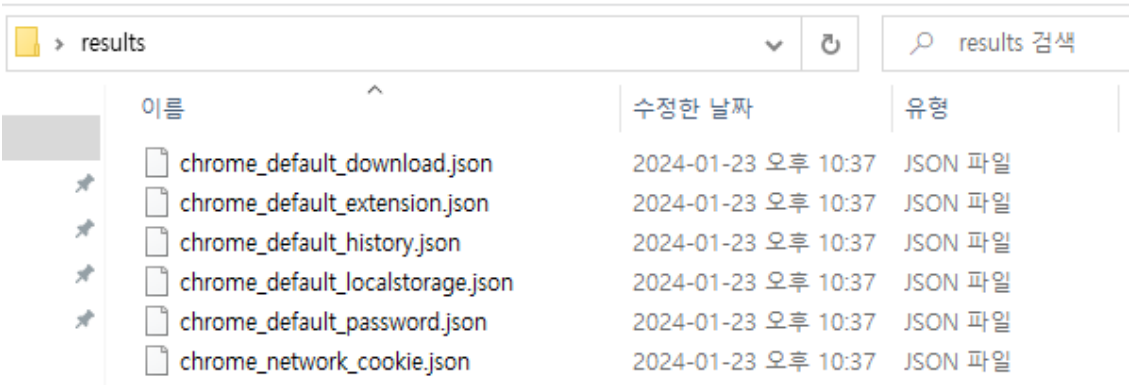
```
--------------------Google Chrome Password--------------------------
--------------------Mozila Firefox Password-----------------------
Mozila Firefox isn't install..
--------------------Internet Explorer Password--------------------
Internet Explorer => uname: justtest    pwd: testpass   site: https://www.ahnlab.com/

--------------------Opera < v60-------------------------------
--------------------Opera < v80-------------------------------
opera isn't install..
--------------------Naver Whale-------------------------------
whale browser isn't install..
--------------------Outlook-----------------------------------------
```

The results presented below shows the outcomes of utilizing AhnLab MDS to identify the activities associated with the theft of user account credentials from web browsers and the Outlook client. This pertains to the Infostealer utilized in the APT attacks orchestrated by the Andariel group. This means that in environments where AhnLab MDS is installed, the information-stealing behavior is detected when the threat actor attempts to additionally install an Infostealer. This allows users to prevent threat actors from seizing control of the organization's network via lateral movement and stealing internal information.

B. Kimsuky

Kimsuky is a threat group known to be supported by North Korea and has been active since 2013. At first, they attacked North Korea-related research institutes in South Korea before attacking a Korean energy corporation in 2014. Since 2017, their attacks have been targeting countries other than South Korea as well. They primarily target national defense, defense industries, media, diplomacy, government agencies, and academic fields via spear phishing attacks with the purpose of stealing internal information and technology **[4]**.

The Kimsuky group employs various malware for remote control, including customized malware like AppleSeed and AlphaSeed, as well as tools like TinyNuke (HVNC) and TightVNC. However, since these malware lack any direct feature for stealing account credentials, they are often supplemented with Infostealer which is responsible for such a feature. The following is an Infostealer that was used in recent attacks to steal various user information, including account credentials, cookies, and browsing history stored in web browsers before creating a json file in the same directory.



AhnLab MDS can also detect when the Infostealer used in the Kimsuky group's APT attacks steals user account credentials stored in web browsers. This allows for the detection and prevention of information theft on infected systems in advance, enabling administrators to be aware of the attack and prevent the next stage of the attack.

4. Conclusion

Threat actors can steal user account credentials through various methods and use the stolen information to laterally move and ultimately take control of an organization's network. Therefore, stealing user credentials is a crucial step in the attack process, and threat actors use both known malware and customized Infostealer for this purpose.

AhnLab MDS is a sandbox-based file analysis solution that executes files in a virtual environment to analyze their behavior. Both already known malware and new ones crafted by threat actors in APT attacks invariably engage in information-stealing behavior during their execution. By detecting these information-stealing behaviors, AhnLab MDS enables administrators to become aware of the attack and preemptively block the threat actor's next move.

Behavior Detection

– Infostealer/MDP.Behavior.M10087
– CredentialAccess/MDP.infostealer.M10258
– CredentialAccess/MDP.infostealer.M10266
– CredentialAccess/MDP.Outlook.M11577

– CredentialAccess/MDP.IExplore.M11582
– Execution/MDP.Lokibot.M10952
– Execution/MDP.AgentTesla.M11002

To learn more about **AhnLab MDS**'s sandbox-based behavioral analysis, please click the banner below.

Source: https://asec.ahnlab.com/en/61082/