TLP: GREEN

Why Hackers Love Automatic Logins

AhnLab Contents Planning Team

2022. 09. 05

AhnLab

Guide on Document Classification

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

Classification	Distribution Targets	Notices
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can be only 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	2022-09-05	Why Hackers Love Automatic Logins

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.

Overview

Infostealers never fail to make the list in discussions regarding recently trending malware. As the word itself implies, Infostealer targets various types of user information. Particularly, if users use the automatic login feature of websites or programs, credentials of many multiple service accounts can be stolen once their computers are infected with Infostealer. The risk is high for ordinary users who usually use multiple services with the same account and password.

In this report, AhnLab will discuss the principles behind Infostealer stealing information from users through automatic login features and share ways to minimize damage.

Why Hackers Love Automatic Logins

Infostealer is a type of malware that steals credentials and various kinds of information saved in the OS or programs. The term usually refers to the type automatically collecting and leaking information when it is executed.

The attack frequency of Infostealer has been continuously on the rise. At the same time, the variations and the types of information they steal are becoming more diversified. Even in ASEC Weekly Malware Statistics that AhnLab posts on ASEC blog every week, Infostealer has been in the top rankings for a significantly long time.

Figure 1. Weekly malware statistics for the 2nd week of August

Infostealer steals user information in various forms. This report will explain the principles behind information leakage when the automatic login feature is used for programs - particularly web browsers.

Basic Concept

When users utilize the 'automatic login' feature of programs, the credentials are normally encrypted into a file or database format to be saved. Some programs do not encrypt but rather encode. In some cases, the credentials may even be saved in plain text. Encryption methods are often easy to crack, so if attackers know the password information save path of the targeted program and the algorithm, they can steal the credentials.

Methods that hackers use to steal information are widely categorized into two types: ▲using password recovery programs and ▲using information stealing features within malware.

Password recovery programs are tools that users can use when they forget their passwords for Windows or web browsers. Attackers use such programs to find out the password. While some use the tools without any modifications, many choose to execute them in the memory area to avoid detection by users.

Information stealing features in malware are relatively well known and are included in the malware to leak Internet banking information or as a backdoor. DarkCrystal, Formbook, and XLoader are major examples of malware that can leak information.

Why Infostealer Is a Threat

The greatest issue with Infostealer is that the attacker can steal all credentials saved in the program. So by analyzing a few of the user's passwords, attackers can guess the passwords for other websites or those that may be used in the future. Simply put, it has the potential to cause secondary damage.

Also, attackers do not simply stop at stealing information such as login information and credit card numbers; they can use the collected information to infiltrate organizations. The information collected with Infostealer is often uploaded or sold on the dark web. Attackers download or purchase credentials for certain corporations or organizations to use in their attacks.

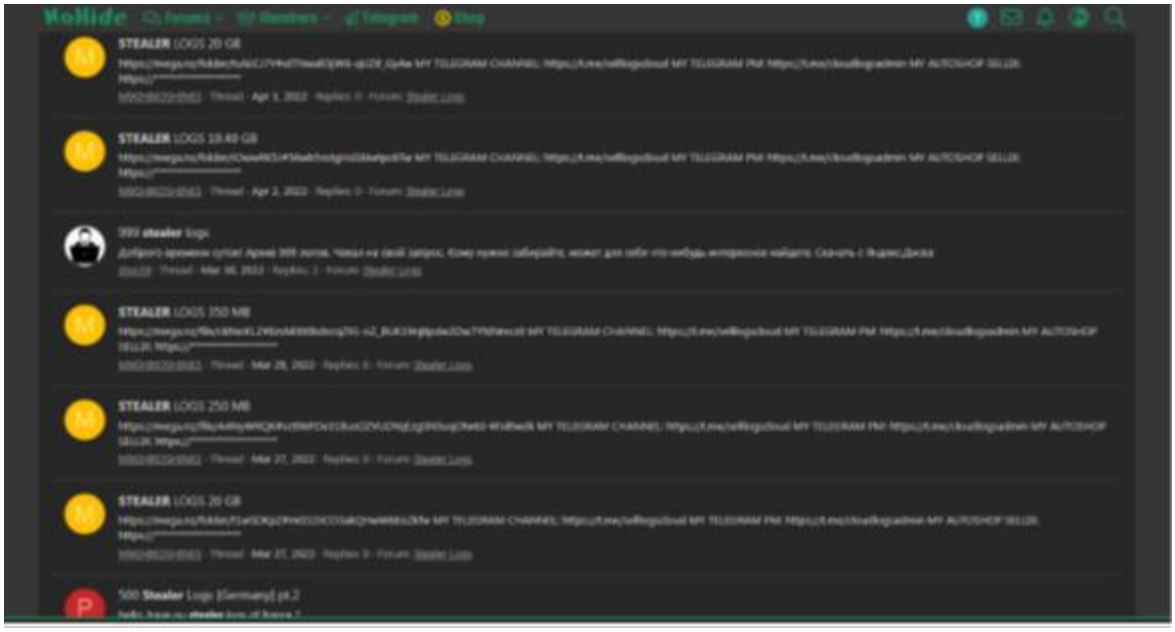

Figure 2. Credentials uploaded on the dark web

Besides cybercrime organizations, threat groups that are thought to be supported by certain governments that have recently been actively using Infostealer. A major example is the discovery of Infostealer from Andariel group in October 2020, a group suspected to be supported by North Korea. This malware steals the login credentials saved in web browsers such as Chrome, Firefox, and Internet Explorer.

Until now, the information targeted by attackers had been system information or login credentials of various programs. However, it was found recently that the range of targets has been expanding to include cryptocurrency wallets and games. At the same time, there is an increasing number of malware strains that exclude Internet Explorer from the target list as the number of its users has seen a steep decline since 2018. This indicates that the attackers are evolving their attack methods in line with the changing trend for maximum gains.

Infostealer, much like other malware types, infects user computers through users opening email attachments, visiting websites, and downloading programs. Attackers often include malware in cracks, keygens, KMS (Key Management Service), etc. Particularly, KMS certification programs are used both by individual users and large corporations, so malware developers use them frequently to distribute malware.

Moreover, as more people are working remotely during the pandemic, there has been an increasing number of cases of using personal or shared family computers for work. There were cases of Infostealer infection as users downloaded cracks to use programs without a

license to do their tasks. Though rare, there have been cases of attacks against supply networks as well.

How Information is Stolen With Automatic Login

In the introduction of this report, it was mentioned that it becomes easier to steal information with Infostealer when users use the automatic login feature of programs and web browsers. What is the reason behind this? Out of the various relevant cases, let us examine how information saved in web browsers and programs highly accessed by users can be stolen.

1) Chromium based browsers

Chromium is an open source web browser developed and managed by Google and the most commonly used web browser engine. Major examples include Chrome, Edge, and Opera, which were all developed based on the Chromium code.

Chromium based web browsers store account (ID and password) information, cookie data, credit and debit card information, history, and autofill information that users save while surfing the web in an SQLite DB file in the local system.

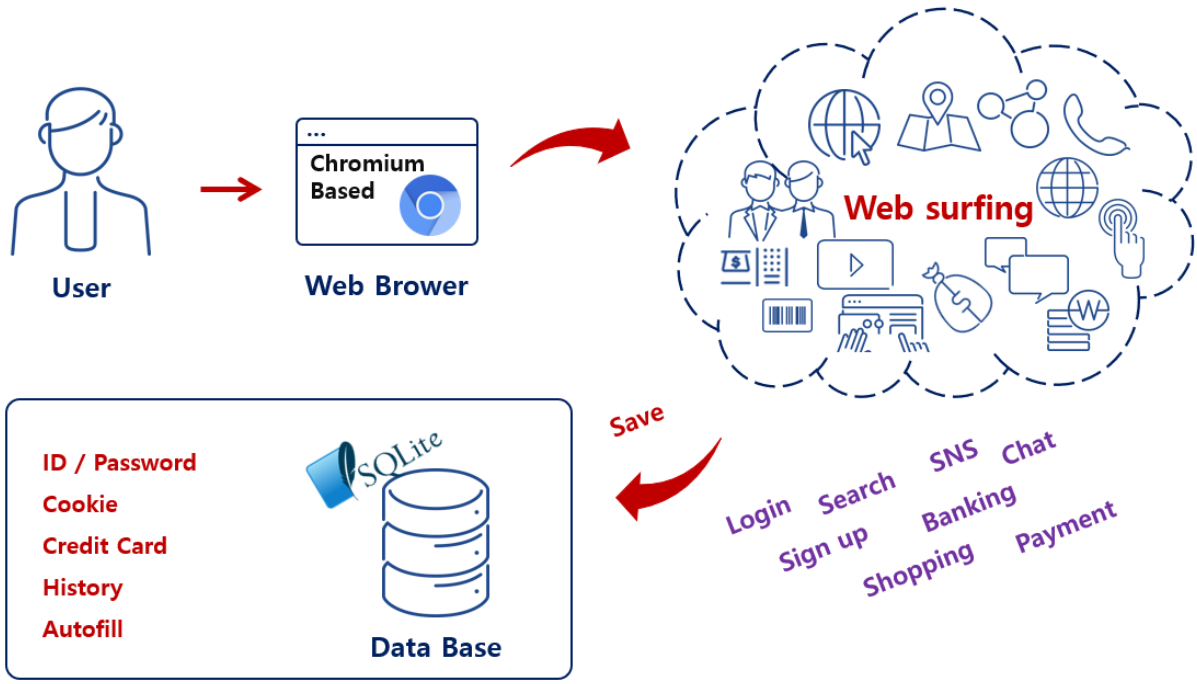

Figure 3. Information saved in browsers

Some sensitive data within the SQLite DB file are kept encrypted using AES (Advanced Encryption Standard). Chromium's encrypted data management only allows users of the local system to decrypt this information. The AES key is stored as a DPAPI blob encrypted by DataProtection API. This data is Base64-encoded and saved in (omitted)...₩User Data₩Local State JSON file's "os_crypt" : {"encrypted_key"}.

Infostealer extracts the data it needs through an SQL query to the target DB file that holds information on the account, cookies, cards, history, and autofill. Then, it decrypts the AES key to collect the plain text version of the encrypted text.

Category	Path	Table	Encryption
ID/PW	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩Login Data	logins	O
Cookies	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩Network₩Cookies	cookies	O
Card	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩Web Data	credit_cards	O
History	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩History	urls	X
Autofill	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩Web Data	autofil	X

Table 1. Major data files saved in Chromium

Category	Target	SQL Query
ID/PW	Login Data	SELECT origin_url, username_value, password_value FROM logins
Cookies	Network₩Cookies	SELECT host_key, name, Path, expires_utc, is_secure, value, encrypted_value FROM cookies
Card	Web Data	SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM

		credit_cards
History	History	SELECT url, title, visit_count, last_visit_time FROM urls
Autofill	Web Data	SELECT name, value FROM autofill

Table 2. SQL queries to collect information from Chromium

Also, passwords and all encrypted field values can be decrypted into plain text through the same method. Information that can be decrypted includes ▲encrypted_value of the Cookies table, ▲Credit_Card table's card_number_encrypted field, etc.

2) Gecko based browsers

Gecko is an open source web browser engine developed and managed by the Mozilla foundation. The web browsers that use this engine include Firefox, Thunderbird, IceDragon, and Cyberfox. This is the second most used web browser engine after Chromium.

The account credentials saved in Gecko browsers are stored in the logins.json file after being encrypted. The encryption data management of Gecko browsers uses the NSS library's PK11SDR_Encrypt/PK11SDR_Decrypt function developed by Mozilla. To put the internal processes of this function in simple terms, the Master Key and Salt values of the key4.db file are extracted to be encrypted and decrypted by 3DES-CBC.

Infostealer dynamically loads the PK11SDR_Decrypt function of nss3.dll that Gecko based browsers use. It can then decrypt the encrypted account credentials extracted from logins.json into plain text.

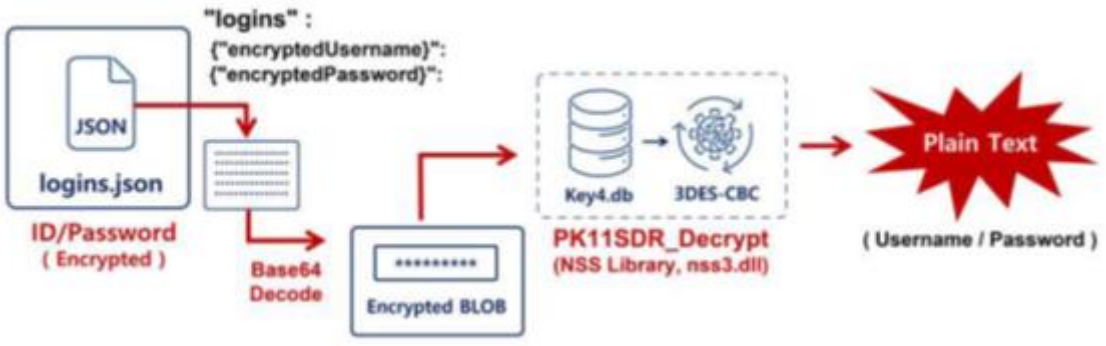

Figure 4. Decryption process for Gecko-based browsers

Tables 3 and 4 show the information about Gecko based browser related major files and browser data collection SQL queries.

Category	Path	Encryption
ID/PW	%AppData%Mozilla₩Firefox₩Profiles₩[Random Value]₩logins.json JSON	O
Cookies	%AppData%Mozilla₩Firefox₩Profiles₩[Random Value]₩cookies.sqlite	X
History	%AppData%Mozilla₩Firefox₩Profiles₩[Random Value]₩places.sqlite	X

Table 3. Gecko based major file information

Category	Target	SQL Query
Cookies	cookies.sqlite	SELECT host, name, path, value, creationTime, expiry, isSecure FROM moz_cookies
History	places.sqlite	SELECT url, title, visit_count, last_visit_date FROM moz_places

Table 4. SQL queries to collect information from Gecko

Gecko browsers' cookie information is stored in cookies.sqlite and the history in places.sqlite. Aside from the account credentials, other pieces of information are not encrypted but stored in plain text, meaning attackers can easily obtain them.

A Real Threat: Infostealer Targets Automatic Login

When a user uses the automatic login feature of web browsers or programs, it becomes easy for Infostealer to steal information. Moreover, breach incidents caused by such attacks occur in Korea as well, so users must be cautious.

While investigating a breach incident for a company's internal network in December 2021,

AhnLab's ASEC analysis team noticed that the VPN account used to access the company network was leaked from a personal PC used by an employee working from home. The company where the incident occurred was providing VPN service for its employees to access the company network. Employees were connected to the network through the VPN connection by the laptop provided by the company or from their own PCs.

The employee who was attacked saved the account credentials of the VPN website in the web browser using its password save feature. The computer was infected with malware targeting account credentials, resulting in various account credentials of websites being leaked. These included the company's VPN account. The leaked account was used in a hacking incident targeting the company's internal network about three months later.

The infected PC had been used by all members of the employee's family and managed inadequately. As a result, it was infected with various malware strains. While a different company's anti-malware software was installed, it was not working properly.

In fact, the infected computer included a Redline Stealer-type malware. Redline Stealer, which first appeared on the Russian dark web in March 2020, collects account credentials saved in web browsers. The malware was distributed online by being disguised as a crack program for SoundShifter, a program for adjusting sound pitch. The user searched and downloaded the file after typing the software name with keywords such as 'crack' and 'free,' eventually infecting the PC by running the downloaded file.

Prevention Is the Best Security

As previously seen, Infostealer can easily steal account credentials when the automatic login feature is used. Breach incidents related to the feature exists as well. So how can one minimize the risk of information theft?

When we catch a cold, we use various methods to cure the illness and minimize discomfort. We visit a hospital for a checkup and get prescribed fever medicine or antibiotics, or might seek self-treatment at home by drinking hot tea and getting rest. In most cases, such measures allow us to overcome the illness. However, fundamentally the best method is to stay healthy and not catch a cold in the first place. To do so, we adhere to basic hygiene principles such as frequently washing our hands and keeping the body hydrated. For the same reason, we keep our masks on while the COVID-19 pandemic rages.

Cybersecurity, especially the damage caused by information leakage covered in this report, can be understood in the same way as the example of described above. It is important to control damage after the information has been stolen with follow-up measures, but the best strategy is to keep to basic security principles to prevent information theft in the first place. First, it is best not to save account credentials when using websites or programs. Of course, it is a convenient feature. Yet as shown in this report, the stored information can be easily leaked once the computer is infected with malware; therefore users should refrain from using the feature.

One should also avoid the following behaviors, as emphasized by AhnLab and other institutions: ▲Downloading and using illegal software ▲Accessing websites that cannot be trusted ▲Executing suspicious email attachments. Users must also always check if their security software such as anti-malware and programs, are up to date.

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