COVID Omicron Variant Lure Used to Distribute RedLine Stealer

fortinet.com/blog/threat-research/omicron-variant-lure-used-to-distribute-redline-stealer

January 10, 2022

Just like the previous year, 2021 ended with COVID and 2022 started with the same. The only difference is that the world is now dealing with the new Omicron variant rather than the Delta variant, which emerged in April 2021. While reportedly less lethal than its predecessor, the Omicron variant has a much higher transmission rate, and as a result, daily counts of new Omicron patients have become a global concern. This has renewed heightened concern about the pandemic, and as we have all sadly learned, threat actors don't shy away from using misery and fear to their advantage.

FortiGuard Labs recently came across a curiously named file, "Omicron Stats.exe", which turned out to be a variant of Redline Stealer malware. This blog will look at the Redline Stealer malware, including what's new in this variant, its core functions, how it communicates with its C2 server, and how organizations can protect themselves.

Affected Platforms: Windows
Impacted Users: Windows users
Impact: Various data including confidential information on the compromised machine will be stolen
Severity Level: Medium

RedLine Stealer

Before talking specifics on this new RedLine Stealer variant, let's review what we know about RedLine Stealer in general.

The first reports of RedLine Stealer go back to at least March of 2020 and it quickly became one of the more popular infostealers sold in underground digital markets. The Information harvested by RedLine Stealer is sold on the dark net marketplace for as low as 10 US dollars per set of user credentials. The malware emerged just as the world began to deal with increased numbers of COVID patients and the growing fear and uncertainty that can cause people to lower their guard, which may have prompted its developers to use COVID as its lure.

According to the CIA, open source intelligence, or OSINT, is intelligence "drawn from publicly available material," although it can include sources only available to specialists or subscribers. Based on the global OSINT information collected and analyzed by FortiGuard Labs, the current Redline Stealer includes the following functionalities.

Normally, these are the victims whose systems have been infected with any of the above-mentioned stealers, due to which victim have unknowingly had their account passwords and full browser details recorded, and then sent to marketplace operators. Generally, in such cases, each user profile includes login credentials for accounts on online payment portals, e-banking services, file-sharing or social networking platforms. As such, it attempts to collect the following information from browsers installed on the compromised machine, including all Chromium-based browsers and all browsers based on Gecko (i.e. Mozilla):

1. Stored system information:
    1. Login and passwords
    2. Cookies
    3. Auto-Fill Forms
    4. Browser User Agent Details
    5. Credit Card information
    6. Browser history
2. Installed FTP clients
3. Installed IM clients
4. It also engages in highly configurable information collection based on file path and file extension, including searching in subfolders.
5. It sets up a blacklist of countries where Redline Stealer will not function

6. It also collects the following machine information
    1. IP
    2. Country
    3. City
    4. Current user name
    5. Hardware ID
    6. Keyboard layouts
    7. Screenshot
    8. Screen resolution
    9. Operating system
    10. UAC settings
    11. User-Agent
    12. Information about PC components such as video cards and processors
    13. Installed antivirus solution
    14. Data/Files from common folders such as desktop/downloads, etc.

The current variant continues to perform all these functions. However, this new version includes additional changes and improvements, which are detailed below:

Infection vector for the RedLine Stealer variant (Omicron Stats.exe)

While we have not been able to identify the infection vector for this particular variant, we believe that it is being distributed via email. Past RedLine Stealer variants are known to have been distributed in COVID-themed emails to lure victims. The file name of this current variant, “Omicron Stats.exe,” was used just as the Omicron variant was becoming a global concern, following the pattern of previous variants. And given that this malware is embedded in a document designed to be opened by a victim, we have concluded that email is the infection vector for this variant as well.

Victimology

Based on the information collected by FortiGuard Labs, potential victims of this RedLine Stealer variant are spread across 12 countries. This indicates that this is a broad-brush attack and that the threat actors did not target specific organizations or individuals.

Functionality

Once Omicron Stats.exe is executed, it unpacks resources encrypted with triple DES using ciphermode ECB and padding mode PKCS7. Unpacked resources are then injected into vbc.exe. It copies itself to C:\Users\[Username]\AppData\Roaming\chromedrlvers.exe and creates the following scheduled task for persistence:

```
schtasks /create /sc minute /mo 1 /tn "Nania" /tr
"'C:\Users\[Username]\AppData\Roaming\chromedrlvers.exe'" /f
```

The malware then attempts to exfiltrate the following system information from Windows Management Instrumentation (WMI):

- Graphics card name
- BIOS manufacturer, identification code, serial number, release date and version
- Disk drive manufacturer, model, total heads and signature
- Processor (CPU) information like unique ID, processor ID, manufacturer, name, max clock speed and motherboard information

The malware also decrypts strings with base64 and xor key "Margented." The decrypted strings are "freelancer.com" and 207[.]32.217.89. It then accesses a Command and Control (C2) server (207[.]32[.]217[.]89:14588). It uses a unique header ,"Authorization: ns1=d8cc092a9e22f3fc55d63aad32150529" to verify itself, and the decrypted ID “freelancer.com” to prevent connections from other malware or researchers.

Figure 1. Configuration file of the RedLine Stealer variant

The malware searches for the following strings on the compromised machine to locate relevant folders for data exfiltration:

- wallet.dat (information related to cryptocurrency)
- wallet (information related to cryptocurrency)
- Login Data
- Web Data
- Cookies
- Opera GX Stable
- Opera GX

Figure 2. Code to search cryptocurrency wallets on the compromised machine

The malware also looks for the following files for data exfiltration:

- \Telegram Desktop\tdata folder, which Telegram stores images and conversations.
- %appdata%\discord\Local Storage\leveldb, which stores Discord channel and channel-specific information that a user has joined, for the following files:
    - .log and .db files
    - Files that match the following regular expression: [A-Za-z\d]{24}\.[\w-]{6}\.[\w-]{27}

[A-Z] is a regular expression used to search for files with names using any upper case alphabet from A-Z
[a-z] is a regular expression used to search for files with names using any lower case alphabets from a-z
\d is a regular expression used to search for any digits

{24} is a regular expression used to match the previous tokens exactly 24 times
\. Is a regular expression used to find “.” (\ is an escape)
\w is a regular expression used to find any word characters that include underscore

Tokens.txt (used for Discord access)

Figure 3. Code to search log files under %appdata%\discord\Local Storage\leveldb on the compromised machine

The malware also looks for and attempts to steal the following stored browser data:

- Login Data
- Web Data
- Browser User Agent Details
- Cookies
- Extension Cookies
- Autofill
- Credit Card information

The malware also attempts to collect the following system information:

- Processors
- Graphics cards
- Total of RAM
- Installed programs
- Running processes
- Installed languages
- Username
- Installed Windows version
- Serial number

The RedLine Stealer variants steals stored credentials for the following VPN applications:

- NordVPN
- OpenVPN
- ProtonVPN

C2 Infrastructure

This variant uses 207[.]32.217.89 as its C2 server through port 14588. This IP is owned by 1gservers. Over the course of the few weeks after this variant was released, we noticed one IP address in particular communicating with this C2 server. Some telemetry data is shown below.

IP Address	Start Time	End Time

149.154.167.91	2021-11-26 04:34:54	2021-11-26 10:05:15
149.154.167.91	2021-12-05 12:06:03	2021-12-05 13:19:35
149.154.167.91	2021-12-09 16:18:46	2021-12-09 20:00:13
149.154.167.91	2021-12-22 18:38:18	2021-12-23 11:33:58

This 149[.]154.167.91 IP address is located in Great Britain and is part of the Telegram Messenger Network. It seems that the C2 server may be controlled by the Redline operators through an abused Telegram messaging service. This conclusion is not a huge leap as the malware author(s) offer both dedicated purchasing and support lines through their respective Telegram groups.

Conclusion

RedLine Stealer takes advantage of the ongoing COVID crisis and is expected to continue that trend. While it is not designed to have a catastrophic effect on the compromised machine, the information that it steals can be used for malicious actions by the same cybercriminal or sold to another threat actor for future activities. Stay outside of the red zone by exercising basic security practices, detailed below:

Fortinet Protections

FortiGuard Labs provides the following AV coverage against the RedLine Stealer variant:

PossibleThreat.PALLASNET.H

FortiGuard Labs provides the IPS signature “RedLine.Stealer.Botnet” to detect RedLine Stealer’s communication with Command and Control (C2) servers. Please note that the signature is set to “pass” by default and needs to be toggled to “drop” to block communications with its C2.

All network IOCs are blocked by the WebFiltering client.

FortiEDR blocks all malicious files based on reputation and behavioral detection.

Indicators of Compromise (IOCs) for this variant:

SHA2
15FE4385A2289AAF208F080ABB7277332EF8E71EDC68902709AB917945A36740

Network
207.32.217.89:14588 (C2)

Other RedLine Stealer variant IOCs:

SHA2

891aba61b8fec4005f25d405ddfec4d445213c77fce1e967ba07f13bcbe0dad5

216a733c391337fa303907a15fa55f01c9aeb128365fb6d6d245f7c7ec774100

73942b1b5a8146090a40fe50a67c7c86c739329506db9ff5adc638ed7bb1654e

2af009cdf12e1f84f161a2d4f2b4f97155eb6ec6230265604edbc8b21afb5f1a

bf31d8b83e50a7af3e2dc746c74b85d64ce28d7c33b95c09cd46b9caa4d53cad

b8ebdc5b1e33b9382433151f62464d3860cf8c8950d2f1a0278ef77679a04d3b

8d7883edc608a3806bc4ca58637e0d06a83f784da4e1804e9c5f24676a532a7e

1b4fcd8497e6003009010a19abaa8981366922be96e93a84e30ca2885476ccd7

fdeadd54dd29fe51b251242795c83c4defcdade23fdb4b589c05939ae42d6900

af4bf44056fc0b8c538e1e677ed1453d1dd884e78e1d66d1d2b83abb79ff1161

Network:

hxxps://privatlab[.]com/s/s/nRqOogoYkXT3anz2kbrO/2f6ceecb-a469-40b5-94a2-2c9cc0bc8445-Ewdy5l6RAylbLsgDgrgjNjVbn

hxxps://privatlab[.]com/s/s/3Qa0YRMaVaij07Z8BqzZ/7ca69d4c-c5bb-4ab3-b5a9-87c17b7167b5-86yYgEGqbQMnoszgm0OmgGb6g

hxxp://data-host-coin-8[.]com/files/9476_1641477642_2883[.]exe

hxxp://data-host-coin-8[.]com/files/541_1641407973_7515[.]exe

hxxp://data-host-coin-8[.]com/files/7871_1641415744_5762[.]exe

hxxps://transfer[.]sh/get/HafwDG/rednovi[.]exe

hxxp://91[.]219.63.60/downloads/slot8[.]exe

91.243.32.13:1112 (C2)

185.112.83.21:21142 (C2)

23.88.11.67:54321 (C2)

178.20.44.131:8842 (C2)

91.243.32.94:63073 (C2)

95.143.177.66:9006 (C2)

45.147.230.234:1319 (C2)

31.42.191.60:62868 (C2)

135.181.177.210:16326 (C2)

FortiGuard Labs provide the following AV coverage against the RedLine Stealer variants listed above:

W32/Agent.A7D6!tr

MSIL/Agent.DFY!tr

W32/PossibleThreat

PossibleThreat.PALLASNET.H

W32/GenKryptik.FNMI!tr

W32/AgentTesla.FDFF!tr

All network IOCs are blocked by the WebFiltering client.

FortiEDR blocks all of the files based on reputation and as well behavioral detection.

Additionally, FortiGuard Labs also provides the following AV coverage against RedLine Stealer malware in general:

MSIL/Redline.5418!tr

W32/Redline.HV!tr

W32/Redline.HU!tr

W32/Redline.HP!tr

W32/Redline.HL!tr

W32/Redline.HT!tr

W32/Redline.AOR!tr

W32/Redline.HQ!tr

W32/Redline.HS!tr

W32/Redline.HM!tr

W32/Redline.HX!tr

W32/Redline.HR!tr

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.