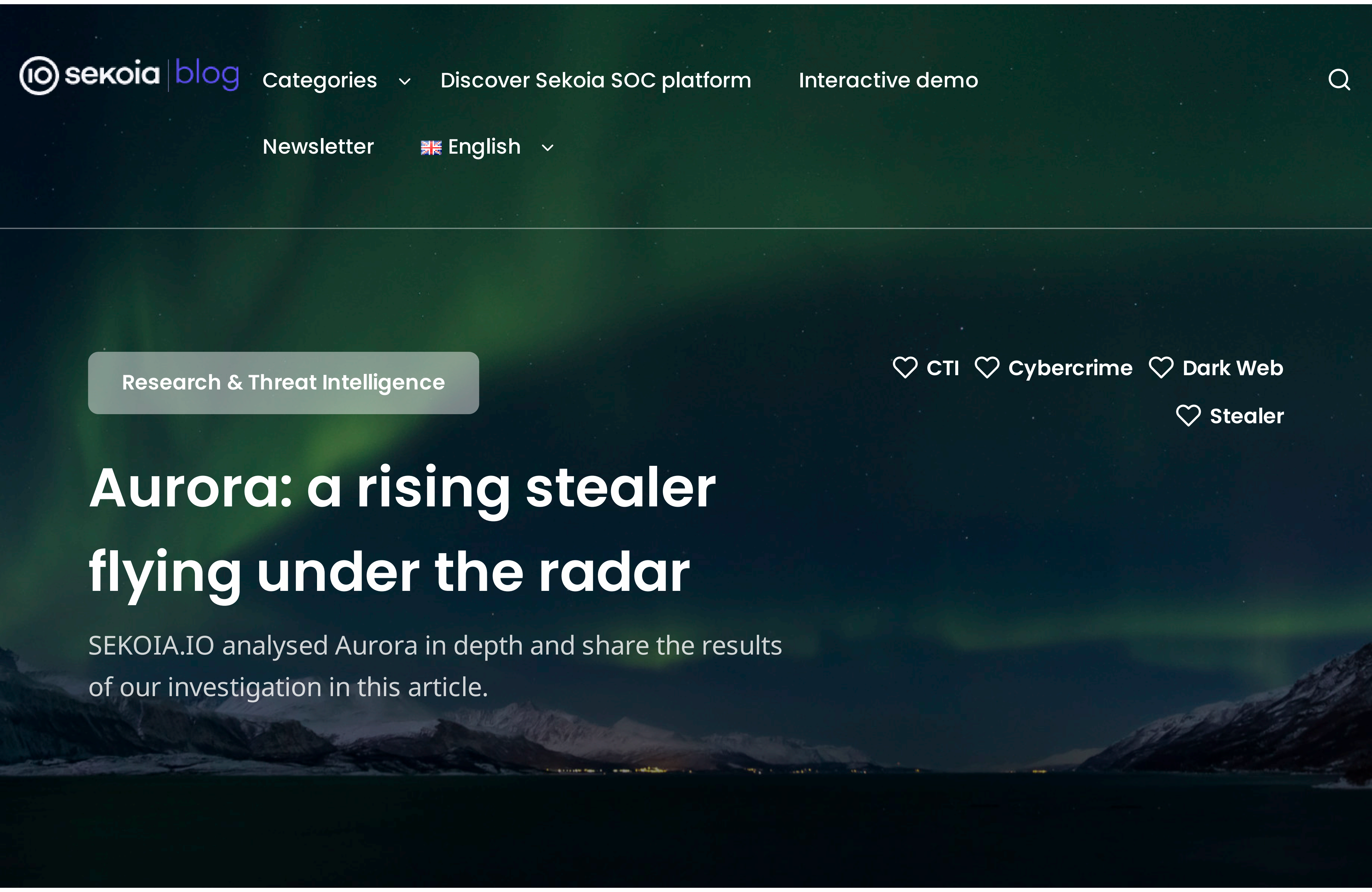

Research & Threat Intelligence

CTI Cybercrime Dark Web Stealer

Aurora: a rising stealer flying under the radar

SEKOIA.IO analysed Aurora in depth and share the results of our investigation in this article.

Quentin Bourgue, Pierre Le Bourhis and Sekoia TDR
November 21 2022

Read it later 12 minutes reading

Table of contents

Summary

In July 2022, Sekoia.io discovered a new Golang botnet advertised by its alleged developer as Aurora botnet since April 2022. Since we published an analysis of the malware and the profile of the threat actor advertising Aurora on underground forums for our clients, the botnet's activity slowed down.

Since September 2022, Aurora malware is advertised as an infostealer and several traffers teams announced they added it to their malware toolset. Furthermore, Sekoia.io observed an increase in the number of Aurora samples distributed in the wild, as well as C2 servers.

As the Aurora malware is widespread, not well detected, or publicly documented either, Sekoia.io analysed Aurora in depth and share the results of our investigation in this article.

Context

The evolution from botnet to stealer

First advertised on Russian-speaking underground forums in April 2022, Aurora is a multi-purpose botnet with stealing, downloading and remote access capabilities. The botnet was sold as a Malware-as-a-Service (MaaS) by a threat actor going by the handle *Cheshire*.

In July 2022, we identified around 50 samples, the majority of which belonging to the "Cheshire" and "Zelizzard" botnets, and less than a dozen C2 servers associated with Aurora botnets. In late July, the Aurora servers were no longer active, and no more recent Aurora samples were submitted on an online public repository. At the time, Sekoia.io assessed that
ear at standstill.

r stopped publishing about Aurora botnet on Dark Web
at the beginning of June 2022. Another publication on
d that *Cheshire* developers shifted to developing
e observations, we assess it is possible that the Aurora
andoned.

In late August 2022, Aurora was advertised as a stealer instead of a botnet on Telegram and underground forums.

Figure 1. Advertisement for Aurora stealer on XSS forum (English version), published by KO7MO on September 8, 2022

A popular stealer in the traffers landscape

Based on the Dark Web cybercrime forums, Sekoia.io identified 9 traffers teams that announced they added Aurora in their infostealer arsenal. Most of them created their team after the advertisement of Aurora as a stealer, and are still very active.

Traffers Team	Malware arsenal	Launch date	Last observed activity
SpaceTeam	Aurora	18/11/2022	25/11/2022
BrazzzersLogs	Aurora, Raccoon	14/11/2022	14/11/2022
DevilsTraff	Aurora, Raccoon	30/10/2022	14/11/2022
BartLogs	Aurora	25/10/2022	25/10/2022
RavenLogs	Aurora, Redline	17/10/2022	24/11/2022
Gfbg6	Aurora	14/09/2022	24/10/2022
SAKURA	Aurora	10/08/2022	04/11/2022
HellRide	Aurora	09/07/2022	21/11/2022
YungRussia	Aurora	05/04/2022	31/10/2022

Table 1. List of monitored traffers teams that announced distributing Aurora stealer, as of November 25, 2022 (updated)

At the time of writing, BrazzzersLogs Team is the most recently created traffers team that publicly announced their use of Aurora stealer on the Lolz Guru cybercrime forums. Based on the illustration promoting their team, the threat group rates Raccoon stealer and Aurora equally

Figure 2. Advertisement aiming at recruiting traffers in BrazzzersLogs Team and rating Raccoon and Aurora stealer (Source: Lolz Guru forum)

The adoption of Aurora stealer by several traffers teams suggests that the malware gained in popularity among threat actors.

In October and November 2022, several hundreds of collected samples and dozens of active C2 servers contributed to confirm Sekoia.io previous assessment that Aurora stealer would become a prevalent infostealer. Additionally, Sekoia.io observed multiple chains of infection leading to the execution of Aurora stealer. These infection chains leveraged phishing pages impersonating download pages of legitimate software, including cryptocurrency wallets or remote access tools, and the 911 method making use of YouTube videos and SEO-poised fake cracked software download websites. Analysis of two infection chains is provided in

ess that several threat actors distribute Aurora Stealer,

s.

sis

As previously introduced, Aurora is a Golang information stealer. Following is an overview of the Aurora stealer capabilities: data collection, exfiltration to its C2 server and load of the next-stage payload.

Data collection

Fingerprint

Aurora mainly uses the lxn/win library to interact with the Windows API, this library relies on Windows Management Instrumentation Command (WMIC).

To fingerprint the host, Aurora executes three commands on the infected host:

- `wmic os get Caption`
- `wmic path win32_VideoController get name`
- `wmic cpu get name`

Figure 3. Aurora commands executed on the infected host in Sekoia.io XDR

Like previously analysed stealers, Aurora also takes one screenshot of the infected host.

Data from browsers, extensions and applications

To collect information, Aurora targets multiple web browsers, as well as browser extensions including those managing cryptocurrency wallets and applications such as Telegram.

Targeted extensions are listed in the sample, applications, web browsers are written in the sample (see Annex 2). The malware uses the function walk of the built-in module path to loop over files and directories until it matches a filename or directory name of one of the targeted applications or extensions.

the stealer gathers a list of directories to search for files

Figure 4. Disassembly code of grabber functionality

Command and Control communications

Canal, format and structure

The malware communicates using TCP connection on ports 8081 and 9865 – 8081 being the most widespread open port. Exfiltrated data are in JSON format.

All messages abide by the same structure, each keys are described below:

- Browser: name of the browser where data was collected (ex: Mozilla, Chromium, *etc.*);
- Cache: content of the stolen file encoded in base64;
- FileName: name of the stolen file (*e.g.* cookies.sqlite, Login Data);
- GRB: likely the grabber configuration. Of note, Sekoia.io only observed the value "null";
- Info: host fingerprint information, including:
  - Name: a random name defined by threat actor;
  - BuildID: name of the build, the value often matches a threat actor's Telegram account;
  - OS: Windows version;
  - HWID: hardware ID;
  - GPU: graphical card information;
  - CPU: CPU name and vendor;
  - RAM: amount of memory;
  - Location: execution path of Aurora sample;
  - Screen: size of the screen of the infected host;
  - IP: expecting the IP address of the infected host but the value is always an empty string.
- MasterKey: encryption key used to read the data of the stolen file, for instance some browsers store the saved password encrypted;

Browser-Mozilla, Screenshot, *etc.*).

data exfiltrated to the C2 Aurora Server:

Figure 5. Exfiltrated fingerprint data of infected host

Exfiltrated data

The logic of Aurora in terms of network communication is straightforward, if a file name matches the stealer logic, the file is encoded in base64 and sent to the C2, following the message structure detailed in the previous section.

Figure 6: Summary of network communication with the C2 of a host infected by Aurora

The analysed stealer always exfiltrated the screenshot first, and then the stolen files.

Next-stage loading

Aurora's promoter claims the stealer has a file grabber and a loader capabilities. During the investigation, only the loader capabilities were observed (see Annex 1).

Aurora loader is straightforward, it downloads a remote payload using *net_http_Get* from the built-in library net/http, then the file is written on the disk in the temporary directory with a random name. The stealer executes the next stage using the following PowerShell command:

```
powershell.exe start-process
"C:\Users\Admin\AppData\Local\Temp\oH7P8GCPXQ.exe"
```

embly code of the loader functionality

Conclusion

Aurora is another **infostealer targeting data from browsers, cryptocurrency wallets, local systems, and acting as a loader**. Sold at a high price on market places, **collected data** is of particular interest to cybercriminals, allowing them to **carry out follow-up lucrative campaigns**, including **Big Game Hunting operations**.

As multiple threat actors, including traffers teams, **added the malware to their arsenal**, Aurora Stealer is becoming a prominent threat. As observed by Sekoia.io, cybercriminal threat actors **widely distribute it using multiple infection chains** including phishing websites masquerading legitimate ones, YouTube videos and fake "free software catalogue" websites.

To provide our customers with actionable intelligence, Sekoia.io analysts will continue to monitor emerging and prevalent infostealers, including Aurora.

Annex

Annex 1 – Infection Chains

Here are two infection chains distributing the Aurora stealer in the wild.

Cryptocurrency phishing site

Aurora stealer is distributed using a phishing site impersonating Exodus Wallet (cryptocurrency wallet) hosted on hxxps://mividajugosa[.]com/.

Figure 8. Phishing webpage impersonating the Exodus Wallet download page (mividajugosa[.]com)

Clicking on the "Download" button at the top right initiates the download of a ZIP "*ExodusWeb3.zip*" (SHA256: *2e9dbda19d9c75a82dabac8ffba5ea76689ada81639867c41c395a29aeaba788*) that contains the executable "*ExodusWeb3.exe*" (SHA256: *9db1744112aea85c625cd046fc737bf28bef254bebfbf7123df6844f62167759*) detected as Aurora stealer. It communicates to its C2 server on *79.137.195[.]171:8081*.

911 infection chain

This infection consists in the following steps:

1. A YouTube video on a stolen account describing how to install a cracked software for free and providing a link;

2. From the link provided in the YouTube video, the victim can access a "free software catalogue" website (*e.g. winsofts[.]cloud*);

website (winsoft[.]cloud) luring the user to download Aurora sample

ate file sharing platform and embeds Aurora Stealer.

s the archive and executes the file "*setup.exe*".

4. Aurora sample communicates to its C2 on *45.15.156[.]97:8081* and downloads a second-stage payload *(oH7P8GCPXQ.exe)*.

Related URLs:

- YouTube videos: *hxxps://www.youtube[.]com/watch?v=oy7NPaccBnk*
- Malicious free software catalogue website: *hxxps://winsofts[.]cloud/*
- Next-stage payload: *hxxps://cdn.discordapp[.]com/attachments/1037000444813254768/1042401882041237524/Adobe_Acrobat.zip*

File hashes:

- Downloaded archive (*Adobe_Acrobat.zip*)
  SHA256: *88e02def17fda0021d4dba5ea812772c542b0fa6ca8930bcf06c42375c00bd29*
- Aurora sample (*setup.exe*)
  SHA256: *47332ce5b904b959aa814ddfde8662931fdfb5233422dc45053ad04cffc44fb4*
- Next-stage payload (*oH7P8GCPXQ.exe*)
  SHA256: *8e24e96e1e87cf00e27c3a3745414636fbf6e148077c0f6815a2b87bacf85c8d*

Emulating this infection chain on a system monitored by Sekoia.io XDR resulted in raising 5 security alerts, as shown hereunder.

- The CTI detection rule detected communications with the Aurora C2 server and the malicious domain hosting the fake free software catalogue.
- The correlation rule detected the sequence of Aurora fingerprinting commands using WMIC.
- Other generic detection rules detected the change in the Windows Defender configuration to exclude the location "C:\Program Data\" (via the Windows Defender event ID 5007 and via the executed command line). This behaviour corresponds to the next-stage payload dropped by the Aurora sample.

koia.io XDR following the execution of Aurora Stealer sample

Annex 2 – Collected data

Cryptocurrency desktop wallets:

Path of targeted file	Cryptocurrency wallet desktop application
\Armory	Armory
\bytecoin	Bytecoin
\Electrum\wallets	Electrum
\Ethereum\keystore	Ethereum
\Exodus\exodus.wallet	Exodus
\Guarda\Local Storage\leveldb	Guarda
\com.liberty.jaxx\IndexedDB	Jaxx Liberty
\Zcash	Zcash

Cryptocurrency browser extensions:

Extension id	Cryptocurrency wallet browser extensions
aeachknmefphepccionboohckonoeemg	Coin98
aiifbnbfobpmeekipheeijimdpnlpgpp	Terra Station
amkmjjmmflddogmhpjloimipbofnfjih	Wombat
aodkkagnadcbobfpggfnjeongemjbjca	BOLT X
bfnaelmomeimhlpmgjnjophhpkkoljpa	Phantom
blnieiiffboillknjnepogjhkgnoapac	Equal
cgeeodpfagjceefieflmdfphplkenlfk	EVER
cjelfplplebdjjenllpjcblmjkfcffne	Jaxx Liberty
dngmlblcodfobpdpecaadgfbcggfjfnm	Maiar DeFi
ffnbelfdoeiohenkjibnmadjiehjhajb	Yoroi
fhbohimaelbohpjbbldcngcnapndodjp	Binance
fhilaheimglignddkjgofkcbgekhenbh	Oxygen
[illegible]	BitApp
[illegible]	Ronin
[illegible]	Harmony
[illegible]	XDEFI
[illegible]	Coinbase
hpglfhgfnhbgpjdenjgmdgoeiappafln	Guard

ibnejdfjmmkpcnlpebklmnkoeoihofec	TronLink
jbdaocneiiinmjbjlgalhcelgbejmnid	Nifty
kncchdigobghenbbaddojjnnaogfppfj	iWallet
kpfopkelmapcoipemfendmdcghnegimn	Liquality
lpfcbjknijpeeillifnkikgncikgfhdo	Nami
mgffkfbidihjpoaomajlbgchddlicgpn	Pali
nanjmdknhkinifnkgdcggcfnhdaammmj	Guild
nkbihfbeogaeaoehlefnkodbefgpgknn	MetaMask
nkddgncdjgjfcddamfgcmfnlhccnimig	Saturn
nlbmnnijcnlegkjjpcfjclmcfggfefdm	MEW CX
odbfpeeihdkbihmopkbjmoonfanlbfcl	Brave
pdadjkfkgcafgbceimcpbkalnfnepbnk	KardiaChain

Other application:

Path of targeted file	Application
\AppData\Roaming\Telegram Desktop\tdata	Telegram

Annex 3 – Aurora sample BuildID

@im_HiLLi, @dddaw22123, @t0mi0k4, Zack, DEV, @feozz, @huy, @dgdima, @mutedall, @huy, @HelixHuntter, 5397150605_99, @tipok734, @Ggtwp, 11, @t0mi0k4, shellar, @dzynO1k, shellarlogs, @sou_bss, DEV, zack, INSTALLS, yjrc, shellar, egorix, DEV, 123

IoCs & Technical Details

IoCs

The list of IoCs is available on Sekoia.io github repository.

Aurora C2

138.201.92[.]44:8081
146.19.24[.]118:8081

45.144.30[.]140:8081

45.15.156[.]115:8081

45.15.156[.]22:8081

45.15.156[.]33:8081

45.15.156[.]80:8081

45.15.156[.]97:8081

45.15.157[.]137:8081

49.12.222[.]119:8081

49.12.97[.]28:8081

5.9.85[.]111:8081

65.108.253[.]85:8081

65.109.25[.]109:8081

78.153.144[.]31:8081

79.137.195[.]171:8081

81.19.140[.]21:8081

82.115.223[.]218:8081

85.192.63[.]114:8081

89.208.104[.]160:8081

95.214.55[.]225:8081

Aurora SHA256

a485913f71bbd74bb8a1bdce2e2c5d80c107da7d6c08bf088599c1ee62ccb109

f6b17c5c0271074fc27c849f46b70e25deafa267a060c35f1636ab08dda237d6

51a2fe0ea58a7a656bc817e91913f6d6c50e947823b96a3565e7593eea2fd785

73485bc0ca251edcca9e4c279cbc4876b1584fb981a5607a4bdeae156a70d082

2bdba09d02482f3016df62a205a456fc5e253f5911543bf40da14a59ad2bc566

459a8faa7924a25a15f64c34910324baed5c24d2fe68badd9a4a320628c08cb8

aa504264669e5bdbda0aac3ada1cd16964499c92d2b48d036a16ba22d79f44f6

4b5450b61a1be5531d43fe36f731c78a28447b85f2466b4389ea7bbb09ecec9c

04b2edcc9d62923a37ef620f622528d70edab52ccd340981490046ad3aa255e5

a4a3a66aee74f3442961a860b8376d2a2dc2cf3783b0829f6973e63d6d839e5b

A query to find more Aurora samples on VirusTotal based on the specific behavior:

```
behavior_processes:"wmic os get Caption" behavior_processes:"wmic path
win32_VideoController get name" behavior_processes:"wmic os get Caption"
```

More IoCs are available in the Sekoia.io CTI.

are distributing Aurora

	RL
	n.discordapp[.]com/attachments/1037343714319794236/103735
	n.discordapp[.]com/attachments/1036703574828269658/103713
hxxps://alls0ft[.]cloud/	hxxps://cdn.discordapp[.]com/attachments/1036677135621951653/103714

hxxps://onesoftware[.]site/	hxxps://cdn.discordapp[.]com/attachments/1041004296050835459/104145
hxxps://unisoft[.]store/	hxxps://cdn.discordapp[.]com/attachments/1028937934763720724/103887
hxxps://freesoft[.]digital/	hxxps://cdn.discordapp[.]com/attachments/1041004296050835459/104174
hxxps://cheatcloud[.]info/	hxxps://www.dropbox[.]com/s/dl/0wzz3wsk5sy7kck/Fortnite%20Hack%20%

YARA

```
rule infostealer_win_aurora {
    meta:
        malware = "Aurora"
        description = "Finds Aurora samples based on characteristic strings"
        source = "SEKOIA.IO"
        reference = "https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-
the-radar/"
        classification = "TLP:CLEAR"

    strings:
        $str00 = "I'm a teapot" ascii
        $str01 = "wmic cpu get name" ascii
        $str02 = "wmic path win32_VideoController get" ascii
        $str03 = "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Time Zones"
ascii
        $str04 = "Exodus\\exodus.wallet" ascii
        $str05 = "PaliWallet" ascii
        $str06 = "cookies.sqlite" ascii
        $str07 = "Startup\\Documents\\User Data" ascii
        $str08 = "atomic\\Local Storage\\leveldb" ascii
        $str09 = "com.liberty.jaxx\\IndexedDB" ascii
        $str10 = "Guarda\\Local Storage\\leveldb" ascii
        $str11 = "AppData\\Roaming\\Telegram Desktop\\tdata" ascii
        $str12 = "Ethereum\\keystore" ascii
        $str13 = "Coin98" ascii
        $str14 = ".bat.cmd.com.css.exe.gif.htm.jpg.mjs.pdf.png.svg.xml.zip" ascii
        $str15 = "type..eq.main.Grabber" ascii
        $str16 = "type..eq.main.Loader_A" ascii
        $str17 = "type..eq.net/http.socksUsernamePassword" ascii
        $str18 = "powershell" ascii
        $str19 = "start-process" ascii
        $str20 = "http/httpproxy" ascii

    condition:
        uint16(0)==0x5A4D and 15 of them and filesize > 4MB
}
```

TPs

d Scripting Interpreter: Windows Command Shell

ment Instrumentation

Files or Information

e/Decode Files or Information

Session Cookie

Credential Access T1555.003 – Credentials from Password Stores: Credentials from Web

Browsers
Discovery T1012 – Query Registry
Discovery T1082 – System Information Discovery
Discovery T1083 – File and Directory Discovery
Discovery T1614 – System Location Discovery
Collection T1005 – Data from Local System
Collection T1113 – Screen Capture
Collection T1119 – Automated Collection
Command and Control T1071.001 – Application Layer Protocol: Web Protocols
Command and Control T1105 – Ingress Tool Transfer
Command and Control T1571 – Non-Standard Port
Exfiltration T1041 – Exfiltration Over C2 Channel

External References

https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem/

Thank you for reading this blogpost. You can also consult the following articles:

- Traffers: a deep dive into the information stealer ecosystem
- Raccoon Stealer v2 – Part 2: In-depth analysis
- BlueFox Stealer: a newcomer designed for traffers teams
- Raccoon Stealer v2 – Part 1: The return of the dead
- NOBELIUM's EnvyScout infection chain goes in the registry, targeting embassies
- The DPRK delicate sound of cyber
- Unveiling of a large resilient infrastructure distributing information stealers
- Raspberry Robin's botnet second life
- coon infostealers gaining in popularity – Part 1
- coon infostealers gaining in popularity – Part 2
- cybersecurity quest
- XDR platform

- SOC platform
- Tools for SOC analyst
- SIEM solution

Share this post:

What's next

Lucky Mouse: Incident Response to Detection Engineering

This blogpost discusses how the Tactics, Techniques and Procedures (TTPs) used by the APT27 (Lucky Mouse) intrusion set in...

Guillaume C. and Sekoia TDR

Calisto show interests into entities involved in Ukraine war support

Calisto (aka Callisto, COLDRIVER) is suspected to be a Russian-nexus intrusion set active since at least April 2017. Although...

Felix Aimé, Maxime A. and Sekoia TDR

How to use Sekoia.io indicators in Microsoft Sentinel ?

Since May 20221,2, Sekoia.io indicators can be integrated into Microsoft Sentinel. In this blogpost, we will cover how to...

SEKOIA.IO

Trending topics

SOC ♡

SOC platform ♡

Detection Engineering ♡