Aurora: The Dark Dawn and its Menacing Effects

research.loginsoft.com/threat-research/aurora-the-dark-dawn-and-its-menacing-effects/

March 23, 2023

Aurora Stealer Background

March 24, 2023
By **Saharsh Agrawal**

Aurora Stealer a non-friendly program in your neighborhood is developed in Go-lang. The malware was developed for threat actors to steal victims' sensitive data. Since its initial release, there have been many adaptations to the malware. It started as a botnet having info-stealer capabilities but currently it is a full-time info-stealer which is being sold by the threat actor labelled Cheshire on Russian speaking dark-net forums mentioned by cybersecurity firm Sekoia.

The malware has a knack for stealing the victim's browser data including cookies, passwords, login data and many more. It has the horizon to steal data from most browsers. The stealer also targets crypto wallets to pilfer victim's data. The malware does not stop here, it can exfiltrate files and data stored in different software from the victim's machine. Once all the super-sensitive data is possessed by the stealer it delivers the data to the attacker.

Operating Model

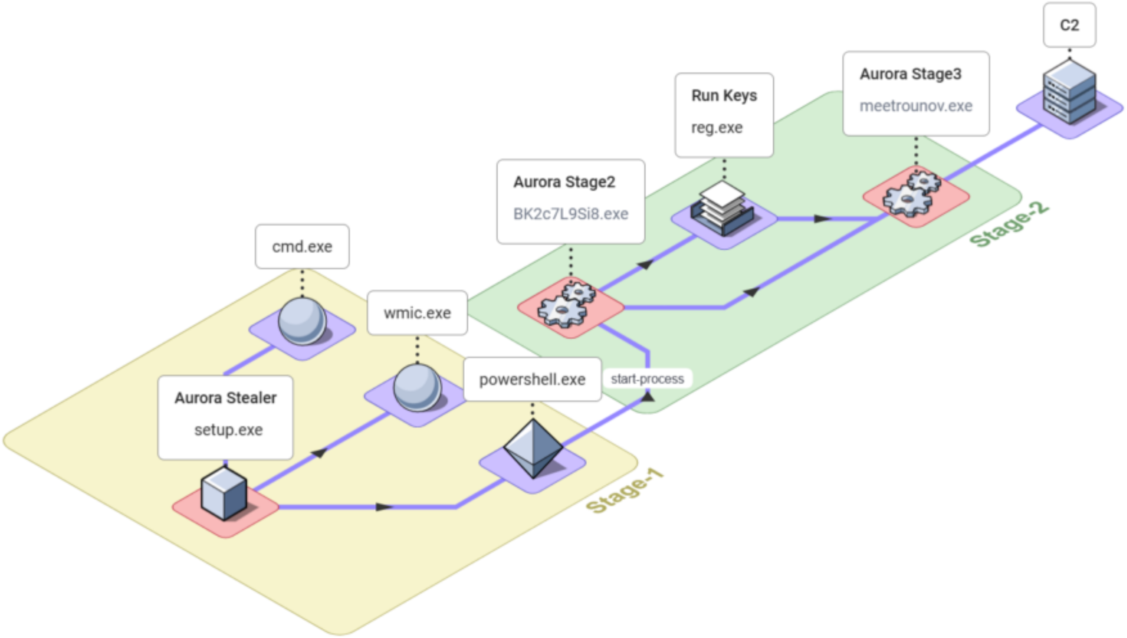
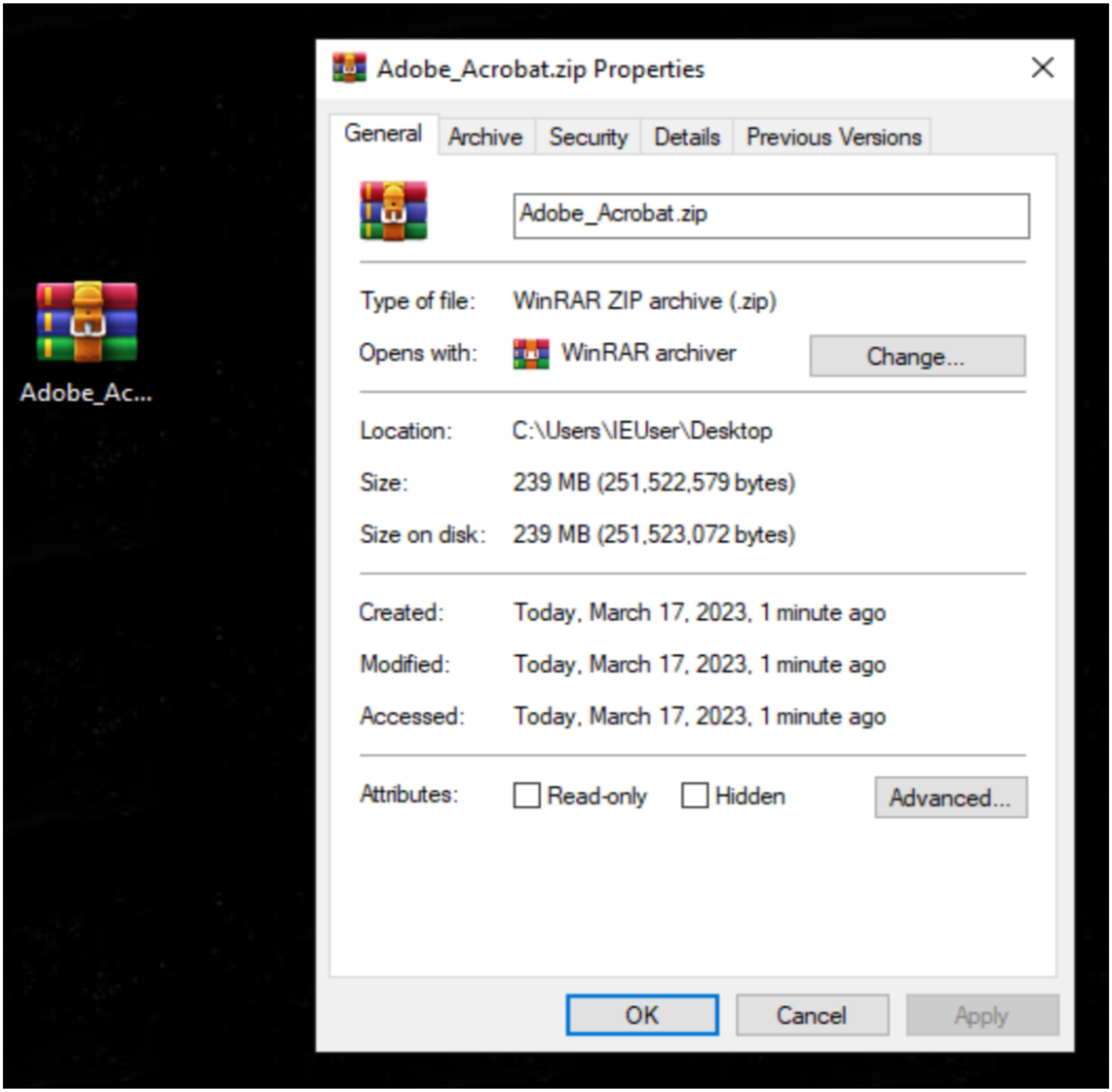


Figure1: Attack Chain of Aurora Stealer

The malware is being spread among victims in the hospitality industry through phishing emails as seen by Trendmirco. Besides phishing campaigns, the threat actors also have utilized SEO poisoning technique to deliver the malware via malicious ads of notepad++ according to SANS finding.

Upon the detonation of the malware, our observations revealed the implementation of multiple sophisticated techniques by the malware to evade detection by antivirus software. One such technique involved the incorporation of binary padding, resulting in an increase in the file size allowing the malware to circumvent the antivirus software and evade detection.



Adobe_Acrobat.zip Properties

Adobe_Acrobat.zip

Type of file: WinRAR ZIP archive (.zip)

Opens with: WinRAR archiver

Location: C:\Users\IEUser\Desktop

Size: 239 MB (251,522,579 bytes)

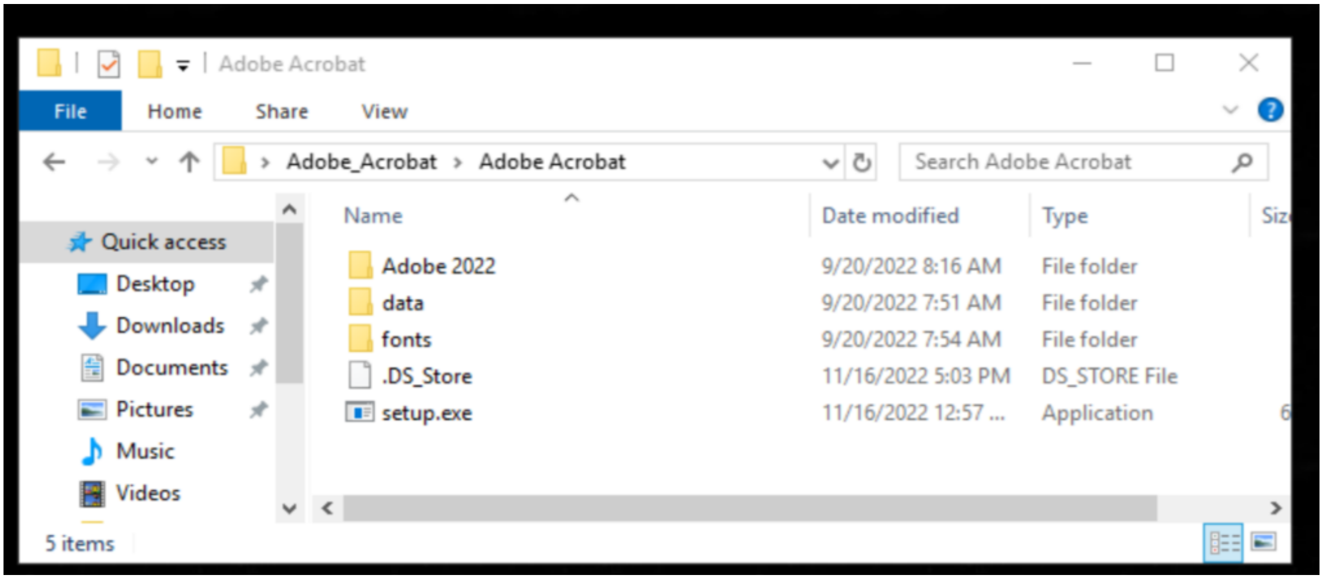
Size on disk: 239 MB (251,523,072 bytes)

Created: Today, March 17, 2023, 1 minute ago

Modified: Today, March 17, 2023, 1 minute ago

Accessed: Today, March 17, 2023, 1 minute ago

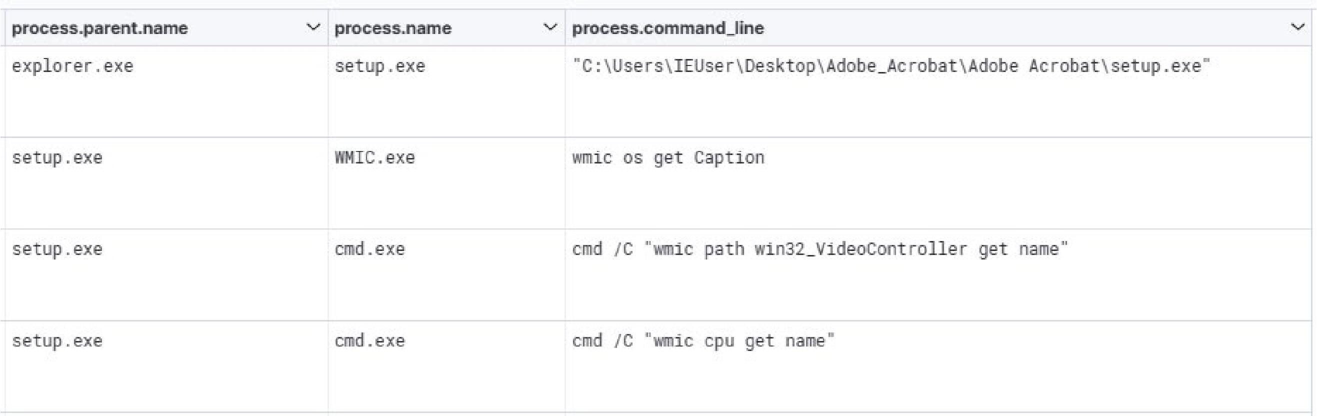
Attributes: □ Read-only □ Hidden



Name	Date modified	Type	Siz
Adobe 2022	9/20/2022 8:16 AM	File folder	
data	9/20/2022 7:51 AM	File folder	
fonts	9/20/2022 7:54 AM	File folder	
.DS_Store	11/16/2022 5:03 PM	DS_STORE File	
setup.exe	11/16/2022 12:57 ...	Application	6

Figure2: Fake Adobe Acrobat Installer Downloaded from SEO Poisoning Campaign

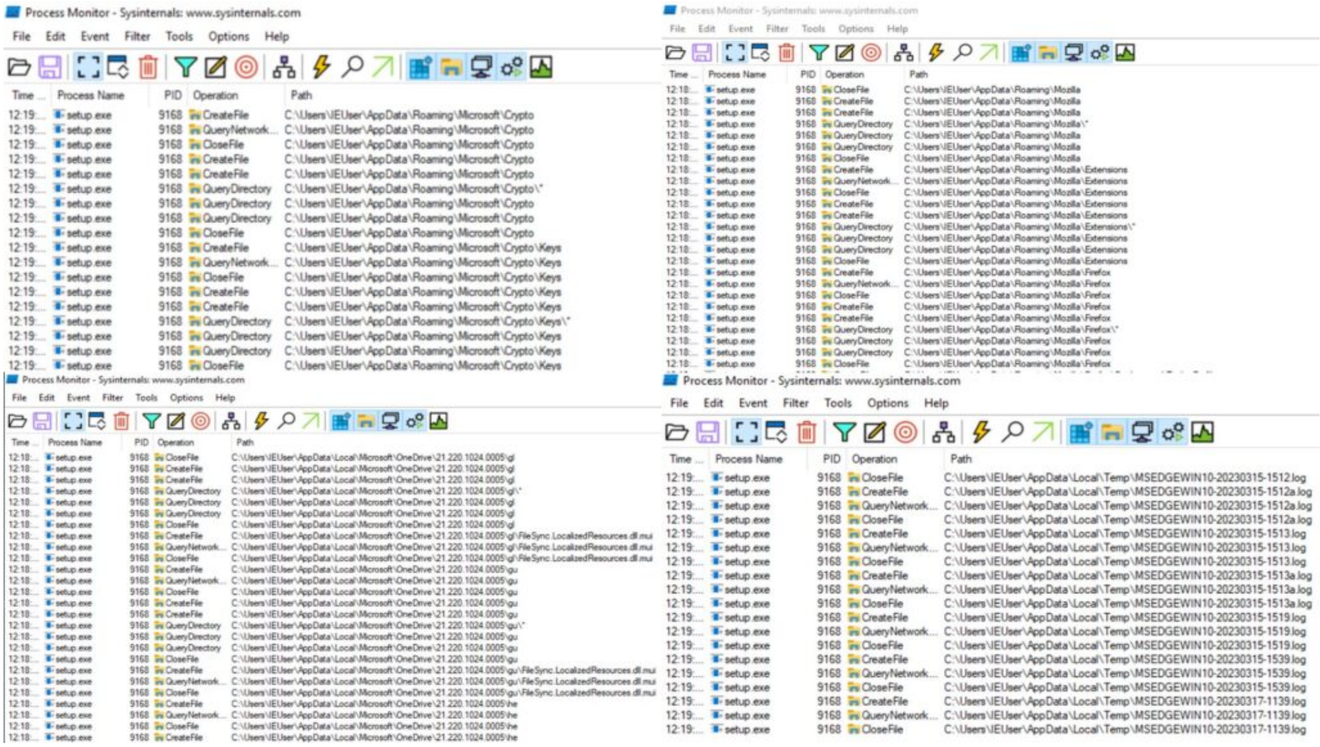
After successful infiltration, the malware utilizes Windows Management Instrumentation (WMI) commands to gather pertinent system information. This behavior was consistently observed in all samples of Aurora stealer that we analyzed. Additionally, independent research conducted by Cyble and other industry experts has reported this observation.



process.parent.name	process.name	process.command_line
explorer.exe	setup.exe	"C:\Users\IEUser\Desktop\Adobe_Acrobat\Adobe Acrobat\setup.exe"
setup.exe	WMIC.exe	wmic os get Caption
setup.exe	cmd.exe	cmd /C "wmic path win32_VideoController get name"
setup.exe	cmd.exe	cmd /C "wmic cpu get name"

Figure2.1 : WMI Commands getting Executed

We also captured Aurora stealer's actions that were aimed at extracting sensitive information from files and folders located in various browsers, cryptocurrency wallets, and drives, as illustrated below.



```
Time ...  Process Name  PID   Operation        Path
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto
12:19:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto
12:19:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\*
12:19:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto
12:19:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\Keys
12:19:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\Keys
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\Keys
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\Keys
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\Keys
12:19:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\Keys\*
12:19:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\Keys
12:19:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\Keys
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Microsoft\Crypto\Keys
```

```
Time ...  Process Name  PID   Operation        Path
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Mozilla
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Mozilla
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Mozilla
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Mozilla\*
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Mozilla
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Mozilla
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Mozilla
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Mozilla\Extensions
12:18:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Roaming\Mozilla\Extensions
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Mozilla\Extensions
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Mozilla\Extensions
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Mozilla\Extensions
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Mozilla\Extensions\*
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Mozilla\Extensions
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Mozilla\Extensions
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Mozilla\Extensions
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox
12:18:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox\*
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Roaming\Mozilla\Firefox
```

```
Time ...  Process Name  PID   Operation        Path
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl\*
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl\FileSync.LocalizedResources.dll.mui
12:18:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl\FileSync.LocalizedResources.dll.mui
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gl\FileSync.LocalizedResources.dll.mui
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu
12:18:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu\*
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu
12:18:... setup.exe     9168  QueryDirectory   C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu\FileSync.LocalizedResources.dll.mui
12:18:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu\FileSync.LocalizedResources.dll.mui
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\gu\FileSync.LocalizedResources.dll.mui
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\he
12:18:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\he
12:18:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\he
12:18:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\21.220.1024.0005\he
```

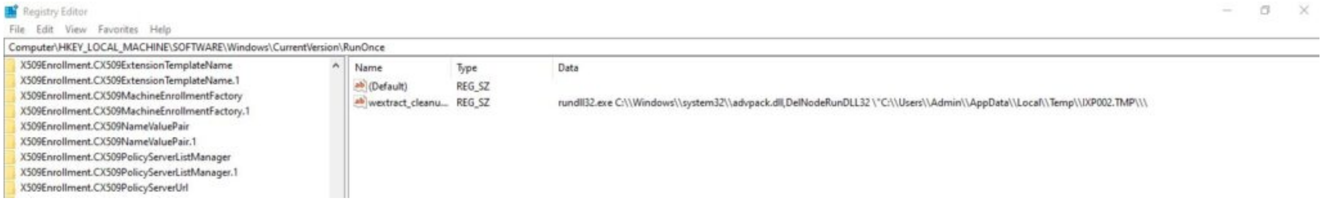
```
Time ...  Process Name  PID   Operation        Path
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1512.log
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1512a.log
12:19:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1512a.log
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1512a.log
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1513.log
12:19:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1513.log
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1513.log
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1513a.log
12:19:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1513a.log
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1513a.log
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1519.log
12:19:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1519.log
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1519.log
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1539.log
12:19:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1539.log
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230315-1539.log
12:19:... setup.exe     9168  CreateFile       C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230317-1139.log
12:19:... setup.exe     9168  QueryNetwork...  C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230317-1139.log
12:19:... setup.exe     9168  CloseFile        C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10-20230317-1139.log
```

Figure3: Stealing Browser and Crypto Data

Aurora leverages PowerShell to facilitate the execution of its second stage, employing the following command:

```
powershell "" "start-process C:\Users\Admin\AppData\Local\Temp\BK2c7L9Si8.exe"
```

During the second stage of Aurora, an entry to the “run keys” in the registry was observed, enabling the malware to automatically execute its third stage DLL via RUNDLL32.exe at each user login.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Windows\CurrentVersion\RunOnce

X509Enrollment.CX509ExtensionTemplateName
X509Enrollment.CX509ExtensionTemplateName.1
X509Enrollment.CX509MachineEnrollmentFactory
X509Enrollment.CX509MachineEnrollmentFactory.1
X509Enrollment.CX509NameValuePair
X509Enrollment.CX509NameValuePair.1
X509Enrollment.CX509PolicyServerListManager
X509Enrollment.CX509PolicyServerListManager.1
X509Enrollment.CX509PolicyServerUrl

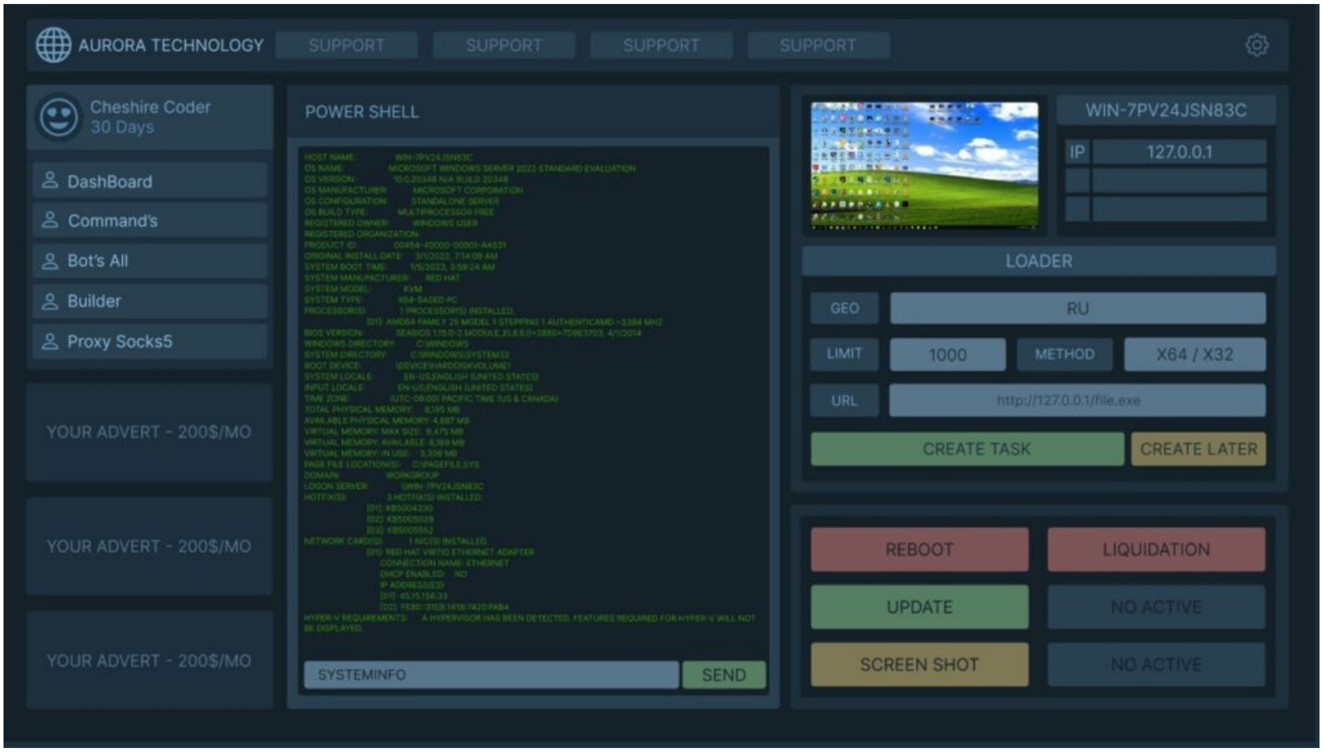
Name	Type	Data
(Default)	REG_SZ	
wextract_cleanu...	REG_SZ	rundll32.exe C:\\Windows\\system32\\advpack.dll,DelNodeRunDLL32 \"C:\\Users\\Admin\\AppData\\Local\\Temp\\IXP002.TMP\\\

Figure4: Run Key Added for DLL Execution

The third stage of the malware executes an encoded PowerShell command allowing it to delay execution for certain duration using the following command before it exfiltrates the data to the attacker.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc
UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAAMwA0AA==
```

Once all the data and information are collected, the malware employs advanced encoding techniques to conceal the information and prepare it for shipment to the attacker over the C2 channel. The attacker can retrieve the encoded data and use it for nefarious purposes, such as identity theft or financial fraud.



```
HOST NAME:                 WIN-7PV24JSN83C
OS NAME:                   MICROSOFT WINDOWS SERVER 2022 STANDARD EVALUATION
OS VERSION:                10.0.20348 N/A BUILD 20348
OS MANUFACTURER:           MICROSOFT CORPORATION
OS CONFIGURATION:          STANDALONE SERVER
OS BUILD TYPE:             MULTIPROCESSOR FREE
REGISTERED OWNER:          WINDOWS USER
REGISTERED ORGANIZATION:
PRODUCT ID:                00454-40000-00001-AA531
ORIGINAL INSTALL DATE:     3/1/2022, 7:14:09 AM
SYSTEM BOOT TIME:          1/5/2023, 3:59:24 AM
SYSTEM MANUFACTURER:       RED HAT
SYSTEM MODEL:              KVM
SYSTEM TYPE:               X64-BASED PC
PROCESSOR(S):              1 PROCESSOR(S) INSTALLED.
                           [01]: AMD64 FAMILY 25 MODEL 1 STEPPING 1 AUTHENTICAMD ~3394 MHZ
BIOS VERSION:              SEABIOS 1.15.0-2.MODULE_EL8.6.0+2880+7D9E3703, 4/1/2014
WINDOWS DIRECTORY:         C:\WINDOWS
SYSTEM DIRECTORY:          C:\WINDOWS\SYSTEM32
BOOT DEVICE:               \DEVICE\HARDDISKVOLUME1
SYSTEM LOCALE:             EN-US;ENGLISH (UNITED STATES)
INPUT LOCALE:              EN-US;ENGLISH (UNITED STATES)
TIME ZONE:                 (UTC-08:00) PACIFIC TIME (US & CANADA)
TOTAL PHYSICAL MEMORY:     8,195 MB
AVAILABLE PHYSICAL MEMORY: 4,887 MB
VIRTUAL MEMORY: MAX SIZE:  9,475 MB
VIRTUAL MEMORY: AVAILABLE: 6,169 MB
VIRTUAL MEMORY: IN USE:    3,306 MB
PAGE FILE LOCATION(S):     C:\PAGEFILE.SYS
DOMAIN:                    WORKGROUP
LOGON SERVER:              \\WIN-7PV24JSN83C
HOTFIX(S):                 3 HOTFIX(S) INSTALLED.
                           [01]: KB5004330
                           [02]: KB5005039
                           [03]: KB5005552
NETWORK CARD(S):           1 NIC(S) INSTALLED.
                           [01]: RED HAT VIRTIO ETHERNET ADAPTER
                                 CONNECTION NAME: ETHERNET
                                 DHCP ENABLED:    NO
                                 IP ADDRESS(ES)
                                 [01]: 45.15.156.33
                                 [02]: FE80::31EB:1418:7420:FAB4
HYPER-V REQUIREMENTS:      A HYPERVISOR HAS BEEN DETECTED. FEATURES REQUIRED FOR HYPER-V WILL NOT
BE DISPLAYED.
```

SYSTEMINFO

Figure5: C2 Panel; source: twitter

Detection

The infernal behavior of this malware can be detected using SIGMA rules.
To begin with, we attribute different WMI commands getting executed in sequence to detect Aurora Stealer malware.

```
logsource:
 category: process_creation
 product: windows
detection:
 selection:
 Image|endswith: '\wmic.exe'
 CommandLine|contains:
 - 'wmic os get Caption'
 - 'wmic path win32_VideoController get name'
 - 'wmic cpu get name'
 condition: selection
```

One detection would be to capture changes in ‘run key’ registry which execute DLL using RUNDLL32.exe

```
logsource:
 product: windows
 category: registry_set
detection:
 selection:
 EventType: SetValue
 TargetObject|contains:
'\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce'
 Details|re: .*rundll32.exe.C:\\\\Windows\\\\system32\\\\advpack.dll,DelNodeRunDLL32
\\"C:\\\\Users\\\\.*\\AppData\\\\Local\\\\Temp\\\\IXP[0-9]{1,3}.TMP.*
 condition: selection
```

Based on the general behavior followed by Aurora and different malwares, we have developed several detection methods. We also observed changes in the configuration of Windows Defender, where the path ‘C:\Program Data’ is excluded.

```
logsource:
 product: windows
 category: registry_set
detection:
 selection:
 EventType: SetValue
 TargetObject|contains: '\Microsoft\Windows Defender\Exclusions'
 Details: 'C:\Program Data\'
 condition: selection
```

Another detection would be by tracing event id `5007`, which can be activated by enabling Windows Defender operation logs. This particular event is triggered whenever there is a modification made to the configuration of Microsoft Defender Antivirus.

```
logsource:
 product: windows
 service: windefend
detection:
 selection:
 EventID: 5007
 NewValue|contains: 'C:\Program Data\'
 condition: selection
```

Additionally, one clever way to detect this malware is to monitor the execution of obfuscated PowerShell commands.

The same campaign can be detected using OSQUERY rules. Below are some rules that will help you keep your organization safe.

```
query_wmic:
    SELECT name,
           pid,
           cmdline,
           path,
           parent
    FROM processes
    WHERE LOWER(name) = 'wmic.exe'
    AND
    (
      cmdline LIKE '%OS Get Caption%'
      OR cmdline LIKE '%path win32_VideoController get name%'
      OR cmdline LIKE '%cpu get name%'
    );
 query_regsitry:
    SELECT key,
           path,
           name,
           type,
           data
    FROM registry
    WHERE path LIKE
'HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\%'
    AND data LIKE '%rundll32.exe C:\\Windows\\system32\\advpack.dll,DelNodeRunDLL32
"C:\\Users\\%\\AppData\\Local\\Temp\\IXP%.TMP\\%';
query_exclusion:
    SELECT key,
           path,
           name,
           type,
           data
    FROM registry
    WHERE path LIKE 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
Defender\Exclusions\Paths\%'
    AND
    (
      data LIKE '%c:\programdata%'
      OR data LIKE '%\appdata\roaming\microsoft\windows\start menu\programs\startup%'
```

For more threat analytics reach us here.

The above rules have been vindicated by simulating Aurora stealer in a sandbox environment.

MITRE ATT&CK Techniques

Tactic	Technique ID	Technique Name

Execution	T1204 T1059.001 T1059.003 T1047	User Execution Command and Scripting Interpreter: PowerShell Command and Scripting Interpreter: Windows Command Shell Windows Management Instrumentation
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Defense Evasion	T1562.001 T1027 T1218.011 T1497	Impair Defenses Obfuscated Files or Information System Binary Proxy Execution: Rundll32 Virtualization/Sandbox Evasion
Credential Access	T1555.003 T1056 T1003 T1528 T1539 T1552.002	Credentials from Password Stores: Credentials from Web Browsers Input Capture OS Credential Dumping Steal Application Access Token Steal Web Session Cookie Credentials in Registry
Discovery	T1087 T1083 T1012 T1082 T1518.001 T1614 T1497	Account Discovery File and Directory Discovery Query Registry System Information Discovery Software Discovery: Security Software Discovery System Location Discovery Virtualization/Sandbox Evasion
Collection	T1119 T1005 T1056 T1113	Automated Collection Data from Local System Input Capture Screen Capture
Command and Control	T1071.001 T1105 T1095 T1571	Application Layer Protocol: Web Protocols Ingress Tool Transfer Non-Application Layer Protocol Non-Standard Port

Threat Bites

Threat Actor

Targeted Country

Targeted Industry

First Seen

Last Seen

LOLBAS

Telemetry

Samples

:

:

:

:

:

:

:

:

Unknown

Worldwide

Hotels

April 2022

March 2023

Wmic, Reg, Rundll32

Sysmon, Security, Windefend, PowerShell

https://tria.ge/230118-f1ewcaac94/behavioral1

Author: Saharsh Agrawal
Security Researcher, Loginsoft