ThreatMon

SOLVING THE PUZZLE: REVERSING THE NEW STEALER JIGSAW

Contents

Introduction

This report focuses on the threat intelligence gathered on the Jigsaw Stealer, a malicious software available for sale on a hacker's forum. During our investigation, our team of analysts made a significant discovery that the Jigsaw Stealer is an exact replica of the Meow Stealer, with the only difference being the name change. The hacker behind this malware is attempting to deceive potential buyers by rebranding the same stolen software.

The Meow Stealer first appeared on Telegram in September 2022 and later resurfaced on a hacker's forum in April 2023. Notably, this sophisticated malware possesses the capability to extract data from various software, and it boasts a minimal detection rate when a crypter is employed.

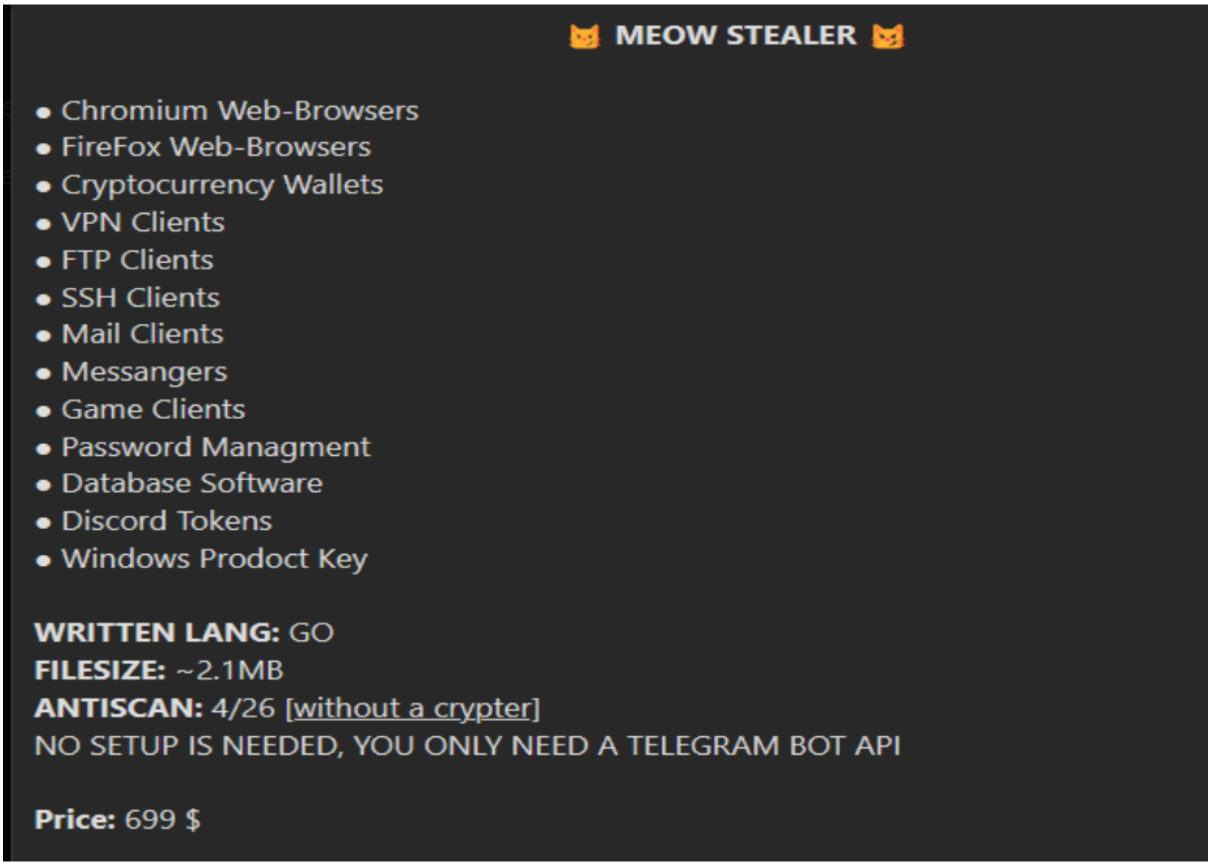
Our Threatmon Malware Research Team engaged in direct communication with the seller on the forum, successfully obtaining a sample of the Jigsaw Stealer for thorough technical analysis. In this report, we will explore the core functionalities, evasion techniques, and unique characteristics of the Jigsaw Stealer, shedding light on its potential impact and providing insights for improved cybersecurity measures.

In addition to our technical analysis, we have proactively contributed to the cybersecurity community by sharing Indicators of Compromise (IOCs), MITRE ATT&CK techniques associated with the Jigsaw Stealer, and a YARA rule for detection. By sharing this valuable information, we aim to enhance the collective defense against this specific threat and support efforts to identify and mitigate similar threats in the future.

Collaborative efforts and information sharing are essential in the fight against cyber threats, and we are committed to fostering a more secure digital environment for all stakeholders. Through open collaboration and the dissemination of threat intelligence, we can strengthen our defenses and better protect organizations and individuals from the ever-evolving landscape of cyber threats.

Threat Intelligence Phase

The Jigsaw Stealer is being offered for sale on a forum, but our analysts have discovered that it is an exact replica of another stealer called Meow Stealer. The same hacker is attempting to sell their stolen software by simply changing the name of the stealer.



🐱 **MEOW STEALER** 🐱

- Chromium Web-Browsers
- FireFox Web-Browsers
- Cryptocurrency Wallets
- VPN Clients
- FTP Clients
- SSH Clients
- Mail Clients
- Messangers
- Game Clients
- Password Managment
- Database Software
- Discord Tokens
- Windows Prodoct Key

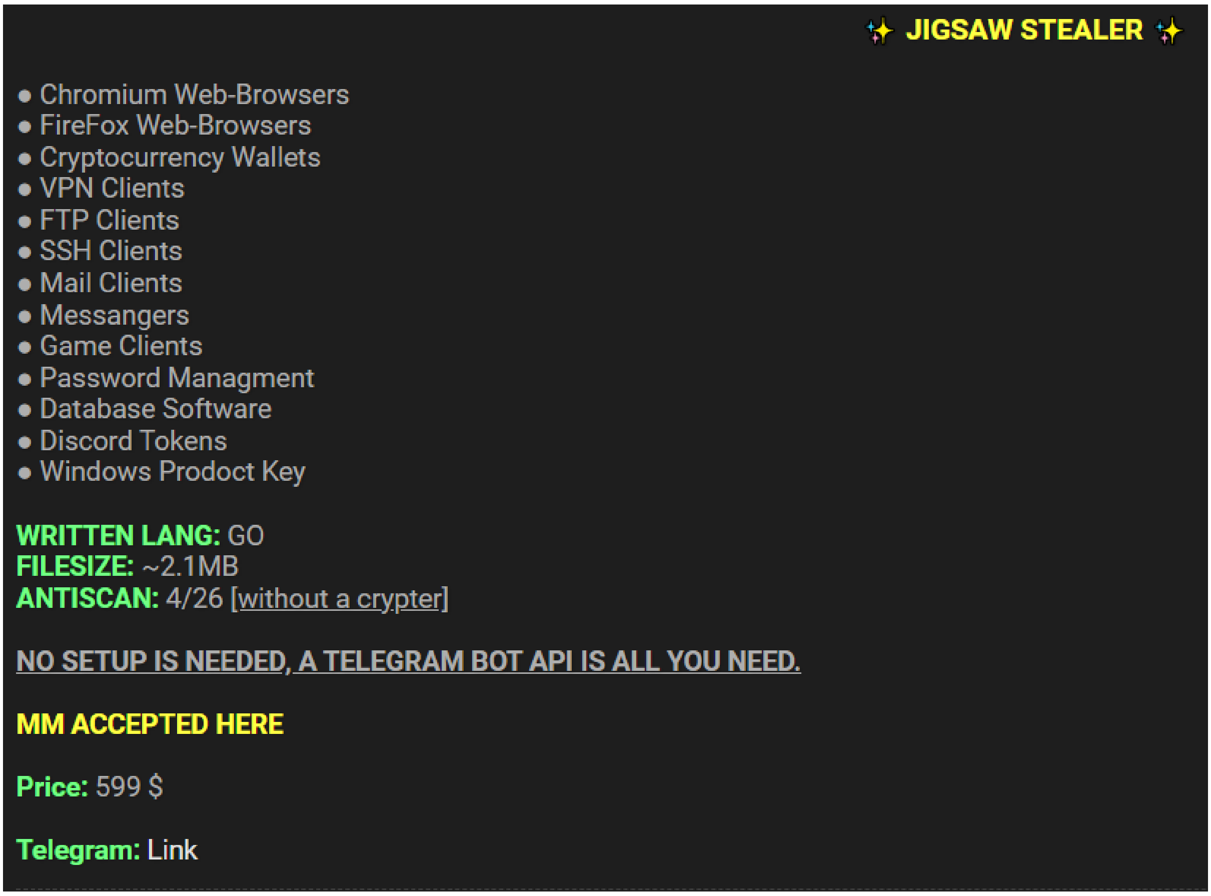
WRITTEN LANG: GO
FILESIZE: ~2.1MB
ANTISCAN: 4/26 [without a crypter]
NO SETUP IS NEEDED, YOU ONLY NEED A TELEGRAM BOT API

Price: 699 $

Figure 0 - Meow Stealer Sale on forum

After being initially posted on Telegram in September 2022, Meow Stealer has reappeared on a hacker's forum in April 2023. Capable of extracting data from diverse software, it possesses a minimal detection rate unless employing a crypter.

In the image provided below, you can observe an identical post on the forum, albeit with a different name for the stealer.



✨ **JIGSAW STEALER** ✨

- Chromium Web-Browsers
- FireFox Web-Browsers
- Cryptocurrency Wallets
- VPN Clients
- FTP Clients
- SSH Clients
- Mail Clients
- Messangers
- Game Clients
- Password Managment
- Database Software
- Discord Tokens
- Windows Prodoct Key

WRITTEN LANG: GO
FILESIZE: ~2.1MB
ANTISCAN: 4/26 [without a crypter]

NO SETUP IS NEEDED, A TELEGRAM BOT API IS ALL YOU NEED.

MM ACCEPTED HERE

Price: 599 $

Telegram: Link

Figure 1 - Jigsaw Stealer Sale on forum

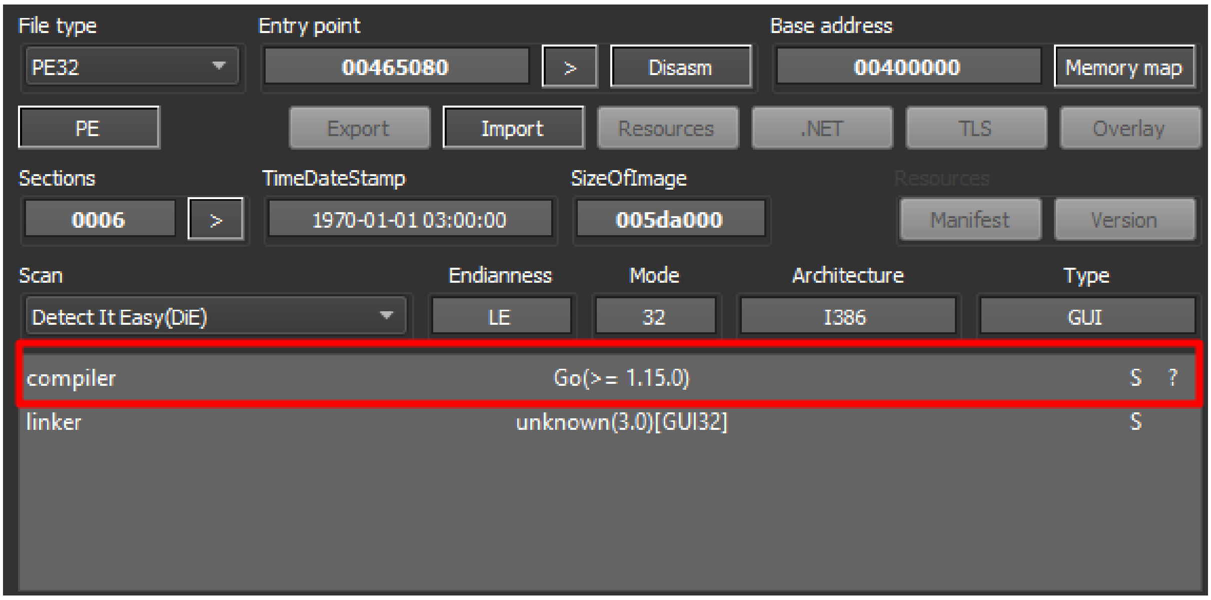
Threatmon Malware Research Team engaged in a discussion with the seller and successfully obtained a sample of malware.

Figure 2 - Conversation with the seller

Technical Analysis

Name	jigsaw_stealer.exe
MD5	AA66B539B3156A123724AC17E5AF3034
SHA256	994E7DCF0C4FB89A255484A4A48F5F567717C2F20D38291FDA22A854CDEF81CC
File Type	PE/32

The Jigsaw stealer stands out in terms of size (6MB) compared to other stealers due to its implementation in the Golang programming language.

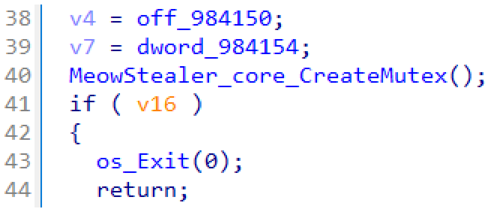


File type: PE32
Entry point: 00465080
Base address: 00400000
Sections: 0006
TimeDateStamp: 1970-01-01 03:00:00
SizeOfImage: 005da000
Scan: Detect It Easy(DiE)
Endianness: LE
Mode: 32
Architecture: I386
Type: GUI

```
compiler    Go(>= 1.15.0)           S  ?
linker      unknown(3.0)[GUI32]     S
```

Figure 3 - Jigsaw Stealer Written in GO

The execution begins by creating a mutex. Malware utilizes mutexes to achieve persistence and evade detection. By ensuring that only one instance is running, the malware maintains persistence and employs unique names to evade detection.

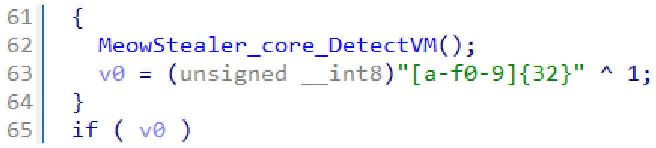


```
v4 = off_984150;
v7 = dword_984154;
MeowStealer_core_CreateMutex();
if ( v16 )
{
  os_Exit(0);
  return;
```

Figure 4 - Mutex Creation

Evasion

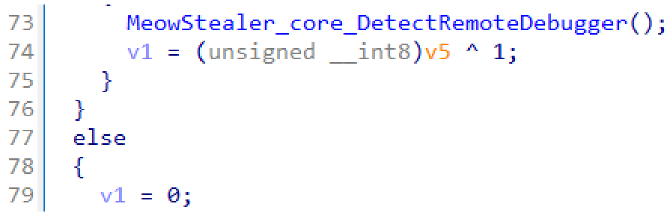
Following that, it proceeds to the evasion phase, where its primary objective is to identify whether it is running within a virtual machine (VM) environment or not.



```
{
  MeowStealer_core_DetectVM();
  v0 = (unsigned __int8)"[a-f0-9]{32}" ^ 1;
}
if ( v0 )
```

Figure 5 - VM Detection

Subsequently, it attempts to identify whether it is operating under a debugger or not.

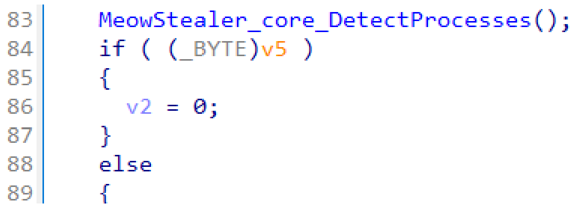


```
    MeowStealer_core_DetectRemoteDebugger();
    v1 = (unsigned __int8)v5 ^ 1;
  }
}
else
{
  v1 = 0;
```

Figure 6 - Debugger Detection

Next, it verifies the presence of particular processes commonly utilized by malware analysts.

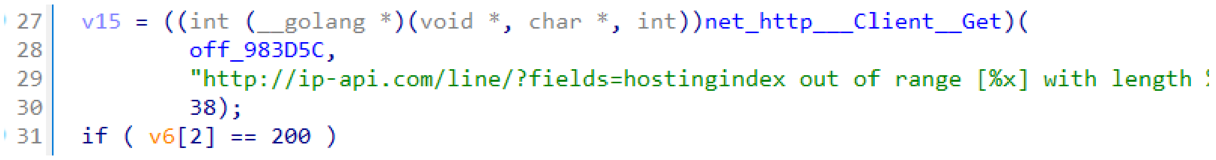
- process hacker
- netstat
- netmon
- tcpview
- wireshark
- filemon
- regmon
- cain



```
  MeowStealer_core_DetectProcesses();
  if ( (_BYTE)v5 )
  {
    v2 = 0;
  }
  else
  {
```

Figure 7 - Process Detection

Next, it verifies whether it is being executed within a particular hosting environment or not.

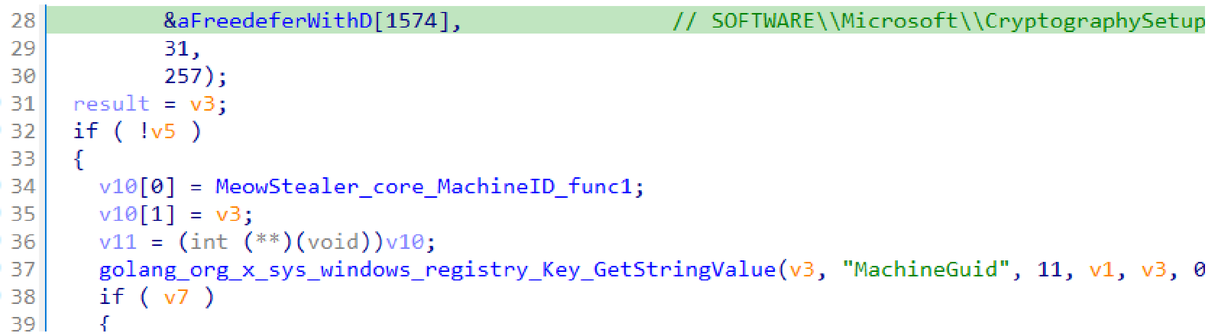


```
v15 = ((int (__golang *)(void *, char *, int))net_http___Client__Get)(
        off_983D5C,
        "http://ip-api.com/line/?fields=hostingindex out of range [%x] with length 
        38);
if ( v6[2] == 200 )
```

Figure 8 - Hosting Detection

Core Functionality

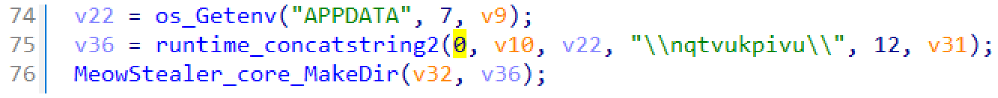
Initially, the stealer gathers machine GUID (Globally Unique Identifier) information.



```
        &aFreedeferWithD[1574],                // SOFTWARE\\Microsoft\\CryptographySetup
        31,
        257);
result = v3;
if ( !v5 )
{
  v10[0] = MeowStealer_core_MachineID_func1;
  v10[1] = v3;
  v11 = (int (**)(void))v10;
  golang_org_x_sys_windows_registry_Key_GetStringValue(v3, "MachineGuid", 11, v1, v3, 0
  if ( v7 )
  {
```

Figure 9 - Collecting Machine GUID

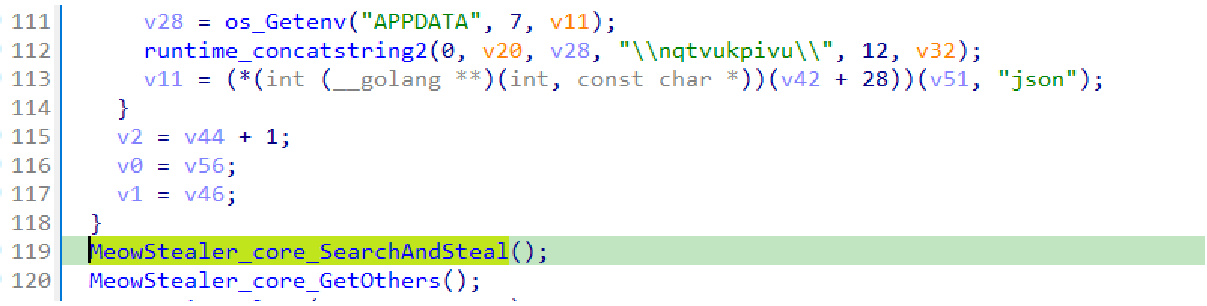
Subsequently, it creates a directory within %APPDATA% to serve as the storage location for the stolen data.



```
v22 = os_Getenv("APPDATA", 7, v9);
v36 = runtime_concatstring2(0, v10, v22, "\\nqtvukpivu\\", 12, v31);
MeowStealer_core_MakeDir(v32, v36);
```

Figure 9 - Creating Directory to Store Data

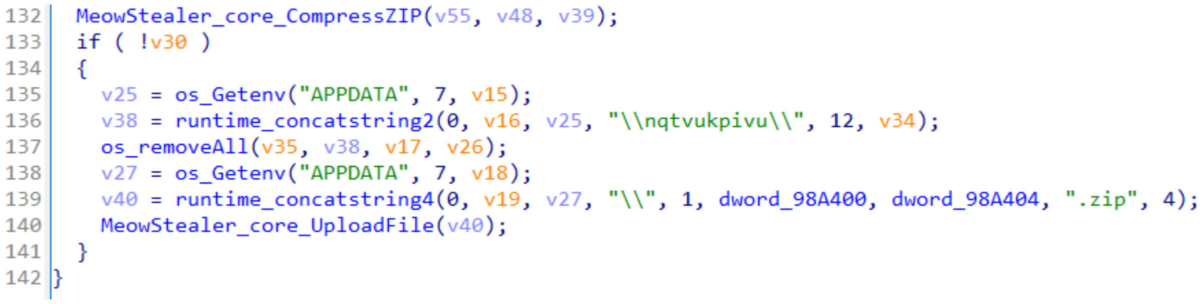
Next, it initiates a data-stealing process similar to that of other stealers.



```
    v28 = os_Getenv("APPDATA", 7, v11);
    runtime_concatstring2(0, v20, v28, "\\nqtvukpivu\\", 12, v32);
    v11 = (*(int (__golang **)(int, const char *))(v42 + 28))(v51, "json");
  }
  v2 = v44 + 1;
  v0 = v56;
  v1 = v46;
}
MeowStealer_core_SearchAndSteal();
MeowStealer_core_GetOthers();
```

Figure 10 - Data Stealing Process

Afterward, the stolen data is compressed into a zip file and transmitted to the C2 (Command and Control) server.

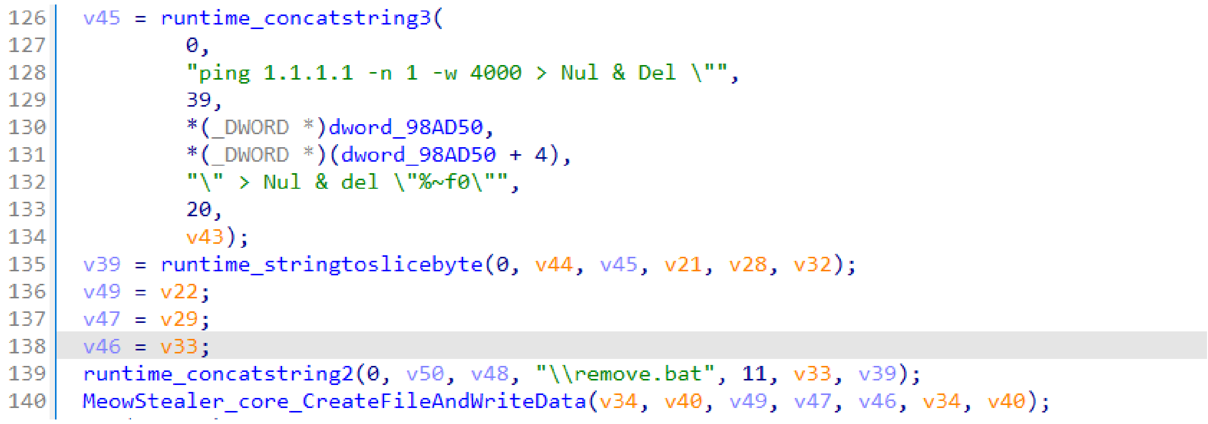


```
MeowStealer_core_CompressZIP(v55, v48, v39);
if ( !v30 )
{
  v25 = os_Getenv("APPDATA", 7, v15);
  v38 = runtime_concatstring2(0, v16, v25, "\\nqtvukpivu\\", 12, v34);
  os_removeAll(v35, v38, v17, v26);
  v27 = os_Getenv("APPDATA", 7, v18);
  v40 = runtime_concatstring4(0, v19, v27, "\\", 1, dword_98A400, dword_98A404, ".zip", 4);
  MeowStealer_core_UploadFile(v40);
}
}
```

Figure 11 - Exfiltration

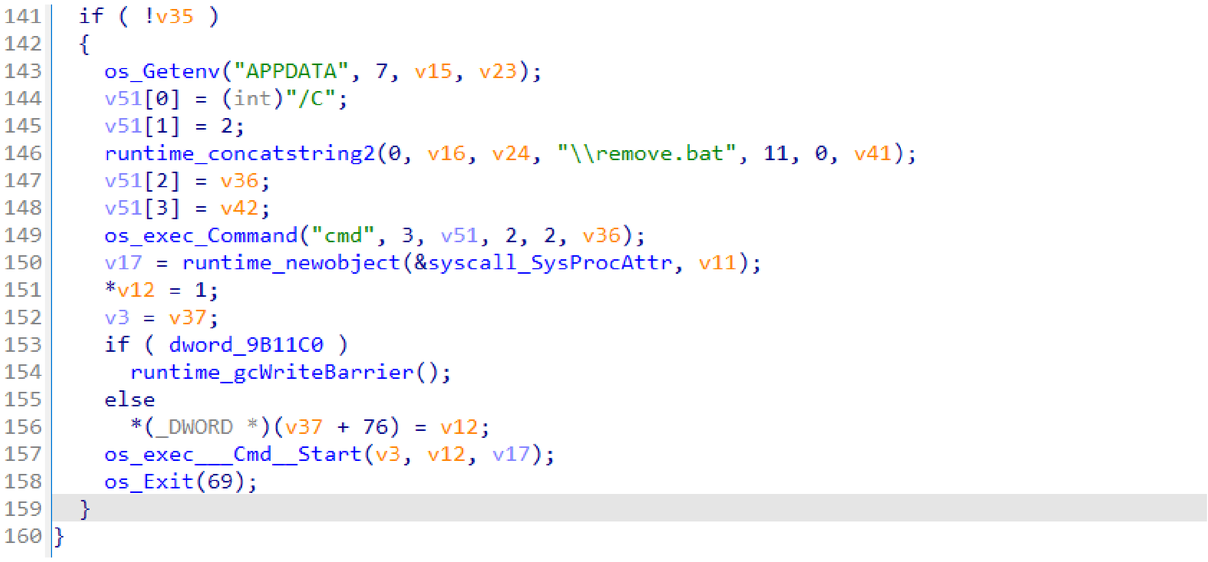
Cleanup

Finally, it cleans up the environment before exiting.



```
v45 = runtime_concatstring3(
        0,
        "ping 1.1.1.1 -n 1 -w 4000 > Nul & Del \"",
        39,
        *(_DWORD *)dword_98AD50,
        *(_DWORD *)(dword_98AD50 + 4),
        "\" > Nul & del \"%~f0\"",
        20,
        v43);
v39 = runtime_stringtoslicebyte(0, v44, v45, v21, v28, v32);
v49 = v22;
v47 = v29;
v46 = v33;
runtime_concatstring2(0, v50, v48, "\\remove.bat", 11, v33, v39);
MeowStealer_core_CreateFileAndWriteData(v34, v40, v49, v47, v46, v34, v40);
```

Figure 12 - Creates Remove.bat



```
if ( !v35 )
{
  os_Getenv("APPDATA", 7, v15, v23);
  v51[0] = (int)"/C";
  v51[1] = 2;
  runtime_concatstring2(0, v16, v24, "\\remove.bat", 11, 0, v41);
  v51[2] = v36;
  v51[3] = v42;
  os_exec_Command("cmd", 3, v51, 2, 2, v36);
  v17 = runtime_newobject(&syscall_SysProcAttr, v11);
  *v12 = 1;
  v3 = v37;
  if ( dword_9B11C0 )
    runtime_gcWriteBarrier();
  else
    *(_DWORD *)(v37 + 76) = v12;
  os_exec___Cmd__Start(v3, v12, v17);
  os_Exit(69);
}
}
```

Figure 13 - Executes the remove.bat then exits

MITRE ATT&CK

Technique Name	Technique ID
Windows Management Instrumentation	T1047
Command and Scripting Interpreter	T1059
Virtualization/Sandbox Evasion	T1497
Process Discovery	T1057
System Discovery	T1033
Data From Local System	T1005
Application Layer Protocol	T1071

Mitigations

- Limit access to Windows Management Instrumentation (WMI) by restricting privileges to trusted users and applications.
- Implement application whitelisting to control and restrict the execution of scripts and interpreters.
- Employ anti-evasion techniques in virtual environments to detect and prevent sandbox detection.
- Use endpoint security solutions that can detect and block suspicious process discovery activities.
- Limit user privileges and access to sensitive system information.
- Encrypt sensitive data at rest and in transit to protect against data theft.
- Implement network monitoring and analysis to detect unusual or malicious application layer protocol usage.

Detection

For YARA Rules and Indicators of Compromise (IOCs) check our github.

ThreatMon

"See the Invisible"

Advanced Threat Intelligence Platform

With External Attack Surface Management
and Digital Risk Protection

30 Days of Premium Trial

@ThreatMon

@MonThreat

@threatmon

@TMRansomMonitor