Darktrace's Investigation of Raspberry Robin Worm

By Alexandra Sentenac

Published: 2024-04-02 · Archived: 2026-04-05 15:17:46 UTC

Introduction

In the face of increasingly hardened digital infrastructures and skilled security teams, malicious actors are forced to constantly adapt their attack methods, resulting in sophisticated attacks that are designed to evade human detection and bypass traditional network security measures.

One such example that was recently investigated by Darktrace is Raspberry Robin, a highly evasive worm malware renowned for merging existing and novel techniques, as well as leveraging both physical hardware and software, to establish a foothold within organization’s networks and propagate additional malicious payloads.

What is Raspberry Robin?

Raspberry Robin, also known as ‘QNAP worm’, is a worm malware that was initially discovered at the end of 2023 [1], however, its debut in the threat landscape may have predated this, with Microsoft uncovering malicious artifacts linked to this threat (which it tracks under the name Storm-0856) dating back to 2019 [4]. At the time, little was known regarding Raspberry Robin’s objectives or operators, despite the large number of successful infections worldwide. While the identity of the actors behind Raspberry Robin still remains a mystery, more intelligence has been gathered about the malware and its end goals as it was observed delivering payloads from different malware families.

Who does Raspberry Robin target?

While it was initially reported that Raspberry Robin primarily targeted the technology and manufacturing industries, researchers discovered that the malware had actually targeted multiple sectors [3] [4]. Darktrace’s own investigations echoed this, with Raspberry Robin infections observed across various industries, including public administration, finance, manufacturing, retail, education and transportation.

How does Raspberry Robin work?

Initially, it appeared that Raspberry Robin's access to compromised networks had not been utilized to deliver final-stage malware payloads, nor to steal corporate data. This uncertainty led researchers to question whether the actors involved were merely “cybercriminals playing around” or more serious threats [3]. This lack of additional exploitation was indeed peculiar, considering that attackers could easily escalate their attacks, given Raspberry Robin’s ability to bypass User Account Control using legitimate Windows tools [4].

However, at the end of July 2022, some clarity emerged regarding the operators' end goals. Microsoft researchers revealed that the access provided by Raspberry Robin was being utilized by an access broker tracked as DEV-

0206 to distribute the FakeUpdates malware downloader [2]. Researchers further discovered malicious activity associated with Evil Corp TTPs (i.e., DEV-0243) [5] and payloads from the Fauppod malware family leveraging Raspberry Robin's access [8]. This indicates that Raspberry Robin may, in fact, be an initial access broker, utilizing its presence on hundreds of infected networks to distribute additional payloads for paying malware operators. Thus far, Raspberry Robin has been observed distributing payloads linked to FIN11, Clop Gang, BumbleBee, IcedID, and TrueBot on compromised networks [12].

Raspberry Robin's Continued Evolution

Since it first appeared in the wild, Raspberry Robin has evolved from "being a widely distributed worm with no observed post-infection actions [...] to one of the largest malware distribution platforms currently active" [8]. The fact that Raspberry Robin has become such a prevalent threat is likely due to the continual addition of new features and evasion capabilities to their malware [6] [7].

Since its emergence, the malware has "changed its communication method and lateral movement" [6] in order to evade signature detections based on threat intelligence and previous versions. Endpoint security vendors commonly describe it as heavily obfuscated malware, employing multiple layers of evasion techniques to hinder detection and analysis. These include for example dropping a fake payload when analyzed in a sandboxed environment and using mixed-case executing commands, likely to avoid case-sensitive string-based detections.

In more recent campaigns, Raspberry Robin further appears to have added a new distribution method as it was observed being downloaded from archive files sent as attachments using the messaging service Discord [11]. These attachments contained a legitimate and signed Windows executable, often abused by attackers for side-loading, alongside a malicious dynamic-link library (DLL) containing a Raspberry Robin sample.

Another reason for the recent success of the malware may be found in its use of one-day exploits. According to researchers, Raspberry Robin now utilizes several local privilege escalation exploits that had been recently disclosed, even before a proof of concept had been made available [9] [10]. This led cyber security professionals to believe that operators of the malware may have access to an exploit seller [6]. The use of these exploits enhances Raspberry Robin's detection evasion and persistence capabilities, enabling it to propagate on networks undetected.

Through two separate investigations carried out by Darktrace's Threat Research team, first in late 2022 and then in November 2023, it became evident that Raspberry Robin was capable of integrating new functionalities and tactics, techniques and procedures (TTPs) into its attacks. Darktrace DETECT™ provided full visibility over the evolving campaign activity, allowing for a comparison of the threat across both investigations. Additionally, if Darktrace RESPOND™ was enabled on affected networks, it was able to quickly mitigate and contain emerging activity during the initial stages, thwarting the further escalation of attacks.

Raspberry Robin Initial Infection

The most prevalent initial infection vector appears to be the introduction of an infected external drive, such as a USB stick, containing a malicious .LNK file (i.e., a Windows shortcut file) disguised as a thumb drive or network share. When clicked, the LNK file automatically launches cmd.exe to execute the malicious file stored on the external drive, and msiexec.exe to connect to a Raspberry Robin command-and-control (C2) endpoint and

download the main malware component. The whole process leverages legitimate Windows processes and is therefore less likely to raise any alarms from more traditional security solutions. However, Darktrace DETECT was able to identify the use of Msiexec to connect to a rare endpoint as anomalous in every case investigated.

Little is currently known regarding how the external drives are infected and distributed, but it has been reported that affected USB drives had previously been used for printing at printing and copying shops, suggesting that the infection may have originated from such stores [13].

A method as simple as leaving an infected USB on a desk in a public location can be a highly effective social engineering tactic for attackers. Exploiting both curiosity and goodwill, unsuspecting individuals may innocently plug in a found USB, hoping to identify its owner, unaware that they have unwittingly compromised their device.

As Darktrace primarily operates on the network layer, the insertion of a USB endpoint device would not be within its visibility. Nevertheless, Darktrace did observe several instances wherein multiple Microsoft endpoints were contacted by compromised devices prior to the first connection to a Raspberry Robin domain. For example, connections to the URI '/fwlink/?LinkID=252669&clcid=0x409' were observed in multiple customer environments prior to the first Raspberry Robin external connection. This connectivity seems to be related to Windows attempting to retrieve information about installed hardware, such as a printer, and could also be related to the inserting of an external USB drive.

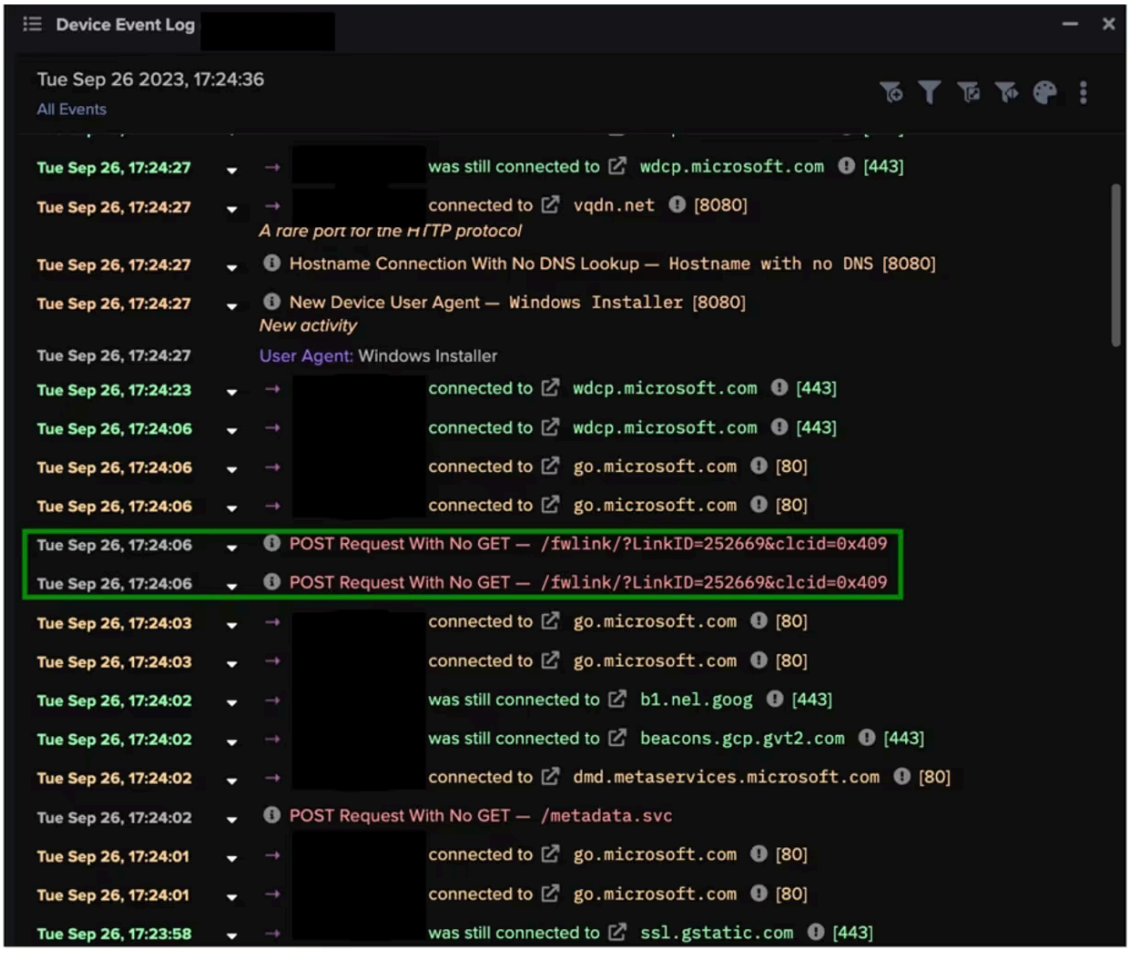

Figure 1: Device Event Log showing an affected device making connections to Microsoft endpoints, prior to contacting the Raspberry Robin C2 endpoint ‘vqdn[.]net’.

Raspberry Robin Command-and-Control Activity

In all cases investigated by Darktrace, compromised devices were detected making HTTP GET connections via the unusual port 8080 to Raspberry Robin C2 endpoints using the new user agent 'Windows Installer'.

The C2 hostnames observed were typically short and matched the regex /[a-zA-Z0-9]{2,4}.[a-zA-Z0-9]{2,6}/, and were hosted on various top-level domains (TLD) such as '.rocks', '.pm', and '.wf'. On one customer network, Darktrace observed the download of an MSI file from the Raspberry Robin domain 'wak[.]rocks'. This package contained a heavily protected malicious DLL file whose purpose was unknown at the time.

However, in September 2022, external researchers revealed that the main purpose of this DLL was to download further payloads and enable lateral movement, persistence and privilege escalation on compromised devices, as well as exfiltrating sensitive information about the device. As worm infections spread through networks automatically, exfiltrating device data is an essential process for threat actor to keep track of which systems have been infected.

On affected networks investigated by Darktrace, compromised devices were observed making C2 connections that contained sensitive device information, including hostnames and credentials, with additional host information likely found within the data packets [12].

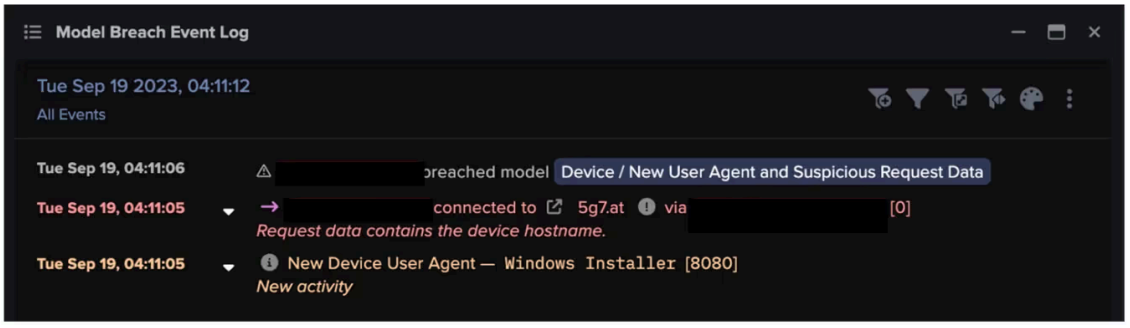

Figure 2: Model Breach Event Log displaying the events that triggered the the 'New User Agent and Suspicious Request Data' DETECT model breach.

As for C2 infrastructure, Raspberry Robin leverages compromised Internet of Things (IoT) devices such as QNAP network attached storage (NAS) systems with hijacked DNS settings [13]. NAS devices are data storage servers that provide access to the files they store from anywhere in the world. These features have been abused by Raspberry Robin operators to distribute their malicious payloads, as any uploaded file could be stored and shared easily using NAS features.

However, Darktrace found that QNAP servers are not the only devices being exploited by Raspberry Robin, with DETECT identifying other IoT devices being used as C2 infrastructure, including a Cerio wireless access point in one example. Darktrace recognized that this connection was new to the environment and deemed it as suspicious, especially as it also used new software and an unusual port for the HTTP protocol (i.e., 8080 rather than 80).

In several instances, Darktrace observed Raspberry Robin utilizing TOR exit notes as backup C2 infrastructure, with compromised devices detected connecting to TOR endpoints.

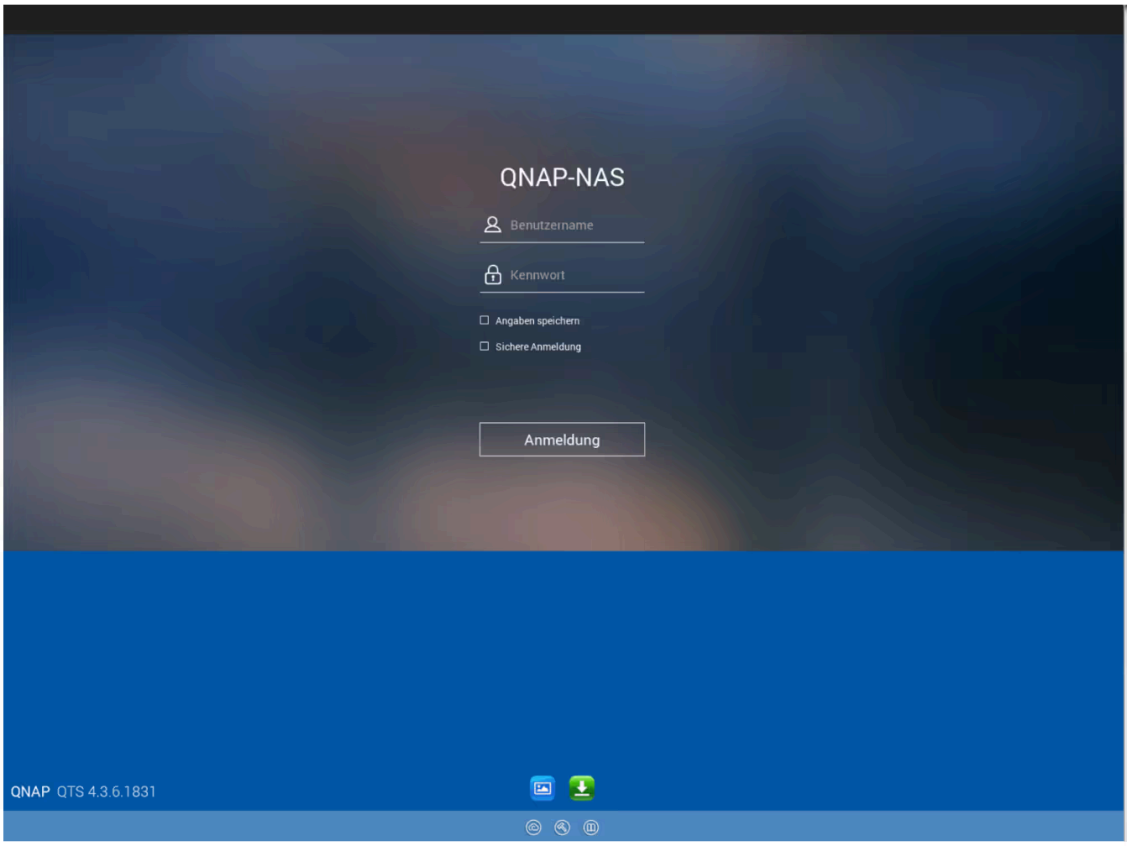

Figure 3: Raspberry Robin C2 endpoint when viewed in a sandbox environment.

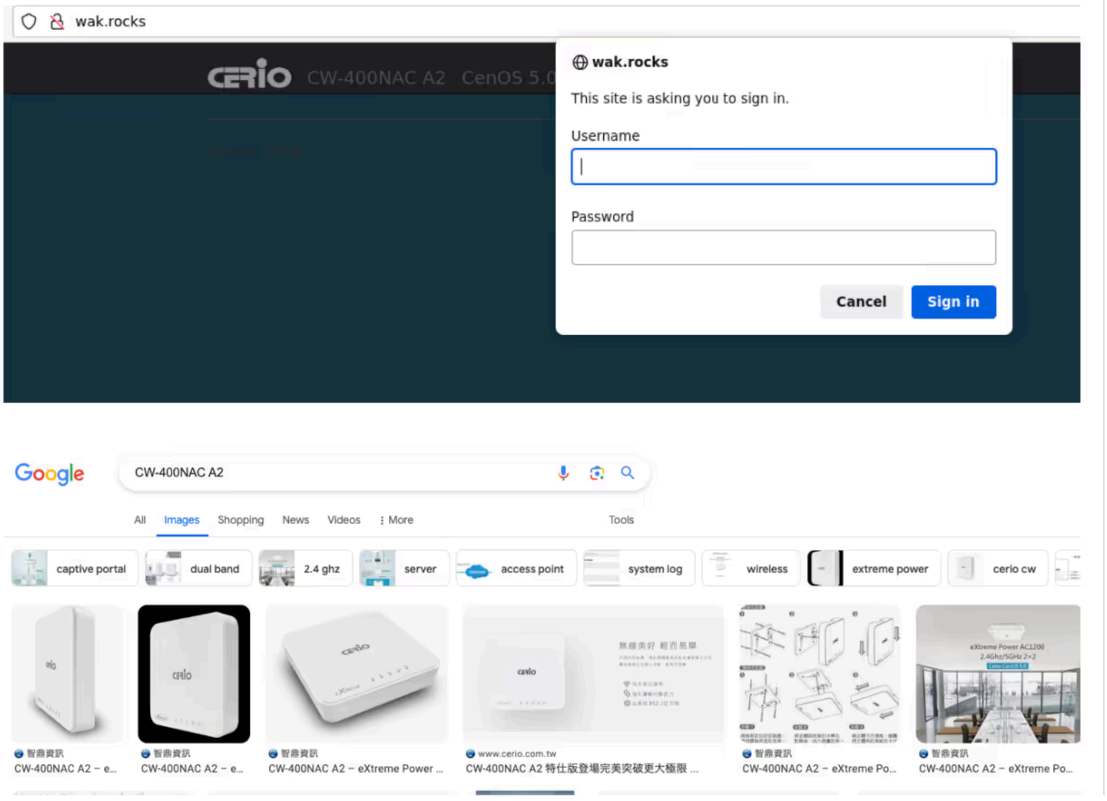

Figure 4: Raspberry Robin C2 endpoint when viewed in a sandbox environment.

Raspberry Robin in 2022 vs 2023

Despite the numerous updates and advancements made to Raspberry Robin between the investigations carried out in 2022 and 2023, Darktrace's detection of the malware was largely the same.

DETECT models breached during first investigation at the end of 2022:

- Device / New User Agent
- Anomalous Server Activity / New User Agent from Internet Facing System
- Device / New User Agent and New IP
- Compromise / Suspicious Request Data
- Compromise / Uncommon Tor Usage
- Possible Tor Usage

DETECT models breached during second investigation in late 2023:

- Device / New User Agent and New IP
- Device / New User Agent and Suspicious Request Data
- Device / New User Agent
- Device / Suspicious Domain
- Possible Tor Usage

Darktrace's anomaly-based approach to threat detection enabled it to consistently detect the TTPs and IoCs associated with Raspberry Robin across the two investigations, despite the operator's efforts to make it stealthier and more difficult to analyze.

In the first investigation in late 2022, Darktrace detected affected devices downloading addition executable (.exe) files following connections to the Raspberry Robin C2 endpoint, including a numeric executable file that appeared to be associated with the Vidar information stealer. Considering the advanced evasion techniques and privilege escalation capabilities of Raspberry Robin, early detection is key to prevent the malware from downloading additional malicious payloads.

In one affected customer environment investigated in late 2023, a total of 12 devices were compromised between mid-September and the end of October. As this particular customer did not have Darktrace RESPOND, the Raspberry Robin infection was able to spread through the network unabated until the customer acted upon Darktrace DETECT's alerts.

Had Darktrace RESPOND been enabled in autonomous response mode, it would have been able to take immediate action following the first observed connection to a Raspberry Robin C2 endpoint, by blocking connections to the suspicious endpoint and enforcing a device's normal 'pattern of life'.

By enforcing a pattern of life on an affected device, RESPOND would prevent it from carrying out any activity that deviates from this learned pattern, including connections to new endpoints using new software as was the case in Figure 5, effectively shutting down the attack in the first instance.

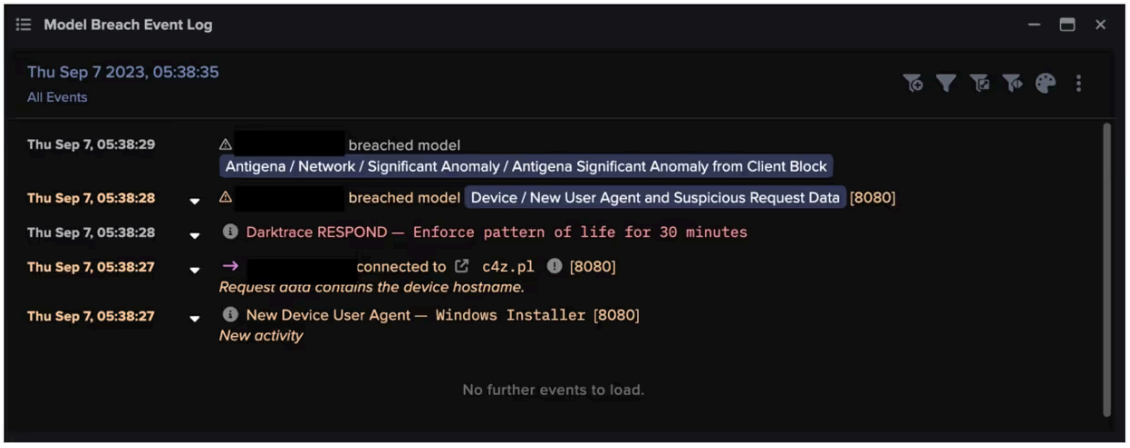

Figure 5: Model Breach Event Log showing RESPOND's actions against connections to Raspberry Robin C2 endpoints.

Conclusion

Raspberry Robin is a highly evasive and adaptable worm known to evolve and change its TTPs on a regular basis in order to remain undetected on target networks for as long as possible. Due to its ability to drop additional malware variants onto compromised devices, it is crucial for organizations and their security teams to detect Raspberry Robin infections at the earliest possible stage to prevent the deployment of potentially disruptive secondary attacks.

Despite its continued evolution, Darktrace's detection of Raspberry Robin remained largely unchanged across the two investigations. Rather than relying on previous IoCs or leveraging existing threat intelligence, Darktrace DETECT's anomaly-based approach allows it to identify emerging compromises by detecting the subtle deviations in a device's learned behavior that would typically come with a malware compromise.

By detecting the attacks at an early stage, Darktrace gave its customers full visibility over malicious activity occurring on their networks, empowering them to identify affected devices and remove them from their environments. In cases where Darktrace RESPOND was active, it would have been able to take autonomous follow-up action to halt any C2 communication and prevent the download of any additional malicious payloads.

Credit to Alexandra Sentenac, Cyber Analyst, Trent Kessler, Senior Cyber Analyst, Victoria Baldie, Director of Incident Management

Appendices

Darktrace DETECT Model Coverage

Device / New User Agent and New IP

Device / New User Agent and Suspicious Request Data

Device / New User Agent

Compromise / Possible Tor Usage

Compromise / Uncommon Tor Usage

MITRE ATT&CK Mapping

Tactic - Technique

Command & Control - T1090.003 Multi-hop Proxy

Lateral Movement - T1210 Exploitation of remote services

Exfiltration over C2 Data - T1041 Exfiltration over C2 Channel

Data Obfuscation - T1001 Data Obfuscation

Vulnerability Scanning - T1595.002 Vulnerability Scanning

Non-Standard Port - T1571 Non-Standard Port

Persistence - T1176 Browser Extensions

Initial Access - T1189 Drive By Compromise / T1566.002 Spearphishing Link

Collection - T1185 Man in the browser

List of IoCs

IoC - Type - Description + Confidence

vqdn[.]net - Hostname - C2 Server

mwgq[.]net - Hostname - C2 Server

wak[.]rocks - Hostname - C2 Server

o7car[.]com - Hostname - C2 Server

6t[.]nz - Hostname - C2 Server

fcgz[.]net - Hostname - Possible C2 Server

d0[.]wf - Hostname - C2 Server

e0[.]wf - Hostname - C2 Server

c4z[.]pl - Hostname - C2 Server

5g7[.]at - Hostname - C2 Server

5ap[.]nl - Hostname - C2 Server

4aw[.]ro - Hostname - C2 Server

0j[.]wf - Hostname - C2 Server

f0[.]tel - Hostname - C2 Server

h0[.]pm - Hostname - C2 Server

y0[.]pm - Hostname - C2 Server

5qy[.]ro - Hostname - C2 Server

g3[.]rs - Hostname - C2 Server

5qe8[.]com - Hostname - C2 Server

4j[.]pm - Hostname - C2 Server

m0[.]yt - Hostname - C2 Server

zk4[.]me - Hostname - C2 Server

59.15.11[.]49 - IP address - Likely C2 Server

82.124.243[.]57 - IP address - C2 Server

114.32.120[.]11 - IP address - Likely C2 Server

203.186.28[.]189 - IP address - Likely C2 Server

70.124.238[.]72 - IP address - C2 Server

73.6.9[.]83 - IP address - Likely C2 Server

References

[1] https://redcanary.com/blog/raspberry-robin/

[2] https://www.bleepingcomputer.com/news/security/microsoft-links-raspberry-robin-malware-to-evil-corp-attacks/

[3] https://7095517.fs1.hubspotusercontent-na1.net/hubfs/7095517/FLINT%202022-016%20-%20QNAP%20worm_%20who%20benefits%20from%20crime%20(1).pdf

[4] https://www.bleepingcomputer.com/news/security/microsoft-finds-raspberry-robin-worm-in-hundreds-of-windows-networks/

[5] https://therecord.media/microsoft-ties-novel-raspberry-robin-malware-to-evil-corp-cybercrime-syndicate

[6] https://securityaffairs.com/158969/malware/raspberry-robin-1-day-exploits.html

[7] https://research.checkpoint.com/2024/raspberry-robin-keeps-riding-the-wave-of-endless-1-days/

[8] https://redmondmag.com/articles/2022/10/28/microsoft-details-threat-actors-leveraging-raspberry-robin-worm.aspx

[9] https://www.bleepingcomputer.com/news/security/raspberry-robin-malware-evolves-with-early-access-to-windows-exploits/

[10] https://www.bleepingcomputer.com/news/security/raspberry-robin-worm-drops-fake-malware-to-confuse-researchers/

[11] https://thehackernews.com/2024/02/raspberry-robin-malware-upgrades-with.html

[12] https://decoded.avast.io/janvojtesek/raspberry-robins-roshtyak-a-little-lesson-in-trickery/

[13] https://blog.bushidotoken.net/2023/05/raspberry-robin-global-usb-malware.html

---