

脅威インサイトレポート

Q2 - 2022

Fake postal notifications deliver AsyncRAT through HTML smuggling

One of the most popular lures we see are fake delivery notifications. In Q2, we analyzed a malware campaign spreading AsyncRAT that imitated Israel Post. In this case, an employee received an email purportedly from Israel Post to their personal email address. Using webmail, the user opened the malicious HTML attachment on a business computer. Since the attachment was downloaded from the web, HP Wolf Security treated the file as untrusted and opened it in a micro-VM, isolating the threat by design. Using personal webmail on business computers can be risky, as this example shows, since webmail providers typically offer less protection than an organization's email gateway.

The threat actor used the HTML smuggling (T1027.006) technique to deliver an ISO archive to the user by embedding it in the HTML attachment.¹² If the HTML attachment is opened, the user's web browser prompts them to download the ISO file. When the user opens the ISO file, it is mounted as a drive. There is only one file inside, a Visual Basic script. The script is obfuscated and runs a PowerShell command, which in turn downloads a file from the web and executes it. The downloaded file is a PowerShell script. It contains two encoded executables, a dynamic link library (DLL) and an .exe.

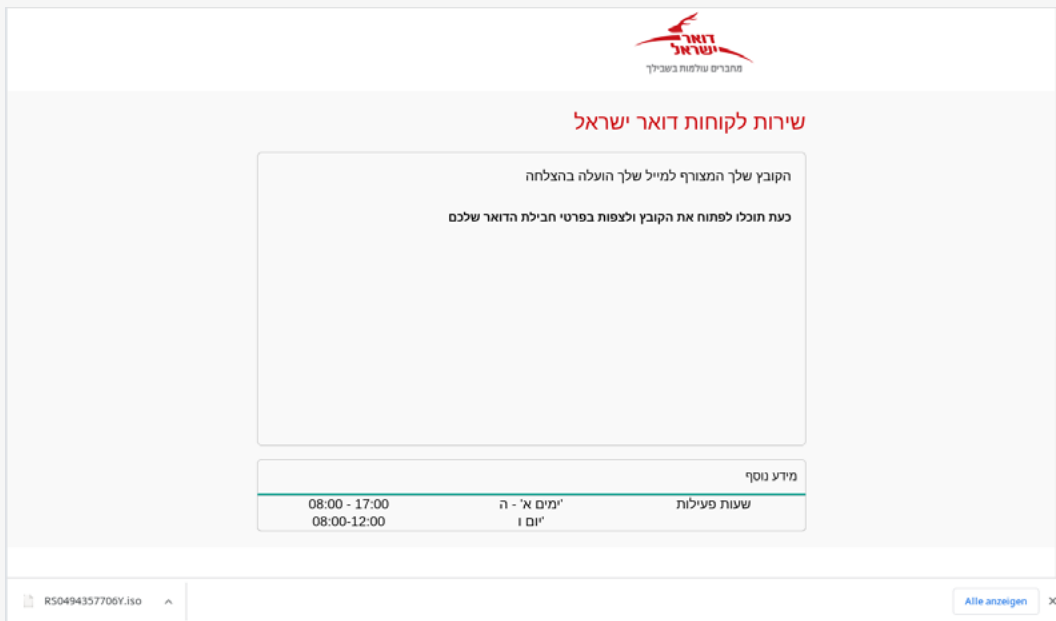


Figure 4 - HTML attachment used to deliver .iso file

When the script is run, a web browser window opens the Israel Post website as a diversion. Meanwhile, in the background, the malware saves a Visual Basic script, a batch script, a PowerShell script and the two executables to a local folder and then executes the Visual Basic script. This triggers an infection chain where one script after another runs until finally, the DLL is loaded using PowerShell. After the DLL is loaded into memory, a method is called, passing a process name and the location of the .exe as arguments. The DLL uses the RunPE technique to inject the .exe into the chosen process, in this case, aspnet_compiler.exe.¹³

The injected malware is AsyncRAT, a popular .NET remote access trojan (RAT) that can monitor and control the infected system.¹⁴ Its capabilities include data collection and exfiltration. Unlike most .NET malware samples, the sample delivered in the campaign was not obfuscated, making it a straightforward task to extract its configuration. The configuration is encrypted using AES, but since the key is stored in the malware, it can be decrypted and used for threat hunting.¹⁵

Notable Techniques

Shellcode hidden in documents spreads SVCReady Loader

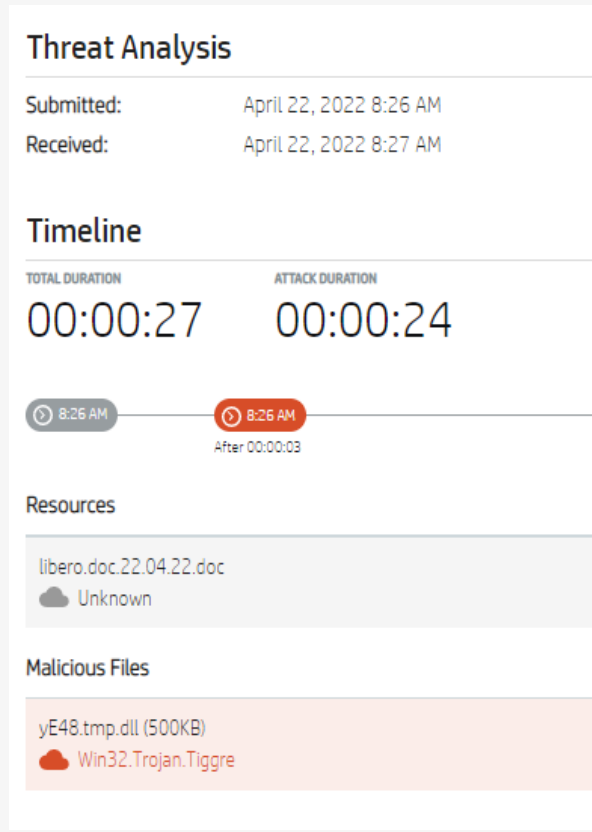


Figure 5 - SVCReady sample isolated by HP Wolf Security in April 2022

At the end of April, we spotted new malicious spam campaigns spreading a previously unknown malware family called SVCReady Loader.¹⁶ The malware is notable for the unusual way it is delivered to target PCs - using shellcode hidden in the properties of Microsoft Office documents - and because it is likely in an early stage of development, given that its authors updated the malware several times in May.

The documents contain Visual Basic for Applications (VBA) AutoOpen macros that are used to execute malicious code. But unlike most other Office malware, the document does not use PowerShell or MSHTA to download further payloads from the web. Instead, the VBA macro runs shellcode stored in the properties of the document, which then drops and runs SVCReady Loader. The malware is a DLL that is started using rundll32.exe. Its primary function is to download other payloads to the infected computer, with additional features for collecting system information, taking screenshots, and communicating this information back to a C2 server.

Communication with the C2 server occurs via HTTP, but the data is encrypted using the RC4 cipher. Interestingly, RC4 encryption was not implemented in the first malware samples we analyzed in April. This suggests that the C2 encryption was only added during May and that the malware is being actively developed. The malware suffers software bugs, notably in its persistence mechanism and duplication in the reconnaissance data it collects. This, as well as the low frequency and volume of the campaigns, suggest that the malware is in the early stages of development.

Email-borne malware detected by HP Wolf Security that had bypassed an email gateway scanner

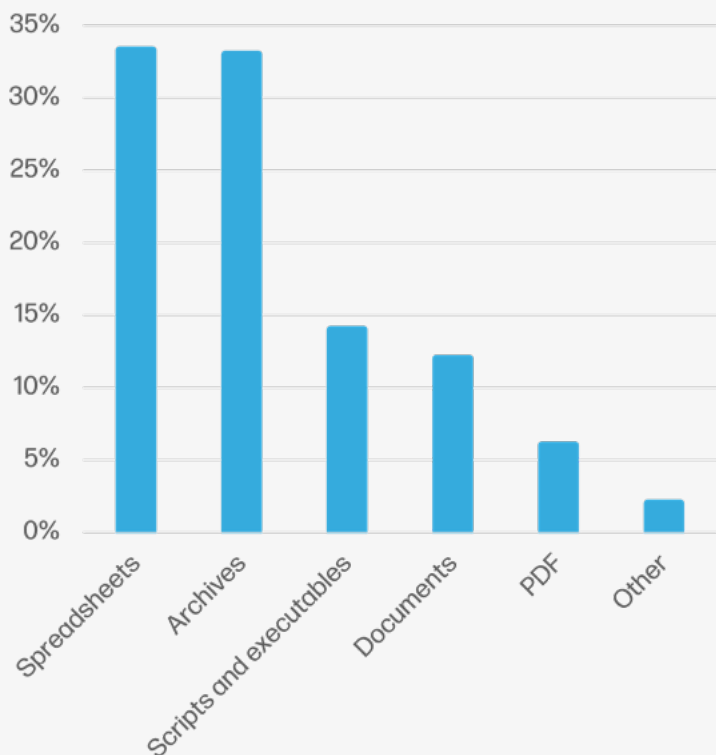
14%

Notable Trends

Rise in malware inside archives isolated over previous quarter

11%

Top malware file types



Attackers shift to “macro-free” formats to distribute malware

For years, attackers have relied on malicious macros as the first step to infect target computers. In February, Microsoft announced that Office will disable macros in documents downloaded from the web by default, effectively closing off this technique to attackers.¹⁷ In Q2, we have seen threat actors respond to this change by experimenting with alternative, macro-free code execution techniques.

One significant change was in the distribution of Emotet on 22 April when its operators started testing shortcut (.lnk) files to deliver the malware instead of Office documents. The new shortcut files work by specifying a command in the target path of the shortcut file, which downloads and runs the malware from the web. An early version of these malicious shortcut files used the “findstr” command to extract and run a Visual Basic script appended to the shortcut file. In Q2, we also saw variants where the commands are batch or PowerShell scripts.

In 2022, we have seen other threat actors spreading malware families through shortcut files, including OakBot, IcedID, Bumblebee, NjRAT and RedLine Stealer. Responding to the demand for tooling, since mid-June several shortcut file malware builders have appeared for sale on hacking forums. These builders are designed to make it easy to create weaponized shortcut files to spread malware.

11% increase in archive threats over Q1

There was an 11% increase in threats delivered in archives and a 15% drop in scripts and executables since Q1. This was likely due to attackers placing malware inside archives before sending them to targets, such as malicious .lnk shortcuts being stored in .zip archives. Archive file formats are far more likely to be allowed through email gateways and can be encrypted, increasing attackers’ ability to reach users and bypass security controls that rely on scanning to detect malicious content.

Top threat vectors

69%

Email

17%

Web browser downloads

14%

Other

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.^{18 19}

Shipment lures on the rise

Q2 saw a rise in shipment-themed malware campaigns delivering RATs such as Agent Tesla, with “shipment” (8th) and “DHL” (9th) rising into the top 10 most common malicious email subject keywords.

Spreadsheets remain top malware file type

Spreadsheets remained the top file type for delivering malware across all vectors in Q2, with the most popular lures being business transactions. This file type was favored by ongoing Emotet campaigns targeting organizations in the Asia Pacific region.

Malicious portable executables are still making it past email gateways

In Q2, the top five malware file formats for threats delivered by email were .xlsx, .xls, .rar, .zip and .doc. For threats delivered by web browsers, the most popular malware formats were .exe, .msi, .rar, .zip and .pdf. Unsurprisingly, this suggests attackers are using formats that are familiar to users. More surprisingly, 1% of threats delivered by email in Q2 were .exe's, indicating that some organizations aren't blocking risky file formats at their email gateways.

- 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.²⁰
- 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.²¹ For the latest threat research, head over to the HP Wolf Security blog.²²

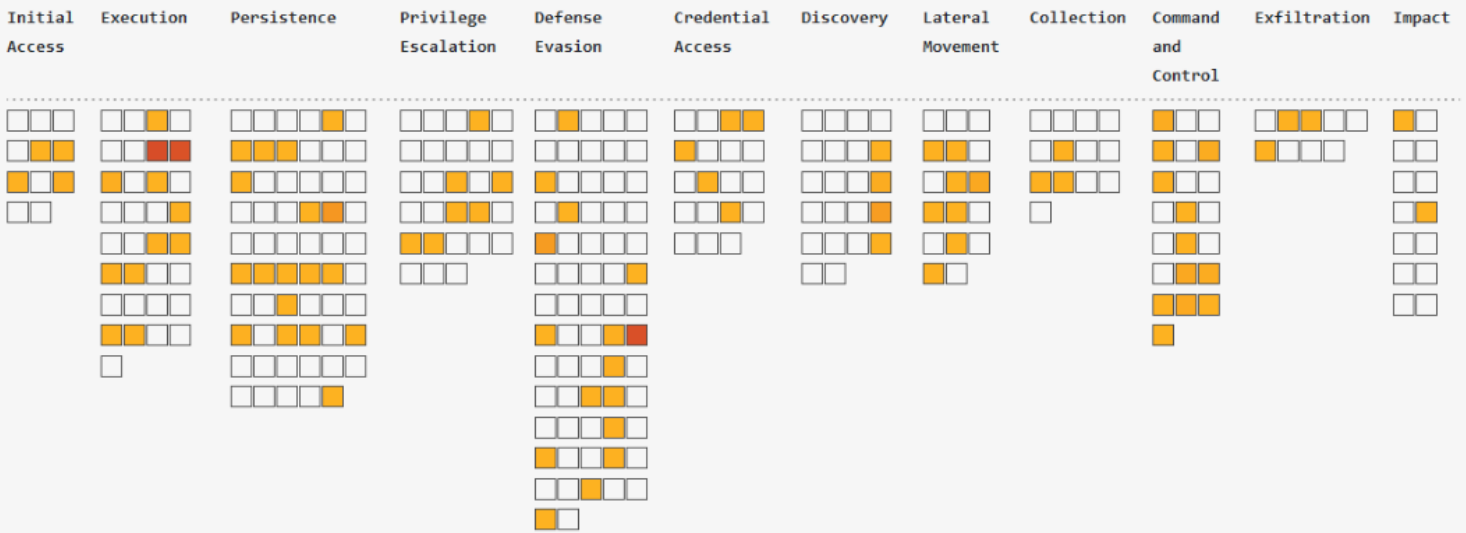


Figure 6 - MITRE ATT&CK heatmap of adversary techniques isolated by HP Wolf Security in Q2 2022²³

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[®] 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://www.techspot.com/news/94766-new-follina-zero-day-vulnerability-microsoft-office-works.html>
- [3] <https://www.bleepingcomputer.com/news/security/windows-msdt-zero-day-now-exploited-by-chinese-apt-hackers/>
- [4] <https://www.bleepingcomputer.com/news/security/russian-hackers-start-targeting-ukraine-with-follina-exploits/>
- [5] <https://therecord.media/hackers-using-follina-windows-zero-day-to-spread-qbot-malware/>
- [6] <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190>
- [7] [https://www.morphisec.com/hubfs/2020 State of Endpoint Security Final.pdf](https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf)
- [8] <https://benjamin-altpeter.de/doc/thesis-electron.pdf>
- [9] <https://thepeninsulaqatar.com/article/20/06/2022/expo-2023-doha-will-be-second-largest-global-event-in-qatar-official>
- [10] <http://www.webdav.org/specs/rfc4918.html>
- [11] [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/gg651155\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/gg651155(v=ws.11))
- [12] <https://attack.mitre.org/techniques/T1027/006/>
- [13] <https://www.malwarebytes.com/glossary/runpe-technique>
- [14] <https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat>
- [15] <https://github.com/hpthreatresearch/iocs/blob/main/asyncrat/iocs.txt>
- [16] <https://threatresearch.ext.hp.com/svcready-a-new-loader-reveals-itself/>
- [17] <https://docs.microsoft.com/en-us/deployoffice/security/internet-macros-blocked>
- [18] <https://enterprisesecurity.hp.com/s/article/Threat-Forwarding>
- [19] <https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence>
- [20] <https://enterprisesecurity.hp.com/s/>
- [21] <https://github.com/hpthreatresearch/>
- [22] <https://threatresearch.ext.hp.com/blog>
- [23] <https://attack.mitre.org/>

LEARN MORE AT HP.COM



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.