HP WOLF SECURITY

Threat Insights Report

Q3 - 2022

Threat Landscape

Welcome to the Q3 2022 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

Malware delivered in archives

42%

- Archives are now the most popular file type for delivering malware, seeing a 12% growth in samples isolated compared to Q2, overtaking Office formats for the first time
- Attackers are bypassing perimeter network security controls, such as email gateway scanners, by encrypting malicious payloads inside archives and HTML files
- Threat actors are increasingly using script-based malware formats to run malicious code on PCs and are relying heavily on built-in operating system utilities to evade endpoint defenses
- Attackers are spending more effort creating effective social engineering templates, often by copying well-known brands and online services, to deliver malware through HTML smuggling

Notable Threats

Malware distributors rely on HTML smuggling to infect systems

After a hiatus in August 2022, HP Wolf Security detected an uptick in QakBot malware campaign activity in early September. QakBot is a highly capable malware family that has been used by threat actors to steal data and deploy ransomware.[2] Notably, most of these new campaigns rely on HTML smuggling to infect systems, marking a move away from malicious Office documents as the preferred delivery mechanism for this malware family.

In these campaigns, malicious HTML files masquerading as PDF documents were sent to victims by email. Opening the HTML file causes the target's web browser to show a fake online document viewer. The web page decodes a ZIP archive, which is offered for download by the user.

The archive is encrypted, requiring the user to enter the password shown on the web page. Encrypting malware inside archives benefits attackers because perimeter network security controls, such as email gateway scanners, cannot inspect encrypted files without the password. The result is that encrypted archives containing malware are far more likely to reach the users' inboxes without being blocked, increasing the risk of a successful infection.

Inside the archive is a malicious shortcut file (LNK). If opened, the shortcut runs malicious commands that download and execute the QakBot payload in the form of a dynamic link library (DLL). The malware is launched using regsvr32.exe (T1218.010), a tool built into Windows for registering DLLs within the operating system but also commonly abused by attackers to run malicious code.[3]

Unlike the HTML smuggling seen earlier this year, the samples in this campaign used templates that abuse well-known brands and services to trick users into running the malware. We expect HTML smuggling design variations and brand abuse to accelerate as attackers experiment to find the most effective lures.

Fake online document viewers are proving to be a popular lure template among threat actors. The distributors of IcedID, another malware family known to lead to human-operated ransomware attacks, adopted a template almost identical to QakBot's to deliver the malware.

Documents

Image	Similarity Hash	Malware	Date	File Types
	003f3f3f3f3f0000	IcedID	2022-11-07	text/html
	003f3f3f3f3f0000	IcedID	2022-11-01	text/html
	3e3f3e3f3f3e0000	IcedID	2022-11-01	text/html

Figure 1 - IcedID HTML smuggling templates

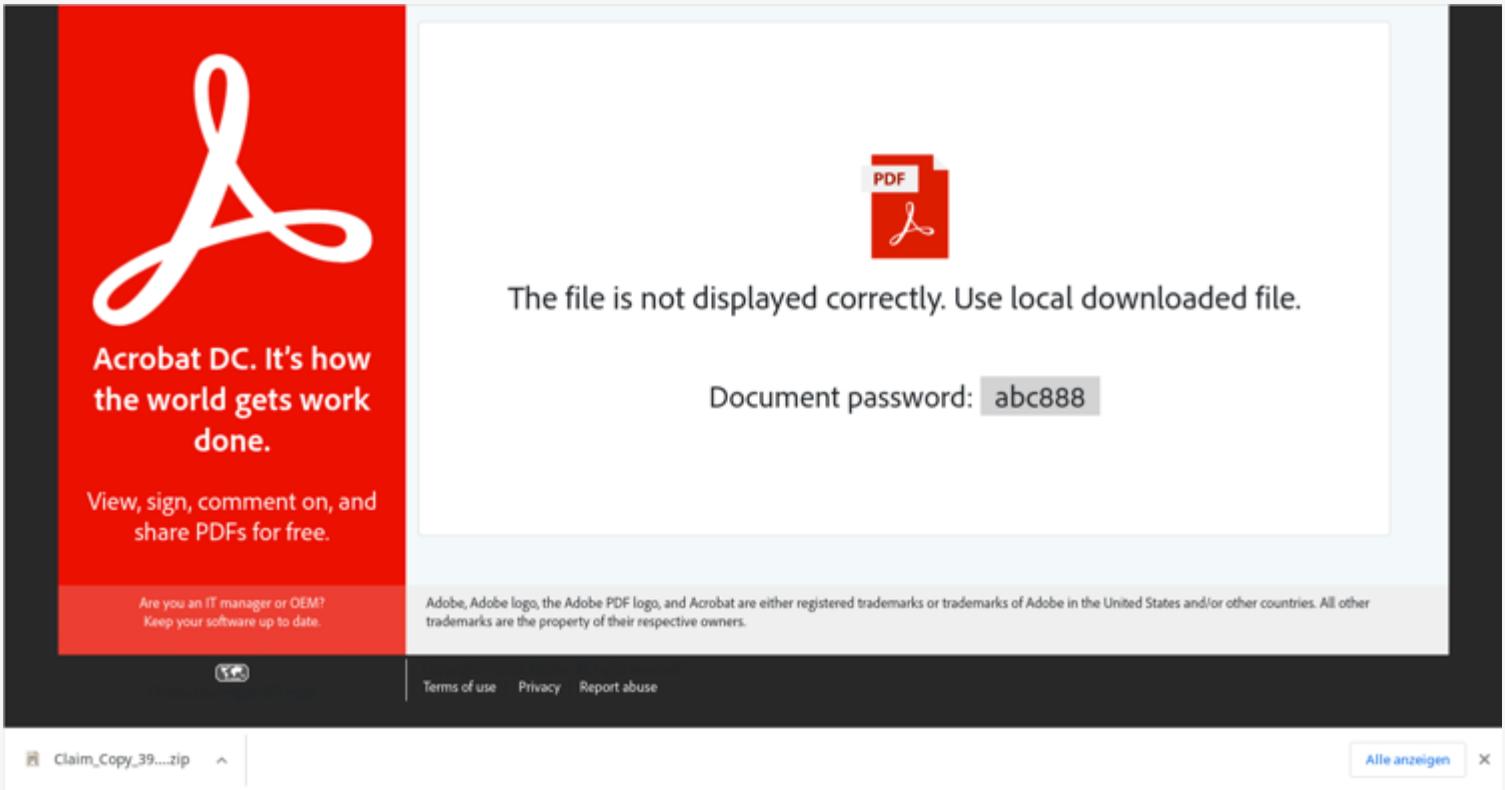


Figure 2 - Fake document viewer used to trick victims into infecting systems with QakBot

Stealthy OpenDocument malware deployed against Latin American hotels

In late June, HP Wolf Security isolated an unusually stealthy malware campaign that used OpenDocument text (.odt) files to spread AsyncRAT, an open-source remote access Trojan (RAT) written in C#.[4] The campaign targeted the hotel industry in Latin America through emails that purported to be booking requests.

OpenDocument is an open, vendor-neutral file format compatible with several popular office productivity suites, including Microsoft Office, LibreOffice and Apache OpenOffice. The malicious document was sent as an email attachment. If the user opens the document, they are shown a prompt asking whether fields with references to other files should be updated. An Excel file opens if they click "Yes" to this prompt.

Afterwards, the user is shown another prompt asking whether macros should be enabled or disabled. If the user allows macros, this triggers the infection chain. The Visual Basic for Applications (VBA) macro inside the Excel documents is lean, running a command using the mshta.exe (T1218.005) tool built into Windows that downloads and executes additional code from the web.[5]

At this point, a complex chain of PowerShell, VBScript and batch scripts are started, finally decoding and executing AsyncRAT.[6] A scheduled task is created to make the malware persistent on the infected PC. The task re-launches the malware every two hours.

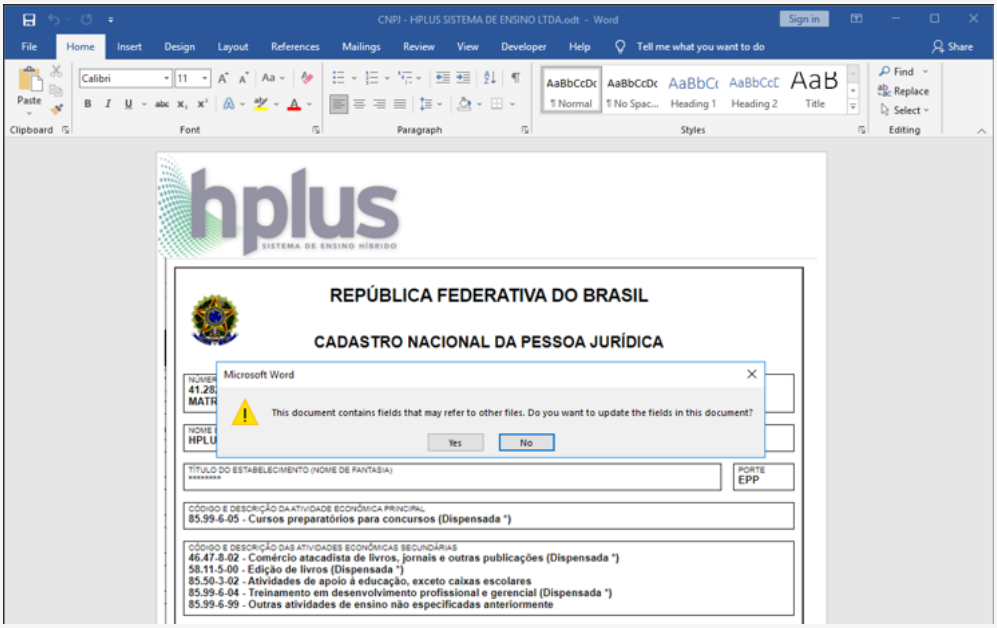


Figure 3 - Lure document asking user to update fields in the document

Unlike many malicious documents, analyzing the OpenDocument file reveals no hidden macros. However, the document references Object Linking and Embedding (OLE) objects hosted remotely. In total, the document references 20 documents hosted on a domain, webnar[.]info.

The use of OpenDocument files to distribute malware was notable because threat actors seldom use this format in campaigns. Strikingly, the malicious document was poorly detected by anti-virus scanners, with a 0% detection rate for more than a week after the sample was uploaded to VirusTotal.

Attackers are always hunting for stealthy ways of evading endpoint security to deploy malware. This campaign illustrates how OpenDocument text files can be abused to deliver malware through external OLE references with extremely low detection rates.

Magniber and threat of single-client ransomware

In recent years, "Big Game Hunting" ransomware attacks against enterprises have dominated media headlines because of their high-profile victims and substantial ransom demands. Yet single-client ransomware – a type of ransomware that infects individual computers, rather than fleets of devices – can still cause significant damage to individuals and organizations.

In September, HP Wolf Security isolated a ransomware campaign masquerading as software updates that targeted home users. The campaign spread Magniber, a single-client ransomware family known to demand $2,500 from victims.[7] Notably, the attackers used clever techniques to evade detection, such as running the ransomware in memory, bypassing User Account Control (UAC) and avoiding detection by using syscalls instead of standard Windows API libraries.

The infection chain starts with a web download from an attacker-controlled website. The user is asked to download a ZIP archive containing a JavaScript file purporting to be an important anti-virus or Windows 10 software update. Previously Magniber was spread through MSI and EXE files, but in September distribution of the ransomware switched to JavaScript.

The attackers used a variation of the DotNetToJScript technique, allowing a .NET executable to be loaded in memory, meaning the ransomware is not saved to disk.[8] This technique bypasses security tools that monitor files written to disk and reduces artifacts left on an infected system.

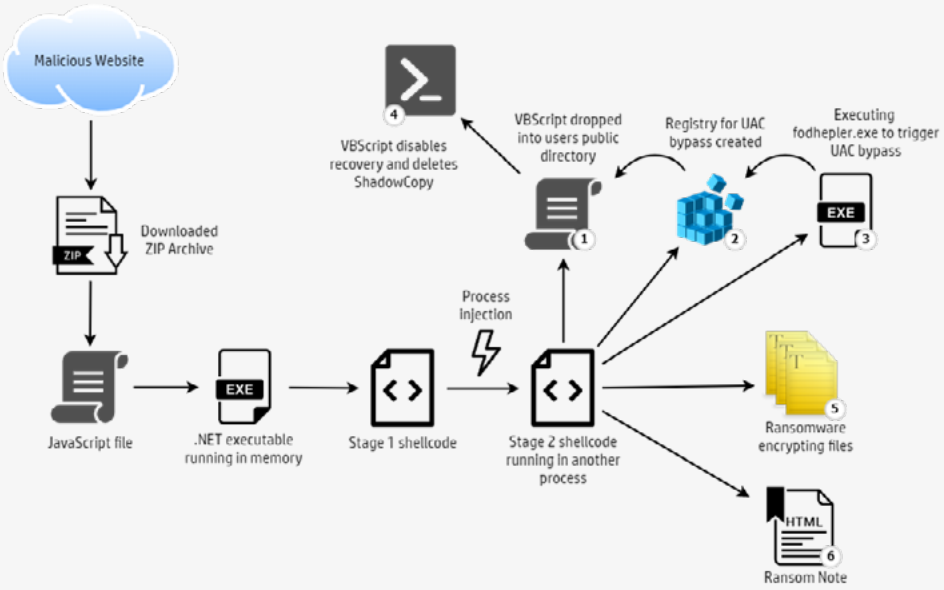


Figure 4 - Magniber infection chain

The .NET code decodes shellcode and injects it into another process. The ransomware code runs from this process – first deleting shadow copy files and disabling Windows' backup and recovery features, before encrypting the victim's files.

Magniber requires administrator privileges to disable the victim's ability to recover their data, so the malware uses a User Account Control (UAC) bypass using fodhelper.exe to run commands without alerting the user. For this to work, the logged-in user must be part of the Administrators group.

Interestingly, the Magniber build in this campaign campaign supports recent versions of Windows, including Windows 11 and pre-release versions. This suggests home users rather than enterprises were the intended targets of the campaign, since enterprises tend to use older operating systems.

For the encryption task, the malware enumerates files and checks its file extension against a list. If the extension is in the list, the file is encrypted. Finally, the malware places a ransom note in each directory with an encrypted file and shows it to the victim by opening the demand in a web browser.

Modular infection chain infects PCs with RATs and cryptocurrency miners

In mid-September, we detected a malware campaign that relied on an unusually complex infection chain to infect systems with malware. The campaign started typically enough - with an email and a Microsoft Word attachment sent to a target. The sender address was spoofed to increase its credibility and the attachment successfully evaded spam filters, reaching the user's inbox.

When opened, the document asks to user to allow an embedded Excel spreadsheet to be loaded. If allowed, the spreadsheet uses mshta.exe to download and run malicious encoded files hosted on file sharing websites. Depending on the sequence, these files contain encoded PowerShell and batch scripts or executable files.

In one of the more interesting sequences, a PowerShell script saves a setup information file (INF) file and another PowerShell script to the infected system. The malware then launches the built-in Microsoft Connection Manager Profile Installer (cmstp.exe) utility to install the INF file and run the PowerShell script linked in it.

This results in another PowerShell script that bypasses the Antimalware Scan Interface (AMSI) in Windows and runs a batch script. The script defines file and process exceptions for Microsoft Defender, creates a local admin user, disables the intrusion prevention system and the local firewall. Lastly, the script attempts to stop Microsoft Defender and delete its service.

Other sequences in the infection chain are used to deploy Agent Tesla, AsyncRAT and a cryptocurrency miner.[9] The attackers hosted different components of the malware campaign on remote web servers and used a variety of techniques to execute the payload malware. This modular approach benefits attackers because it enables payloads to be swapped out easily and for the exection flow to be modified mid-campaign.

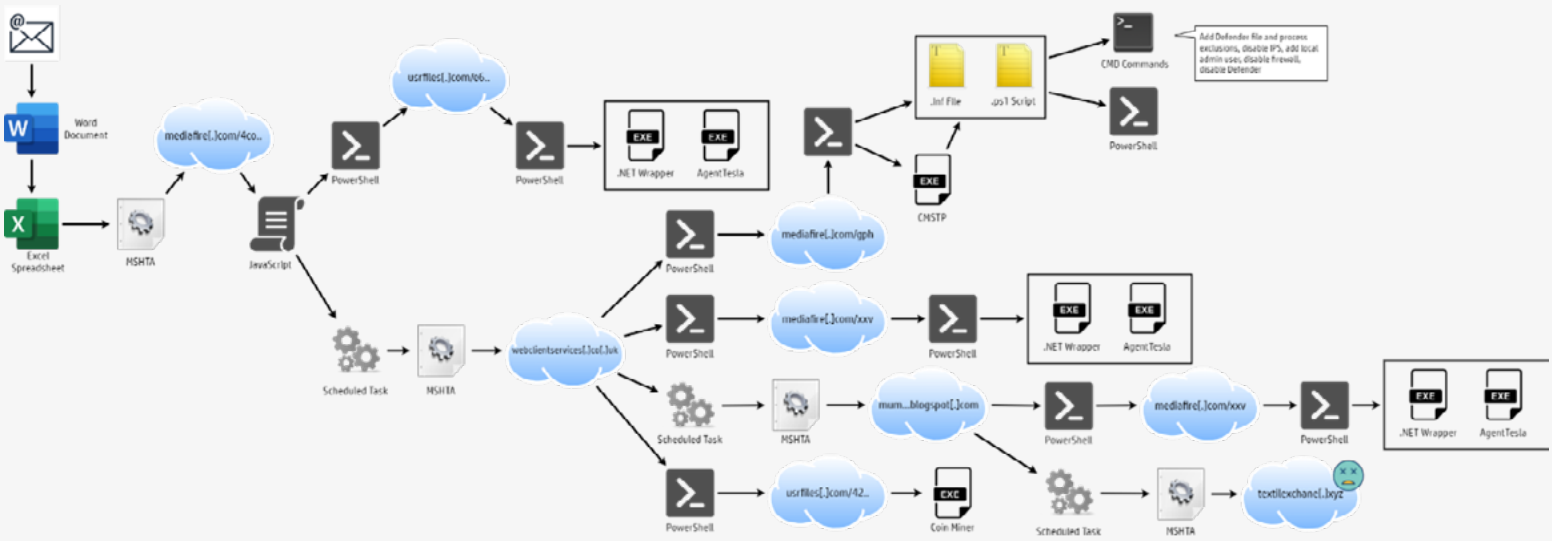


Figure 5 - Infection chain leading to different payloads

Notable Techniques

Magniber bypasses signature validation

Figure 6 - Corrupted Magniber signature

Within the Windows ecosystem, downloaded files are marked based on their origin using an indicator called the Mark-of-the-Web (MOTW).[10] This feature enables Windows to determine if a file originated from a risky location, such as the Internet. Tracking the origin of files is useful because it enables the operating system to warn users if they open a file from an untrusted location.

One exception to a warning being shown is when the downloaded file has been digitally signed. During our analysis of the Magniber ransomware campaign seen in September 2022, we noticed the JavaScript files did not trigger such a warning, despite being downloaded from a website.

Analyzing the JavaScript malware found that the attackers had signed the files with a corrupt signature, mostly likely with the intention of bypassing the risky origin warning dialogue. Specifically, the signature contained several corrupt fields, including invalid certificate dates and an object length that was inconsistent with the segment length definition.

As a result of the corrupted signature, the Magniber samples did not trigger a security warning, thereby removing a barrier to infection.

File formats used to deliver malware

150

Malware delivered in Office formats

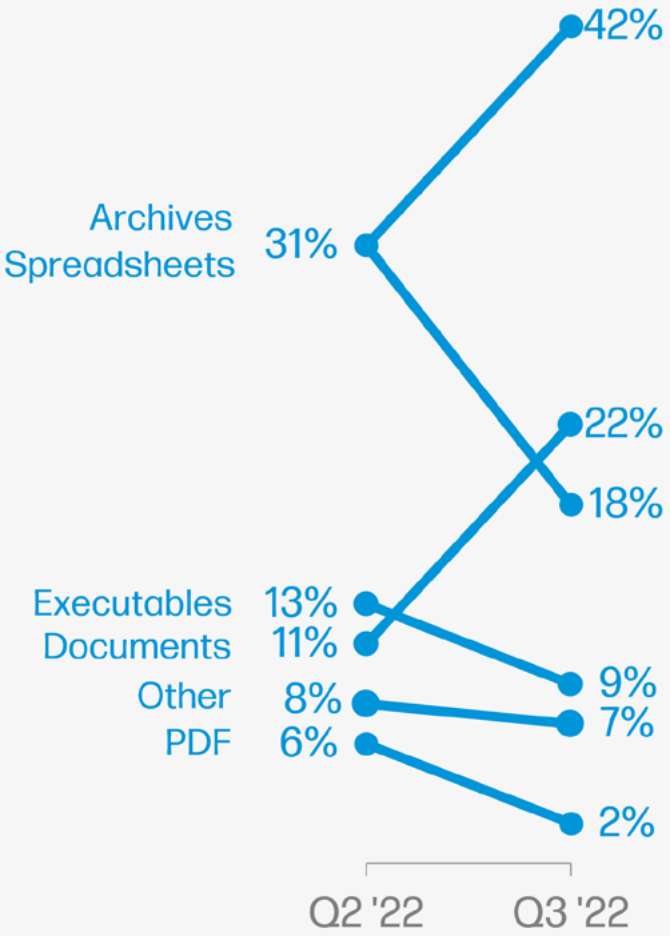
40%

Notable Trends

Rise in archive malware over Q2

12%

Top malware file types



Archives overtake malicious documents as most popular malware file type

In Q3, 42% of malware was delivered in archive file formats, such as ZIP and RAR - overtaking Office formats (down 2% from Q2 at 40%) as the most popular malware file type. The popularity of the archive formats has surged in 2022, rising 23% since Q1, as threat actors increasingly move to script-based malware. Archives are attractive to threat actors because they are easily encrypted, making them difficult for web proxies, sandboxes and email scanners to detect malware. Moreover, many organizations use encrypted archives for legitimate reasons, making it challenging to reject encrypted archive email attachments by policy. As a result, archives are increasing the ability of attackers to reach users' inboxes and bypass security controls that rely on scanning to detect malicious content.

Email remains most dangerous delivery vector

Email remained the top malware delivery vector in Q3, accounting for 69% of all threats detected by HP Wolf Security. In fact, excluding potentially unwanted applications, 88% of threats were sent by email, emphasizing how dangerous this vector is for most users. Q3 saw a 1% rise in threats delivered by web browser downloads and a 1% fall in other vectors compared to Q2.

Top threat vectors

69%

Email

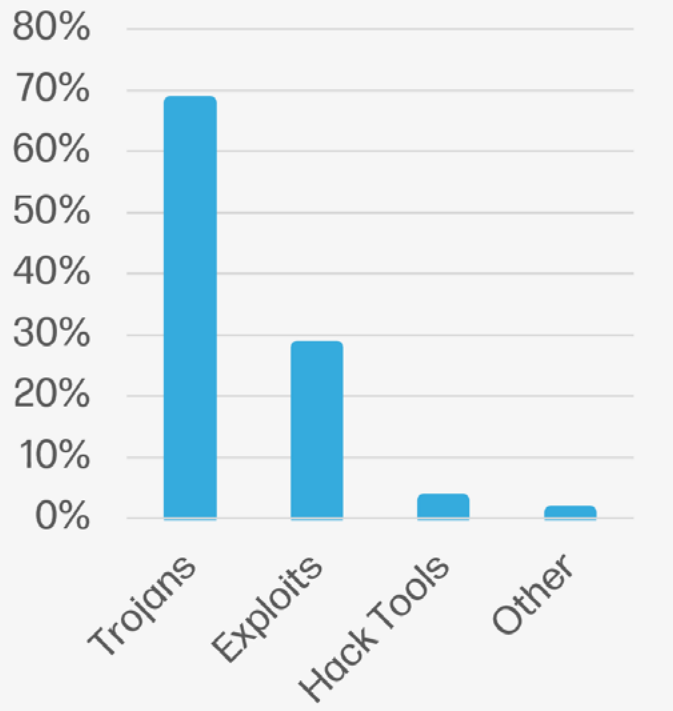
18%

Web browser downloads

13%

Other

Top malware types



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.[11] [12]
- 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.[13]
- 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.[14] For the latest threat research, head over to the HP Wolf Security blog.[15]

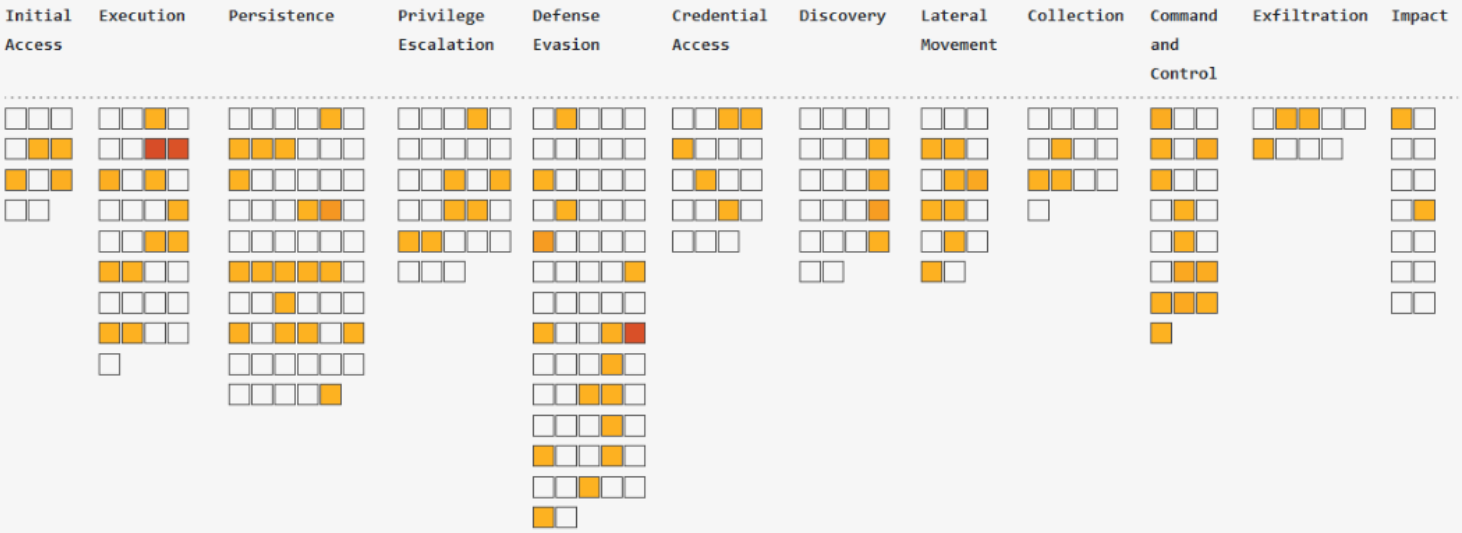


Figure 6 - MITRE ATT&CK heatmap of adversary techniques isolated by HP Wolf Security in Q3 2022[16]

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/T1218/010/

[4] https://threatresearch.ext.hp.com/stealthy-opendocument-malware-targets-latin-american-hotels/

[5] https://attack.mitre.org/techniques/T1218/005/

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

[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.magniber

[8] https://github.com/tyranid/DotNetToJScript

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

[10] https://attack.mitre.org/techniques/T1553/005/

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

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

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

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

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

[16] https://attack.mitre.org/