

Threat Insights Report

Q1 - 2023



Threat Landscape

Welcome to the Q1 2023 edition of the HP Wolf Security Threat Insights Report

Executive Summary

Email threats that bypassed email gateway security

14%

Notable Threats

OneNote abused by attackers to deliver malware

Each quarter our security experts highlight notable malware campaigns, trends and techniques identified by HP Wolf Security. By isolating threats that have evaded detection tools and made it to endpoints, HP Wolf Security gives an insight into the latest techniques cybercriminals use, equipping security teams with the knowledge to combat emerging threats and improve their security postures.¹

- Q1 saw threat actors spreading malware through OneNote notebooks to bypass macro restrictions affecting some Microsoft Office file formats. The attacks trick victims into clicking on fake UI elements, triggering malicious scripts that download and infect PCs with backdoors and remote access trojans (RATs).
- In March, HP Wolf Security detected a new ChromeLoader malware campaign infecting victims with malicious Google Chrome extensions. The new variant, ChromeLoader Shampoo, is distributed through websites hosting pirated films and video games. The malware's capabilities include redirecting search queries and injecting adverts into browsing sessions, so it is likely its operators are motivated by financial gain.
- Malware delivery techniques and file types continued to diversify in Q1, with some malicious spam distributors switching file types weekly. The volume of gzip and HTML threats seen by HP Wolf Security rose significantly in Q1, growing by 53% and 37% over Q4.
- Attackers tried to bypass Office's macro restrictions in Q1 by using compromised Microsoft 365 accounts to send malicious emails to co-workers. The attackers attempted to infect PCs with Formbook, a malware family sold on hacking forums capable of recording keystrokes and stealing sensitive information.

In January, the distributors of QakBot and IcedID crimeware – common precursors to human-operated ransomware attacks – started spreading their malware through malicious Microsoft OneNote notebooks.^{2 3} OneNote is a popular free note-taking and collaboration application. Its file format, indicated by the file extension .one, can store many types of multimedia.⁴ Users can easily embed content within notebooks and share them with others by email.

Unfortunately, attackers are abusing OneNote's ability to embed content to spread malware. As is typical with malware involving Office, PDF and HTML files, attackers rely on social engineering images that look like legitimate program prompts and UI elements to trick victims into running malicious code on their PCs.

In the OneNote malware campaigns observed in Q1, users see a message asking them to double-click a button that will supposedly load all the files in the notebook. However, lurking behind the button is a malicious script that downloads and infects the PC with malware. Attackers have used different scripting languages and obfuscation techniques to evade detection, including PowerShell, batch, and JScript in Windows Script Files (WSF) and HTML Applications (HTA).

In Q1, this method of delivering malware also became more popular among attackers spreading commodity malware like remote access trojans and information stealers. In mid-March, distributors of Emotet, the notorious crimeware family, also briefly returned with new spam campaigns using OneNote notebooks.⁵ However, the campaigns did not last long, and the botnet fell silent again after about two weeks.

OneNote notebooks will likely remain a popular vehicle for spreading malware because attackers can run malicious code without relying on macros. Enterprises and individuals should check and implement defenses to block this infection vector. For example, if you don't expect to receive notebooks by email from people outside your organization you can configure an HP Sure Click Enterprise policy to stop users from trusting notebooks from risky external sources.⁶

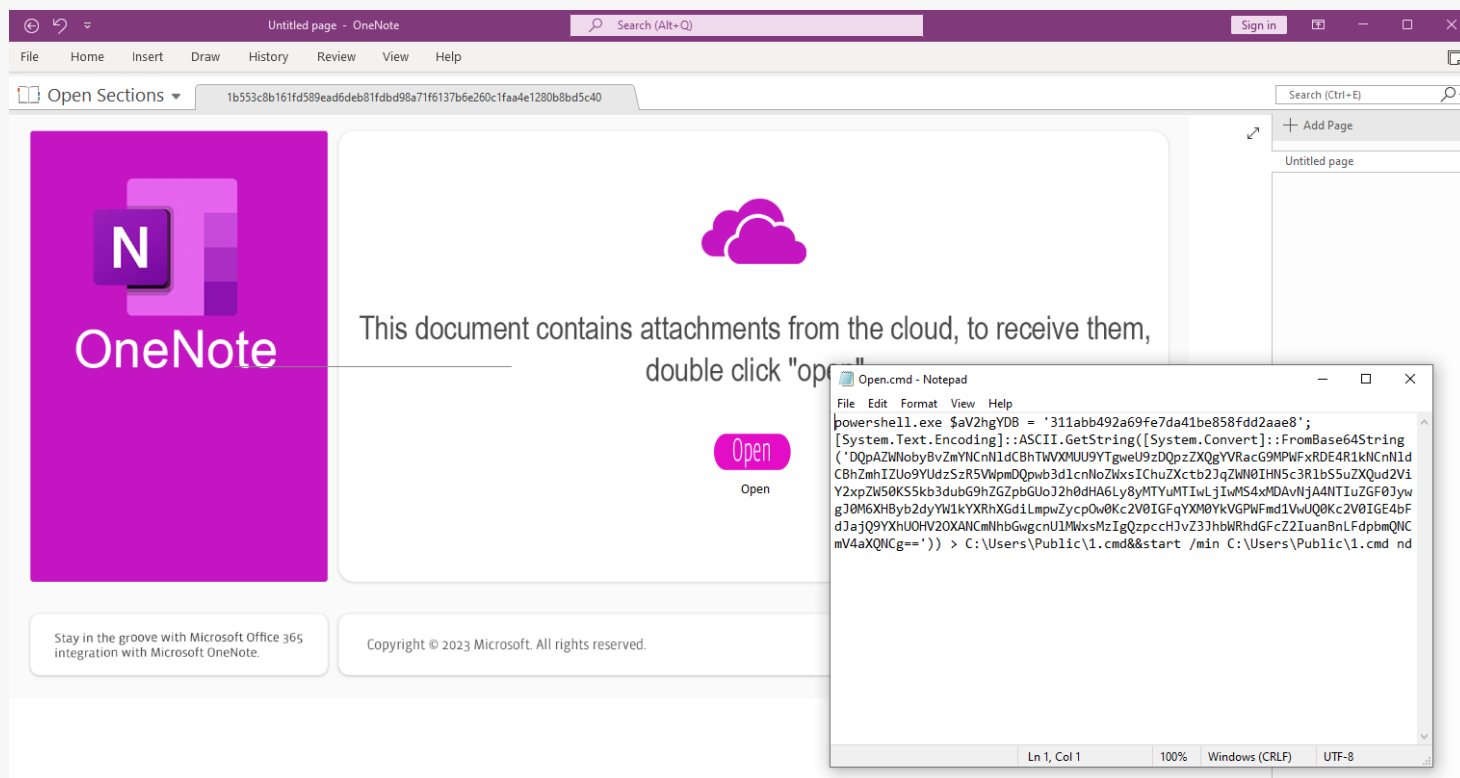


Figure 1 - OneNote notebook hiding a malicious batch script

New ChromeLoader campaign infects users seeking pirated content

From blocking advertisements to managing passwords, browser extensions are powerful programs that improve our web browsing experience. Cybercriminals have for decades abused the extensibility of web browsers for financial gain and stealing personal information, first through rogue toolbars and, more recently, dubious extensions.⁷

In March, HP Wolf Security detected users attempting to download a malicious Google Chrome extension named Shampoo. Unlike legitimate extensions, Shampoo has not been reviewed and published in the Chrome Web Store. Instead, it infects PCs by tricking victims into running malicious VBScript. This triggers a series of scripts to download the extension, load it into a new browsing session, and set up persistence mechanisms making it harder to remove.

Shampoo is a variant of ChromeLoader, a family of Google Chrome browser extension malware first analyzed in early 2022 by security researchers.⁸ Its goal is to install a malicious extension in Chrome to make money for its operators by redirecting search queries and injecting adverts. ChromeLoader Shampoo has a complex infection chain, beginning with the victim downloading malicious scripts from websites hosting illegal content, such as pirated films and video games.

Many victims notice the malicious extension when Chrome redirects them to different web pages, unexpectedly closes and reopens, or they spot the extension's icon in the toolbar. Removing ChromeLoader Shampoo is not as simple as uninstalling a legitimate extension, however. The malware relies on looping scripts and a Windows scheduled task to reinstall the extension whenever the victim removes it or reboots their device.

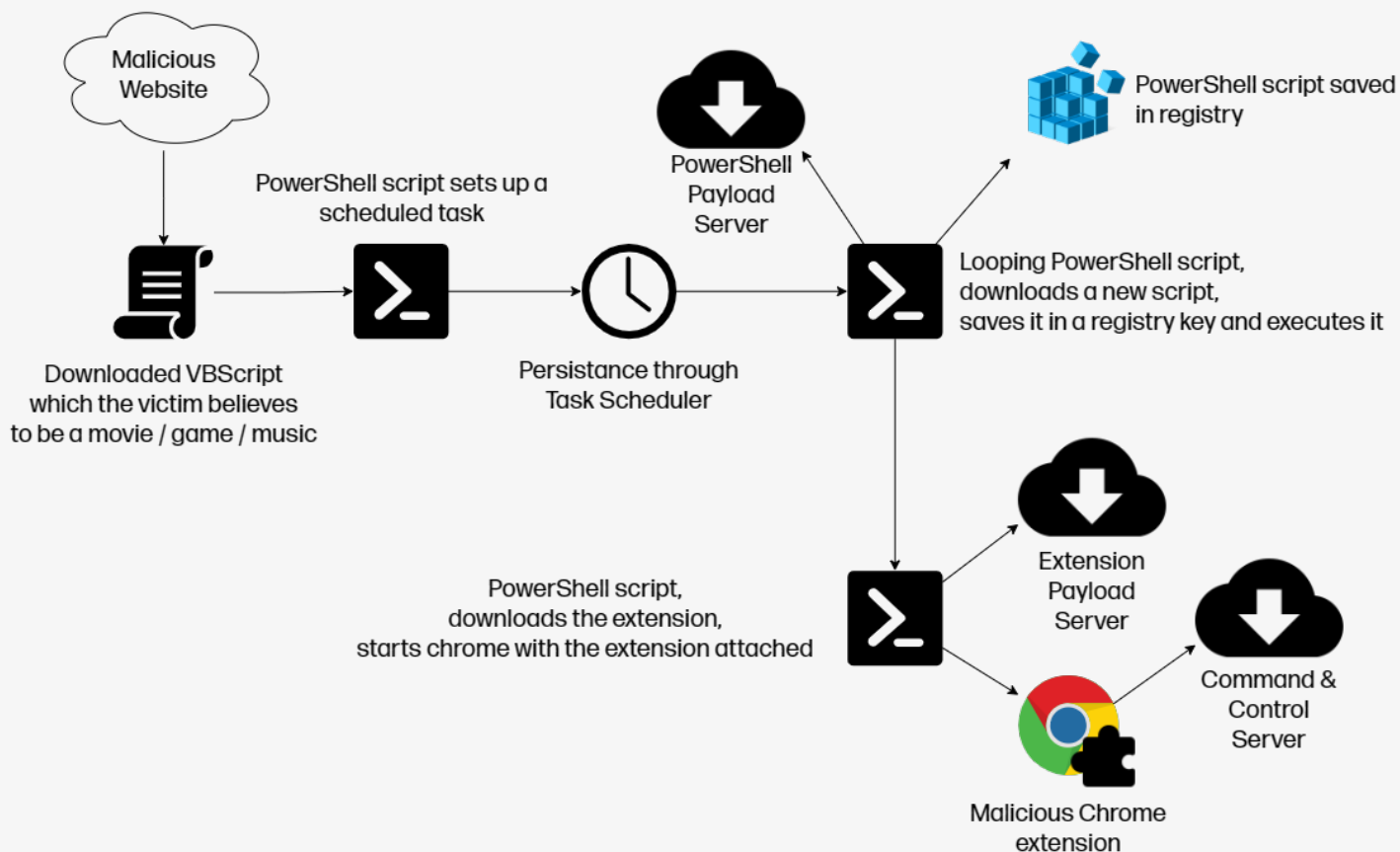


Figure 2 - ChromeLoader infection chain, March 2023

The human factors of this campaign are worth highlighting. The malware does not hide itself. The victim will almost certainly notice ChromeLoader's presence. Despite this, users may be reluctant to ask their IT department for help to remove the malware. ChromeLoader is often delivered through malicious VBScript files that users download from websites hosting illegal content. Users may fear repercussions for breaking their organization's acceptable IT use policy.

Good endpoint visibility, reinforcing a positive security culture by regularly educating users about threats, and turning on controls that enforce what extensions can be installed are practical steps to mitigate malicious browser extensions. HP Sure Click Enterprise Secure Browser enables IT teams to block unknown or unauthorized extensions from being installed through a centrally managed policy.⁹

To get rid of ChromeLoader Shampoo, victims need to disable its persistence mechanism:

- A scheduled task prefixed with "chrome_". Legitimate Chrome scheduled tasks are normally prefixed with "Google".
- A registry key "HKCU:\Software\Mirage Utilities\".
- A looping script. This is temporarily disabled by restarting the machine.

These removal steps must be completed quickly before the looping script reinstalls the malware.

A simple way of detecting if Shampoo, or another ChromeLoader variant, is present on a machine is to check if Chrome is running with the "--load-extension" argument. ChromeLoader relies on this argument to load the extension into a Chrome session.

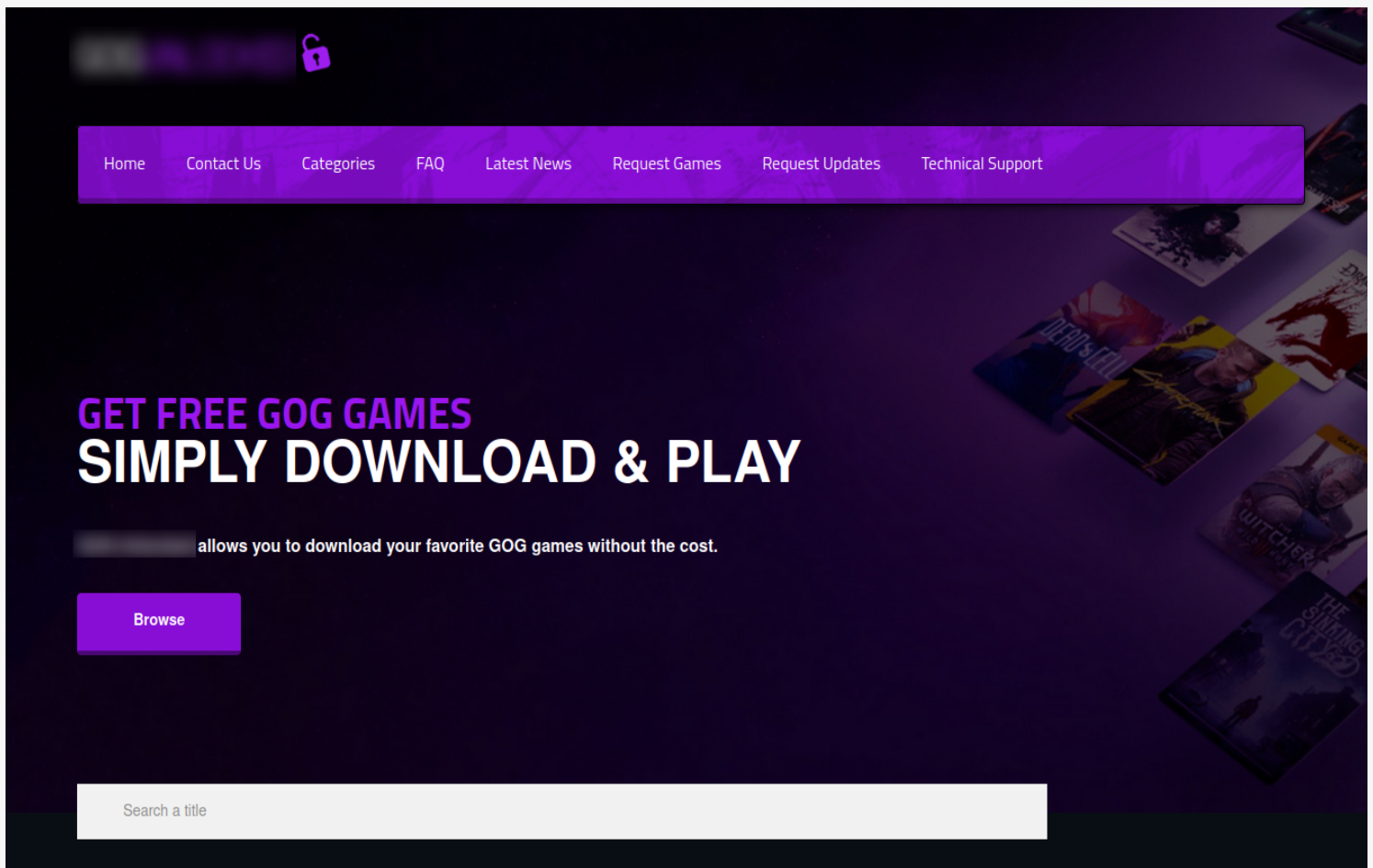


Figure 3 - Website distributing Shampoo malware

Attackers abuse trusted domains to deliver Formbook

As a result of Microsoft's tightening of Office's default security policy, threat actors have changed and diversified their attack techniques.¹⁰ VBA macros are now disabled by default for documents downloaded from untrusted sources, such as the web. However, in a campaign we saw at the beginning of March, some attackers are skilfully bypassing this restriction.

The attackers first obtained access to an employee's Microsoft 365 credentials. Next, they used these credentials to log into Outlook for Web, where they set up a new email address masquerading as the target organization's finance department. To extend the intrusion, the attackers emailed an internal distribution list of other employees in the organization with malicious Word documents.

Had the email originated from an external sender, the attack would not have succeeded. But since they were sent within the same domain, the documents were considered trustworthy by Office, meaning VBA macros were not disabled. Because the sender was a fellow employee, the malicious emails would appear more credible and less likely to flag suspicions.

The VBA macros of the malicious document were simple, using the curl.exe data transfer tool to download and run a malware payload from a URL. The downloaded malware was Formbook, an information stealer sold on hacking forums capable of recording keystrokes and stealing sensitive information.¹¹

The case highlights how automatically trusting files by domain can fail to protect against attacks where threat actors have already compromised an account within a target environment. Extending the principle of least privilege to files received by endpoints - a zero-trust approach - would have protected users from the secondary infection.


Received From	emp1@domain.com <emp1@domain.com>
Sent To	emp2@domain.com <emp2@domain.com>
Date Sent	March 6, 2023 11:11 AM
Subject	FW: PI -0145
Attachments	pi-0147.docm (20KB)  Script-Macro.Trojan.Heuristic

Figure 4 - Redacted email trying to spread Formbook via an internal distribution list

Top threat vectors

80%

Email

13%

Web browser downloads

7%

Other

Rise in gzip archive malware over Q4

53%

Notable Trends

Malware delivery file types and techniques continue to diversify

Q1 saw a continued diversification of file types and techniques used by attackers to deliver malware, part of an ongoing trend since Q1 2022. In particular, IcedID, Qakbot and Ursnif's distribution methods have varied significantly compared to their older campaign activity.¹² In 2022, there has been a steady change in malware delivery techniques. In June, for example, Qakbot distributors switched to HTML smuggling (T1027.006).¹³ Then, in December, attackers started sending PDF documents containing malicious links in spam campaigns. And in January 2023, we saw a shift to OneNote notebooks containing malicious scripts.

However, it didn't stop there. Over the last three months, attackers have alternated their use of these techniques. If PDF lures were sent one week, it might be followed by HTML smuggling campaigns the next. This switching behavior differs from historical campaigns where attackers primarily relied on a handful of Office formats to deliver malware, such as Word documents and Excel spreadsheets.

Apart from using different file types, attackers are also exploring other infection vectors beyond email. We saw a continuation of the fake software malvertising trend noted in Q4 2022, where attackers use search engine advertisements to lure victims to bogus software project websites hosting malware.¹⁴

Rise in HTML threats over Q4

37%

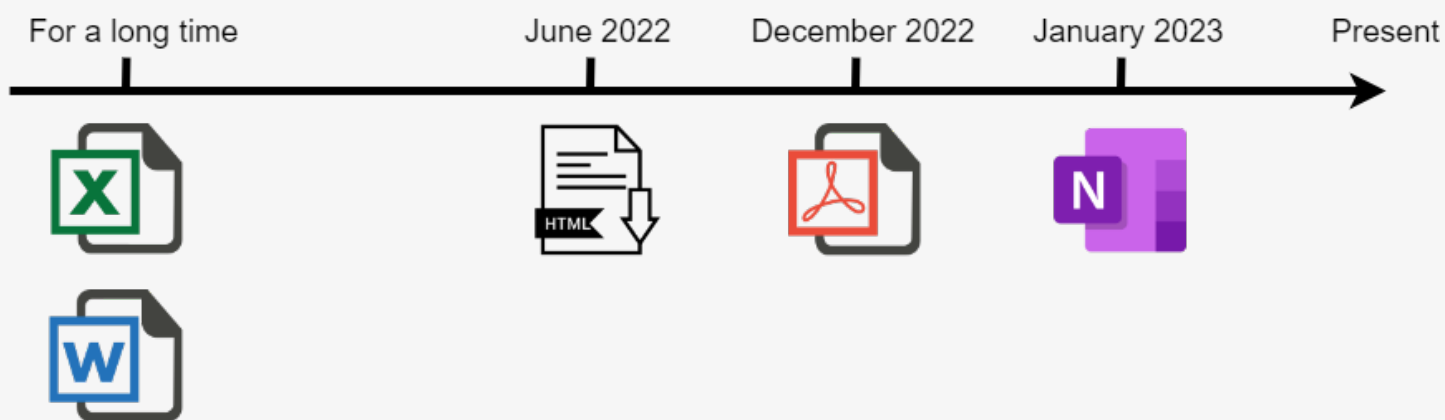
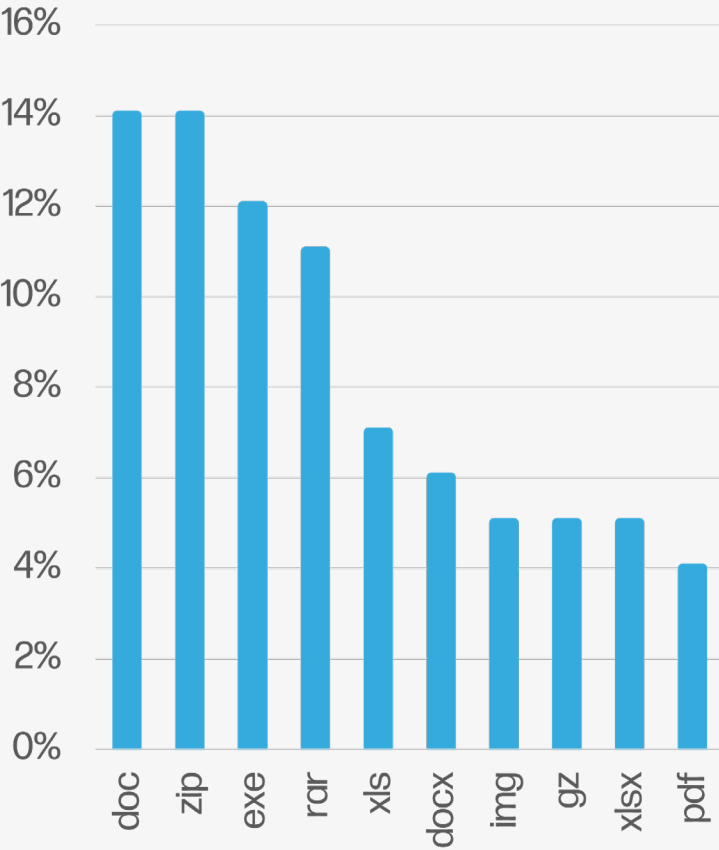


Figure 5 - QakBot delivery technique timeline showing switching behavior throughout 2022 and early 2023

Top malware file extensions



Document threats containing exploits in Q1

85%

Threat file type trends

Archives remained the most popular malware delivery file type for the fourth quarter, seeing a two percentage point increase in threats in Q1 over Q4. Notably, there was a 53% rise in gzip (.gz) archive malware in Q1 compared to last quarter, driven by purchase order malicious spam delivering RATs like Remcos, Agent Tesla and Ave Maria.^{15 16 17} Since gzip files lack a default file handler in Windows, attackers are likely relying on users having file archivers like 7-Zip installed to extract the malware. Zip archive threats identified by HP Wolf Security also rose by 8% in Q1.

There was a six percentage point drop in spreadsheet malware in Q1 compared to Q4, from 19% to 13%, as attackers moved away from Office formats. Most Office threats now rely on exploits to achieve code execution rather than macros. 85% of Word threats stopped by HP Wolf Security in Q1 relied on exploits, such as CVE-2017-11882, rather than malicious macros.¹⁸ Similarly, 62% of Excel threats stopped by HP Wolf Security contained exploits.

HTML threats, including HTML smuggling, continue to grow. Q1 saw a 37% rise in threats of this file type stopped by HP Wolf Security compared to Q4.

Threat vector trends

Email remained the top vector for delivering threats to endpoints. 80% of threats identified by HP Wolf Security were sent by email in Q1, up three percentage points compared to Q4.

The number of email threats that had bypassed email security also increased in Q1. 14% of email threats detected by HP Wolf Security had bypassed one or more email gateway scanner, up one percentage point over the previous quarter.

Malicious web browser downloads fell slightly by one percentage point to 13% in Q1. Threats delivered by other vectors, such as removable media, fell by two percentage points to 7% over Q4.

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.^{19 20}

- 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.²¹

- 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.²² For the latest threat research, head over to the HP Wolf Security blog.²³

About the HP Wolf Security Threat Insights Report

Enterprises are most vulnerable from users opening email attachments, clicking on hyperlinks in emails, and downloading files from the web. HP Wolf Security protects the enterprise by isolating risky activity in micro-VMs, ensuring that malware cannot infect the host computer or spread onto the corporate network. HP Wolf Security uses introspection to collect rich forensic data to help our customers understand threats facing their networks and harden their infrastructure. The HP Wolf Security Threat Insights Report highlights notable malware campaigns analyzed by our threat research team so that our customers are aware of emerging threats and can take action to protect their environments.

About HP Wolf Security

HP Wolf Security is a new breed^c of endpoint security. HP's portfolio of hardware-enforced security and endpoint-focused security services are designed to help organizations safeguard PCs, printers, and people from circling cyber predators. HP Wolf Security provides comprehensive endpoint protection and resiliency that starts at the hardware level and extends across software and services.

References

- [1] <https://hp.com/wolf>
- [2] <https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot>
- [3] <https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid>
- [4] https://learn.microsoft.com/en-us/openspecs/office_file_formats/ms-one/73d22548-a613-4350-8c23-07d15576be50
- [5] <https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet>
- [6] <https://www.hp.com/us-en/security/products.html#section=SureClickEnterprise>
- [7] <https://www.malwarebytes.com/blog/threats/toolbars>
- [8] <https://www.gdatasoftware.com/blog/2022/01/37236-qr-codes-on-twitter-deliver-malicious-chrome-extension>
- [9] <https://enterprisesecurity.hp.com/s/article/Using-Browsers-with-vSentry>
- [10] <https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked>
- [11] <https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook>
- [12] <https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi>
- [13] <https://attack.mitre.org/techniques/T1027/006/>
- [14] <https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-q4-2022/>
- [15] <https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos>
- [16] https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla
- [17] https://malpedia.caad.fkie.fraunhofer.de/details/win.ave_maria
- [18] <https://nvd.nist.gov/vuln/detail/cve-2017-11882>
- [19] <https://enterprisesecurity.hp.com/s/article/Threat-Forwarding>
- [20] <https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence>
- [21] <https://enterprisesecurity.hp.com/s/>
- [22] <https://github.com/hpthreatresearch/>
- [23] <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.