HP WOLF SECURITY

Threat Insights Report

Q4 - 2022

Threat Landscape

Welcome to the Q4 2022 edition of the HP Wolf Security Threat Insights Report

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

Executive Summary

Email threats that bypassed email gateway security

13%

- For the third quarter in a row, archives were the most popular file type for delivering malware (42%). Archive malware has risen 20% since Q1 2022 as attackers shift away from Office file formats to alternatives that do not rely on macros, such as disk image files (IMG, ISO).
- Q4 saw a surge of attackers imitating popular software projects to trick users into infecting their PCs with malware. The attacks rely on users clicking on search engine adverts leading to malicious websites that look almost identical to legitimate websites.
- Attackers are bypassing perimeter network security controls, such as email gateway scanners, by embedding malicious links in PDF files. 13% of email threats identified by HP Wolf Security had bypassed one or more email gateway scanner, highlighting the limitations of relying on detection-based security controls.
- Threat actors are experimenting with QR codes in their lures to steal credit and debit card details from victims. In this type of attack, targets are more likely to access malicious websites from their mobile phones, which may lack protection against phishing.

Notable Threats

Attackers use PDF lures to deliver malware and bypass email security

With the decline of Office documents and spreadsheets as a method of delivering malware to PCs, we saw attackers experiment with alternative techniques like HTML smuggling and malicious shortcut (LNK) files. HTML smuggling is effective at bypassing email gateway security because attackers can encrypt their malware inside HTML attachments, preventing scanners from inspecting malicious content. We continue to see this method being used in the wild, but attackers are always trying fresh techniques to evade detection. One technique that gained momentum in December were PDF documents. HP Wolf Security saw a 38% rise in PDF malware in Q4 compared to the previous quarter.

The infection chain begins with an attacker sending a PDF document to a victim by email. As with HTML smuggling, the attackers imitate well-known brands to catch the recipient's attention. Figure 1 shows an example of a fake online document viewer seen in Q4, a popular lure template. The PDF document contains a link that leads to a ZIP archive file hosted on a web server. Since the PDF attachment does not contain any executable code, it is less likely to be detected by email gateways. To increase the likelihood of evading detection, the attackers also encrypt the archive, providing the password and instructions in the PDF document sent to the recipient.

Often the downloaded ZIP archive contains a disk image file (.ISO or .IMG) containing a shortcut file. The recipient must open the shortcut file to trigger the infection. We have seen this technique used to deliver malware families including QakBot and IcedID, both known precursors to human-operated ransomware attacks.[2] [3]

The number of steps to trigger an infection through malicious PDF and HTML attachments is higher than macro-enabled Office documents. But despite more user interaction being required to execute malware, attackers are still successfully compromising networks because users are falling for such lures.

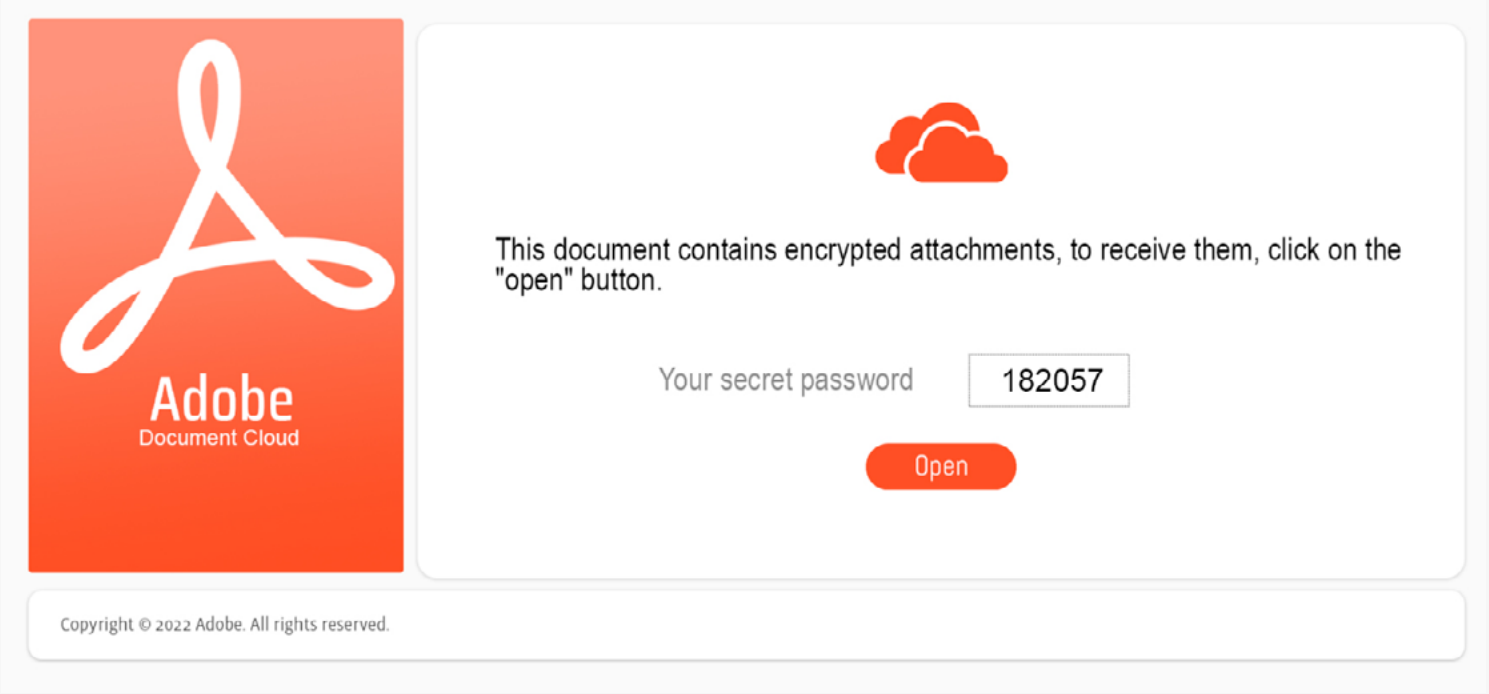


Figure 1 - Fake document viewer used to trick victims into infecting systems with QakBot

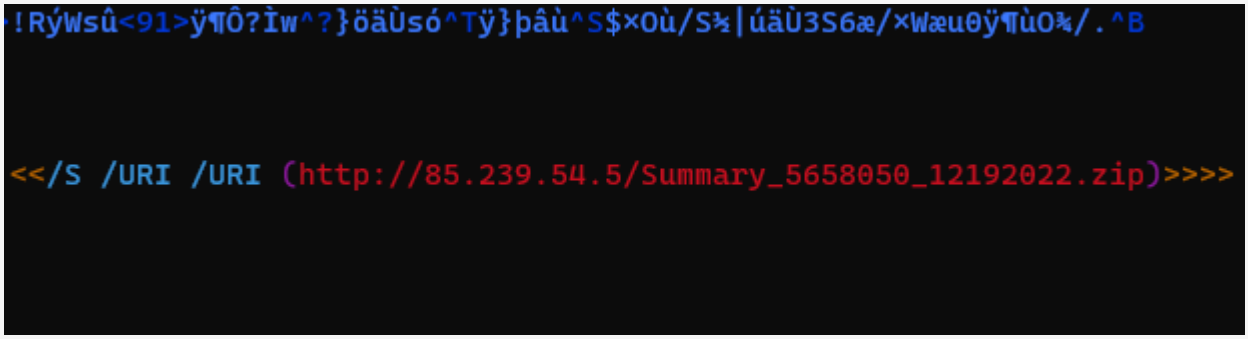


Figure 2 - Link embedded in a PDF that downloads a malicious archive when clicked

Attackers experiment with QR codes to steal sensitive information

At the end of November 2022, we spotted an unusual Chinese-language phishing campaign that abused QR codes to steal credit card details and other sensitive information.[4] We discovered the campaign through our internal analysis system, which compares images used in phishing and malware incidents. In this campaign, the attackers used a QR code to lure the user to a malicious website.

The attack starts with a Word document sent to a recipient by email. The document claims the recipient is entitled to a government grant and meets the classic elements of an effective phishing lure: its reliance on authority, urgency and a financial incentive for taking action.

To receive the grant, the recipient is asked to scan the QR code using WeChat, a popular instant messaging, social media and mobile payment app, and then follow the instructions on the website.

Using QR codes is an effective way to force the target to switch from a computer to a mobile device, which may be protected by weaker phishing protection and detection mechanisms. QR codes also benefit attackers because email gateways are less likely to inspect the destination web addresses the codes lead to, meaning phishing emails stand a greater chance of reaching users' inboxes compared to standard hyperlinks.

Figure 3 - Lure document asking user to update fields in the document

Since the end of October, we have observed these phishing campaigns almost daily at a high cadence. The attackers vary the document lures and domains every day. While we cannot make conclusive statements about the size of these campaigns, the attacker's choice of a dynamic phishing framework indicates that scalability was a consideration. It is plausible these campaigns are being distributed in high volumes. The structure of the phishing kit makes the content and the theme of a campaign easily interchangeable.

We have also seen QR codes used in English-language phishing campaigns masquerading as parcel delivery companies seeking payment, so individuals and organizations should be on the lookout for such campaigns.

Figure 4 - Phishing website asking for the target's credit card details

Fake software malvertising on the rise

When setting up a new PC, many of us have go-to software packages we like to install. But if you're not careful, you might end up installing malware masquerading as your favorite software. Since November, we have seen a significant rise in campaigns using malvertising to deliver malware to unsuspecting victims.[5]

With malvertising, malicious actors buy advertisements in search engine results, redirecting users to websites hosting malware. Buying adverts enable attackers to achieve a higher search engine ranking for their malicious websites for software-related queries. In some examples we analysed, attackers imitated popular open-source projects such as Audacity, Blender and GIMP. A user who searches for one of these software packages may be served an advert leading to a malicious website.

Figure 5 shows an example of a fake sponsored link. Looking closely, you'll notice the advert's domain name differs from the software project's genuine website. But the difference between the domains is subtle and easily missed. Clicking the advert leads to a fake website that copies the design of the legitimate Audacity website.

Number of imitated software projects in malvertising campaigns in Q4

24

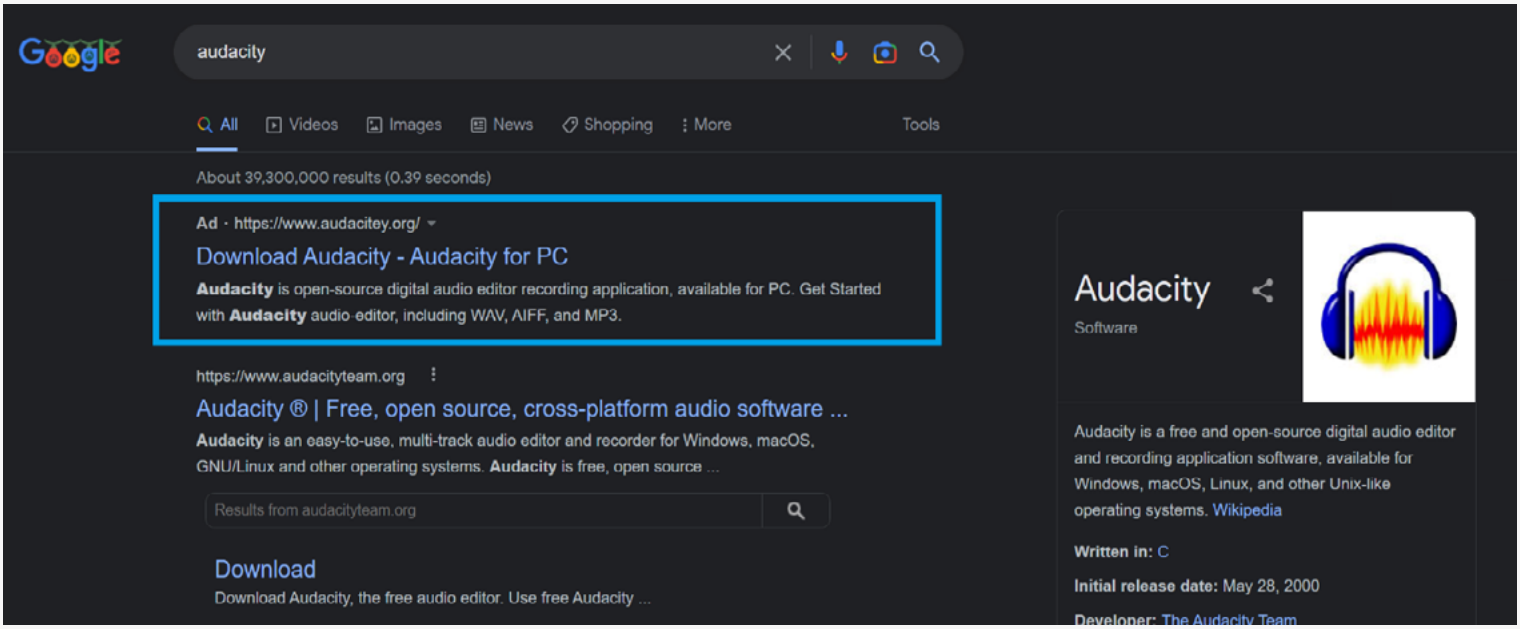


Figure 5 - Search engine advert leading to malicious website serving malware

The fake website looks almost identical to the real one, making it hard for the user to spot that it's fake (Figure 6). When the user clicks on the download button, an .exe file masquerading as an installer is served, in this case, "audacity-win-x64.exe". This example delivered Vidar Stealer, a commodity information stealer.[6] Vidar Stealer isn't the only family being distributed through malvertising. We have also seen this fake software malvertising theme used to spread at least eight malware families, including infostealers like Rhadamanthys Stealer and BatLoader and others.[7] [8] However, since mid-November, the largest campaigns we've seen using this delivery approach are those spreading the IcedID trojan.

As with Vidar Stealer, the attackers imitate the legitimate websites of software projects to spread malware. The attackers tend not to vary the domains' properties across campaigns, making it possible to identify the fake websites based on their domain registrar, name servers and domain names.

Over two months, our search identified 92 domains that mimic 24 different software projects that have been or could still be used to distribute malware through malvertising (Figures 7 & 8). We expect this trend to continue to grow as threat actors diversify their methods of malware delivery.

Figure 6 - Fake Audacity website serving Vidar Stealer

Domain	Registrar	Created	Name Server
wvw-irs-forms.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 29, 2022, 4:12 p.m.	a.dnspod.com c.dnspod.com
vvv-discord.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 29, 2022, 10:49 a.m.	a.dnspod.com c.dnspod.com
mlcrosofteams.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 29, 2022, 10:49 a.m.	a.dnspod.com c.dnspod.com
wvvw-citrix.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 28, 2022, 9:42 a.m.	a.dnspod.com c.dnspod.com
wvw-adobe.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 28, 2022, 9:42 a.m.	a.dnspod.com c.dnspod.com
vwvv-discord.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 28, 2022, 9:42 a.m.	a.dnspod.com c.dnspod.com
www-microsofteams.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 27, 2022, 1:44 p.m.	a.dnspod.com c.dnspod.com
vwv-discord.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 27, 2022, 1:44 p.m.	a.dnspod.com c.dnspod.com
www-onenote.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 26, 2022, 10:27 a.m.	a.dnspod.com c.dnspod.com
www-microsoftteams.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 26, 2022, 10:11 a.m.	a.dnspod.com c.dnspod.com

Figure 7 - Typosquatted domains registered in December 2022

Campaign date	Imitated software		Malware family
December 2021	Discord		Redline Stealer
February 2022	Windows 11 OS upgrade		Redline Stealer
November 2022 – ongoing	Audacity Blender GIMP Notepad++ Microsoft Teams Citrix Adobe OneNote LibreOffice Slack TeamViewer Any Desk	Thunderbird Fortinet Webex Sandboxie Plus Docker Basecamp VMWare OBS WhatsApp Tor Browser Crypto Browser Brave Browser	IcedID Vidar Stealer Rhadamanthys Stealer BatLoader Redline Stealer Aurora Stealer Gozi Raccoon Stealer

Figure 8 - Table summarizing fake software malvertising campaigns

Emotet distributors work around strict Office macro policy to infect PCs

Emotet campaigns were been few and far between in Q4.[9] However, from 2 to 11 November, the malware returned with new spam campaigns after a break of several months. The malware was distributed as usual through malicious macro-enabled Excel spreadsheets attached to emails. However, we spotted a change in the design of the documents.

After years of being abused by attackers, in February 2022 Microsoft disabled by default Visual Basic for Application macros in many Microsoft Office file formats downloaded from the web.[10] This change has contributed to the ongoing trend of attack file type diversification. Interestingly, rather than moving away from macros, Emotet's distributors simply tried to work around the policy.

Figure 9 - Social engineering image used in Emotet campaign in November 2022

When the recipient opens the spreadsheet, they are shown a social engineering image masquerading as an Office banner. The instructions tell the user that to see the contents of the spreadsheet they must copy the file to one of the folders indicated in the image and then reopen it. Like HTML smuggling and PDF malware delivery, this method requires a high level of user interaction to trigger the infection. Before the Office policy change, users could inadvertently trigger the malware's execution with two clicks.

If the user's follows the instructions, the malicious macro runs. The code saves four DLL files with different names in the user's directory and then runs them using regsvr32.exe (T1218.010), which leads to the execution of the Emotet payload.[11] Due to the complex user instructions, it is possible this campaign was a test comparing the infection rate of this delivery technique versus other methods.

Rise in disk image malware over Q3

31%

Top threat vectors

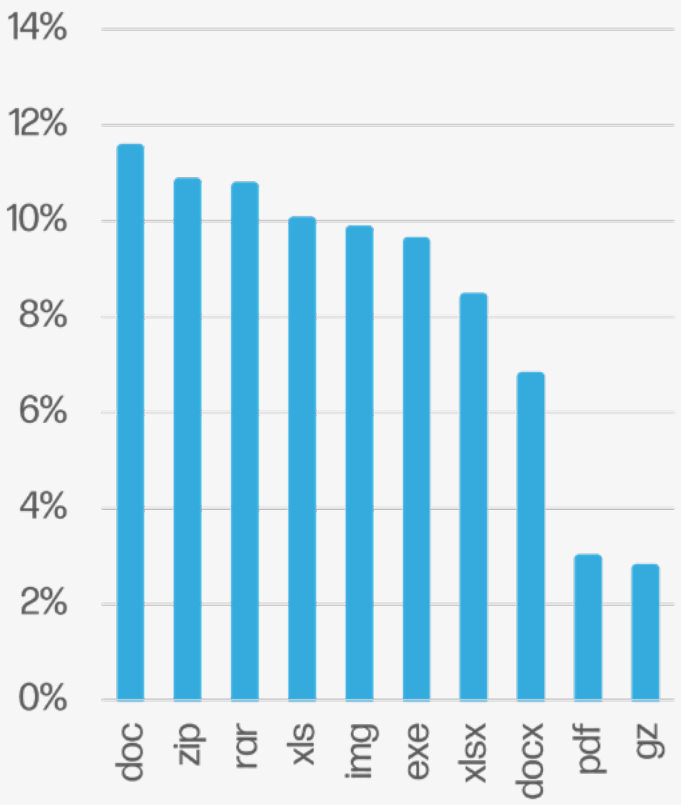
77%
Email

14%
Web browser downloads

9%
Other

Notable Trends

Top malware file extensions



Archives remain most popular malware delivery file type for third consecutive quarter

In Q4, 42% of malware was delivered in archive file formats, such as ZIP and RAR. Archives remained the most popular malware file format group for the third quarter, ahead of Office formats (38%). The popularity of archives have risen 20% since Q1 2022, as threat actors increasingly prefer scripts to execute their payloads.

Four of the top 10 malware file extensions were archive formats (ZIP, RAR, IMG, GZ). Notably, there was a 31% increase in disk image (IMG) malware compared to Q3, with the format rising two places to become the fifth most popular malware file type in Q4. Attackers are abusing the auto-mount feature in Windows that enables targets to easily mount and access malware stored inside IMG files by double-clicking them.

RAR, another type of archive, also rose in the rankings to third place, with 11% of malware seen using this file format. Overall, the top 10 file formats accounted for 83% of malware isolated and detected by HP Wolf Security.

Archives are attractive to threat actors because they are easily encrypted, making them difficult for web proxies, sandboxes and email scanners to detect malware. Many organizations use encrypted archives for legitimate reasons, making it challenging to reject encrypted archive email attachments by policy.

Rise in HTML threats over Q3

44%

HTML threats grow in Q4

HTML threats, including HTML smuggling, rose by 44% in Q4 to become the 15th most popular malware format (up two places from 17th in Q3), indicating the growing popularity of this technique among threat actors to spread malware.

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.[12] [13]
- 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.[14]
- 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.[15] For the latest threat research, head over to the HP Wolf Security blog.[16]

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://threatresearch.ext.hp.com/chinese-phishing-campaign-abuses-qr-codes-to-steal-credit-card-details/

[5] https://threatresearch.ext.hp.com/adverts-mimicking-popular-software-leads-to-malware/

[6] https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.rhadamanthys

[8] https://malpedia.caad.fkie.fraunhofer.de/details/win.bat_loader

[9] https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet

[10] https://attack.mitre.org/techniques/T1218/010/

[11] https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

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

[13] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence

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

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

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