HP WOLF SECURITY

THREAT INSIGHTS REPORT

Q4 - 2021

THREAT LANDSCAPE

Welcome to the Q4 2021 edition of the HP Wolf Security Threat Insights Report. Here our security experts highlight malware trends identified by **HP Wolf Security** from the fourth quarter of 2021, equipping security teams with the knowledge to combat emerging threats and improve their security postures.[1]

NOTABLE THREATS

Surge in attackers using Excel add-ins (.XLL) to infect systems

In Q4 2021, HP Wolf Security detected a near sixfold increase (588%) in malware campaigns using malicious Microsoft Excel add-in (XLL) files to infect systems compared to Q3. This technique is tracked in MITRE ATT&CK as **T1137.006**.[2] The purpose of add-ins is that they contain high-performance functions called from an Excel worksheet via an application programming interface (API). This feature enables users to extend the functionality of Excel beyond other scripting interfaces like Visual Basic for Applications (VBA) because it supports more capabilities, such as multithreading. Attackers taking advantage of legitimate APIs and scripting features is not new, but the growing popularity of this technique illustrates how threat actors are continually looking for ways to abuse legitimate features in software to achieve their goals.

588%

RISE IN XLL MALWARE DETECTED BY HP WOLF SECURITY IN Q4 2021 COMPARED TO Q3.

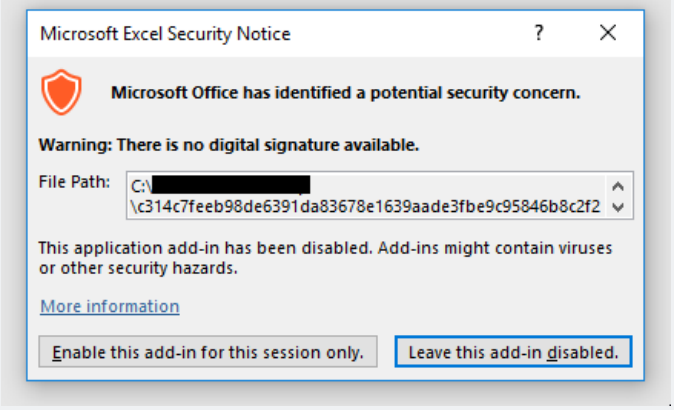
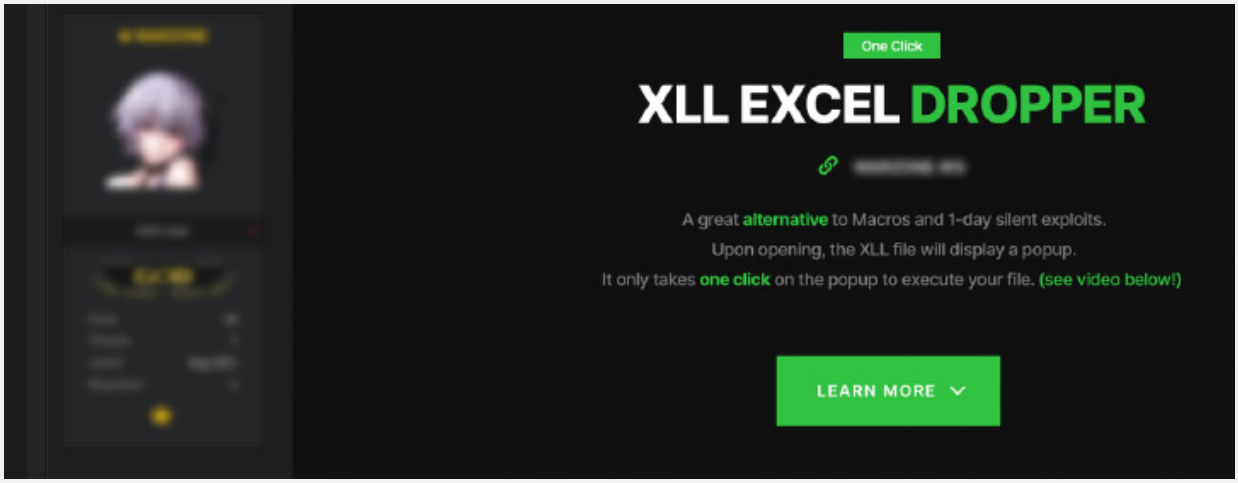


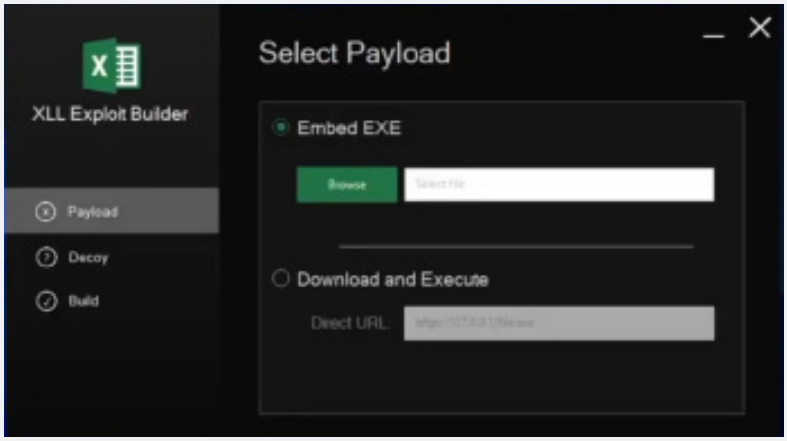
Figure 1 – Prompt shown to user when opening an XLL file

In the campaigns we analyzed, emails with malicious XLL attachments or links were sent to users.[3] Double-clicking the attachment opens Microsoft Excel, which prompts the user to install and activate the add-in. Attackers usually place their code in the **xlAutoOpen** function, which runs immediately after the add-in is activated. This technique is dangerous because only one click is required to execute the malware, unlike VBA macros which require the user to disable Microsoft Office's Protected View and enable macro content. However, some email gateways already block XLL files because they are dynamic link libraries (DLLs), a file type that is rarely sent by email. We recommend organizations consider the following mitigations:

- Configure your email gateway to block inbound emails containing XLL attachments
- Configure Microsoft Excel only to permit add-ins signed by trusted publishers
- Configure Microsoft Excel to disable proprietary add-ins entirely

In Q4 2021, we identified seven malware families – **Dridex**, **IcedID**, **BazaLoader**, **Agent Tesla**, **Raccoon Stealer**, **Formbook** and **Bitrat** – that were delivered via malicious Excel add-ins during the initial infection of systems. We also found adverts on underground forums promoting XLL malware and services, including some builders costing as much as **$2,100 USD**. Figure 2 shows a forum post from a malware author selling a purported XLL dropper used for delivering malware to systems. The user specifies an executable file or a link to the malware payload they wish to deliver and a decoy document to fool users after they have opened the add-in. The tool generates a malicious XLL file which can then be used in attacks. The increasing volume of Excel add-in malware in Q4 suggests threat actors are interested in exploring this technique. Still, it remains to be seen if it will surpass the popularity of tried and tested delivery techniques like Excel4 macros, Dynamic Data Exchange (DDE) and VBA. Enterprises should nonetheless stay vigilant to such attacks.





Figures 2 & 3 – Forum post advertising an XLL dropper (above) and screenshot of its user interface (below)

QakBot gives attackers access to infected systems to deliver ransomware

QakBot was one of the top malware families isolated by HP Wolf Security in Q4 2021. After a global law enforcement operation disrupted **Emotet** botnet infrastructure in January 2021, QakBot presented itself as an alternative way for malware operators to access infected systems. Like Emotet, Qakbot can hijack email threads. The malware uses stolen email conversations to generate a fake reply, raising the lure's credibility and the chance of infection. In the malicious spam campaigns in Q4 that delivered QakBot, the emails contained a link that downloads a ZIP archive containing a **Microsoft Excel Binary Workbook (XLSB)** file. If the workbook is extracted and opened, a malicious macro downloads a DLL containing the QakBot Trojan, then renames and runs it. To hide on the system, QakBot writes its code into a legitimate process, explorer.exe in the samples we analyzed, using a technique called **process injection** (Figure 4). Under the disguise of this legitimate process, the malware creates a Scheduled Task to remain persistent on the infected PC.

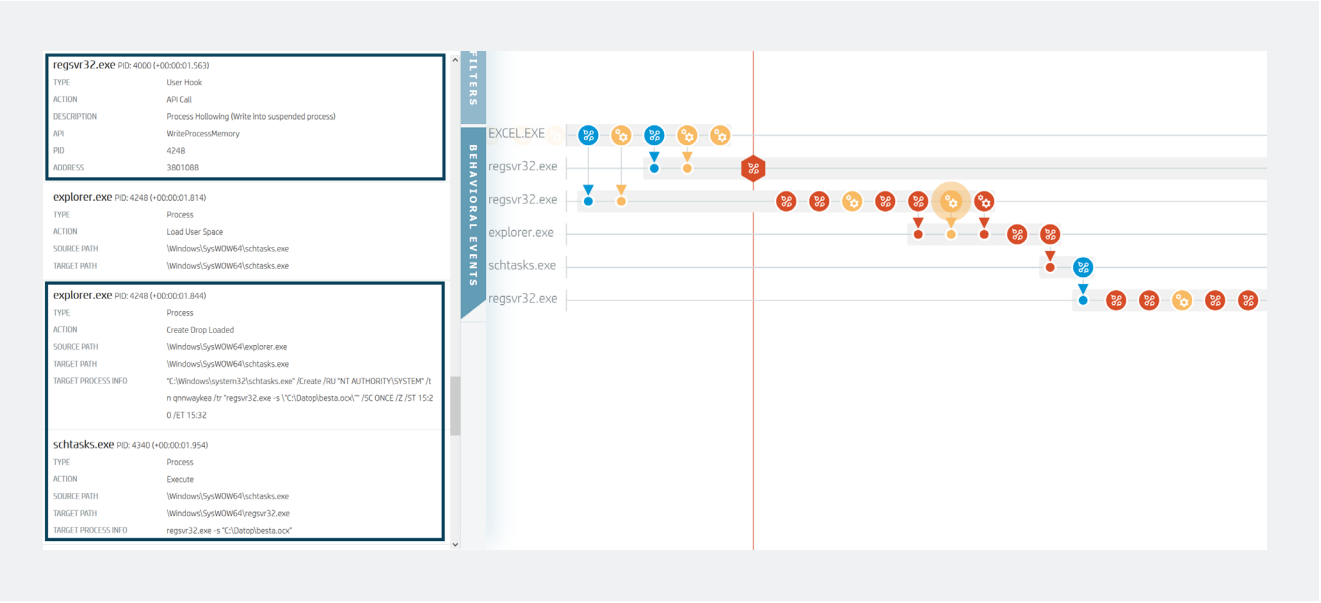


Figure 4 – QakBot sample from Q4 2021 running inside an isolated HP Sure Click micro-VM

QakBot's operators are understood to monetize the botnet by selling access to computers infected with the malware to other threat actors. This is an example of the broader trend of **cybercriminal specialization**, namely selling a service to other threat actors to fulfill their need for access to systems. QakBot's infection chain has been seen leading to **Conti** ransomware, suggesting that their customers include ransomware affiliates. Despite Emotet's return in November 2021, QakBot remains a common threat that security teams should keep a watchful eye on.

Aggah targets South Korean organizations with malicious PowerPoint add-ins (.PPA)

Aggah is a financially motivated threat actor linked to the Green Havildar threat group that is understood to be based in Pakistan.[4] We previously wrote about how Aggah changed their tactics, techniques and procedures (TTPs) in July 2020 to target European organizations.[5] In a campaign detected by HP Wolf Security in December 2021, Aggah targeted Korean-speaking organizations with fake purchase orders. The purchase orders were malicious PowerPoint Add-In files (.PPA) used to deliver **Agent Tesla**, a remote access Trojan (RAT). When opened, a malicious VBA macro triggers the execution of a VBScript using mshta.exe, the Microsoft HTML Application engine built into Windows. Interestingly, instead of hosting malicious code on their own infrastructure, the attackers stored malicious VBScript and PowerShell scripts embedded in HTML pages on the Blogger blog-hosting website via subdomains of blogspot[.]com. PowerPoint malware is unusual, making up 1% of malware isolated by HP Sure Click in Q4 2021.

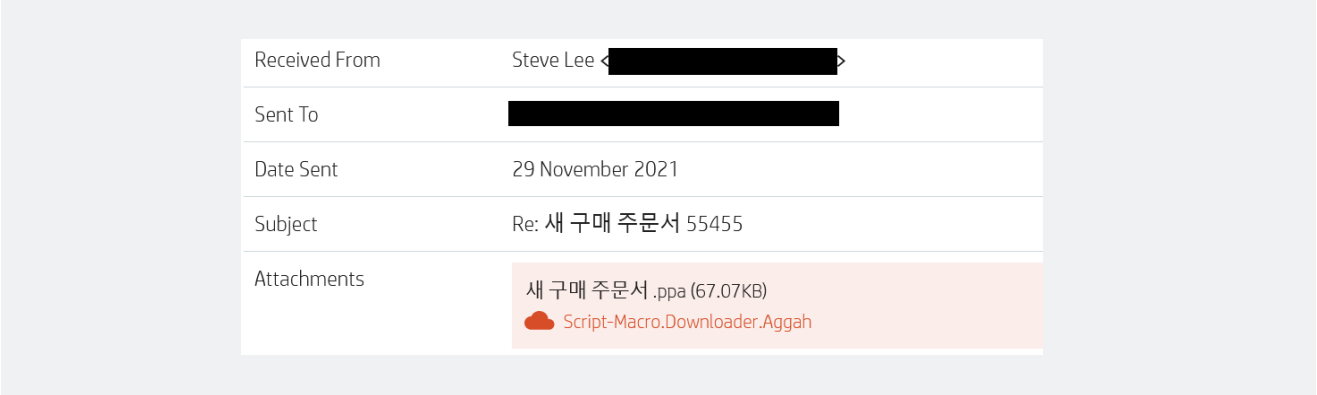


Figure 5 – Korean lure used by Aggah to deliver Agent Tesla malware via a malicious PowerPoint add-in

TA505's links to MirrorBlast

From mid-September to mid-November 2021, an entirely new malware campaign called **MirrorBlast** emerged that caught the attention of security researchers because of its unusual tooling and techniques. Despite the differences, the TTPs of the new campaign shared many similarities with old campaigns orchestrated by **TA505** – a notorious financially motivated threat actor. These similarities included the procedures the attackers followed to set up their infrastructure, domain registration patterns, campaign cadence, similar download websites and lure documents, similar target selection mechanisms and the same follow-up malware. Together these similarities suggest with moderate confidence that TA505 is behind MirrorBlast. If this is the case, the MirrorBlast campaign shows how threat actors are willing to invest in new tools and techniques to keep their infection rates high. No MirrorBlast activity has been seen since November 2021, raising the question of whether this was a test campaign or an experiment by TA505. You can read our full investigation on the HP Wolf Security blog.[6]

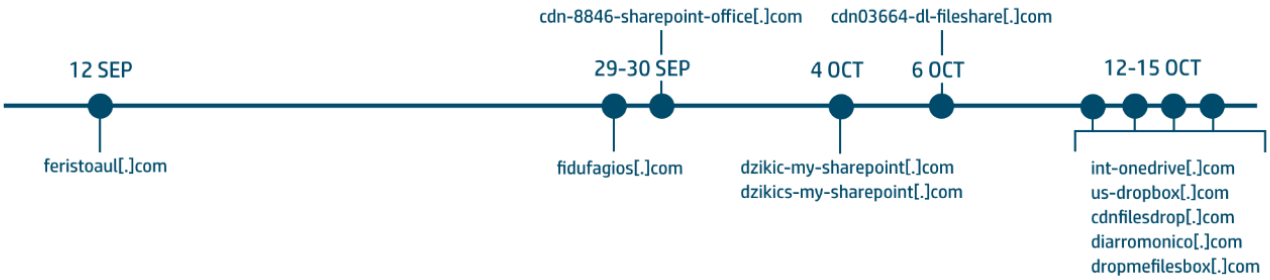


Figure 6 – Timeline showing MirrorBlast domain registrations from September to October 2021

Ongoing courier spam delivers Ursnif malware to Italian-speaking organizations

In Q4, HP Wolf Security detected a large ongoing malicious spam campaign targeting Italian organizations originating from the **Cutwail** botnet that delivered **Usrnif**, a banking Trojan. The campaign primarily targeted Italian-speaking users in at least 248 organizations across manufacturing and local government. The attackers spoofed the sender domain of BRT, an Italian courier company, to trick users into opening their emails. Each email contained an Excel (.XLS) spreadsheet attachment named according to the regular expression ***XSG\d{7}\.xls***. Opening the attachment in Microsoft Excel causes a malicious macro to download and run the Ursnif payload on the system. The subject line followed the regular expression ***BRT - Abbiamo preso in carico la tua spedizione (ID\d{7})***, which translates to "We have taken charge of your shipment" in English. Ursnif is a banking Trojan capable of stealing login credentials for banking websites.

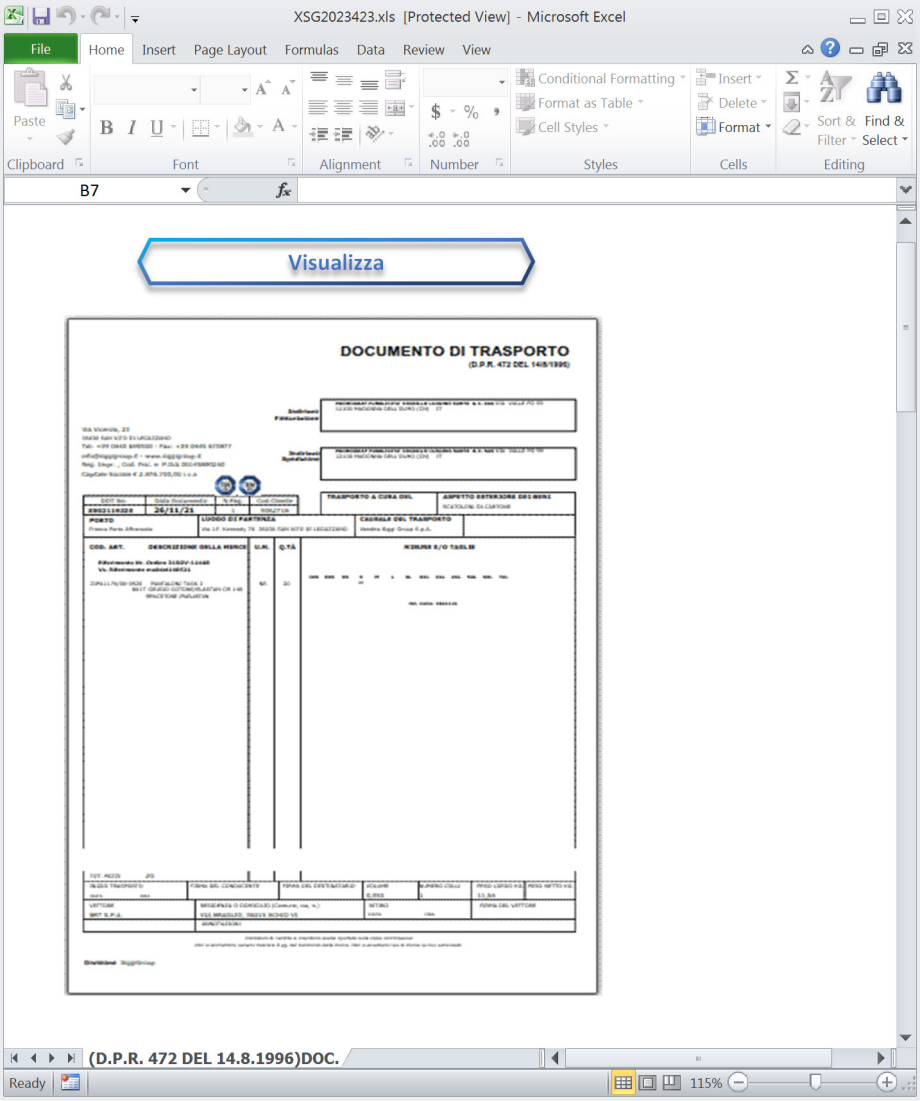
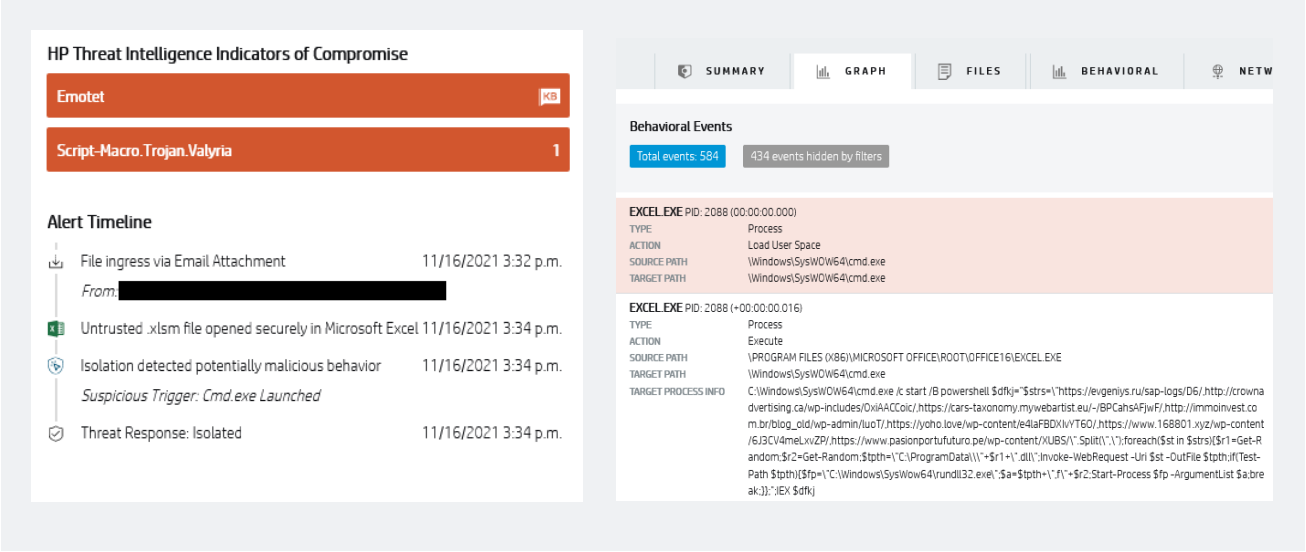


Figure 7 – Fake delivery lure that downloads Ursnif malware

The return of Emotet and its reversal of roles

On 15 November 2021, HP Sure Click isolated a new **Emotet** campaign targeting a large enterprise after an almost 10-month break.[7] One of the changes is that Emotet's operators have switched to using an Excel downloader to deliver the malware instead of Word and JavaScript downloaders they used previously. Another notable change in TTPs is that some PCs infected with **TrickBot** now deploy Emotet. This is a reversal of what was seen before January 2020. Back then, Emotet performed the initial compromise before dropping TrickBot, followed by ransomware – an infection chain known as the "Triple Threat". In other cases, security researchers have seen Emotet samples drop Cobalt Strike Beacon, a backdoor, rather than an intermediary stage of malware like TrickBot.[8] This change benefits attackers because it enables Emotet's customers to reduce the time it takes to deploy ransomware, minimizing the dwell time spent in a victim's network. Not deploying intermediary malware also reduces the exposure of being detected by security tools.



Figures 8 & 9 – Emotet samples isolated by HP Sure Click in November 2021

Fake Discord website serves RedLine malware posing as installer

In December 2021, we spotted a malware campaign spreading **RedLine**, an information stealer, disguised as an installer for the popular messaging application, Discord. The fake webpage mimicked the legitimate Discord website and was designed to trick unsuspecting visitors into clicking the "Download" button, which delivered the malicious installer. The attackers registered a typosquatted domain, **discrodappp[.]com**, on 1 December, which served the fake installer – DiscordSetup.js – in a zip file. Clicking on the JScript file downloads an executable that runs a batch script. The batch script generates an AutoIT executable, then runs an AutoIT script containing the encoded and compressed RedLine payload. The malware is decompressed using the RtlDecompressBuffer Windows API function.

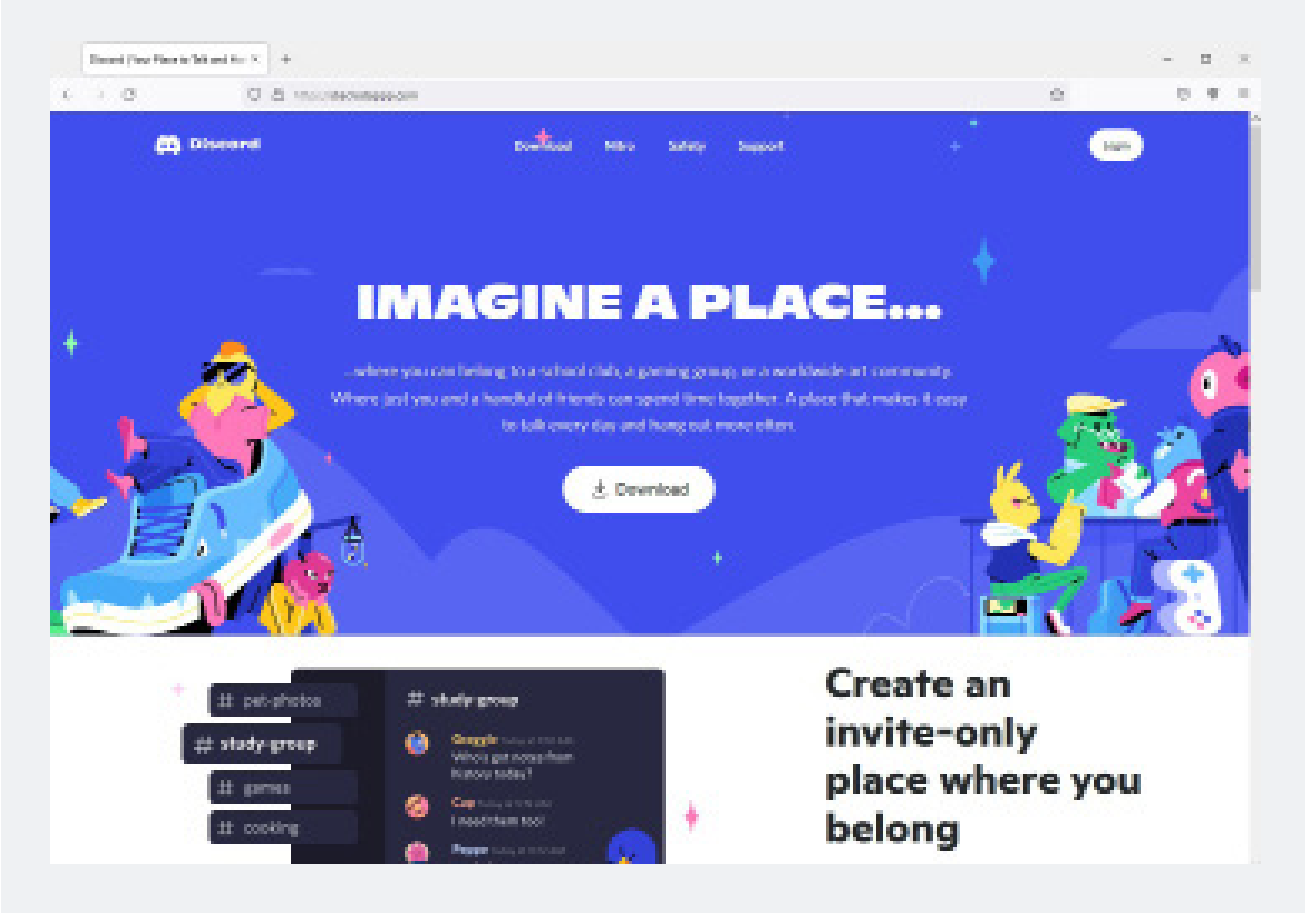


Figure 10 – Fake Discord website serving RedLine malware to unsuspecting visitors

NOTABLE TRENDS

In Q4 2021 HP Wolf Security detected a 4% increase in CVE-2017-11882 Equation Editor exploits and a 14 % increase in CVE-2017-0199 Rich Text File exploits compared to Q3. There also were higher levels of malicious Office documents this quarter, with threats targeting Microsoft Word seeing a 6% increase and Excel threats growing by 4% compared to Q3. Archives were less popular as a malware vector, dropping by 10% in Q4.

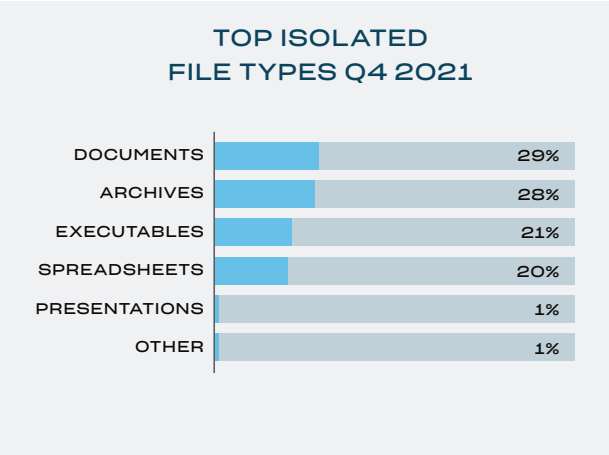
Slightly more email threats bypassed gateway security controls in Q4 too. 13% of email-borne malware isolated by HP Sure Click in Q4 2021 bypassed at least one gateway scanner compared to 12% in Q3. Additionally, 2% of email malware HP Sure Click blocked had failed a Sender Policy Framework check yet were still delivered to users' inboxes.

Email remained the top infection vector, with 77% of threats isolated by HP Sure Click using this vector in Q4. 13% of threats were downloaded via a web browser, while 11% were user-initiated, for example, opening a file that turned out to be malicious.

TOP 10 EMAIL LURE KEYWORDS

1. "ORDER"
2. "2021"
3. "PAYMENT"
4. "NEW"
5. "2021/2022"
6. "REQUEST"
7. "INVOICE"
8. "QUOTATION"
9. "PURCHASE"
10. "DEC"

Figure 11 – Top email subject lures of threats isolated by HP Wolf Security in Q4 2021



Figures 12 & 13 – Top exploits (left) and file types (above) isolated by HP Wolf Security in Q4 2021

2021 THREAT TRENDS & OUTLOOK

Looking back across the last 12 months of HP Wolf Security and external threat data, here are the primary security trends that organizations should be aware of.

Supply chain attacks became more commonplace while victims suffered higher impact breaches

Historically supply chain attacks have been associated with advanced persistent threat actors, but high profile attacks in 2021 – such as the REvil ransomware attack on **Kaseya** in July – show how well-resourced and capable criminal actors can also exploit supply chain vulnerabilities. Managed service providers (MSPs) continue to be an attractive propagation vector for malicious actors. Compared to previous examples of supply chain attacks, which tended to focus on information theft, the immediate impact of recent attacks have been higher because of the popularity of ransomware as a method of monetizing attacks.[9] [10] 2021 also saw examples of popular software packages being hijacked with malicious code, such as the **UA-Parser-JS** JavaScript package, highlighting the challenges enterprises face in detecting Trojanized code in software dependencies.[11] One of the ways enterprises can reduce their risk of supply chain compromise is by thoroughly assessing MSPs and vendors before purchasing services. Maintaining up-to-date software inventories can also speed up detection and remediation of Trojanized software.

MALWARE FAMILIES USED TO DELIVER RANSOMWARE DETECTED BY HP WOLF SECURITY IN 2021

DRIDEX
QAKBOT
EMOTET
ICEDID
TRICKBOT
BAZALOADER

Emboldened ransomware operators and affiliates disrupted critical infrastructure, leading to strong responses from governments and law enforcement

Ransomware remained the tool of choice for cybercriminals to monetize their access to networks. Since ransomware relies on disabling systems, one of the consequences of the current state of very high volumes of attacks is that some intrusions will affect critical services. In healthcare, the ransomware attack on the Irish Health Service Executive in May 2021 resulted in cancelled hospital appointments and the records of 520 patients being leaked, with damage estimated at €100 million.[12] The highest-profile ransomware incident in 2021 impacted Colonial Pipeline in May 2021, leading to fuel shortages caused by panic buying. 100 GB of data stolen was stolen by the perpetrators, a group called DarkSide, with $4.4 million USD paid in ransom.[13] The attack led to US president Biden issuing Executive Order 14028 to improve the defenses of the US federal government and its suppliers.[14] One of the possible outcomes of these interventions is that ransomware operators shift away from targets that are likely to draw the ire of law enforcement and governments.

INDICATORS AND TOOLS

The HP Threat Research team regularly publishes Indicators of Compromise (IOCs), signatures, and tools to help security teams defend against threats. You can access these resources from the **HP Threat Research GitHub repository**.[15]

STAY CURRENT

The HP Wolf Security Threat Insights Report is made possible by customers who opt to share their threats with HP. Alerts that are forwarded to us are analyzed by our security experts and annotated with additional contextual information about each threat.

We recommend that customers take the following actions to ensure that you get the most out of your **HP Wolf Enterprise Security** deployments:[a]

• Enable Threat Intelligence Services and Threat Forwarding in **HP Wolf Security Controller**.[b] These enable augmented threat intelligence for automated threat triage and labeling, plus automatic rules file updates to ensure accurate detection and protection against the latest attack techniques. To learn more, review the Knowledge Base articles about these features.[16, 17]

• Plan to update HP Wolf Security Controller with every new release to receive new dashboards and report templates. See the latest release notes and software downloads available on the Customer Portal.[18]

• Update HP Wolf Security endpoint software at least twice a year to stay current with detection rules added by our threat research team. For the latest threat research, head over to the **HP Wolf Security blog**, where our security experts regularly dissect new threats and share their findings.[19]

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. Since the malware is contained, HP Wolf Security collects rich forensic data to help our customers 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

From the maker of the world's most secure PCs[c] and Printers[d], HP Wolf Security is a new breed of endpoint security.[e] 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://attack.mitre.org/techniques/T1137/006/

[3] https://threatresearch.ext.hp.com/how-attackers-use-xll-malware-to-infect-systems/

[4] https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

[5] https://threatresearch.ext.hp.com/aggah-campaigns-latest-tactics-victimology-powerpoint-dropper-and-cryptocurrency-stealer/

[6] https://threatresearch.ext.hp.com/mirrorblast-and-ta505-examining-similarities-in-tactics-techniques-and-procedures/

[7] https://threatresearch.ext.hp.com/emotets-return-whats-different/

[8] https://www.bleepingcomputer.com/news/security/emotet-now-drops-cobalt-strike-fast-forwards-ransomware-attacks/

[9] https://www.pwc.co.uk/issues/cyber-security-services/insights/operation-cloud-hopper.html

[10] https://www.reuters.com/article/uk-usa-cyber-treasury-exclusive-idUKKBN28N0PI

[11] https://www.cisa.gov/uscert/ncas/current-activity/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js

[12] https://www.irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136

[13] https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown

[14] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

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

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

[17] https://enterprisesecurity.hp.com/s/article/Bromium-Threat-Intelligence-Cloud-Service

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

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

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 unique and comprehensive security capabilities at no additional cost among vendors on HP Elite PCs with Windows and 8th Gen and higher Intel® processors or AMD Ryzen™ 4000 processors and higher; HP ProDesk 600 G6 with Intel® 10th Gen and higher processors; and HP ProBook 600 with AMD Ryzen™ 4000 or Intel® 11th Gen processors and higher.

d. HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2021 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/PrinterSecurityClaims.

e. HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.

HP WOLF SECURITY