HP Inc.
1501 Page Mill
Palo Alto, CA 94304

hp.com

News Release

# HP finds cybercriminals Excel-ing at tricking users

## Stealthy techniques and growing Excel malware campaigns are putting victims in the crosshairs of ransomware gangs

**PALO ALTO, Calif., January 27, 2022** – HP Inc. (NYSE: HPQ) today released its latest global HP Wolf Security Threat Insights Report, providing analysis of real-world cybersecurity attacks. By isolating threats that have evaded detection tools and made it to user endpoints, HP Wolf Security has specific insight into the latest techniques being used by cybercriminals.

The HP Wolf Security threat research team identified a wave of attacks utilizing Excel add-in files to spread malware, helping attackers to gain access to targets, and exposing businesses and individuals to data theft and destructive ransomware attacks. There was a huge six-fold increase **(+588%)** in attackers using malicious Microsoft Excel add-in (.xll) files to infect systems compared to last quarter – a technique found to be particularly dangerous as it only requires one click to run the malware. The team also found adverts for .xll dropper and malware builder kits on underground markets, which make it easier for inexperienced attackers to launch campaigns.

Additionally, a recent QakBot spam campaign used Excel files to trick targets, using compromised email accounts to hijack email threads and reply with an attached malicious Excel (.xlsb) file. After being delivered to systems, QakBot injects itself into legitimate Windows processes to evade detection. Malicious Excel (.xls) files were also used to spread the Ursnif banking Trojan to Italian-speaking businesses and public sector organizations through a malicious spam campaign, with attackers posing as Italian courier service BRT. New campaigns spreading Emotet malware are now using Excel instead of JavaScript or Word files too.

Other notable threats isolated by the HP Wolf Security threat insight team include:

- **The return of TA505?** HP identified a MirrorBlast email phishing campaign sharing many tactics, techniques, and procedures (TTPs) with TA505, a financially motivated threat group known for massive malware spam campaigns and monetizing access to infected systems using ransomware. The attack targeted organizations with the FlawedGrace Remote Access Trojan (RAT).
- **Fake gaming platform infecting victims with RedLine:** A spoofed Discord installer website has been discovered, tricking visitors into downloading the RedLine infostealer and stealing their credentials.
- **Switching up uncommon file types is still bypassing detection:** The Aggah threat group targeted Korean-speaking organizations with malicious PowerPoint add-in (.ppa) files disguised as

purchase orders, infecting systems with remote access Trojans. PowerPoint malware is unusual, making up 1% of malware.

"Abusing legitimate features in software to hide from detection tools is a common tactic for attackers, as is using uncommon file types that may be allowed past email gateways. Security teams need to ensure they are not relying on detection alone and that they are keeping up with the latest threats and updating their defenses accordingly. For example, based on the spike in malicious .xll sightings we are seeing, I'd urge network administrators to configure email gateways to block incoming .xll attachments, only permit add-ins signed by trusted partners or disable Excel add-ins entirely," explains Alex Holland, Senior Malware Analyst, HP Wolf Security threat research team, HP Inc.

"Attackers are continually innovating to find new techniques to evade detection, so it's vital that enterprises plan and adjust their defenses based on the threat landscape and the business needs of their users. Threat actors have invested in techniques such as email thread hijacking, making it harder than ever for users to tell friend from foe."

The findings are based on data from the many millions of endpoints running HP Wolf Security. HP Wolf Security tracks malware by opening risky tasks in isolated, micro Virtual Machines (micro-VMs) to understand and capture the full infection chain, helping to mitigate threats that have slipped past other security tools. This has let customers click on over 10 billion email attachments, web pages, and downloads with no reported breaches[1]. By better understanding the behavior of malware in the wild, HP Wolf Security researchers and engineers can bolster endpoint security protection and overall system resilience.

Other key findings in the report include:

- 13% of email malware isolated had bypassed at least one email gateway scanner.
- Threats used 136 different file extensions in their attempts to infect organizations.
- 77% of malware detected was delivered via email, while web downloads were responsible for 13%.
- The most common attachments used to deliver malware were documents (29%), archives (28%), executables (21%), spreadsheets (20%).
- The most common phishing lures were related to the New Year or business transactions such as "Order", "2021/2022", "Payment", "Purchase", "Request" and "Invoice".

"Today, low-level threat actors can carry out stealthy attacks and sell access onto organized ransomware groups, leading to large-scale breaches that could cripple IT systems and grind operations to a halt," comments Dr. Ian Pratt, Global Head of Security for Personal Systems, HP Inc.

"Organizations should focus on reducing the attack surface and enabling quick recovery in the event of compromise. This means following Zero Trust principles and applying strong identity management, least privilege and isolation from the hardware level. For example, by isolating common attack vectors such as email, browsers or downloads using micro-virtualization, any potential malware or exploits lurking within are contained, rendering them harmless."

## About the data

This data was gathered within HP Wolf Security customer virtual-machines from October-December 2021.

-

## About HP

HP Inc. is a technology company that believes one thoughtful idea has the power to change the world. Its product and service portfolio of personal systems, printers, and 3D printing solutions helps bring these ideas to life. Visit http://www.hp.com.

## About HP Wolf Security

From the maker of the world's most secure PCs[2] and Printers[3], HP Wolf Security is a new breed[4] 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.

---

[1] Assumptions based on HP internal analysis of customer reported insights and installed base.

[2] 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.

[3] 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

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