HP Inc.
1501 Page Mill
Palo Alto, CA 94304

hp.com

News Release

HP threat research shows attackers exploiting zero-day vulnerability before enterprises can patch

HP Wolf Security threat research team sees cybercriminals using legitimate cloud providers to host malware, and switching up file and script types to evade detection tools

PALO ALTO, Calif., October 14, 2021 – 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 a unique insight into the latest techniques being used by cybercriminals.

The HP Wolf Security threat research team found evidence that cybercriminals are mobilizing quickly to weaponize new zero-day vulnerabilities. Exploits of the zero-day CVE-2021-40444[1] – a remote code execution vulnerability that enables exploitation of the MSHTML browser engine using Microsoft Office documents – were first captured by HP on September 8, a week before the patch was issued on September 14.

By September 10 – just three days after the initial threat bulletin – the HP threat research team saw scripts designed to automate the creation of this exploit being shared on GitHub. Unless patched, the exploit enables attackers to compromise endpoints with very little user interaction. It uses a malicious archive file, which deploys malware via an Office document. Users don't have to open the file or enable any macros, viewing it in File Explorer's preview pane is enough to initiate the attack, which a user often will not know has happened. Once the device is compromised, attackers can install backdoors to systems, which could be sold on to ransomware groups.

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

- **Rise in cybercriminals using legitimate Cloud and web providers to host malware**: A recent GuLoader campaign was hosting the Remcos Remote Access Trojan (RAT) on major platforms like OneDrive to evade intrusion detection systems and pass whitelisting tests. HP Wolf Security also discovered multiple malware families being hosted on gaming social media platforms like Discord.
- **JavaScript malware slipping past detection tools:** A campaign spreading various JavaScript RATs spread via malicious email attachments. JavaScript downloaders have a lower detection rate than Office downloaders or binaries. RATs are increasingly common as attackers aim to steal credentials for business accounts or crypto wallets.
- **Targeted campaign found posing as the Ugandan National Social Security fund:** Attackers used "typosquatting" – using a spoofed web address similar to an official domain name – to lure

targets to a site that downloads a malicious Word document. This uses macros to run a PowerShell script that blocks security logging and evades the Windows Antimalware Scan Interface feature.

- **Switching to HTA files spreads malware in a single click:** The Trickbot Trojan is now being delivered via HTA (HTML application) files, which deploy the malware as soon as the attachment or achive file containing it is opened. As an uncommon file type, malicious HTA files are less likely to be spotted by detection tools.

"The average time for a business to apply, test and fully deploy patches with the proper checks is 97 days, giving cybercriminals an opportunity to exploit this 'window of vulnerability'. While only highly capable hackers could exploit this vulnerability at first, automated scripts have lowered the bar for entry, making this type of attack accessible to less knowledgeable and resourced threat actors. This increases the risk to businesses substantially, as zero-day exploits are commoditized and made available to the mass market in venues like underground forums," explains Alex Holland, Senior Malware Analyst, HP Wolf Security threat research team, HP Inc. "Such novel exploits tend to be effective at evading detection tools because signatures may be imperfect and become obsolete quickly as the understanding of the scope of an exploit changes. We expect threat actors to adopt CVE-2021-40444 as part of their arsenals, and potentially even replace common exploits used to gain initial access to systems today, such as those exploiting Equation Editor."

"We are also seeing major platforms like OneDrive allowing hackers to conduct 'flash in the pan' attacks. While malware hosted on such platforms are generally taken down quickly, this does not deter attackers because they can often achieve their objective of delivering malware in the few hours the links are live," Holland continues. "Some threat actors are changing the script or file type they are using every few months. Malicious JavaScript and HTA files are nothing new, but they are still landing in employee inboxes, putting the enterprise at risk. One campaign deployed Vengeance Justice Worm, which can spread to other systems and USB drives."

The findings are based on data from the 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[2]. 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.

Key findings in the report include:

- 12% of email malware isolated had bypassed at least one gateway scanner
- 89% of malware detected was delivered via email, while web downloads were responsible for11%, and other vectors like removable storage devices for less than 1%
- The most common attachments used to deliver malware were archive files (38% – up from 17.26% last quarter), Word documents (23%), spreadsheets (17%), and executable files (16%)
- The top five most common phishing lures were related to business transactions such as "order", "payment", "new", "quotation" and "request"
- The report found 12% of malware captured was previously unknown[3]

"We can't keep relying on detection alone. The threat landscape is too dynamic and, as we can see from the analysis of threats captured in our VMs, attackers are increasingly adept at evading detection,"

comments Dr. Ian Pratt, Global Head of Security for Personal Systems, HP Inc. “Organizations must take a layered approach to endpoint security, following zero trust principles to contain and isolate the most common attack vectors like email, browsers, and downloads. This will eliminate the attack surface for whole classes of threats, while giving organizations the breathing room needed to coordinate patch cycles securely without disrupting services.”

- ENDS -

About the data

This data was gathered within HP Wolf Security customer virtual-machines from July - September 2021.

-

About HP

HP Inc. creates technology that makes life better for everyone, everywhere. Through our product and service portfolio of personal systems, printers, and 3D printing solutions, we engineer experiences that amaze. More information about HP Inc. is available at http://www.hp.com.

About HP Wolf Security

From the maker of the world’s most secure PCs[4] and Printers[5], HP Wolf Security is a new breed[6] 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.

HP WOLF SECURITY

[1] Microsoft credited security researchers Rick Cole (MSTIC), Dhanesh Kizhakkinan of Mandiant, Haifei Li of EXPMON, and Bryce Abdo of Mandiant for discovering the zero-day vulnerability.
[2] Assumptions based on HP internal analysis of customer reported insights and installed base.
[3] Based on first-seen in the wild data from multiple antivirus engines.
[4] 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.
[5] 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.
[6] HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.