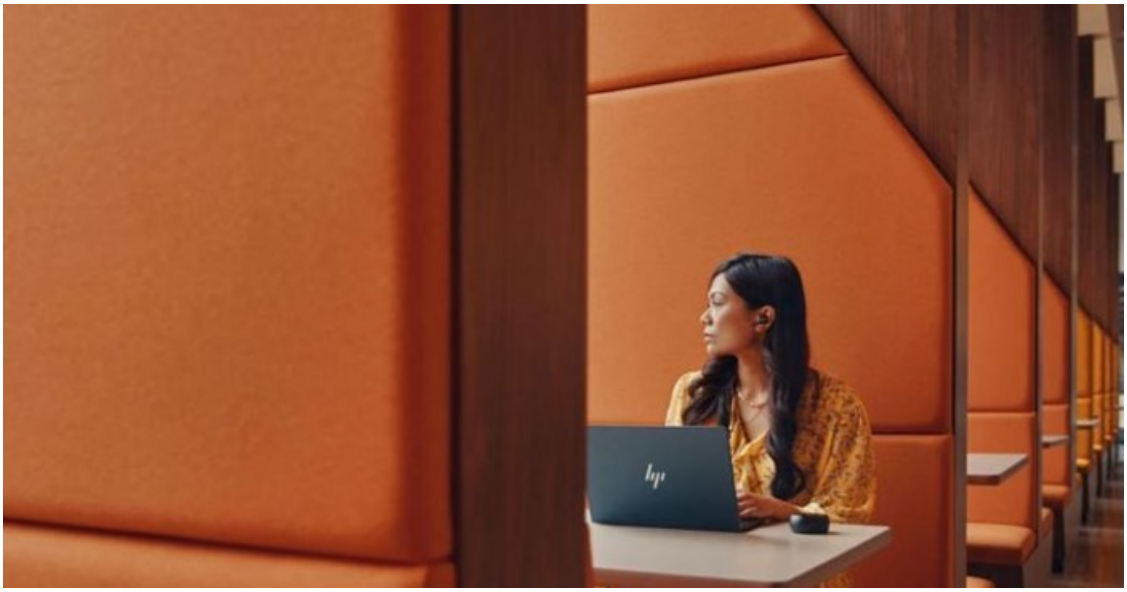
Cybersecurity threat report points to PDF and Discord malware danger

HP has released its latest Wolf Security Threat Insights Report, highlighting the persistent and innovative methods cyber attackers are using to manipulate users and compromise endpoints. The report reveals significant campaigns including the DarkGate campaign that utilises ad tools to enhance attacks, a shift from macros to Office exploits, an increase in PDF malware, and the use of Discord and TextBin to host malicious files. These findings reflect the evolving nature of cyber threats and an industry-wide need for constant vigilance and robust cybersecurity measures.



“Cybercriminals are becoming adept at getting into our heads and understanding how we work,” explains Alex Holland, senior malware analyst in the HP Wolf Security threat research team.

“For instance, the design of popular cloud services is always being refined, so when a fake error message appears, it won’t necessarily raise an alarm, even if a user hasn’t seen it before.”

> *“With GenAI generating even more convincing malicious content at little-to-no cost, distinguishing real from fake will only get harder”*

The HP Wolf Security research team has identified several significant campaigns, including:

A DarkGate campaign utilises ad tools to enhance attacks. Malicious PDF attachments, masquerading as OneDrive error messages, direct users to sponsored content hosted on a well-known ad network, leading to the DarkGate malware.

By utilising ad services, threat actors can analyse which lures generate clicks and infect the most users, thereby refining their campaigns for maximum impact.

They can also use CAPTCHA tools to prevent sandboxes from scanning malware and halting attacks by ensuring only humans click. DarkGate provides backdoor access for cybercriminals into networks, exposing victims to risks such as data theft and ransomware.

> *“ ﷺ We've analyzed a newcampaign using malicious PDF attachments to spread #DarkGate malware – with users directed to popular ad networks, these lures appear trustworthy, posing a greater risk.ﷺ More in our Threat Insights Report: https://t.co/rRV27hAFHZ*
> *— HP Wolf Security (@hpsecurity) February 15, 2024* ”

A shift from macros to Office exploits. In Q4, at least 84% of attempted intrusions involving spreadsheets, and 73% involving Word documents, sought to exploit vulnerabilities in Office applications. This continues the trend away from macro-enabled Office attacks.

However, macro-enabled attacks still have their place, particularly for attacks leveraging inexpensive commodity malware like Agent Tesla and XWorm.

An increase in PDF malware. About 11% of malware analysed in Q4 used PDFs to deliver malware, a significant increase from just 4% in Q1 and Q2 2023. A notable example was a WikiLoader campaign using a counterfeit parcel delivery PDF to deceive users into installing Ursnif malware.

SA hospitality sector a target for new malware campaign
Ross Anderson 15 Feb 2024

Discord and TextBin used to host malicious files. Threat actors are exploiting legitimate file and text sharing websites to host malicious files. These sites are often trusted by organisations, helping the sites to evade anti-malware scanners and increasing the chances of attackers remaining undetected.

Cyber criminals are using the same tools as businesses

“Cybercriminals are applying the same tools a business might use to manage a marketing campaign to optimise their malware campaigns, increasing the likelihood the user will take the bait,” says Dr Ian Pratt, global head of security for personal systems at HP Inc.

“To protect against well-resourced threat actors, organisations must follow zero trust principles, isolating and containing risky activities like opening email attachments, clicking on links, and browser downloads."