U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0318

FAKE MS SYSTEM UPDATE DROPS AURORA STEALER

DATE ISSUED: 15th May 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Malwarebytes has discovered a malvertising campaign used by threat actors to trick users with in-browser malicious ads that redirect users to a fake Windows security update page. Utilising advertisements to deliver malware is called malvertising.

BREAKDOWN

According to researchers at Malwarebytes, threat actors are buying pop-under ads targeting adult traffic and redirecting potential victims to a malware-serving location. Pop-under ads are ‘pop-up’ ads that launch behind the active browser window, staying hidden from the user until they close or move the main browser window. However, the threat actor devised an imaginative idea where the pop-under renders a full-screen browser window that simulates a Windows system update screen. Browsing the web is a daily habit for almost anyone with an internet connection. The researchers analysed the domains used in this campaign, many appearing to impersonate adult websites that mimicked the fake Windows update. The domain served for downloading a file named "ChromeUpdate.exe," revealing the deception of the full-screen browser screen. However, the Chrome updater is a ‘fully undetectable’ (FUD) malware called ‘Invalid Printer’. Invalid Printer first checks the host’s graphic card to determine if it’s running on a virtual machine or in a sandbox environment. The researchers found that it unpacks and launches a copy of the Aurora information stealer.

REMEDIATION STEPS

- Educate employees about the importance of proper cyber security and how to protect themselves. Offer regular refresher training for the whole company, including training on new data processes and laws.
- Implement and regularly update the Anti-virus and Anti-malware software.
- Implement a Next Generation Firewall to detect malicious, inbound and outbound activity.
- Configure regular scans and monitor to identify unusual traffic and behaviour patterns that may indicate malware activity.
- Patch known vulnerabilities in all remote access and external facing devices

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/fake-in-browser-windows-updates-push-aurora-info-stealer-malware/
Malwarebytes	https://www.malwarebytes.com/blog/threat-intelligence/2023/05/fake-system-update-drops-new-highly-evasive-loader