Threat Image

As October arrives, we mark the 20th anniversary of Cybersecurity Awareness Month—a significant milestone. Cybersecurity month is a valuable opportunity to bolster cybersecurity awareness within your organization. Numerous free online resources and engaging activities will be awaiting your participation. Cybersecurity and Infrastructure Security Agency (CISA) has published Resources and Partner Toolkit (1), and their complimentary webinars are recommended resources for your internal campaign (2).

According to CISA, there are a few essential steps to stay safe online (2):

1. Use strong passwords
2. Turn on MFA
3. Recognize and report fishing
4. Update software

Threat actors are selling a new crypter and loader called ASMCrypt. Researchers describe ASMCrypt malware as an evolved version of another known loader malware called DoubleFinger (3). According to Kaspersky (4), the idea behind this type of malware is to load the final payload without the loading process or the payload itself being detected by AV/EDR, etc. It uses hard-coded credentials to connect with a backend service on the TOR network. Buyers can customize payloads for their campaigns by creating encrypted blobs hidden inside PNG files and uploading them to image hosting sites. (3)

At the end of September, Google released a patch for an actively exploited Zero-Day Vulnerability. It is the 5th one this year. Recent high-severity zero-day (CVE-2023-5217) involves a heap buffer overflow in the VP8 encoding of the libvpx video codec library. While Google didn't disclose specific details about the attacks, they have taken proactive measures to protect users. Google advises users to update Chrome to version 117.0.5938.132 to safeguard against potential threats. (5)

Most recent online cybersecurity risks (6):

- CLOP Gang Stolen Data From Major North Carolina Hospitals
- Sponsor with batch-filed whiskers: Ballistic Bobcat's scan and strike backdoor
- Improper Usage of SAS Token Leads to Massive Microsoft Data Leakage
- PSA: Ongoing Webex Malvertising Campaign Drops BatLoader
- Inside the Code of a New XWorm Variant
- New MidgeDropper Variant

(1) https://www.cisa.gov/resources-tools/resources/cybersecurity-awareness-month-2023-resources-and-partner-toolkit
(2) https://www.cisa.gov/cybersecurity-awareness-month
(3) https://thehackernews.com/2023/09/cybercriminals-using-new-asmcrypt.html
(4) https://securelist.com/crimeware-report-asmcrypt-loader-lumma-stealer-zanubis-banker/110512/
(5) https://thehackernews.com/2023/09/update-chrome-now-google-releases-patch.html
(6) https://innovatecybersecurity.com/security-threat-advisory/