GovCERT.HK

Weekly IT Security News Bulletin, 2022-W21

23 May – 29 May 2022

Headlines

Browser-hijacking malware targeting Windows and macOS users

- Security researchers from Red Canary warned of a surge of browser-hijacking malware dubbed ChromeLoader. ChromeLoader is a browser extension and spreads through social media platforms and websites for cracked or pirated software. The researchers suggested that ChromeLoader is designed to redirect user traffic to advertising websites by modifying the web browser's settings.

- Attackers distribute ChromeLoader via an ISO file masquerading as a cracked video game or pirated movie. The ISO file included an executable file and once executed, the file would create a scheduled task using the Task Scheduler API. The scheduled task was configured to execute a Base64-encoded PowerShell command to add a malicious extension to a victim's Chrome browser, allowing attackers to hijack users' search queries.

- The researchers uncovered that ChromeLoader not only targeted Windows users but also affected macOS users. Instead of using the PowerShell command, a macOS variant of ChromeLoader was found using an encoded bash script to load the malicious extension in both Chrome and Safari web browsers.

Advice

- Enforce application whitelisting to avoid malicious programs or processes from running on the systems.
- Implement detection mechanism to look for the execution of encoded PowerShell commands or bash scripts on the systems.

Sources

- Red Canary
- Binary Defense

Warn of fake Windows 11 downloads to distribute info-stealer

- While Microsoft is promoting its new Windows 11 installations, security researchers found some phishing websites providing fake Windows 11 downloads that were used to distribute an information-stealing malware named Vidar. The phishing websites impersonated the official download portal to lure victims to download the malicious ISO file that contained the Vidar malware.

- The Vidar malware was able to exfiltrate data from compromised systems, including system information, browser history, online account credentials, financial data, and various cryptocurrency wallet credentials, to its command and control (C2) servers. The actual URLs of C2 servers used by the malware were fetched from attacker-controlled social media channels hosted on Telegram and Mastodon.

- In addition to fake Windows 11 downloads, the researchers also discovered that backdoored versions of Adobe Photoshop were used to distribute the Vidar malware.

Advice

- Stay alert of the risk of phishing attacks and be vigilant when clicking on URLs that are seemingly for Windows 11.
- Only download software from the vendor's official websites.

Sources

- ZDNet
- Zscaler

Product Vulnerability Notes & Security Updates

1. Citrix

https://support.citrix.com/article/CTX457048

2. Debian

https://www.debian.org/security/2022/dsa-5140
https://www.debian.org/security/2022/dsa-5142
https://www.debian.org/security/2022/dsa-5143
https://www.debian.org/security/2022/dsa-5144
https://www.debian.org/security/2022/dsa-5145
https://www.debian.org/security/2022/dsa-5146
https://www.debian.org/security/2022/dsa-5147
https://www.debian.org/security/2022/dsa-5148

3. F5 Products

https://support.f5.com/csp/article/K08832573
https://support.f5.com/csp/article/K32760744
https://support.f5.com/csp/article/K54724312

4. Horner Automation Cscape Csfont

https://us-cert.cisa.gov/ics/advisories/icsa-22-146-02

5. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211020-01-outofwrite-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220601-01-f75b152f-en

6. Keysight N6854A Geolocation server and N6841A RF Sensor software

https://us-cert.cisa.gov/ics/advisories/icsa-22-146-01

7. Matrikon OPC Server

https://us-cert.cisa.gov/ics/advisories/icsa-22-144-02

8. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/2UEZ3PJ3DAR7WW2V4JZQJRIGUJPQLXAM/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/3KBBNULLJDSNJL4TX5G6CQQKGRTS2P4P/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/3NGRELWLSJFFDNLB6BPNKDYNQZTP6PPE/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4BXZJPBMKANARAA3VO6JSVP3WW4VVBOD/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/6SKSNREEUCKR3NCO6RCBRLJRHMS5HJNX/

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/7NQSHXNFEE2OGIYVYN23S2BDDQTAGLSJ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/A4FXCISHLK7JAPLSWW5AVMMWZDDJXZPL/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ALZK7XVGKV7AHWFYGIHMQ7I3SNSEFBCZ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/H2A43RISVL27M3ODDCLLDJKV265ATZ43/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/H67WLPQ3LF4GRKIXDOTJFA2DT732SNIG/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/HYUWTFEQRRF6UNFTUF4BLNNFIPVSZV3I/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/JEVUIGDCWRXB5ZFSV2K4UGVJCEMNQQ2X/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/MXOV3UNFRYPSEHTASLNZW4RV4B6YIQTO/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/NERGELOQ43TXPK5SCGTMYFI4KDXITL74/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/QPGDG7DXWS6TFXU77I5W47YWDVVMA4QB/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/SUDOFXIJEWHRB6222QAVZD3Q3CXXNW7K/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/TECGPMBMRF6XCLE3FXG3LMK4ZGTK275U/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/U4SLHXE2O3IXMI4KAK7QSBITGXIK6OW2/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/U7GUMTUMSI224PUGUBEIBEQ3BB4IECEG/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/UG3NXFDYPIEMY6XALMADAPU5W5UKN4LK/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/VZEKTX6LOHELIEEVJYSONO5MX6DZOZIA/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WPP6RRBCICFV3YEFQ4AXK2HP5GANL2SF/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/X57Z3J7LFHBDM7POCXSQXKTVJZIVTNPE/

9. Oracle Linux

https://linux.oracle.com/errata/ELSA-2022-4729.html
https://linux.oracle.com/errata/ELSA-2022-9409.html
https://linux.oracle.com/errata/ELSA-2022-9410.html
https://linux.oracle.com/errata/ELSA-2022-9412.html
https://linux.oracle.com/errata/ELSA-2022-9413.html
https://linux.oracle.com/errata/ELSA-2022-9419.html
https://linux.oracle.com/errata/ELSA-2022-9421.html
https://linux.oracle.com/errata/ELSA-2022-9422.html
https://linux.oracle.com/errata/ELSA-2022-9423.html
https://linux.oracle.com/errata/ELSA-2022-9425.html
https://linux.oracle.com/errata/ELSA-2022-9426.html
https://linux.oracle.com/errata/ELSA-2022-9427.html
https://linux.oracle.com/errata/ELSA-2022-9432.html
https://linux.oracle.com/errata/ELSA-2022-9433.html

10. Red Hat

https://access.redhat.com/errata/RHSA-2022:2263
https://access.redhat.com/errata/RHSA-2022:2264
https://access.redhat.com/errata/RHSA-2022:2265
https://access.redhat.com/errata/RHSA-2022:2268
https://access.redhat.com/errata/RHSA-2022:2272
https://access.redhat.com/errata/RHSA-2022:2283
https://access.redhat.com/errata/RHSA-2022:4699
https://access.redhat.com/errata/RHSA-2022:4711
https://access.redhat.com/errata/RHSA-2022:4712
https://access.redhat.com/errata/RHSA-2022:4717
https://access.redhat.com/errata/RHSA-2022:4721
https://access.redhat.com/errata/RHSA-2022:4722
https://access.redhat.com/errata/RHSA-2022:4729
https://access.redhat.com/errata/RHSA-2022:4745
https://access.redhat.com/errata/RHSA-2022:4764

11. Rockwell Automation Logix Controllers

https://us-cert.cisa.gov/ics/advisories/icsa-22-144-01

12. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.368760
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.372629
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.380055
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.459263

13. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20221762-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221764-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221768-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221771-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221783-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221796-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221803-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221804-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221805-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221808-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221815-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221817-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221818-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221819-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221829-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221830-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221831-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20221832-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221833-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221835-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221836-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221840-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221842-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221844-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221845-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221846-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221847-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221849-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221853-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221859-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221861-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221862-1/

14. Trend Micro

https://success.trendmicro.com/solution/000291042

15. Ubuntu

https://ubuntu.com/security/notices/USN-5402-2
https://ubuntu.com/security/notices/USN-5404-2
https://ubuntu.com/security/notices/USN-5432-1
https://ubuntu.com/security/notices/USN-5433-1
https://ubuntu.com/security/notices/USN-5434-1
https://ubuntu.com/security/notices/USN-5436-1
https://ubuntu.com/security/notices/USN-5437-1
https://ubuntu.com/security/notices/USN-5438-1
https://ubuntu.com/security/notices/USN-5439-1
https://ubuntu.com/security/notices/USN-5440-1
https://ubuntu.com/security/notices/USN-5441-1
https://ubuntu.com/security/notices/USN-5442-1
https://ubuntu.com/security/notices/USN-5443-1
https://ubuntu.com/security/notices/USN-5444-1
https://ubuntu.com/security/notices/USN-5445-1
https://ubuntu.com/security/notices/USN-5446-1
https://ubuntu.com/security/notices/USN-5447-1
https://ubuntu.com/security/notices/USN-5448-1
https://ubuntu.com/security/notices/USN-5449-1

16. VMware

https://www.vmware.com/security/advisories/VMSA-2022-0015.html

Sources of product vulnerability information:

- Citrix
- Debian
- F5 Products
- Huawei
- openSUSE
- Oracle Linux
- Red Hat
- Slackware
- SUSE
- Trend Micro
- Ubuntu
- US-CERT
- VMware

Contact:

cert@govcert.gov.hk