GovCERT.HK

Weekly IT Security News Bulletin, 2021-W52

27 December 2021 – 2 January 2022

Headlines

Password stealer targeting accounts saved in web browsers

- A recent information-stealing campaign was found distributing malware dubbed RedLine in an attempt to steal account credentials from an infected system. Attackers then used the stolen credentials to compromise relevant accounts for malicious purposes or financial gain.

- RedLine is a popular information-stealing malware distributed through phishing campaigns, social media platforms, and websites for cracked software. In addition to stealing credentials stored in web browsers, VPN and FTP clients, RedLine is capable of extracting cookies and autofill information stored in web browsers, deploying additional software, and executing commands on the infected system.

- A security researcher recently found a collection of accounts stolen in the campaign using RedLine in an exposed server. Those accounts have been included in the "Have I Been Pwned (HIBP)" data breach notification website to let users check their compromised status.

Advice

- Use a unique password for each system or service account and change all passwords promptly if they are suspected of being compromised or disclosed to others.
- Enable multi-factor authentication for accounts if available.
- Consider using a dedicated password management solution instead of the autofill feature in web browsers to securely store passwords.

Sources

- AhnLab ASEC
- Bleeping Computer

A growing threat of malicious dormant domains

- A recent report published by Palo Alto Networks revealed a growing trend of threat actors using dormant domains for malicious activities to evade security detection, after analysing the traffic associated with tens of thousands of domains. Among the analysed domains, almost 3.8% are malicious domains.

- The report also showed that dormant domains involved in malicious activities were threefold more than newly registered domains. The significant increase was attributed to the fact that using a domain dormant for years in malware campaigns could less likely be blocked by some reputation-based detectors.

- To identify a malicious dormant domain, a sudden increase in the volume of traffic through the domain and the domain generation algorithm (DGA) subdomain could be an indicator of malicious nature. Incomplete or missing registrant details of a domain could also imply its malicious nature.

Advice

- Enable DNS logging on network devices and monitor the domain name resolution traffic for detection of suspicious activities.
- Consider using network security solutions to identify and block suspicious domains.

Sources

- Palo Alto Networks
- Bleeping Computer

Product Vulnerability Notes & Security Updates

1. Debian

https://www.debian.org/security/2021/dsa-5030
https://www.debian.org/security/2021/dsa-5031
https://www.debian.org/security/2021/dsa-5032

2. F5 Products

https://support.f5.com/csp/article/K14122652
https://support.f5.com/csp/article/K16090693
https://support.f5.com/csp/article/K53280389

3. Fortinet

https://www.fortiguard.com/psirt/FG-IR-21-253

4. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180815-01-cpu-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20211229-01-xss-en

5. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/3W3FKE7L66ATNR7X2EAUWUFKP5BK5SZM/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4BQ3YNECTWF6XMIQDZ7C5QEDQ3QPQT4W/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DLVFS4U5WQY3UT4TIXF3TKNGVMQCDKHC/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DUJZLITO4GTLR5FP75FBCLDYZMUY2AFI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FID3SSV5OLDMECWDA753FLD5OC6YLAUG/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/HKG4SHDRVYYGSRQNKBCCH6YJUQX2D54K/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/KMK3AKW3Y2J574OXHVFX4QFELTEHM6MR/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/KZGJOQCY3UVCSZY3XFCDUYHPVWB2IH7T/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/MUGBIA3IOPBRCHCVWXL5KMYQ6TB5Z5XI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/NOF2UA3DXYGYPKJVCZWZ5HMXL2PTHSJR/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/QD3TW7GD6PF3ZSKL2TJG3Z462FFFLJND/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/VHZ7COSTMBF33SO76DMFLY7V62XQUQLS/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/XCIUJE3F5UEWI5TYYL5CQ7SCQZU5V76Q/

6. **Red Hat**

   https://access.redhat.com/errata/RHSA-2021:5235
   https://access.redhat.com/errata/RHSA-2021:5236

7. **Slackware**

   https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.501086

8. **SUSE**

   https://www.suse.com/support/update/announcement/2021/suse-su-20214190-1/
   https://www.suse.com/support/update/announcement/2021/suse-su-20214191-1/
   https://www.suse.com/support/update/announcement/2021/suse-su-20214192-1/
   https://www.suse.com/support/update/announcement/2021/suse-su-20214193-1/
   https://www.suse.com/support/update/announcement/2021/suse-su-20214200-1/
   https://www.suse.com/support/update/announcement/2021/suse-su-20214201-1/
   https://www.suse.com/support/update/announcement/2021/suse-su-20214202-1/

9. **Trend Micro**

   https://success.trendmicro.com/solution/000289996

10. **Wireshark**

    https://www.wireshark.org/security/wnpa-sec-2021-16.html
    https://www.wireshark.org/security/wnpa-sec-2021-17.html
    https://www.wireshark.org/security/wnpa-sec-2021-18.html
    https://www.wireshark.org/security/wnpa-sec-2021-19.html
    https://www.wireshark.org/security/wnpa-sec-2021-20.html
    https://www.wireshark.org/security/wnpa-sec-2021-21.html
    https://www.wireshark.org/security/wnpa-sec-2021-22.html

Sources of product vulnerability information:

Debian
F5 Products
Fortinet
Huawei
openSUSE
Red Hat
Slackware
SUSE
Trend Micro
Wireshark

Contact:

cert@govcert.gov.hk