GovCERT.HK

Weekly IT Security News Bulletin, 2021-W01

4 January – 10 January 2021

Headlines

Malware uses BSSID to find out the geolocation of infected hosts

- It is common that attackers are interested to find out where the infected hosts are located. For example, they may want to check which countries or organisations the hosts are belonging to in order to identify the valuable targets and plan for further exploitation. Usually, the geolocation can be predicted based on IPs. Attackers may make use of Geolocation IP database or APIs which are available for free or paid access.

- The findings in a recent analysis by a researcher show that malware may also try to geolocate the infected host using Basic Service Set Identifier (BSSID). Each access point or router has a BSSID which is the Media Access Control (MAC) address for uniquely identifying the device. When a device is moved from one place to another, the BSS in use may change as the area may be covered by another access point.

- The malware collects the BSSID of the access point or default gateway (for VM environment) and submits a query to Mylnikov's database, a public API of WiFi geolocation database which contains mappings of BSSIDs and geographical location. The latitude and longitude values returned by the database can then be used to identify the city or country of the victims using another public web service (Geocode.xyz).

- Such approach is considered a more accurate method to determine the physical geolocation of the victims and can be used to cross-check the location derived from the IP.

Advice

- Reduce the exposure of your network to reduce the chance of network information being collected and exposed to the public domain.
- Check if there is any access to geo-location database or API by unknown applications or processes.
- Update antivirus definitions in a timely manner.

Sources

- SANS
- ZDNet

Replace deprecated TLS protocol configurations now

- The National Security Agency (NSA) recently published a guidance on how to detect, prioritise and replace deprecated Transport Layer Security (TLS) protocols with ones which are up-to-date and secure.

- While TLS is widely used in online services and applications for providing secure and private communication channel between servers and clients through encryption and authentication, the old and deprecated versions of TLS (e.g., TLS 1.0, TLS 1.1 and SSL) are found to be susceptible to various attacks like Heartbleed, POODLE, BEAST, CRIME due to vulnerabilities in the protocols.

- Using deprecated versions of TLS may open a door for hackers to intercept the communication and decrypt the content therein through man-in-the-middle attacks. To mitigate the risks of data leakage, systems and applications should only use TLS 1.2 or TLS 1.3 which have fixed the flaws in the old versions.

- In the guidance, NSA advises network administrators to detect and replace deprecated TLS configurations in their environments by adopting the recommended tools and methods so as to ensure that only authorised and strong encryption protocols are in use and therefore improve the cybersecurity posture of the organisations. Furthermore, NSA also suggests organisations to set up monitoring and even blocking of any traffic using insecure TLS protocols, cipher suites, and key exchanges with reference to the detection strategies provided.

- In a study conducted last year, over 850,000 websites were found using TLS 1.0 or TLS 1.1. It should be noted that those insecure TLS versions are no longer supported by some web browsers like Chrome and Mozilla.

Advice

- Update any deprecated TLS configurations in your environment to newer and secure versions.
- Do not transfer sensitive data through insecure communication channels using deprecated TLS versions.
- Consider blocking network traffic involving insecure TLS to eliminate the risks of data leakage.

Sources

- NSA
- Bleeping Computer
- Netcraft

Product Vulnerability Notes & Security Updates

1. Android

https://source.android.com/security/bulletin/2021-01-01

2. Debian

https://www.debian.org/security/2021/dsa-4822
https://www.debian.org/security/2021/dsa-4823
https://www.debian.org/security/2021/dsa-4824
https://www.debian.org/security/2021/dsa-4825

3. Delta Electronics Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-005-05
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-06

4. F5 Traffix SDC

https://support.f5.com/csp/article/K44415301

5. Fortinet Products

https://www.fortiguard.com/psirt/FG-IR-20-103
https://www.fortiguard.com/psirt/FG-IR-20-123
https://www.fortiguard.com/psirt/FG-IR-20-124
https://www.fortiguard.com/psirt/FG-IR-20-125
https://www.fortiguard.com/psirt/FG-IR-20-126
https://www.fortiguard.com/psirt/FG-IR-20-177

6. GE Reason RT43X Clocks

https://us-cert.cisa.gov/ics/advisories/icsa-21-005-03

7. Google Chrome

https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html

8. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-0003.html
https://linux.oracle.com/errata/ELSA-2021-0024.html

9. Panasonic FPWIN Pro

https://us-cert.cisa.gov/ics/advisories/icsa-21-005-02

10. Red Hat Products

https://access.redhat.com/errata/RHSA-2021:0003
https://access.redhat.com/errata/RHSA-2021:0004
https://access.redhat.com/errata/RHSA-2021:0019
https://access.redhat.com/errata/RHSA-2021:0024
https://access.redhat.com/errata/RHSA-2021:0028
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-04

11. Schneider Electric Web Server on Modicon M340

https://us-cert.cisa.gov/ics/advisories/icsa-21-005-01

12. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210014-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210015-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210017-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210018-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210019-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210022-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210023-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210027-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210028-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210029-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210031-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210032-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114198-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114592-1/

13. Ubuntu

https://ubuntu.com/security/notices/USN-4668-3
https://ubuntu.com/security/notices/USN-4673-1
https://ubuntu.com/security/notices/USN-4674-1
https://ubuntu.com/security/notices/USN-4674-2
https://ubuntu.com/security/notices/USN-4675-1
https://ubuntu.com/security/notices/USN-4676-1
https://ubuntu.com/security/notices/USN-4677-1
https://ubuntu.com/security/notices/USN-4677-2
https://ubuntu.com/security/notices/USN-4678-1
https://ubuntu.com/security/notices/USN-4679-1
https://ubuntu.com/security/notices/USN-4680-1
https://ubuntu.com/security/notices/USN-4681-1
https://ubuntu.com/security/notices/USN-4682-1
https://ubuntu.com/security/notices/USN-4683-1

Sources of product vulnerability information:

- Android
- Debian
- F5
- Fortinet
- Google Chrome
- Oracle Linux
- Red Hat
- SUSE
- Ubuntu
- US-CERT

Contact:

cert@govcert.gov.hk