GovCERT.HK

Weekly IT Security News Bulletin, 2020-W43

19 October – 25 October 2020

Headlines

Takedown of TrickBot

- TrickBot is a notorious trojan which contributes to the establishment of a huge network of infected devices for carrying out malicious activity like distributing ransomware, sending phishing emails, stealing credentials. Being one of the most successful malware-as-a-service operations, it is reported to have infected over a million of devices since 2016.

- Recently, Microsoft had a coordinated operation with the US Cyber Command to take down the TrickBot network. As reported by Microsoft, about 94% of critical infrastructure of the TrickBot network was taken down in this operation.

- However, it was observed that the cyber criminals behind TrickBot also quickly recovered the infrastructure by setting up new servers in their network and had various fallback mechanisms in place. Furthermore, some TrickBot's command and control servers are located in various places which can be out of the jurisdictions where the court orders were obtained for this takedown operation.

- While TrickBot was not completely removed, the takedown attempt was considered as successful disruption efforts that added additional costs to the cyber criminals and delay their operations and attacks.

Advice

- Apply the latest security patches and install anti-malware tools to safeguard devices against malware.
- Be aware of suspicious emails and do not open any links or attachments from unknown sources.

Sources

- Microsoft
- Dark Reading
- ZDNet

Telegram and email accounts hijacked in SS7 mobile attack

- Nowadays, many applications use short message service (SMS) to deliver verification codes to users. Besides multi-factor authentication, it is also commonly used for password recovery. However, such approach is considered as insecure and vulnerable to attack due to the loopholes in Signaling System No. 7 (SS7), which is a protocol used in mobile phone network across the world.

- In a recent case happened in Israel, attackers hijacked SMS messages by spoofing a short message service center (SMSC) of a carrier and send an update location request for the victims' phone numbers from a foreign carrier network to the carrier. This tricked the carrier to send all SMS messages intended for the victims to the attacker's SMSC. The victims were registered to the foreign carrier network and stopped getting any SMS message.

- By hijacking the SMS services, the attackers successfully gained access to Telegram and email of accounts of the victims and impersonated the victims to send messages.

- Such attack is however not easy and it requires knowledge about the user including their unique international subscriber numbers (MSISDN) and International Mobile Subscriber Identity (IMSI) numbers.

Advice

- Duly consider the associated risks before choosing SMS as a factor for authentication.
- Use encrypted messaging services or applications rather than SMS for communication of sensitive information.
- Keep your device in safe custody at all times and do not disclose any technical details of your mobile service subscription to third-party.

Sources

- Bleeping Computer
- HAARETZ

Product Vulnerability Notes & Security Updates

1. **B. Braun Products**

   https://us-cert.cisa.gov/ics/advisories/icsma-20-296-01
   https://us-cert.cisa.gov/ics/advisories/icsma-20-296-02

2. **Debian**

   https://www.debian.org/security/2020/dsa-4773
   https://www.debian.org/security/2020/dsa-4774
   https://www.debian.org/security/2020/dsa-4775
   https://www.debian.org/security/2020/dsa-4776
   https://www.debian.org/security/2020/dsa-4777
   https://www.debian.org/security/2020/dsa-4778

3. **F5 Products**

   https://support.f5.com/csp/article/K04107324
   https://support.f5.com/csp/article/K85742355

4. **Gentoo Linux**

   https://security.gentoo.org/glsa/202010-01
   https://security.gentoo.org/glsa/202010-02
   https://security.gentoo.org/glsa/202010-03
   https://security.gentoo.org/glsa/202010-04
   https://security.gentoo.org/glsa/202010-05
   https://security.gentoo.org/glsa/202010-06

5. **Google Chrome**

   https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html

6. **Hitachi ABB Power Grids XMC20 Multiservice-Multiplexer**

   https://us-cert.cisa.gov/ics/advisories/icsa-20-294-02

7. **IBM InfoSphere Information Server**

   https://www.ibm.com/support/pages/node/6342985

8. **Microsoft Products**

   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17022
   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17023

9. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00026.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00027.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00028.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00029.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00030.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00031.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00032.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00033.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00034.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00035.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00036.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00037.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00038.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00039.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00040.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00041.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00042.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00043.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00044.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00045.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00046.html
https://lists.opensuse.org/opensuse-security-announce/2020-10/msg00047.html

10. Oracle Linux

https://linux.oracle.com/errata/ELSA-2020-4272.html
https://linux.oracle.com/errata/ELSA-2020-4286.html
https://linux.oracle.com/errata/ELSA-2020-4305.html

11. QNAP Products

https://www.qnap.com/en/security-advisory/qsa-20-07

12. Red Hat

https://access.redhat.com/errata/RHSA-2020:4223
https://access.redhat.com/errata/RHSA-2020:4264
https://access.redhat.com/errata/RHSA-2020:4265
https://access.redhat.com/errata/RHSA-2020:4272
https://access.redhat.com/errata/RHSA-2020:4273
https://access.redhat.com/errata/RHSA-2020:4274
https://access.redhat.com/errata/RHSA-2020:4276
https://access.redhat.com/errata/RHSA-2020:4277
https://access.redhat.com/errata/RHSA-2020:4278
https://access.redhat.com/errata/RHSA-2020:4279
https://access.redhat.com/errata/RHSA-2020:4280
https://access.redhat.com/errata/RHSA-2020:4281
https://access.redhat.com/errata/RHSA-2020:4285
https://access.redhat.com/errata/RHSA-2020:4286

https://access.redhat.com/errata/RHSA-2020:4287
https://access.redhat.com/errata/RHSA-2020:4288
https://access.redhat.com/errata/RHSA-2020:4289
https://access.redhat.com/errata/RHSA-2020:4290
https://access.redhat.com/errata/RHSA-2020:4291
https://access.redhat.com/errata/RHSA-2020:4295
https://access.redhat.com/errata/RHSA-2020:4299
https://access.redhat.com/errata/RHSA-2020:4304
https://access.redhat.com/errata/RHSA-2020:4305
https://access.redhat.com/errata/RHSA-2020:4306
https://access.redhat.com/errata/RHSA-2020:4307
https://access.redhat.com/errata/RHSA-2020:4310
https://access.redhat.com/errata/RHSA-2020:4311
https://access.redhat.com/errata/RHSA-2020:4312
https://access.redhat.com/errata/RHSA-2020:4315
https://access.redhat.com/errata/RHSA-2020:4316
https://access.redhat.com/errata/RHSA-2020:4317

13. Rockwell Automation 1794-AENT Flex I/O Series B

https://us-cert.cisa.gov/ics/advisories/icsa-20-294-01

14. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2020&m=slackware-security.420341
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2020&m=slackware-security.780685

15. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20202712-2/
https://www.suse.com/support/update/announcement/2020/suse-su-20202941-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202942-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202943-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202947-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202951-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202966-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202967-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202968-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202969-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202970-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202972-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202980-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202981-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202988-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202995-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202996-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202997-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202998-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202999-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20203003-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014521-1/

16. Ubuntu

https://ubuntu.com/security/notices/USN-4546-2
https://ubuntu.com/security/notices/USN-4552-2
https://ubuntu.com/security/notices/USN-4586-1
https://ubuntu.com/security/notices/USN-4587-1
https://ubuntu.com/security/notices/USN-4590-1
https://ubuntu.com/security/notices/USN-4591-1
https://ubuntu.com/security/notices/USN-4592-1
https://ubuntu.com/security/notices/USN-4593-1
https://ubuntu.com/security/notices/USN-4593-2
https://ubuntu.com/security/notices/USN-4594-1
https://ubuntu.com/security/notices/USN-4595-1
https://ubuntu.com/security/notices/USN-4596-1
https://ubuntu.com/security/notices/USN-4597-1
https://ubuntu.com/security/notices/USN-4598-1
https://ubuntu.com/security/notices/USN-4600-1
https://ubuntu.com/security/notices/USN-4601-1

17. VMware Horizon Client

https://www.vmware.com/security/advisories/VMSA-2020-0022.html

Sources of product vulnerability information:

Debian
F5
Gentoo Linux
Google Chrome
IBM
Microsoft
openSUSE
Oracle Linux
QNAP
Red Hat
Slackware
SUSE
Ubuntu
US-CERT
VMware

Contact:

cert@govcert.gov.hk