GovCERT.HK

Weekly IT Security News Bulletin, 2020-W35

24 August –30 August 2020

Headlines

Worldwide ransom denial of service (RDoS) attacks

- Multiple financial institutions across the world suffered RDoS attacks from hacker groups named themselves as "Fancy Bear" in August 2020. One of the victims was a stock exchange of which the website was brought down five times within five trading days in late August.

- In the first stage of the attack, the targeted institution received an extortion email. The attackers threatened to launch a big distributed denial of service (DDoS) attack against the institution unless it paid a ransom in Bitcoin.

- If the message was ignored or the ransom not paid, DDoS attacks would be triggered to destruct the victim's backend infrastructure, application programming interface (API) endpoints, and domain name service (DNS) servers. The attacker would also frequently change the network protocols used for hitting the targets, making it difficult for the victim to effectively block attack traffic, resulting in prolonged service interruptions.

Advice

- Subscribe a scalable DDoS mitigation service to protect Internet-facing systems from various magnitudes of attacks.

- Protect the backend infrastructure, API endpoints, and DNS servers in addition to Internet-facing websites and web applications when formulating defence against DDoS attacks.

- Conduct regular vulnerability scanning covering all network protocols in use, fix the vulnerabilities found timely, and minimise the systems' Internet exposure as far as possible.

Sources

- ZDNet
- NZCity

Top three ways of ransomware attacks against enterprises

- It was reported that ransomware attacks against enterprises reached a historical peak in the first half of year 2020. The three most prevalent intrusion methods used by ransomware criminals were identified to be unsecured Remote Desktop Protocol (RDP), unpatched virtual private network (VPN) gateways, and phishing emails.

- Multiple cyber security vendors reported that RDP remarkably topped the list of attack vectors for ransomware infection. The protocol is for making remote connections to Microsoft Windows computers. Millions of computers had their RDP ports exposed on the Internet so that threat actors could scan for exposed computers and attempt to crack their usernames and passwords. The compromised credentials and connections could then be resold to other cyber criminals for further attacks including ransomware attacks.

- A number of severe vulnerabilities in popular VPN appliances disclosed in 2019 were also widely exploited by ransomware attackers to gain entry into enterprise networks. The attackers' favourite picks included Citrix systems' bug CVE-2019-19781 and Pulse Secure Systems' bug CVE-2019-11510, among others. Patches to fix the vulnerabilities have been made available by the corresponding manufacturers.

Advice

- Avoid exposing RDP ports to the Internet.

- Deploy a VPN solution as an additional layer of protection if remote access is required. Review the VPN configurations regularly and patch all known bugs of your VPN appliances immediately.

- Run regular email phishing drills to train all employees to prevent falling victim to phishing attacks.

Sources

- ZDNet
- Coveware
- Emsisoft

Malware pre-installed on mobile phones

- The researchers of a cyber security company found that some 200,000 low-cost Android smartphones of a manufacturer were pre-installed with the Triada malware, leading to 19.2 million suspicious transactions on subscription services without user knowledge or approval.

- Triada is a backdoor software running on Android. It performs malicious actions upon receiving instructions from threat actors' command and control (C2) servers. The researchers observed web traffic from the smartphones to C2 servers under different domains from that of the manufacturer. Triada could also download another malware known as xHelper, which was found in 53,000 of the infected phones. xHelper was used to launch the click or subscription fraud campaigns.

- The Triada and xHelper could survive manual removals, system reboots, and factory resets. They stored their components in an unremovable directory accessible only by the administrator account. When some components were uninstalled, they would be automatically reinstalled from the privileged directory a few minutes later, even though there was no Internet connection.

Advice

- Smartphone manufacturers should secure their supply chains to avoid being pre-installed with infected components; for example, assessing and verifying third-party software development kits or modules before adopting.

- Smartphone consumers should review credibility and capability of manufacturers in providing reliable products and on-going support such as provision of security patches before making purchase decisions.

- End users should install anti-malware solutions on their Android phones to better protect the devices from malware infections.

Sources

- HackRead
- Upstream

Product Vulnerability Notes & Security Updates

1. Advantech iView

https://us-cert.cisa.gov/ics/advisories/icsa-20-238-01

2. Cisco Products

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-cli-dos-GQUxCnTe

3. Citrix Hypervisor

https://support.citrix.com/article/CTX280451

4. Debian

https://www.debian.org/security/2020/dsa-4747
https://www.debian.org/security/2020/dsa-4748
https://www.debian.org/security/2020/dsa-4749
https://www.debian.org/security/2020/dsa-4750
https://www.debian.org/security/2020/dsa-4751
https://www.debian.org/security/2020/dsa-4752

5. F5 Products

https://support.f5.com/csp/article/K00103216
https://support.f5.com/csp/article/K02663161
https://support.f5.com/csp/article/K02705117
https://support.f5.com/csp/article/K05975972
https://support.f5.com/csp/article/K11400411
https://support.f5.com/csp/article/K12936322
https://support.f5.com/csp/article/K20606443
https://support.f5.com/csp/article/K23153696
https://support.f5.com/csp/article/K25160703
https://support.f5.com/csp/article/K29923912
https://support.f5.com/csp/article/K40843345
https://support.f5.com/csp/article/K43404629
https://support.f5.com/csp/article/K45026834
https://support.f5.com/csp/article/K45421311
https://support.f5.com/csp/article/K55873574
https://support.f5.com/csp/article/K57214921
https://support.f5.com/csp/article/K72752002
https://support.f5.com/csp/article/K73302459
https://support.f5.com/csp/article/K82252291
https://support.f5.com/csp/article/K91090139

6. Gentoo Linux

https://security.gentoo.org/glsa/202008-09
https://security.gentoo.org/glsa/202008-10
https://security.gentoo.org/glsa/202008-11
https://security.gentoo.org/glsa/202008-12
https://security.gentoo.org/glsa/202008-13
https://security.gentoo.org/glsa/202008-14
https://security.gentoo.org/glsa/202008-15
https://security.gentoo.org/glsa/202008-16
https://security.gentoo.org/glsa/202008-17
https://security.gentoo.org/glsa/202008-18

7. Google Chrome

https://chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop_25.html

8. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200826-01-buffer_en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200826-01-ddos-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200826-01-fc-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200826-01-pointer_en

9. OpenClinic GA

https://us-cert.cisa.gov/ics/advisories/icsma-20-184-01

10. openSUSE

https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00047.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00048.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00049.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00050.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00051.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00052.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00053.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00054.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00055.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00056.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00057.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00058.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00059.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00060.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00061.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00062.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00063.html
https://lists.opensuse.org/opensuse-security-announce/2020-08/msg00064.html

11. Oracle Linux

https://linux.oracle.com/errata/ELSA-2020-3548.html
https://linux.oracle.com/errata/ELSA-2020-3558.html
https://linux.oracle.com/errata/ELSA-2020-5823.html
https://linux.oracle.com/errata/ELSA-2020-5825.html

12. Red Products

https://access.redhat.com/errata/RHSA-2020:3519
https://access.redhat.com/errata/RHSA-2020:3520
https://access.redhat.com/errata/RHSA-2020:3541
https://access.redhat.com/errata/RHSA-2020:3545
https://access.redhat.com/errata/RHSA-2020:3555
https://access.redhat.com/errata/RHSA-2020:3556
https://access.redhat.com/errata/RHSA-2020:3557
https://access.redhat.com/errata/RHSA-2020:3558
https://access.redhat.com/errata/RHSA-2020:3559
https://access.redhat.com/errata/RHSA-2020:3560
https://access.redhat.com/errata/RHSA-2020:3574
https://us-cert.cisa.gov/ics/advisories/icsa-20-240-01

13. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2020&m=slackware-security.354485
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2020&m=slackware-security.485810

14. SUSE

https://www.suse.com/support/update/announcement/2020/suse-su-20200920-2/
https://www.suse.com/support/update/announcement/2020/suse-su-20202240-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202241-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202242-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202292-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202296-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202303-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202304-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202305-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202306-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202307-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202308-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202311-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202312-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202325-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202326-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202331-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202344-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202346-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202355-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202357-1/
https://www.suse.com/support/update/announcement/2020/suse-su-20202359-1/

https://www.suse.com/support/update/announcement/2020/suse-su-202014460-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014461-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014463-1/
https://www.suse.com/support/update/announcement/2020/suse-su-202014468-1/

15. Ubuntu

https://ubuntu.com/security/notices/USN-4446-2
https://ubuntu.com/security/notices/USN-4468-1
https://ubuntu.com/security/notices/USN-4468-2
https://ubuntu.com/security/notices/USN-4469-1
https://ubuntu.com/security/notices/USN-4470-1
https://ubuntu.com/security/notices/USN-4471-1
https://ubuntu.com/security/notices/USN-4472-1
https://ubuntu.com/security/notices/USN-4473-1
https://ubuntu.com/security/notices/USN-4474-1
https://ubuntu.com/security/notices/USN-4475-1
https://ubuntu.com/security/notices/USN-4476-1
https://ubuntu.com/security/notices/USN-4477-1

16. VMware

https://www.vmware.com/security/advisories/VMSA-2020-0018.html
https://www.vmware.com/security/advisories/VMSA-2020-0019.html

17. WECON LeviStudioU

https://us-cert.cisa.gov/ics/advisories/icsa-20-238-03

18. Xen

https://xenbits.xen.org/xsa/advisory-335.html

Sources of product vulnerability information:

Cisco
Citrix
Debian
F5
Gentoo Linux
Google Chrome
Huawei
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
US-CERT
VMware
Xen

Contact:

cert@govcert.gov.hk