GovCERT.HK

Weekly IT Security News Bulletin, 2017-W24

12 June – 18 June 2017

Headlines

Patch NOW for critical Windows vulnerabilities facing destructive cyber-attacks

- On 13 June 2017, Microsoft released critical security updates covering a wide range of Windows versions from Windows XP, Windows Vista, Windows Server 2003 up to Windows 10 and Windows Server 2016, as well as the Windows Embedded versions. Unpatched Windows systems are subject to "heightened risk of exploitation due to past and threatened nation-state attacks and disclosures".

- The security updates address around 100 vulnerabilities, which could lead to remote code execution, information disclosure, elevation of privilege, security restriction bypass, denial-of-service, or tampering. Three of the vulnerabilities affecting Windows XP, Windows XP Embedded and Windows Server 2003 (CVE-2017-0176, CVE-2017-7269 and CVE-2017-8487) are used by the exploits ESTEEMAUDIT, EXPLODINGCAN, and ENGLISHMANSDENTIST respectively. The hacking group Shadow Brokers have disclosed in April 2017 these three exploits, together with those used in the WannaCry attack.

- Microsoft has provided out-of-band security update for its end-of-life products such as Windows XP and Windows Server 2003 in two consecutive patch release cycles since May 2017 after the WannaCry ransomware outbreak. Such move suggests that the critical updates are much more than a routine precaution and every system administrator and user should action immediately to patch their systems as soon as possible.

Advice

- Patch your Windows systems immediately.

- Check and verify that your systems have been successfully patched even automatic update is enabled.

- Upgrade end-of-life Windows products to supported versions to better assure the availability of update security patches and features.

Sources

- Microsoft
- Bleeping Computer
- The Register

HIDDEN COBRA denial-of-service botnet infrastructure

- The United States Computer Emergency Response Team (US-CERT) publishes details of the botnet tools and infrastructure used in the malicious cyber activity referred to as "HIDDEN COBRA", "Lazarus Group" or "Guardians of Peace". Since 2009, HIDDEN COBRA actors have attacked at the media, aerospace, financial and critical infrastructure sectors globally, including the hack against Sony Pictures Entertainment leading to information leakage in 2014.

- The threat actors are equipped with a tool box of distributed denial-of-service (DDoS) botnets, keyloggers, remote access tools (RATs), and wiper malware. The intrusions commonly target older, unsupported Microsoft operating system versions and exploit vulnerabilities on unpatched Adobe Flash Player or Microsoft Silverlight to gain initial access to a victim's system.

- The DeltaCharlie DDoS bot was identified as part of the HIDDEN COBRA botnet infrastructure, capable of launching Domain Name System (DNS) attacks, Network Time Protocol (NTP) attacks, and Character Generation Protocol attacks. DeltaCharlie malware operates on the victim's system as a svchost-based service and establishes connections with the command and control (C&C) servers for various attack operations.

Advice

- Upgrade unsupported operating systems and software.

- Patch known vulnerabilities of operating systems and software, including the common applications such as Adobe Flash Player and Microsoft Silverlight.

- Keep anti-malware software and its signatures up-to-date, and schedule regular full-scan.

Sources

- US-CERT
- Novetta

Xavier: an information stealing ad library on Android

- More than 800 Android apps embedded with a Trojan ad library called Xavier have been downloaded millions of times from Google Play. The affected apps include utilities such as photo manipulators, wallpaper and ringtone changers. Vietnam, Philippines and Indonesia were the top three countries in total accounting for over 50% of the recorded downloads. Google has removed the infected apps from its store as of 13 June 2017.

- Xavier is the third generation of the AdDown family, which steals user information. The first version called joymobile started to evolve in early 2015. Then came the variant nativemob before Xavier emerged in September 2016. The latest generation gets a more streamlined code than its precedents and is capable of downloading and executing other malicious codes from a remote server.

- Xavier is strong at evading detection. It makes static detection and manual analysis difficult by encrypting all constant contents. HTTPS is adopted to encrypt data communication with its command and control (C&C) server to prevent its traffic from being caught. The malware even uses a wide array of reflection invoking methods to hide away the class name and method at compile time to protect its code from reverse-engineering. It also looks for symptoms of emulator running environment to stop its malicious behaviour to evade sandbox-based dynamic malware analysis.

Advice

- Do not install apps from unknown sources or developers.

- Install and run anti-malware software with up-to-date signatures on Android devices.

- Do not "root" your mobile devices.

- Keep your Android version up-to-date.

Source

- Trend Micro
- SC Media US

Product Vulnerability Notes & Security Updates

1. **Adobe Flash Player**
   https://helpx.adobe.com/security/products/flash-player/apsb17-17.html

2. **Cambium Networks ePMP Network Access Control**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-166-01

3. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-June/022458.html
   https://lists.centos.org/pipermail/centos-announce/2017-June/022459.html
   https://lists.centos.org/pipermail/centos-announce/2017-June/022460.html

4. **Debian**
   https://www.debian.org/security/2017/dsa-3874
   https://www.debian.org/security/2017/dsa-3875
   https://www.debian.org/security/2017/dsa-3876
   https://www.debian.org/security/2017/dsa-3877
   https://www.debian.org/security/2017/dsa-3878
   https://www.debian.org/security/2017/dsa-3879
   https://www.debian.org/security/2017/dsa-3880
   https://www.debian.org/security/2017/dsa-3881
   https://www.debian.org/security/2017/dsa-3882
   https://www.debian.org/security/2017/dsa-3883

5. **Google Chrome**
   https://chromereleases.googleblog.com/2017/06/stable-channel-update-for-desktop_15.html

6. **Huawei UMA Products**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170612-01-uma-en

7. **ISC BIND**
   https://kb.isc.org/article/AA-01495
   https://kb.isc.org/article/AA-01496
   https://kb.isc.org/article/AA-01497

8. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0162.html
   http://advisories.mageia.org/MGASA-2017-0163.html
   http://advisories.mageia.org/MGASA-2017-0164.html
   http://advisories.mageia.org/MGASA-2017-0165.html
   http://advisories.mageia.org/MGASA-2017-0166.html
   http://advisories.mageia.org/MGASA-2017-0167.html
   http://advisories.mageia.org/MGASA-2017-0168.html
   http://advisories.mageia.org/MGASA-2017-0169.html
   http://advisories.mageia.org/MGASA-2017-0170.html
   http://advisories.mageia.org/MGASA-2017-0171.html
   http://advisories.mageia.org/MGASA-2017-0172.html
   http://advisories.mageia.org/MGASA-2017-0173.html
   http://advisories.mageia.org/MGASA-2017-0174.html
   http://advisories.mageia.org/MGASA-2017-0175.html
   http://advisories.mageia.org/MGASA-2017-0176.html

http://advisories.mageia.org/MGASA-2017-0177.html

9. **Microsoft Products**
   https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/40969d56-1b2a-e711-80db-000d3a32fc99
   https://technet.microsoft.com/library/security/4025685
   https://www.hkcert.org/my_url/en/alert/17061401

10. **Mozilla Firefox**
    https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/
    https://www.mozilla.org/en-US/security/advisories/mfsa2017-16/

11. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00009.html

12. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:1430
    https://access.redhat.com/errata/RHSA-2017:1431
    https://access.redhat.com/errata/RHSA-2017:1439
    https://access.redhat.com/errata/RHSA-2017:1440
    https://access.redhat.com/errata/RHSA-2017:1441
    https://access.redhat.com/errata/RHSA-2017:1445
    https://access.redhat.com/errata/RHSA-2017:1450
    https://access.redhat.com/errata/RHSA-2017:1451
    https://access.redhat.com/errata/RHSA-2017:1456
    https://access.redhat.com/errata/RHSA-2017:1461
    https://access.redhat.com/errata/RHSA-2017:1462
    https://access.redhat.com/errata/RHSA-2017:1464
    https://access.redhat.com/errata/RHSA-2017:1470
    https://access.redhat.com/errata/RHSA-2017:1476

13. **RSA BSAFE Cert-C**
    https://exchange.xforce.ibmcloud.com/vulnerabilities/127157
    http://www.securityfocus.com/archive/1/540720/30/0/threaded

14. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.549369
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.574039

15. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20171538-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171557-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171558-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171567-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171568-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171575-1.html

16. **Trend Micro Security 2017**
    https://success.trendmicro.com/solution/1117509

17. **Trihedral VTScada**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-164-01

18. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3317-1/
    https://www.ubuntu.com/usn/usn-3318-1/
    https://www.ubuntu.com/usn/usn-3315-1/
    https://www.ubuntu.com/usn/usn-3319-1/
    https://www.ubuntu.com/usn/usn-3320-1/

19. **VMware Horizon View Client for Mac**
    http://www.vmware.com/security/advisories/VMSA-2017-0011.html
    https://www.hkcert.org/my_url/en/alert/17060901

Sources of product vulnerability information:

Adobe
CentOS
Debian
Google Chrome
HKCERT
Huawei
IBM X-Force Exchange
ICS-CERT
ISC
Mageia
Microsoft
Mozilla Firefox
openSUSE
Red Hat
SecurityForce
Slackware
SUSE
Trend Micro
Ubuntu
VMware

Contacts:

cert@govcert.gov.hk