GovCERT.HK

Weekly IT Security News Bulletin, 2017-W23

5 June – 11 June 2017

Headlines

Botnets overshadowed by ransomware

- Malware that takes complete control over a large number of infected computers to form a botnet is worth more worries than ransomware alone, though the recent WannaCryptor ransomware attack gains considerably more media coverage than other cyber threats.

- A botnet can be directed to send out spam emails, distribute scams, perform distributed denial-of-service (DDoS) attacks, steal victims' credentials or credit card information, break into victims' bank accounts, generate faked advertisement clicks or views, utilize computing power for Bitcoin mining, and encrypt the computers for ransom. Even worse than infected personal computers, botnets also get more processing power by controlling servers and become bigger in size by hijacking Internet of things (IoT). A botnet is therefore regarded as more dangerous than ransomware.

- New botnets have taken the peer-to-peer model instead of the client-server model to evade detection and increase resiliency. Some botnets also employ the so-called fast-flux technology to change IP addresses of the command and control (C&C) and name servers frequently, making them difficult to trace and take down by law enforcement operations. The bottom line for users is to ensure that their systems will not be part of the botnets.

Advice

- Follow your product vendors' advice to update your systems with latest security patches and supported versions.

- Keep your anti-malware software and signatures up-to-date and conduct full-scan of your systems with the anti-malware software regularly.

- Implement layers of defence including not only endpoint protection, but also network security solutions, data protection, backup/recovery solutions as well as security training.

Sources

- Welivesecurity
- RiskAnalytics

Organisations failing to upgrade systems and enforce patches

- The 2017 Duo Trusted Access Report, published by the security vendor, Duo Security, reveals the security health of 4.6 million enterprise endpoints in North America, Europe, Middle East and Africa. The vendor also analyzed the enabled security features of 3.5 million mobile phones and results of simulated phishing campaigns conducted by its enterprise clients.

- 61% of the enterprise endpoints are running Microsoft Windows operating system. 31% of the Windows systems have been upgraded to the latest version Windows 10 while Windows 7 remains at the top being used by 59% of the Windows systems, though it will be de-supported in Jan 2020. For Internet Explorer (IE) browser, 13% of endpoints were using unsupported versions (IE 8/9/10) which no longer receive security patches. For Adobe's Flash plug-in, more than half of the endpoints are running out-of-date versions not protected from the latest known vulnerabilities.

- The analysis found that only 27% of Android phones are running the latest major version 7 while 73% of iPhones are running the supporting iOS 10 or above. In addition, only 29% of mobile endpoints are full-disk encrypted.

- 3,575 simulated phishing campaigns over 80,000 recipients turned out that 25% of recipients clicked on the link within a phishing email and another 13% entered their credentials, reflecting the enterprise risks of malware infection and information leakage.

- Using outdated software is risky and opens your computer or devices to cyber attacks, especially when connecting to the Internet.

Advice

- Patch and update operating systems, browser software and browser plug-ins regularly to protect against known vulnerabilities.

- Plan for the operating system upgrade from Windows 7 to Windows 10 well before the end-of-support date.

- Enable mobile security features such as full disk encryption to protect information.

- Provide security awareness training to all users against phishing campaigns.

Sources

- 2017 Duo Trusted Access Report
- SecurityWeek

Product Vulnerability Notes & Security Updates

1. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-anyconnect
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-ccs
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-cucm1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-cucm2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-dcnm1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-dcnm2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esa
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esa1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc4
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc5
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc6
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc7
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc8
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-esc9
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-fmc
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-ind
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-ncs
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-nxos
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-pca
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-sip
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-staros
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-tele
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf4
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf5
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf6
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usp1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usp2

2. **Debian**
   https://www.debian.org/security/2017/dsa-3873

3. **Digital Canal Structural Wind Analysis**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-157-02

4. **Gentoo Linux**
   https://security.gentoo.org/glsa/201706-01
   https://security.gentoo.org/glsa/201706-02
   https://security.gentoo.org/glsa/201706-03
   https://security.gentoo.org/glsa/201706-04
   https://security.gentoo.org/glsa/201706-05
   https://security.gentoo.org/glsa/201706-06
   https://security.gentoo.org/glsa/201706-07
   https://security.gentoo.org/glsa/201706-08

https://security.gentoo.org/glsa/201706-09
https://security.gentoo.org/glsa/201706-10
https://security.gentoo.org/glsa/201706-11
https://security.gentoo.org/glsa/201706-12
https://security.gentoo.org/glsa/201706-13
https://security.gentoo.org/glsa/201706-14
https://security.gentoo.org/glsa/201706-15

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

6. **Huawei Products**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170607-01-gaussdb-en
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170607-02-gaussdb-en

7. **IBM InfoSphere Information Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg22003016

8. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0153.html
   http://advisories.mageia.org/MGASA-2017-0154.html
   http://advisories.mageia.org/MGASA-2017-0155.html
   http://advisories.mageia.org/MGASA-2017-0156.html
   http://advisories.mageia.org/MGASA-2017-0157.html
   http://advisories.mageia.org/MGASA-2017-0158.html
   http://advisories.mageia.org/MGASA-2017-0159.html
   http://advisories.mageia.org/MGASA-2017-0160.html
   http://advisories.mageia.org/MGASA-2017-0161.html

9. **openSUSE**
   https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00001.html
   https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00002.html
   https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00003.html
   https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00004.html
   https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00005.html
   https://lists.opensuse.org/opensuse-security-announce/2017-06/msg00006.html

10. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:1384
    https://access.redhat.com/errata/RHSA-2017:1390
    https://access.redhat.com/errata/RHSA-2017:1395
    https://access.redhat.com/errata/RHSA-2017:1399
    https://access.redhat.com/errata/RHSA-2017:1410
    https://access.redhat.com/errata/RHSA-2017:1411
    https://access.redhat.com/errata/RHSA-2017:1412
    https://access.redhat.com/errata/RHSA-2017:1413
    https://access.redhat.com/errata/RHSA-2017:1414
    https://access.redhat.com/errata/RHSA-2017:1417
    https://access.redhat.com/errata/RHSA-2017:1422

11. **Rockwell Automation PanelView Plus 6 700-1500**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-157-01

12. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.541305

13. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20171479-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171481-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171489-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171504-1.html

14. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3253-2/
    https://www.ubuntu.com/usn/usn-3308-1/
    https://www.ubuntu.com/usn/usn-3309-1/
    https://www.ubuntu.com/usn/usn-3310-1/
    https://www.ubuntu.com/usn/usn-3311-1/
    https://www.ubuntu.com/usn/usn-3312-1/
    https://www.ubuntu.com/usn/usn-3312-2/
    https://www.ubuntu.com/usn/usn-3313-1/
    https://www.ubuntu.com/usn/usn-3313-2/
    https://www.ubuntu.com/usn/usn-3314-1/
    https://www.ubuntu.com/usn/usn-3316-1/

Sources of product vulnerability information:

Cisco
Debian
Gentoo Linux
Google Chrome
Huawei
IBM
ICS-CERT
Mageia
openSUSE
Red Hat
Slackware
SUSE
Ubuntu

Contacts:

cert@govcert.gov.hk