GovCERT.HK

Weekly IT Security News Bulletin, 2017-W19

8 May – 14 May 2017

Headlines

Massive ransomware infections hit computers around the world

- A ransomware called WannaCry (also dubbed WanaCrypt0r 2.0) was widely spreading and infecting tens of thousands of computers around the world since 12 May 2017. What makes WannaCry different from other ransomware is if one computer is infected, it will connect to TCP port 445 of every computer in the same subnet for lateral movement by exploiting the Microsoft Windows Server Message Block (SMB) vulnerability (MS17-010).

- One possible infection path is via phishing emails. On infection, the malware will call a domain ("xxx.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com") at port 80. If the call is responded, the malware will quit operation; otherwise, it will proceed to encrypt files and connect to the Tor network for the victims to pay the ransom.

- The SMB vulnerability on all supporting Windows operating system can be fixed by applying Microsoft's security update released on 14 March 2017. Seeing businesses and individuals affected by the attacks, Microsoft further provided security updates for even some de-supported Windows platforms, including Windows XP, Windows 8, and Windows Server 2003 on 12 May 2017.

Advice

- Apply latest security patches on all Windows-based systems.

- Block the SMB ports (TCP ports 139 and 445) from Internet access.

- Keep the anti-malware software and signatures up-to-date on all computer systems.

- Perform regular backups on important data assets and keep the backup copies disconnected from the computer.

- Stay vigilant of suspicious emails and websites and avoid clicking unknown attachments and links.

Sources

- Cisco Talos Intelligence
- Microsoft Malware Protection Center
- Microsoft Customer Guidance for WannaCrypt Attacks
- US-CERT
- HKCERT

Deprecation of SHA-1 for SSL/TLS certificates in Microsoft Edge and Internet Explorer 11

- From 9 May 2017 onwards, updated Microsoft Internet Explorer 11 and Edge will block websites with a SHA-1 certificate from loading and an invalid certificate warning will be displayed.

- The change will affect certificates chained to a root in the Microsoft Trusted Root Program if the end-entity certificate or the intermediate issuing certificate is using SHA-1. Enterprise or self-signed certificates will not be affected.

- The SHA-1 hashing algorithm is widely regarded as insecure because it is subject to collision attacks. Attackers could generate alternative documents with the same hash value as an original to spoof information, identities and transactions. The weakness is re-confirmed by the first collision for full SHA-1 in February 2017 by Google and Cryptology Group researchers. Earlier, other popular browsers, including Google Chrome, Mozilla Firefox, and Apple Safari, have also stopped trusting SHA-1 certificates.

Advice

- Migrate any SHA-1 certificates to one with safer cryptographic hashes such as SHA-256 and SHA-3 for website security and code-signing.

- Always keep web browsers updated to latest versions to enable better security protection.

Sources

- Microsoft Security Advisory
- Windows Enforcement of SHA-1 Certificates

台灣 1.7 億項個人資料外泄　犯罪集團涉販賣個人資料牟利

- 台灣調查局於 2017 年 5 月 10 日破獲一宗當地犯罪集團非法盜取及販賣個人資料的案件。事件涉及約 1.7 億項個人資料，牽涉約 2 000 萬人。外泄的資料主要關於業主的資料和聯絡方法，包括姓名、身分證號碼、出生日期、電話、住址等。

- 犯罪集團涉嫌於 2016 年內，以「房仲開發利器」、「房仲省時尋人系統」等名義向地產代理販賣個人資料搜尋系統，最少已賣出 300 套系統。調查發現，集團於買家電腦中遙距安裝該搜尋系統，並利用搜尋系統內的圖形驗證碼(CAPTCHA)破解程式登入政府部門的伺服器，透過自動比對取得民眾的個人資料。

- 調查局懷疑外泄的個人資料來自政府部門，正繼續追查並擴大搜查範圍。同時，當局呼籲各部門需重視資料外泄的問題，以保護民眾的個人資料。

Advice

- 機構應定期審視收集的個人資料是否有實際需要，而又不超乎適度；資料的保留時間亦不應超過達致原來目的的實際所需。

- 機構向員工分配資訊系統的資源和權限時，須貫徹最小權限原則，並按照「有需要知道」原則，賦予用戶數據接達權限。

- 詳細記錄有關批准、授予及管理用戶接達權限的程序，包括用戶登記／取消登記、密碼傳送及密碼重設。

- 明確界定及定期覆檢用戶權限及數據接達權限，並須備存有關批准和覆檢接達權限的記錄。

- 如懷疑密碼已經或正在外泄，或因維修及支援服務的需要而向供應商透露密碼，須立即更改密碼。

Sources

- 台灣法務部調查局
- 明報
- Now 新聞

Product Vulnerability Notes & Security Updates

1. **Adobe Flash Player**
   https://helpx.adobe.com/security/products/flash-player/apsb17-15.html

2. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-May/022402.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022403.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022404.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022405.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022406.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022407.html

3. **Cisco WebEx Meetings Server**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170510-cwms

4. **Debian**
   http://www.debian.org/security/2017/dsa-3845
   http://www.debian.org/security/2017/dsa-3846
   http://www.debian.org/security/2017/dsa-3847
   http://www.debian.org/security/2017/dsa-3848

5. **F5 Products**
   https://support.f5.com/csp/article/K31310492
   https://support.f5.com/csp/article/K77508618
   https://support.f5.com/csp/article/K82851041
   https://support.f5.com/csp/article/K87141725
   https://support.f5.com/csp/article/K99254031

6. **Gentoo Linux**
   https://security.gentoo.org/glsa/201705-01
   https://security.gentoo.org/glsa/201705-02
   https://security.gentoo.org/glsa/201705-03
   https://security.gentoo.org/glsa/201705-04
   https://security.gentoo.org/glsa/201705-05
   https://security.gentoo.org/glsa/201705-06
   https://security.gentoo.org/glsa/201705-07
   https://security.gentoo.org/glsa/201705-08

7. **Google Chrome**
   https://chromereleases.googleblog.com/2017/05/stable-channel-update-for-desktop_9.html

8. **IBM WebSphere Application Server**
   http://www-01.ibm.com/support/docview.wss?uid=swg22003016

9. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0129.html
   http://advisories.mageia.org/MGASA-2017-0130.html
   http://advisories.mageia.org/MGASA-2017-0131.html
   http://advisories.mageia.org/MGASA-2017-0132.html
   http://advisories.mageia.org/MGASA-2017-0133.html
   http://advisories.mageia.org/MGASA-2017-0134.html

http://advisories.mageia.org/MGASA-2017-0135.html
http://advisories.mageia.org/MGASA-2017-0136.html
http://advisories.mageia.org/MGASA-2017-0137.html
http://advisories.mageia.org/MGASA-2017-0138.html
http://advisories.mageia.org/MGASA-2017-0139.html

10. **Microsoft Malware Protection Engine**
    https://technet.microsoft.com/library/security/4022344

11. **Microsoft Products**
    https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/bc365363-f51e-e711-80da-000d3a32fc99

12. **Mozilla Firefox**
    https://www.mozilla.org/en-US/security/advisories/mfsa2017-14/

13. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00012.html
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00013.html
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00014.html
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00015.html
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00016.html
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00018.html

14. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-1201.html
    https://linux.oracle.com/errata/ELSA-2017-1202.html
    https://linux.oracle.com/errata/ELSA-2017-1204.html
    https://linux.oracle.com/errata/ELSA-2017-1206.html
    https://linux.oracle.com/errata/ELSA-2017-1208.html

15. **Phoenix Contact GmbH mGuard**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-131-01

16. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:1201
    https://access.redhat.com/errata/RHSA-2017:1202
    https://access.redhat.com/errata/RHSA-2017:1204
    https://access.redhat.com/errata/RHSA-2017:1205
    https://access.redhat.com/errata/RHSA-2017:1206
    https://access.redhat.com/errata/RHSA-2017:1208
    https://access.redhat.com/errata/RHSA-2017:1209
    https://access.redhat.com/errata/RHSA-2017:1216
    https://access.redhat.com/errata/RHSA-2017:1219
    https://access.redhat.com/errata/RHSA-2017:1220
    https://access.redhat.com/errata/RHSA-2017:1221
    https://access.redhat.com/errata/RHSA-2017:1222
    https://access.redhat.com/errata/RHSA-2017:1228

17. **Rockwell Automation Stratix 5900**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-094-04

18. **SUSE**

https://www.suse.com/support/update/announcement/2017/suse-su-20171182-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171183-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171187-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171188-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171216-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171222-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171229-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171233-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171236-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171238-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171241-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171247-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171248-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171250-1.html

19. **Satel Iberia SenNet Data Logger and Electricity Meters**

https://ics-cert.us-cert.gov/advisories/ICSA-17-131-02

20. **Ubuntu**

https://www.ubuntu.com/usn/usn-3260-2/
https://www.ubuntu.com/usn/usn-3275-1/
https://www.ubuntu.com/usn/usn-3276-1/
https://www.ubuntu.com/usn/usn-3279-1/
https://www.ubuntu.com/usn/usn-3280-1/
https://www.ubuntu.com/usn/usn-3281-1/
https://www.ubuntu.com/usn/usn-3282-1/
https://www.ubuntu.com/usn/usn-3283-1/
https://www.ubuntu.com/usn/usn-3284-1/
https://www.ubuntu.com/usn/usn-3285-1/

Sources of product vulnerability information:

Adobe
CentOS
Cisco
Debian
F5
Gentoo Linux
Google Chrome
IBM
ICS-CERT
Mageia
Microsoft
Mozilla Firefox
openSUSE
Oracle Linux
Red Hat
SUSE
Ubuntu

Contacts:

cert@govcert.gov.hk