GovCERT.HK

Weekly IT Security News Bulletin, 2017-W20

15 May – 21 May 2017

Headlines

Behind WannaCry, Jaff, UIWIX and Adylkuzz line up

- In addition to the "WannaCry" ransomware outbreak, other malwares such as "Jaff", "UIWIX", and "Adylkuzz" continue to emerge. These malwares may not have garnered the attention of "WannaCry", but all computer users and administrators should stay vigilant of the persisting threats.

- "Jaff" is another crypto ransomware wide-spreading in the shadow of the "WannaCry". Unlike "WannaCry", "Jaff" does not directly attack computers from the network but is distributed through phishing emails, which carries a PDF attachment embedded with a Microsoft Word document to run malicious macros.

- "UIWIX" and "Adylkuzz" resemble the "WannaCry" way to exploit the Microsoft Server Message Block (SMB) vulnerabilities from the network. "UIWIX" is a file-less "WannaCry" variant which runs only in memory and is able to stop automatically at a virtual machine or sandbox to bypass the anti-malware detection. "Adylkuzz" does not encrypt files but it performs mining of the cryptocurrency Monero using the computing resources of the infected systems.

Advice

- Backup data and keep the backup offline.

- Apply latest security patches to your systems.

- Keep your anti-malware program and signatures up-to-date.

- Do not open any suspicious emails, attachments and hyperlinks.

Sources

- BleepingComputer
- Cisco Talos Intelligence
- Trend Micro

WannaCry 勒索軟件香港最新狀況

- 生產力促進局資訊科技總經理黃家偉於 2017 年 5 月 20 日出席電視台節目時透露香港電腦保安事故協調中心共收到 33 宗受到網絡勒索程式 WannaCry 攻擊的報告，而過去三天沒收到新的報告。他表示香港在今次事件中情況不算十分嚴重，但他提醒市民勒索軟件只會繼續越來越多，強調最重要是市民大眾做好備份、軟件更新、和防火牆措施。

- 黃預見未來的攻擊目標或會轉移至物聯網，黑客透過病毒將手機上鎖來勒索市民金錢。他呼籲市民須要更新手機應用程式，並安裝防毒軟件，避免開啟來歷不明的電郵，以防遭遇黑客入侵。

- 黃亦特別提醒中小企公司，今次攻擊後果只是加密，但下次如果是資料外泄，可能會影響公司形象，甚至涉及保障私隱責任問題，都不是之後可彌補得到；所以公司要由源頭開始做好資訊保安、完善保安系統、做好備份、和配合公司的政策解決問題。關於對本港中小企資訊保安的支援，除了香港電腦保安事故協調中心提供的免費服務，他建議中小企可透過創新及科技局的「科技券計劃」獲資助提升網絡保安能力。

Advice

- 勒索軟件千變萬化，市民應時刻保持警覺，為電腦做好備份及更新軟件，亦不應開啟來歷不明的電郵和網絡連結，以保障電腦免受勒索軟件的威脅。

- 市民可透過政府資訊科技總監辦公室的資訊安全網（infosec.gov.hk）了解最新資訊和提示。市民如需就網絡保安尋求協助，可致電香港電腦保安事故協調中心的 24 小時熱線 8105 6060。

Sources

- 無綫新聞
- 創新科技署・科技券計劃
- 政府資訊科技總監辦公室

Fake WhatsApp.com URL gets users to install adware

- A domain name "шhатsapp.com" was found using the Cyrillic characters to mislead users to click and install adware on their computers. The domain is actually different from the official WhatsApp domain which should be "whatsapp.com" in English characters. The domain name spoofing is called the internationalized domain name (IDN) homograph attack.

- The fake WhatsApp website claimed to let users install the WhatsApp desktop version with different colours of layout. Once clicking the website link, users were asked to share the link with their friends. Users were then re-directed to install a Chrome extension named BlackWhats.

- The extension is actually an adware rather than the "coloured" WhatsApp application. Google has removed the extension from its Chrome Web Store, but more than 16,000 victims have downloaded and installed the adware.

Advice

- Check for the latest product features and releases only from the official product web sites to verify the truth of related information from the other sources.

- Type in a website URL manually or navigate to the site via a search engine instead of clicking or copying a link from suspicious sources.

- Use latest versions of web browsers, which automatically apply "Punycode" encoding to represent Unicode characters in the URL in ASCII format to defend against the IDN homograph phishing attack. For example, "шhатsapp.com" will be shown as "xn--80aa2cah8a7f73b.com" in Punycode.

Sources

- Reddit
- Softpedia
- TNW
- Phishing with Unicode Domains

Product Vulnerability Notes & Security Updates

1. **Apple iOS, MacOS, iTunes for Windows, Safari and iCloud**
   https://support.apple.com/kb/HT207797
   https://support.apple.com/kb/HT207798
   https://support.apple.com/kb/HT207803
   https://support.apple.com/kb/HT207804
   https://support.apple.com/kb/HT207805

2. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-May/022408.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022409.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022410.html
   https://lists.centos.org/pipermail/centos-announce/2017-May/022411.html

3. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170515-snort
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-cps
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-fpwr
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ie1000csrf
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ise
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-nss1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp4
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp5
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem1
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem2
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem3
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem4
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem5
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem6
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-rem7
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-sip
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-telepresence-ix5000
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ucm
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ucsc

4. **Debian**
   https://www.debian.org/security/2017/dsa-3849
   https://www.debian.org/security/2017/dsa-3850
   https://www.debian.org/security/2017/dsa-3851
   https://www.debian.org/security/2017/dsa-3852
   https://www.debian.org/security/2017/dsa-3853
   https://www.debian.org/security/2017/dsa-3854
   https://www.debian.org/security/2017/dsa-3855

5. **Detcon SiteWatch Gateway**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-136-01

6. **Gentoo Linux**
   https://security.gentoo.org/glsa/201705-09
   https://security.gentoo.org/glsa/201705-10

7. **Hanwha Techwin SRN-4000**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-136-03

8. **Huawei Products**
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170513-01-windows-en
   http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170517-01-ac-en

9. **Joomla**
   https://www.joomla.org/announcements/release-news/5705-joomla-3-7-1-release.html
   https://www.us-cert.gov/ncas/current-activity/2017/05/17/Joomla-Releases-Security-Update-CMS

10. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00024.html
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00025.html
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00026.html
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00037.html
    https://lists.opensuse.org/opensuse-security-announce/2017-05/msg00057.html

11. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-1230.html
    https://linux.oracle.com/errata/ELSA-2017-3565.html
    https://linux.oracle.com/errata/ELSA-2017-3566.html
    https://linux.oracle.com/errata/ELSA-2017-3567.html

12. **PostgreSQL**
    http://www.postgresql.org/about/news/1746/
    https://www.hkcert.org/my_url/en/alert/17051501

13. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:1230
    https://access.redhat.com/errata/RHSA-2017:1232
    https://access.redhat.com/errata/RHSA-2017:1233
    https://access.redhat.com/errata/RHSA-2017:1242
    https://access.redhat.com/errata/RHSA-2017:1243
    https://access.redhat.com/errata/RHSA-2017:1244
    https://access.redhat.com/errata/RHSA-2017:1253
    https://access.redhat.com/errata/RHSA-2017:1254
    https://access.redhat.com/errata/RHSA-2017:1256
    https://access.redhat.com/errata/RHSA-2017:1259
    https://access.redhat.com/errata/RHSA-2017:1260

14. **Schneider Electric Products**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-136-02
    https://ics-cert.us-cert.gov/advisories/ICSA-17-138-02

15. **Slackware**

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.474306
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.549207

16. **SUSE**

https://www.suse.com/support/update/announcement/2017/suse-su-20171277-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171278-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171279-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171280-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171281-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171282-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171283-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171284-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171285-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171287-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171288-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171289-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171290-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171291-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171293-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171294-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171295-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171297-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171299-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171300-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171301-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171302-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171303-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171305-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171306-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171308-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171311-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171313-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171314-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171315-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171316-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171317-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171322-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171328-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171335-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171336-1.html
https://www.suse.com/support/update/announcement/2017/suse-su-20171337-1.html

17. **Ubuntu**

https://www.ubuntu.com/usn/usn-3272-2/
https://www.ubuntu.com/usn/usn-3275-2/
https://www.ubuntu.com/usn/usn-3275-3/
https://www.ubuntu.com/usn/usn-3276-2/
https://www.ubuntu.com/usn/usn-3278-1/
https://www.ubuntu.com/usn/usn-3282-2/
https://www.ubuntu.com/usn/usn-3286-1/

https://www.ubuntu.com/usn/usn-3287-1/
https://www.ubuntu.com/usn/usn-3288-1/
https://www.ubuntu.com/usn/usn-3289-1/
https://www.ubuntu.com/usn/usn-3290-1/
https://www.ubuntu.com/usn/usn-3291-1/
https://www.ubuntu.com/usn/usn-3291-2/
https://www.ubuntu.com/usn/usn-3291-3/
https://www.ubuntu.com/usn/usn-3292-1/
https://www.ubuntu.com/usn/usn-3292-2/
https://www.ubuntu.com/usn/usn-3293-1/
https://www.ubuntu.com/usn/usn-3294-1/
https://www.ubuntu.com/usn/usn-3295-1/

18. WordPress

https://wordpress.org/news/2017/05/wordpress-4-7-5/

Sources of product vulnerability information:

Apple
CentOS
Cisco
Debian
Gentoo Linux
HKCERT
Huawei
ICS-CERT
Joomla
openSUSE
Oracle Linux
PostgreSQL
Red Hat
Slackware
SUSE
Ubuntu
US-CERT
WordPress

Contacts:

cert@govcert.gov.hk