GovCERT.HK

Weekly IT Security News Bulletin, 2021-W15

12 April – 18 April 2021

Headlines

Trends in attacks on corporate mobile devices

- Mobile devices of enterprises have become an attractive targets for attackers, as revealed in a recent report published by a security vendor, where almost all organisations under study had experienced mobile malware attacks in 2020. Over 90% of such attacks originated from device network, mainly phishing and infected websites or URLs.

- About half of the organisations had at least one employee download a mobile app which could pose threats to corporate data and network. Many of these malicious apps contained malware like banking trojans and mobile remote access trojans, which were capable for making unauthorised financial transactions or stealing personal and corporate data. Other emerging threats from mobile apps including premium diallers (subscribing users to premium mobile services) and clickers (mimicking the users to perform clicks on advertisements).

- The report also highlights that Mobile Device Management (MDM) could be breached and become a dangerous attack vector. Given that MDM has control over the whole mobile network, any security compromise happens in it can lead to mass infection of devices within organisations, as happened in the case of Cerberus variants attacks.

- Another notable trend in mobile malware attack is the common use of droppers by attackers to selectively launch payloads in the target devices. The payloads could be retrieved from third-party hosts or embedded in encoded strings which could be decode and loaded upon receiving the command from C2 servers.

Advice

- Establish mobile device security policy and prohibit users from downloading and installing unauthorised mobile apps on corporate devices.
- Deploy anti-malware solution on mobile devices and apply latest updates on applications and operating systems.
- Enforce strong password and encryption on the devices to reduce the chance of unauthorised access and data leakage.

Sources

- Check Point
- Infosecurity

Search Engine Poisoning for Malware Distribution

- A malicious group was found creating a huge number of webpages to trick search engine to achieve high search ranking so as to get their malicious sites containing malware more easily found by the victims.

- To launch search engine poisoning attack, the threat actors create 100,000 unique webpages with common business terms like template and invoice to manipulate web crawlers for a high score for their webpages on specific searches.

- By searching the Internet for business templates with the common terms, users could possibly find the malicious webpages in the top search results and pay a visit to them. When visitors downloaded the template files by clicking the download buttons, they were redirected to malicious websites which hosted an executable disguised as a pdf or word document. By executing the decoy file which was a legitimate pdf reader application, a remote access trojan would be installed together on the victim's machine. The trojan could allow the threat actors to send commands and launch other malware like ransomware, password stealer and banking trojans, to the victims' machines.

Advice

- Avoid opening documents downloaded from untrusted sources.
- Deploy anti-malware solution and perform scanning on files prior to execution.
- Check the SSL/TLS certificate and any other trust indicators (e.g., trust seals or URL padlock) to determine whether a website is trustworthy.

Sources

- eSentire
- The Hacker News

Product Vulnerability Notes & Security Updates

1. **Advantech WebAccessSCADA**

   https://us-cert.cisa.gov/ics/advisories/icsa-21-103-02

2. **CentOS**

   https://lists.centos.org/pipermail/centos-announce/2021-April/048298.html
   https://lists.centos.org/pipermail/centos-announce/2021-April/048299.html
   https://lists.centos.org/pipermail/centos-announce/2021-April/048300.html

3. **Debian**

   https://www.debian.org/security/2021/dsa-4887
   https://www.debian.org/security/2021/dsa-4888
   https://www.debian.org/security/2021/dsa-4889
   https://www.debian.org/security/2021/dsa-4890
   https://www.debian.org/security/2021/dsa-4891

4. **EIPStackGroup OpENer Ethernet/IP**

   https://us-cert.cisa.gov/ics/advisories/icsa-21-105-02

5. **F5 Products**

   https://support.f5.com/csp/article/K16729408

6. **Google Chrome**

   https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html

7. **IBM Products**

   https://www.ibm.com/support/pages/node/6436379
   https://www.ibm.com/support/pages/node/6436411
   https://www.ibm.com/support/pages/node/6436421
   https://www.ibm.com/support/pages/node/6436567
   https://www.ibm.com/support/pages/node/6436589
   https://www.ibm.com/support/pages/node/6436613
   https://www.ibm.com/support/pages/node/6437021
   https://www.ibm.com/support/pages/node/6437195
   https://www.ibm.com/support/pages/node/6437211
   https://www.ibm.com/support/pages/node/6437245
   https://www.ibm.com/support/pages/node/6437247
   https://www.ibm.com/support/pages/node/6437251
   https://www.ibm.com/support/pages/node/6437587
   https://www.ibm.com/support/pages/node/6439991
   https://www.ibm.com/support/pages/node/6439995
   https://www.ibm.com/support/pages/node/6439997
   https://www.ibm.com/support/pages/node/6441063
   https://www.ibm.com/support/pages/node/6441433

https://www.ibm.com/support/pages/node/6443101

8. Joomla!

https://www.joomla.org/announcements/release-news/5835-joomla-3-9-26.html

9. JTEKT TOYOPUC products

https://us-cert.cisa.gov/ics/advisories/icsa-21-103-03

10. Juniper Products

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11115
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11116
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11117
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11118
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11119
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11120
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11121
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11122
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11123
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11124
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11125
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11126
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11127
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11128
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11129
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11130
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11131
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11132
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11133
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11134
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11135
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11136
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11137
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11138
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11139
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11140
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11141
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11142
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11143
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11144
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11145
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11146
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11147
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11148
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11149
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11150
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11151
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11152
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11153
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11154
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11155

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11156
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11157
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11158
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11159
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11160
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11161
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11162
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11163
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11164
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11166
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11167
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11168
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11169
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11171
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11172
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11173
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11174
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11175
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11176

11. McAfee Products

https://kc.mcafee.com/corporate/index?page=content&id=SB10336
https://kc.mcafee.com/corporate/index?page=content&id=SB10353
https://kc.mcafee.com/corporate/index?page=content&id=SB10354
https://kc.mcafee.com/corporate/index?page=content&id=SB10356
https://kc.mcafee.com/corporate/index?page=content&id=SB10357

12. Microsoft Edge (Chromium Based)

https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#april-14-2021
https://docs.microsoft.com/en-us/DeployEdge/microsoft-edge-relnotes-security#april-15-2021

13. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-1064.html
https://linux.oracle.com/errata/ELSA-2021-1086.html
https://linux.oracle.com/errata/ELSA-2021-1197.html
https://linux.oracle.com/errata/ELSA-2021-9169.html
https://linux.oracle.com/errata/ELSA-2021-9172.html
https://linux.oracle.com/errata/ELSA-2021-9175.html
https://linux.oracle.com/errata/ELSA-2021-9176.html

14. Red Hat

https://access.redhat.com/errata/RHSA-2021:1016
https://access.redhat.com/errata/RHSA-2021:1168
https://access.redhat.com/errata/RHSA-2021:1169
https://access.redhat.com/errata/RHSA-2021:1171
https://access.redhat.com/errata/RHSA-2021:1173
https://access.redhat.com/errata/RHSA-2021:1184
https://access.redhat.com/errata/RHSA-2021:1186
https://access.redhat.com/errata/RHSA-2021:1189

https://access.redhat.com/errata/RHSA-2021:1195
https://access.redhat.com/errata/RHSA-2021:1196
https://access.redhat.com/errata/RHSA-2021:1197
https://access.redhat.com/errata/RHSA-2021:1199
https://access.redhat.com/errata/RHSA-2021:1200
https://access.redhat.com/errata/RHSA-2021:1202
https://access.redhat.com/errata/RHSA-2021:1203
https://access.redhat.com/errata/RHSA-2021:1206
https://access.redhat.com/errata/RHSA-2021:1213
https://access.redhat.com/errata/RHSA-2021:1214

15. Schneider Electric Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-103-01
https://us-cert.cisa.gov/ics/advisories/icsa-21-105-01

16. Siemens Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-103-04
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-05
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-06
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-07
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-08
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-10
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-11
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-12
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-15

17. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.407422
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.425276

18. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20211116-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211123-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211125-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211145-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211148-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211152-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211153-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211159-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211161-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211162-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211163-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211164-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211165-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211166-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211168-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211174-1/

https://www.suse.com/support/update/announcement/2021/suse-su-20211175-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211176-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211177-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211179-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211180-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211181-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211182-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211187-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211188-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211189-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211190-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211210-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211211-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20211233-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114690-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114692-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114693-1/

19. Ubuntu

https://ubuntu.com/security/notices/USN-4899-2
https://ubuntu.com/security/notices/USN-4904-1
https://ubuntu.com/security/notices/USN-4905-1
https://ubuntu.com/security/notices/USN-4906-1
https://ubuntu.com/security/notices/USN-4907-1
https://ubuntu.com/security/notices/USN-4909-1
https://ubuntu.com/security/notices/USN-4910-1
https://ubuntu.com/security/notices/USN-4911-1
https://ubuntu.com/security/notices/USN-4912-1
https://ubuntu.com/security/notices/USN-4913-1
https://ubuntu.com/security/notices/USN-4914-1
https://ubuntu.com/security/notices/USN-4915-1
https://ubuntu.com/security/notices/USN-4916-1
https://ubuntu.com/security/notices/USN-4917-1

20. WordPress

https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/

Sources of product vulnerability information:

CentOS
Debian
F5
Google Chrome
IBM
Joomla!
Juniper
McAfee
Microsoft
Oracle Linux
Red Hat
Slackware

SUSE
Ubuntu
US-CERT
WordPress

Contact:

cert@govcert.gov.hk