GovCERT.HK

Weekly IT Security News Bulletin, 2022-W04

24 January – 30 January 2022

Headlines

Be aware of mobile banking trojans

- Researchers have discovered several active campaigns distributing mobile banking Trojans on Android devices through a variety of delivery methods. Threat actors used mock-ups of popular applications posing as QR code scanners or advertisement blockers and sent SMS messages from already-compromised devices to further spread the malware.

- The functionality of the banking Trojans was straightforward and remained the same throughout the campaigns. They would steal banking, contact, SMS and other types of private data from infected devices. They could also perform other malicious activities such as sending SMS messages with content provided by the command-and-control (C2) server which allowed their operators to change the targeted banks dynamically.

- The campaign came in waves with different messages and in different time zones. While the malware remained pretty static, the message used to carry the banking trojans and the domains that host the droppers were constantly changing and adapting.

Advice

- Avoid installing applications from unofficial and third-party app stores and avoid providing credential information in these applications.
- Enable multi-factor authentication (MFA) for online accounts to minimise the risks of credential theft.
- Enable Google Play Protect or install third-party anti-malware apps to scan installed mobile applications regularly.

Sources

- Bitdefender
- Threatpost

New device registration trick in phishing attacks

- Security analysts from Microsoft observed a multi-phase phishing campaign that leveraged stolen credentials to register devices onto the target networks and conduct further attacks. The campaign was initiated by spreading phishing emails with fake notifications to trick victims into entering their credentials on a spoofed Office 365 login page.

- Once credentials were obtained via the spoofed login page, they were used to establish a remote connection via Exchange Online PowerShell. To avoid arousing the victims' suspicions, a number of inbox rules were configured in the victim's inbox to delete non-delivery reports and notification emails.

- In the later phase of the campaign, the attackers registered their Windows devices using the stolen credentials to the target Azure Active Directories that have not enabled Multi-factor authentication (MFA). With a registered device, attackers could launch other waves of phishing emails from a recognised and trusted part of the domain, thereby significantly expanding the success of the phishing campaign.

Advice

- Implement proper credential hygiene and enforce MFA for all users.
- Deploy endpoint protection solutions to detect suspicious PowerShell activities and creation of inbox rules.
- Review the registered devices regularly to identify suspicious devices on the organisation network.
- Implement network segmentation to restrict lateral movement.

Sources

- Microsoft
- Bleeping Computer

Product Vulnerability Notes & Security Updates

1. Apple Products

https://support.apple.com/en-us/HT213054
https://support.apple.com/en-us/HT213055
https://support.apple.com/en-us/HT213056
https://support.apple.com/en-us/HT213058

2. CentOS

https://lists.centos.org/pipermail/centos-announce/2022-January/073550.html
https://lists.centos.org/pipermail/centos-announce/2022-January/073551.html
https://lists.centos.org/pipermail/centos-announce/2022-January/073552.html
https://lists.centos.org/pipermail/centos-announce/2022-January/073553.html

3. Debian

https://www.debian.org/security/2022/dsa-5049
https://www.debian.org/security/2022/dsa-5050
https://www.debian.org/security/2022/dsa-5051
https://www.debian.org/security/2022/dsa-5052
https://www.debian.org/security/2022/dsa-5053
https://www.debian.org/security/2022/dsa-5054
https://www.debian.org/security/2022/dsa-5055
https://www.debian.org/security/2022/dsa-5056
https://www.debian.org/security/2022/dsa-5057
https://www.debian.org/security/2022/dsa-5058
https://www.debian.org/security/2022/dsa-5059
https://www.debian.org/security/2022/dsa-5060
https://www.debian.org/security/2022/dsa-5061
https://www.debian.org/security/2022/dsa-5062
https://www.debian.org/security/2022/dsa-5063

4. GE Gas Power ToolBoxST

https://us-cert.cisa.gov/ics/advisories/icsa-22-025-01

5. Gentoo Linux

https://security.gentoo.org/glsa/202201-01

6. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220126-01-df75863e-en

7. McAfee

https://kc.mcafee.com/corporate/index?page=content&id=SB10359
https://kc.mcafee.com/corporate/index?page=content&id=SB10376

8. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/5POFOWWCWJ3SLTEUIQRMKXQB4GOECNOP/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/6XYIZAS6LJG7AX5XUIXPP347424BX5VK/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/7LMNDFMX4WXDPLRBNT2EQKB2QXZZVISA/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/CXNFO6HH5VY6DMGZN52EB2OJNJXKBC5H/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/E4IIJDMYKSUHPR6X6ARBPWWQRNNXT4HI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FK6EK2KGH7KDPXCBN2Q3SSAVOCIXNCFX/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/G7QRUVRJT5W72APQEDYOZEMCHXZ5CMDO/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/JTS3PI42CZC7TVKVUTBOIMO2PDFTABYC/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/JVCSEXTJ2SI3QLMCUUQNNUT3HNZQJIML/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/JWT2GLRS2EG6EW7X57X2RMJHMFK6GEWU/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/LJ7DM7F3IHCRMEZDBDGMA5O6A5EWNQKE/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/LS5Y2M6XDX2JOBPPLIMAXXAXRPAU65ND/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ORE7QLMZXD7OV3HIKQUG3SXU2RG6ONFC/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/OVT7FRNNNK2PC4PFXSGAPUIG3HECY4P5/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/S44U3IKMS3KZS626YQ5ZYDHA2HLKQNER/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/SGEROI6PUOTOXKFIH2MPKUQ3PI6VWLXQ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/TPIWID3WJ3SMCA23W52QU3RW6AU7JCA7/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WXZCTLOB2POU23DZG3IW6R4QQB3Q2FON/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ZEHXIWSI3LT73BE7YAXGYKT4HEXYVR3X/

9. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-5192.html
https://linux.oracle.com/errata/ELSA-2021-5195.html
https://linux.oracle.com/errata/ELSA-2021-5206.html
https://linux.oracle.com/errata/ELSA-2021-9621.html
https://linux.oracle.com/errata/ELSA-2021-9623.html
https://linux.oracle.com/errata/ELSA-2022-0185.html
https://linux.oracle.com/errata/ELSA-2022-0188.html
https://linux.oracle.com/errata/ELSA-2022-0204.html
https://linux.oracle.com/errata/ELSA-2022-0258.html
https://linux.oracle.com/errata/ELSA-2022-0267.html

https://linux.oracle.com/errata/ELSA-2022-0274.html
https://linux.oracle.com/errata/ELSA-2022-0290.html
https://linux.oracle.com/errata/ELSA-2022-0306.html
https://linux.oracle.com/errata/ELSA-2022-0307.html
https://linux.oracle.com/errata/ELSA-2022-9056.html

10. Red Hat

https://access.redhat.com/errata/RHSA-2022:0165
https://access.redhat.com/errata/RHSA-2022:0166
https://access.redhat.com/errata/RHSA-2022:0181
https://access.redhat.com/errata/RHSA-2022:0185
https://access.redhat.com/errata/RHSA-2022:0204
https://access.redhat.com/errata/RHSA-2022:0209
https://access.redhat.com/errata/RHSA-2022:0211
https://access.redhat.com/errata/RHSA-2022:0228
https://access.redhat.com/errata/RHSA-2022:0229
https://access.redhat.com/errata/RHSA-2022:0230
https://access.redhat.com/errata/RHSA-2022:0231
https://access.redhat.com/errata/RHSA-2022:0232
https://access.redhat.com/errata/RHSA-2022:0233
https://access.redhat.com/errata/RHSA-2022:0236
https://access.redhat.com/errata/RHSA-2022:0237
https://access.redhat.com/errata/RHSA-2022:0239
https://access.redhat.com/errata/RHSA-2022:0246
https://access.redhat.com/errata/RHSA-2022:0254
https://access.redhat.com/errata/RHSA-2022:0258
https://access.redhat.com/errata/RHSA-2022:0260
https://access.redhat.com/errata/RHSA-2022:0265
https://access.redhat.com/errata/RHSA-2022:0266
https://access.redhat.com/errata/RHSA-2022:0267
https://access.redhat.com/errata/RHSA-2022:0268
https://access.redhat.com/errata/RHSA-2022:0269
https://access.redhat.com/errata/RHSA-2022:0270
https://access.redhat.com/errata/RHSA-2022:0271
https://access.redhat.com/errata/RHSA-2022:0272
https://access.redhat.com/errata/RHSA-2022:0273
https://access.redhat.com/errata/RHSA-2022:0274
https://access.redhat.com/errata/RHSA-2022:0288
https://access.redhat.com/errata/RHSA-2022:0289
https://access.redhat.com/errata/RHSA-2022:0290
https://access.redhat.com/errata/RHSA-2022:0291
https://access.redhat.com/errata/RHSA-2022:0294
https://access.redhat.com/errata/RHSA-2022:0296
https://access.redhat.com/errata/RHSA-2022:0297
https://access.redhat.com/errata/RHSA-2022:0303
https://access.redhat.com/errata/RHSA-2022:0304
https://access.redhat.com/errata/RHSA-2022:0305
https://access.redhat.com/errata/RHSA-2022:0306
https://access.redhat.com/errata/RHSA-2022:0307
https://access.redhat.com/errata/RHSA-2022:0308
https://access.redhat.com/errata/RHSA-2022:0310
https://access.redhat.com/errata/RHSA-2022:0312

https://access.redhat.com/errata/RHSA-2022:0317
https://access.redhat.com/errata/RHSA-2022:0318
https://access.redhat.com/errata/RHSA-2022:0321

11. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.412000
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.432416

12. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20220149-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220150-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220151-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220157-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220160-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220161-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220163-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220166-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220169-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220171-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220175-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220176-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220177-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220178-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220179-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220181-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220182-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220183-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220184-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220189-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220190-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220191-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220206-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220210-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220211-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220212-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220213-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220214-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214878-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214879-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214880-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214882-1/

13. Trend Micro

https://success.trendmicro.com/solution/000290416

14. Ubuntu

https://ubuntu.com/security/notices/USN-5064-2
https://ubuntu.com/security/notices/USN-5193-2
https://ubuntu.com/security/notices/USN-5247-1
https://ubuntu.com/security/notices/USN-5249-1
https://ubuntu.com/security/notices/USN-5250-1
https://ubuntu.com/security/notices/USN-5250-2
https://ubuntu.com/security/notices/USN-5252-1
https://ubuntu.com/security/notices/USN-5252-2
https://ubuntu.com/security/notices/USN-5254-1
https://ubuntu.com/security/notices/USN-5255-1

15. Xen

https://xenbits.xen.org/xsa/advisory-393.html
https://xenbits.xen.org/xsa/advisory-394.html
https://xenbits.xen.org/xsa/advisory-395.html

Sources of product vulnerability information:

Apple
CentOS
Debian
Gentoo Linux
Huawei
McAfee
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Trend Micro
Ubuntu
US-CERT
Xen

Contact:

cert@govcert.gov.hk