GovCERT.HK

Weekly IT Security News Bulletin, 2021-W39

27 September – 3 October 2021

Headlines

Be aware of one-time password interception bots

- Many online web applications now support the use of two-factor authentication (2FA) to add extra layers of security for their client accounts, such as one-time passwords (OTPs). A research from a cybersecurity firm called "Intel 471" revealed an upward trend in one-time password interception services that help attackers get OTPs from targets.

- These services abuse popular instant messaging systems to create and manage bots for OTP interception by using some simple commands. The bots would automatically make a call or send messages to targets pertaining to be from a legitimate contact, and lure targets into providing their OTPs.

- These services demonstrated a high success rate as the bots are capable of spoofing the phone number of a legitimate contact.

Advice

- Users should stay vigilant against suspicious calls and messages.
- Users should never send personal and sensitive information to third parties until their identities are verified.
- Organisations should provide user awareness training to their staff to enhance their awareness of phishing attacks.

Sources

- Intel 471
- CSO

Android Trojan found in hundreds of mobile applications

- Security researchers from Zimperium zLabs uncovered a massive mobile campaign that infected over 10 million Android devices since November 2020. Threat actors behind the campaign distributed over 200 trojanised Android apps through both the official Google Play and third-party app stores that contained a malware named GriftHorse. These trojanised apps are designed to subscribe paid SMS services that are charged on a monthly basis for victims without their consent.

- Once these apps were installed and executed, malicious pages would appear on their screens informing victims of a fake free prize offer. Victims who accepted the offer would be redirected to a malicious webpage, asking them to submit their phone numbers for verification purposes. The phone numbers were then used to sign up paid SMS services that add extra charges to the victims' monthly mobile bills without their knowledge and consent.

- To avoid malware detection and infect more potential victims, the URLs of malicious webpages were generated dynamically. The language for these webpages would also be changed based on the geo-location of victims' IP address.

Advice

- Remain vigilant when being asked to provide any personal information to suspicious parties.
- Avoid installing apps from unofficial and third-party app stores.

Sources

- Zimperium
- Bleeping Computer
- The Hacker News

Product Vulnerability Notes & Security Updates

1. CentOS

https://lists.centos.org/pipermail/centos-announce/2021-September/048367.html

2. Debian

https://www.debian.org/security/2021/dsa-4978

3. F5 Products

https://support.f5.com/csp/article/K43700555

4. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4HYGTSDI2IQ34SYGQZGBYMH3NPMCAL2X/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/5AJVQHCUMK7J3JDSTOVI22XABIMBIMGX/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/BGUJWWBS4PDPSJUYSU34VIR2THULULQF/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/CXHELI44TGNRVVE3N32KXRTYBU3O3F3H/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FCVD7RYV2TSOLINPDAIY7P7Q4OSCOREN/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/HT3PAHM4M6Q56XJOJVVIZBROY2Y4SUU2/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/PQ34JCCBYY5MVDLL7VGCWBOZKOQ5EXTK/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/SKQBP2PRAEJOFAWUWOWJ6PIS2W2H7IA2/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WCFOPHTCYLOVNMVIHXDFWZ2NNKEOKROF/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ZDRKVDFEPABXRR653626WGJRZWK5HZ7Y/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ZUSEK4W6EWPU4TCOU42FNZFNKGMKOJLZ/

5. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-3666.html
https://linux.oracle.com/errata/ELSA-2021-9465.html

6. Red Hat

https://access.redhat.com/errata/RHSA-2021:3631
https://access.redhat.com/errata/RHSA-2021:3635
https://access.redhat.com/errata/RHSA-2021:3642
https://access.redhat.com/errata/RHSA-2021:3665
https://access.redhat.com/errata/RHSA-2021:3666
https://access.redhat.com/errata/RHSA-2021:3675
https://access.redhat.com/errata/RHSA-2021:3694

7. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20213234-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213235-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213236-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213237-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213244-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213251-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213254-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213255-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213256-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213257-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213258-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114811-1/

8. Trend Micro

https://success.trendmicro.com/solution/000289038

9. Ubuntu

https://ubuntu.com/security/notices/USN-5090-1
https://ubuntu.com/security/notices/USN-5090-2
https://ubuntu.com/security/notices/USN-5090-3
https://ubuntu.com/security/notices/USN-5090-4
https://ubuntu.com/security/notices/USN-5091-1
https://ubuntu.com/security/notices/USN-5092-1
https://ubuntu.com/security/notices/USN-5092-2
https://ubuntu.com/security/notices/USN-5093-1
https://ubuntu.com/security/notices/USN-5094-1
https://ubuntu.com/security/notices/USN-5095-1
https://ubuntu.com/security/notices/USN-5096-1

Sources of product vulnerability information:

- CentOS
- Debian
- F5 Products
- openSUSE
- Oracle Linux
- Red Hat
- SUSE
- Trend Micro
- Ubuntu

Contact:

cert@govcert.gov.hk