

THREAT INTEL INSIGHTS

DECEMBER 2023






SOUTHEAST ASIAN BANKING APPS TARGETED BY NEW FJORDPHANTOM ANDROID MALWARE

A new and sophisticated Android malware, named FjordPhantom, has been disclosed by cybersecurity researchers. The malware targets users in Southeast Asian countries, including Indonesia, Thailand, and Vietnam, and has been active since early September 2023. Oslo-based mobile app security firm Promon conducted an analysis revealing that FjordPhantom primarily spreads through messaging services, employing a combination of app-based malware and social engineering to defraud banking customers.

2

CARBANAK BANKING MALWARE EMERGES AGAIN WITH NEW RANSOMWARE TACTICS

The banking malware named Carbanak has resurfaced with new and updated tactics and is observed being used in ransomware attacks. The malware returned last month and has been distributed via compromised websites by pretending to be legitimate business-related software, such as Xero, HubSpot, and Veeam. Carbanak was first discovered in the wild in 2014 and is notorious for its remote control and data exfiltration capabilities. It started as a banking malware and has been used a lot by the FIN7 cybercriminal group.



3

CRITICAL CITRIX BLEED VULNERABILITY EXPLOITED IN LOCKBIT RANSOMWARE ATTACKS

Various threat actors, including affiliates of the LockBit ransomware group, took advantage of a recently disclosed vulnerability in Citrix NetScaler application delivery control (ADC) and Gateway appliances. This flaw was exploited as a means to gain initial access to targeted environments. LockBit 3.0 affiliates have been known to be leveraging Citrix Bleed for a while as it allows the attackers to bypass security like password requirements and multifactor authentication (MFA), which in turn leads to the hijacking of legitimate user sessions successfully on Citrix NetScaler ADC and Gateway applications. All this requires elevated permissions for harvesting credentials, accessing data and resources, and moving laterally across the network.

4

THE FAKE SECURITY ADVISORY PROMOTES THE INSTALLATION OF BACKDOOR PLUGINS FOR WORDPRESS

Researchers reported a phishing campaign targeting WordPress users.

The fraudulent email, posing as WordPress, falsely warned of a non-existent Remote Code Execution vulnerability (CVE-2023-45124) on the user's site. The email urges recipients to download a supposed "Patch" plugin, potentially leading to a malicious installation. The entry for the fake plugin shows a likely inflated download count of 500,000, along with multiple phony user reviews elaborating on how the patch restored their compromised site and helped them thwart hacker attacks.

5

NEW CYBER ESPIONAGE CAMPAIGN BY RUSSIAN APT28 THREAT GROUP TARGETS 13 COUNTRIES

The Russian state-backed threat group APT28 was discovered using lures related to the ongoing Palestine-Israel war to deliver a custom backdoor dubbed HeadLace. The adversary is tracked under ITG05 (aka Fancy Bear, BlueDelta, Forest Blizzard, and FROZENLAKE) and is targeting 13 nations worldwide by using authentic documents from finance, academic, and diplomatic centers. The targeted countries include Türkiye, Hungary, Poland, Australia, Belgium, Germany, Ukraine, Azerbaijan, Kazakhstan, Saudi Arabia, Latvia, Italy, and Romania.

6


MICROSOFT WARNS OF OAUTH APPS UTILIZED FOR AUTOMATIC BEC AND CRYPTOMINING ATTACKS

Microsoft issued a warning about financially-motivated cybercriminals who are using OAuth applications to launch automated BEC and phishing attacks, send spam, and deploy virtual machines for cryptomining. It was revealed that the threat actors are primarily focusing on user accounts without authentication mechanisms, such as multifactor authentication, and target them with password-spraying or phishing attacks. The attackers also look for permissions to create or modify OAuth apps in these accounts. The compromised accounts are then used to make new OAuth apps with high privileges, which lets them hide malicious activity while ensuring access to the account.

7

ANDROID BANKING TROJAN CHAMELEON STEALS PINS BY DISABLING FINGERPRINT AUTHENTICATION

The notorious banking trojan Chameleon re-emerged with a new variant that disables fingerprint and face unlock features on Android devices to steal PIN codes. This is achieved by using an HTML page to gain access to the Accessibility service and a method that is capable of disrupting biometric operations which allows the threat actors to steal PINs and unlock the device. The first version of Chameleon was discovered in April 2023 and mainly targeted Australia and pretended to be government agencies, banks, and the CoinSpot cryptocurrency platform. The malware is capable of keylogging, cookie theft, overlay injection, and SMS theft on the infected systems.





300 ORGANIZATIONS WORLDWIDE TARGETED BY PLAY RANSOMWARE USING DOUBLE-EXTORTION

The cybercriminals behind the Play ransomware are said to have impacted about 300 organizations as of October 2023. The ransomware operators employ a double-extortion technique, which encrypts systems after exfiltrating sensitive data. The adversary affected multiple business entities and critical infrastructure in North America, Europe, South America, and Australia. Play (aka PlayCrypt and Balloonfly) was first discovered in 2022 when it exploited vulnerabilities in Microsoft Exchange servers (CVE-2022-41040 and CVE-2022-41082) and Fortinet devices (CVE-2018-13379 and CVE-2020-12812) to infiltrate organizations and deploy malware to encrypt files.