Android Malware Bypasses Two-factor-Authentication and Targets Gmail, Telegram Passwords

A recent Android malware strain has been identified, it is a part of the Rampant Kitten threat group's widespread surveillance campaign that targets mobile apps like Telegram credentials and more.

Modus Operandi

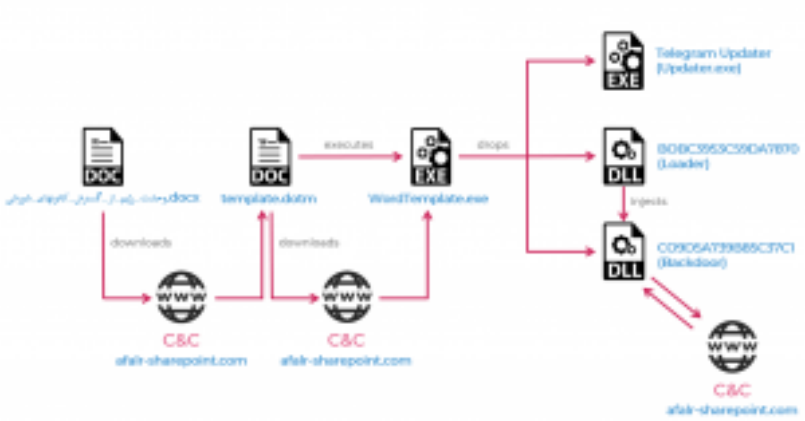
Investigators have recently uncovered a threat group initiating surveillance campaigns that target victims' data on their mobile devices, browser credentials, and even Telegram messaging application files. One notable tool in the group's arsenal is an Android malware that collects all two-factor authentication (2FA) security codes sent to devices, sniffs out Telegram credentials, and launches Google account phishing attacks.

Dubbed AS "Rampant Kitten", this attack has targeted Iranian entities with surveillance campaigns for at least six years. It specifically targets Iranian minorities and anti-regime organizations, including the Association of Families of Camp Ashraf and Liberty Residents (AFALR); and the Azerbaijan National Resistance Organization.

The threat group has relied on a wide array of tools for carrying out their attacks, including four Windows info-stealer variants used for pilfering Telegram and KeePass account information; phishing pages that impersonate Telegram to steal passwords; and the aforementioned Android backdoor that extracts 2FA codes from SMS messages and records the phone's voice surroundings.

The Attacks

Rampant Kitten's attack was discovered through a document, the title of which translates to "The Regime Fears the Spread of the Revolutionary Cannons.docx." It's unclear how this document is spread (via spear-phishing or otherwise), but it purports to describe the ongoing struggle between the Iranian regime and the Revolutionary Cannons, an anti-regime, Mujahedin-e Khalq movement.
The document when opened loads a document template from a remote server (afalr-sharepoint[.]com), which impersonates a website for a non-profit that aids Iranian dissidents.



The attack vector by Check Point Research

It then downloads malicious macro code, which executes a batch script to download and execute a next-stage payload. This payload then checks if the popular Telegram messenger service is installed on the victims' system. If so, it extracts three executables from its resources.

These executables include an information stealer, which lifts Telegram files from the victim's computer, steals information from the KeePass password-management application, uploads any file it can find which ends with a set of pre-defined extensions, and logs clipboard data and takes desktop screenshots.

Researchers were able to track multiple variants of this payload dating back to 2014. These include the TelB (used in June and July 2020) and TelAndExt variants (May 2019 to February 2020), which focus on Telegram; a Python info stealer (February 2018 to January 2020) that is focused on stealing data from Telegram, Chrome, Firefox and Edge; and a HookInjEx variant (December 2014 to May 2020), an info stealer that targets browsers, device audio, keylogging and clipboard data.

Android Backdoor

During their investigation, researchers also discovered a malicious Android application linked to the same threat actors. The application was claiming to be a service to help Persian speakers in Sweden get their driver's license.

Instead, once victims download the application, the backdoor steals their SMS messages and bypasses 2FA by forwarding all SMS messages containing 2FA codes to an attacker-controlled phone number. All incoming SMS messages from Telegram, and other social network apps, are also automatically sent to the attackers' phone number.

The application also launches a phishing attack targeting victims' Google account (Gmail) credentials. The user is presented with a legitimate Google login page, inside Android's WebView. In reality, attackers have used Android's Javascript Interface to steal typed-in credentials, as well as a timer that periodically retrieves the information from the username and password input fields.

Recommendation

One way of keeping safe from phishing attacks when using both android and apple applications on your mobile device is to always use strong passwords. Also, avoid allowing downloaded apps from accessing personal files like contacts and photos saved on your account or device. Ignore or delete suspicious emails and messages from unknown users. Remember to always "Think before you click".

References:

https://bitcoinexchangeguide.com/android-malware-gustuff-found-by-group-ib-targeting-phones-crypto-apps-and-international-banks/
https://www.cnet.com/how-to/4-signs-your-android-phone-has-hidden-malware-and-how-to-deal-with-it/
https://www.zdnet.com/article/this-powerful-android-malware-stayed-hidden-years-infected-tens-of-thousands-of-smartphones/
https://threatpost.com/android-2fa-telegram-gmail/159384/