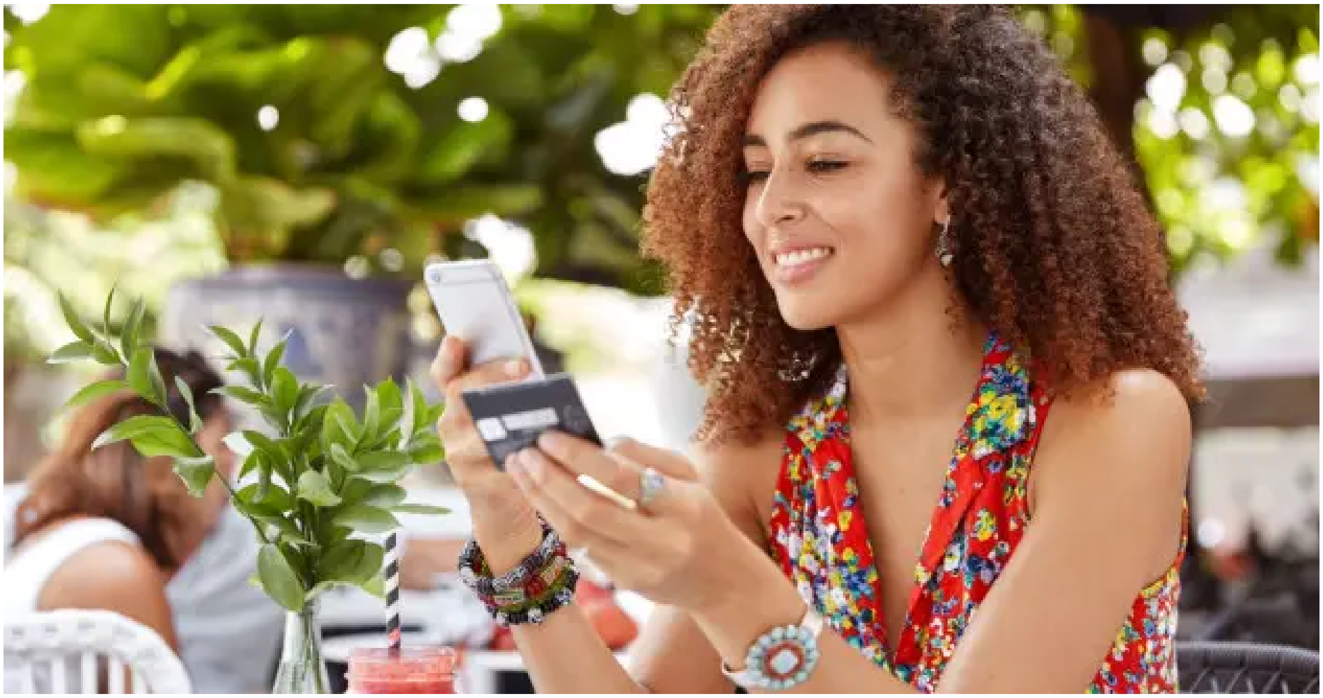
Ginp Malware Operations are on the Rise with Expansions in Turkey

securityintelligence.com/posts/ginp-malware-operations-rising-expansions-turkey/

Home&nbsp/ Application Security

Ginp Malware Operations are on the Rise, Aiming to Expand in Turkey



Application Security June 18, 2020

By Pavel Asinovsky 5 min read

The Ginp mobile banking malware, which emerged in late 2019, is one of the top most prevalent Android banking malware families today. It started as a SMS stealer and rapidly evolved into one of the most advanced actors in the financial fraud landscape. Ginp has primarily targeted Spanish banks, but recent evidence suggests the malware has changed or may change its targeting strategy in the near future to focus on Turkey. The following chart shows infection rates for different Android malware families from the last 90 days and demonstrates that Ginp accounts for nearly 12% of infections during this time.

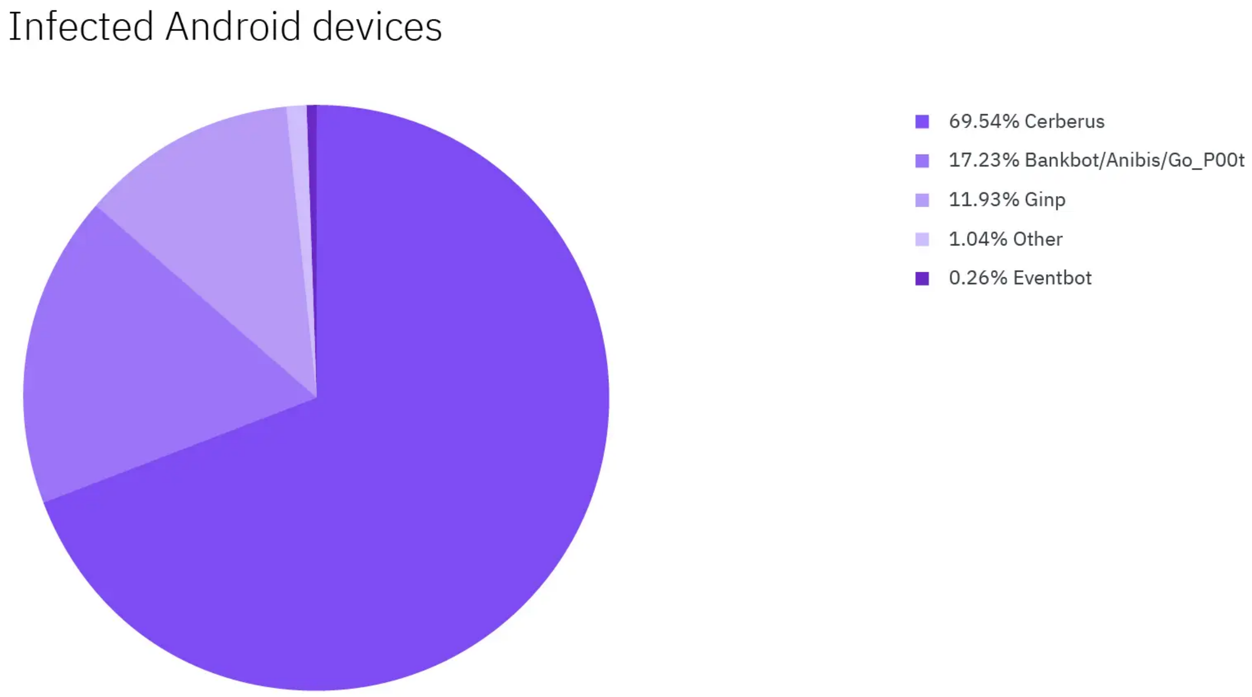


Figure 1: Android banking malware infections from the last 90 days (source: IBM Trusteer)

Ginp Expands Targeting to Turkey

A few weeks ago, IBM’s Trusteer team found evidence that Ginp malware developers intend to broaden their target set to customers of Turkish banks, after targeting Spanish banking customers and customers in Poland and the United Kingdom. Specifically, our team discovered new Ginp overlay pages intended for overlay attacks on mobile devices residing on the malware’s command-and-control (C&C) servers (see Figure 2). These overlay pages are spoofs of legitimate banking pages, meant to deceive mobile device users into sharing confidential banking and other information. Several of these fake overlays mimic banks in Turkey, suggesting that malware operators intend to use these pages in future campaigns to target customers of Turkish banks. These fake overlays have not previously been noted in the security community.

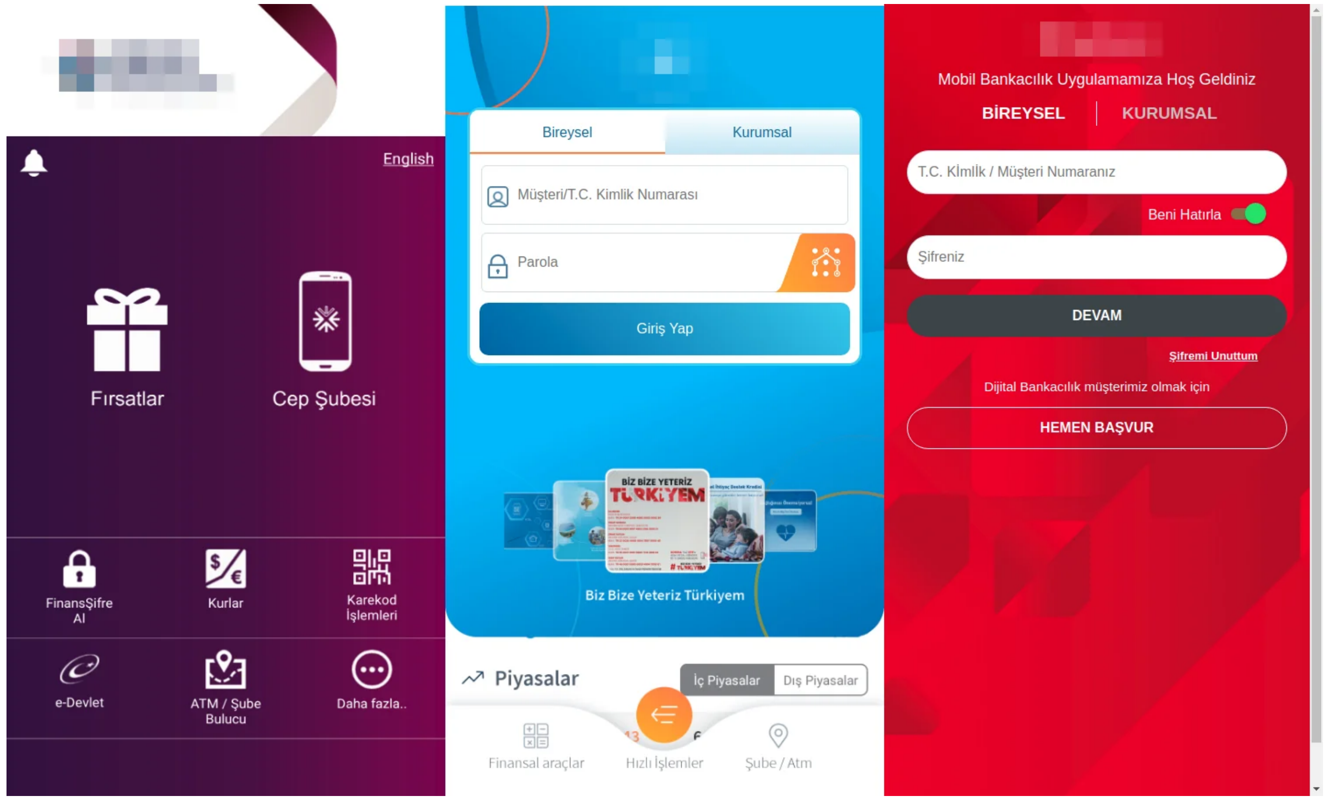


Figure 2: Some of the overlay pages targeting Turkish banks, found on Ginp's C&C server (source: IBM Trusteer)

Ginp's new targeting strategy echoes other mobile banking malware families, which have also expanded target sets to include Turkish banking customers. Cybercriminals appear to be finding this geographical region fruitful for cyber operations. Some observers have attributed this to obsolete systems and widespread poor security management. It also is possible that cybercriminals developing these overlays have recently made several options targeting Turkish banks available on the dark web, which have become a popular commodity in those forums, including for Ginp operators.

Despite Ginp's expansion to Turkey, we assess the group will continue to target Spanish banking customers, as well, based on recent overlay screens our team found on the malware's C&C server aimed at Spanish banks. The malware no longer appears to target Poland or the UK, but that targeting strategy may change at any time.

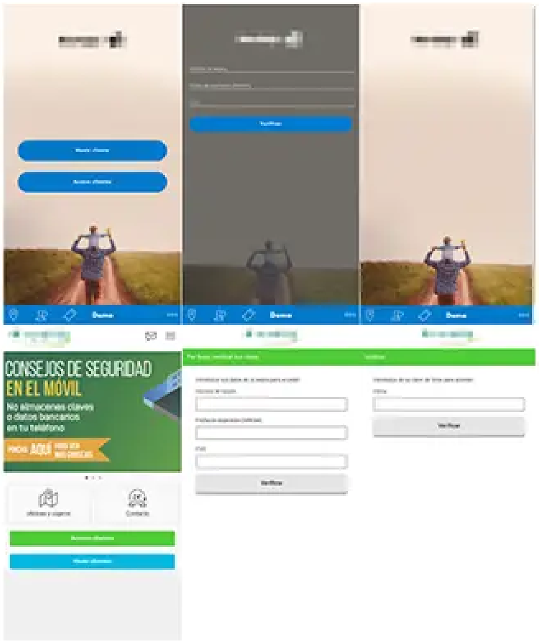

CONSEJOS DE SEGURIDAD
EN EL MÓVIL
No almacenes claves o datos bancarios en tu teléfono
PINCHA AQUÍ PARA VER MÁS CONSEJOS

Figure 3: Overlay pages targeting Spanish banks, recently found on Ginp's C&C server (source: IBM Trusteer)

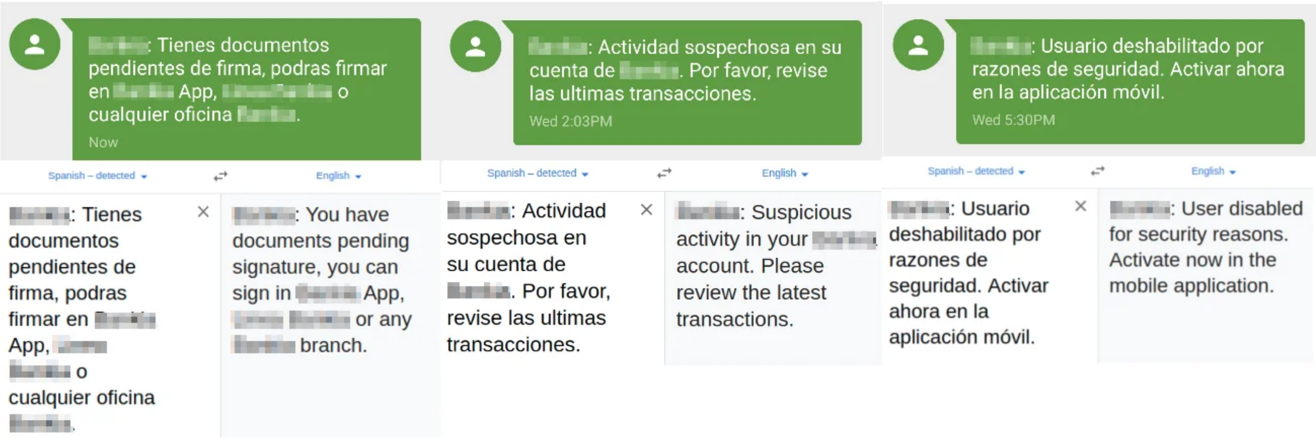
How Ginp's Overlay Attack Works in Practice

Our team has studied how Ginp operators deploy the fake overlay pages to victims' mobile devices. When Ginp starts running, it first obtains information from the victim's device, such as the state of the device and the currently installed applications, and sends it to the server. Based on this information, the server will then decide how to proceed—usually discovering which banking application the victim uses, and then initiating an attack. In most cases, the malware will prompt the victim to click on his or her banking application and then pop a fake overlay onto the screen. In some cases, the malware operators will spy on the target before deciding the best avenue of attack to bypass security countermeasures.

Ginp's C&C server can send an array of commands to the malware. These commands can be sent manually by an operator or automatically in response to information obtained by the malware.

It Starts With Social Engineering

One of the recent features added to Ginp is the ability to make it appear as if a legitimate SMS message is being received on a device. The server sends a command called "INSERT_SMS," which triggers the malware to effectively mimic the process of receiving a new SMS message. The messages reference documents that need to be signed or suspicious activity on a banking account—among other ploys—in an attempt to invoke a sense of urgency and persuade the victim to open his or her mobile banking application.



[redacted]: Tienes documentos pendientes de firma, podras firmar en [redacted] App, [redacted] o cualquier oficina [redacted].

[redacted]: You have documents pending signature, you can sign in [redacted] App, [redacted] or any [redacted] branch.

[redacted]: Actividad sospechosa en su cuenta de [redacted]. Por favor, revise las ultimas transacciones.

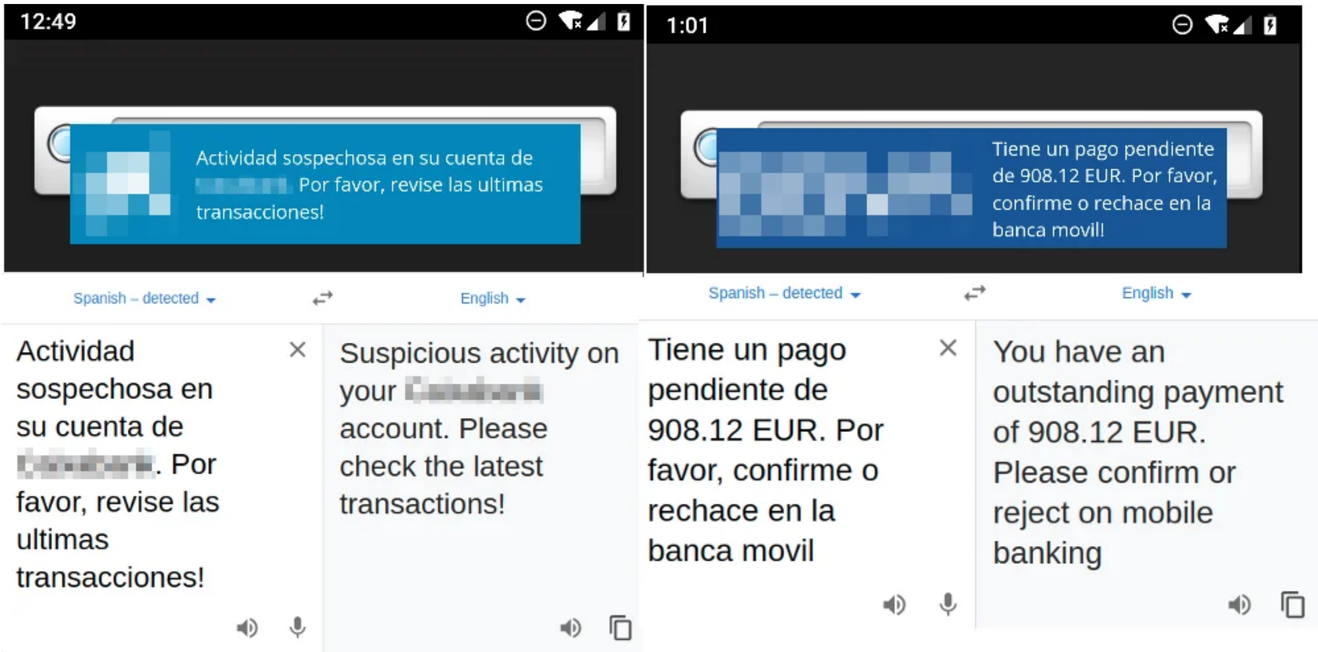
[redacted]: Suspicious activity in your [redacted] account. Please review the latest transactions.

[redacted]: Usuario deshabilitado por razones de seguridad. Activar ahora en la aplicación móvil.

[redacted]: User disabled for security reasons. Activate now in the mobile application.

Figure 4: Fake incoming SMS messages generated by Ginp (source: IBM Trusteer)

An additional technique the malware uses is generating fake push notifications. The server can send a “PUSH_NOTIFY” command to generate a fake “push” notification and make it appear as if it’s coming from the banking app.



Actividad sospechosa en su cuenta de [redacted]. Por favor, revise las ultimas transacciones!

Suspicious activity on your [redacted] account. Please check the latest transactions!

Tiene un pago pendiente de 908.12 EUR. Por favor, confirme o rechace en la banca movil!

Tiene un pago pendiente de 908.12 EUR. Por favor, confirme o rechace en la banca movil

You have an outstanding payment of 908.12 EUR. Please confirm or reject on mobile banking

Figure 5: Fake push notifications generated by Ginp (source: IBM Trusteer)

Activate the Overlay

In general, as soon as the victim uses his or her banking app, this activity is logged and sent to the C&C server. If the banking app is targeted by Ginp, the server will respond with a command of “START_INJ” for the malware to start the overlay attack. This command will trigger the malware to open a WebView on top of the screen and fetch the overlay attack pages. However, Ginp also provides attackers with the flexibility to initiate an overlay attack at any time without relying on the user. For example, an attacker can trigger the overlay as soon as the user sees the fake SMS message or push notification.

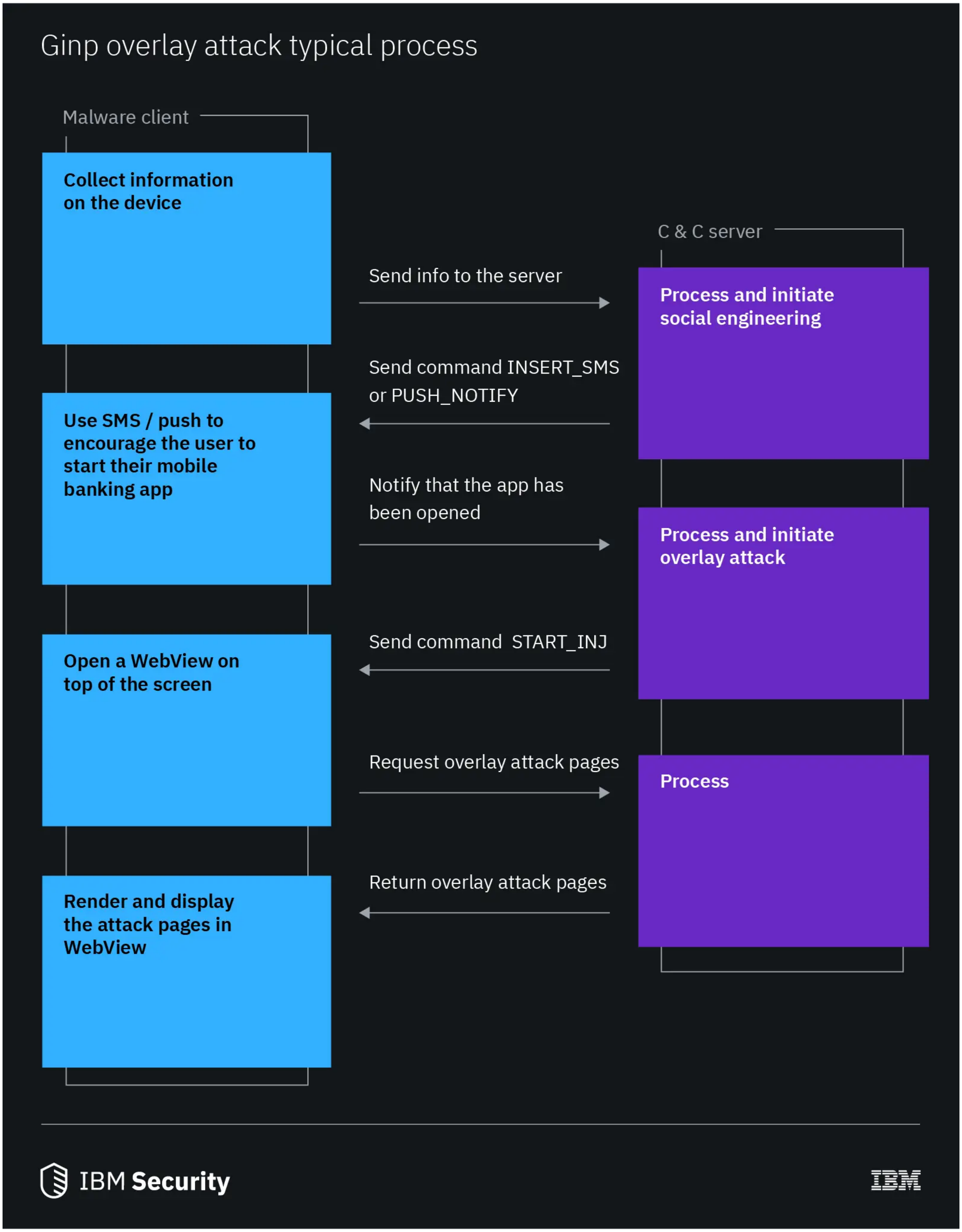

Ginp overlay attack typical process
Malware client
Collect information on the device
Use SMS / push to encourage the user to start their mobile banking app
Open a WebView on top of the screen
Render and display the attack pages in WebView
Send info to the server
Send command INSERT_SMS or PUSH_NOTIFY
Notify that the app has been opened
Send command START_INJ
Request overlay attack pages
Return overlay attack pages
C & C server
Process and initiate social engineering
Process and initiate overlay attack
Process
IBM Security
IBM

Figure 6: The typical process of Ginp's overlay attack (source: IBM Trusteer)

Evolving New Features

The Ginp malware continues to evolve rapidly, with developers frequently releasing new features. Several of these features are worth mentioning.

Fake SMS Push Notifications

This new feature was added December 2019. It is used for faking an incoming SMS message or push notification from the victim’s bank. These techniques allow the attacker to employ social engineering before initiating an overlay attack and help decrease suspicion from a victim.

Notifications Listener (Blocker) Service

A few months ago, Ginp developers introduced a new feature that allows the malware to block all push notifications from legitimate applications. This is particularly helpful to attackers, as it can block notifications about the fraudulent transaction taking place, thus avoiding arousing suspicion from the victim. Additionally, the content of the blocked notification is sent to the C&C server, allowing malware operators to steal second-factor authentication codes or collect social media and instant messaging notifications to spy on the target.

RAT Capabilities

Similar to other banking malware, Ginp operators started implementing Remote Access Trojan (RAT) capabilities around March 2020, which allow them to spy on the victim in real time. This feature allows attackers to exfiltrate valuable information that can enable them to circumvent security controls. More carefully, they can tailor an attack on a victim to increase their chances for success. The RAT also allows malware operators to take control of and conduct transactions from the victim’s device, reducing the risk of being detected by security countermeasures.

Injections Locker

Ginp’s newest feature is the injections locker. This feature was introduced just in the past few weeks and is activated by the “START_LOCK” command. It allows attackers to use an aggressive version of an overlay attack. These overlay pages are similar to the regular ones, but persist on the screen and keep reappearing. This feature blocks the victim from using his or her phone, even after entering their credentials, until their device is released by the malware operator. This feature creates advantages for the attacker by persuading a victim to enter and reveal credentials to unlock the phone, and preventing a victim from accessing a legitimate banking application, which may have security countermeasures.

Pavel Asinovsky
Malware Researcher

Pavel is a malware researcher for IBM Security's Trusteer's group. He has been a member of the Trusteer cybercrime labs for more than two years. Prior to tha...