

The logo for 'allot' is positioned at the top center. The word 'allot' is written in a lowercase, sans-serif font. The 'o' is a solid red circle, while the other letters are white. Below the logo, the tagline 'See. Control. Secure.' is written in a smaller, white, sans-serif font.

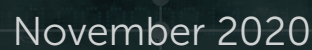
allot  
See. Control. Secure.

The text 'Threat Bulletin' is centered in the lower half of the page. It is written in a white, sans-serif font. A thin red horizontal line is positioned directly beneath the word 'Bulletin'.

Threat Bulletin

The logo for 'GINP' is located at the bottom center. The letters 'G', 'I', and 'N' are red, while the letter 'P' is orange. The font is a bold, sans-serif typeface.

GINP

The text 'November 2020' is centered at the very bottom of the page. It is written in a white, sans-serif font.

November 2020



## Intro

Ginp is a Banker Trojan that targets mobile users and devices, primarily Android. A Banker Trojan is a malicious computer program that intercepts sensitive personal information and credentials for accessing online bank or payment accounts.

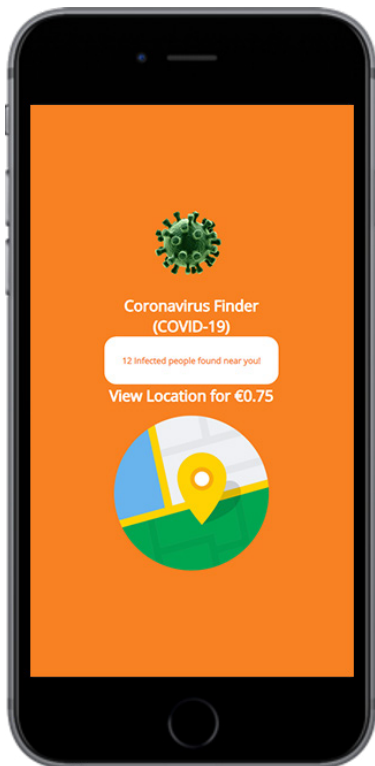
Ginp first appeared in 2019 as an SMS stealer, but quickly evolved into one of the most advanced financial fraud cyberthreats. It re-emerged in a more lethal version in early 2020 that exploited the emerging COVID-19 crisis to trick mobile users into downloading the malicious code. The attack lasted about two months, during May and June of 2020, and targeted primarily Spanish mobile users; though Ginp has also been found in the UK, France, Poland and Turkey. The first wave in Spain seems to have subsided for now, but we expect the cybercriminals behind the attack are busy improving the malware and devising new human engineering techniques before launching the next wave.

## How are Users Infected?

Similar to phishing attacks, the initial infection occurs when a user receives an e-mail or SMS message. In this case the messages claimed to have information about people in the near proximity that are infected with Coronavirus. The message looks and feels like familiar Android Google Maps, includes a specific number of infected people found, and offers to grant access to view their exact locations for a small fee of just 0.75 EURO. The user is then led to download and install the 'Coronavirus Finder' application either directly from the e-mail/SMS message, or via a fraudulent landing page containing a link to download the app. The message plays on people's natural fears and combined with the low price and immediacy of gaining access to the information with a few quick clicks is very compelling.

Once they click, they are led to download an Android Package Kit (APK) from a domain operated by the cybercriminals, not the official Google Play store. APKs are used by developers who want to share app files directly, usually during development stages, and therefore are completely unmonitored and do not go through the vetting and approval process of app on the official Google Play store.

## Malicious Activity



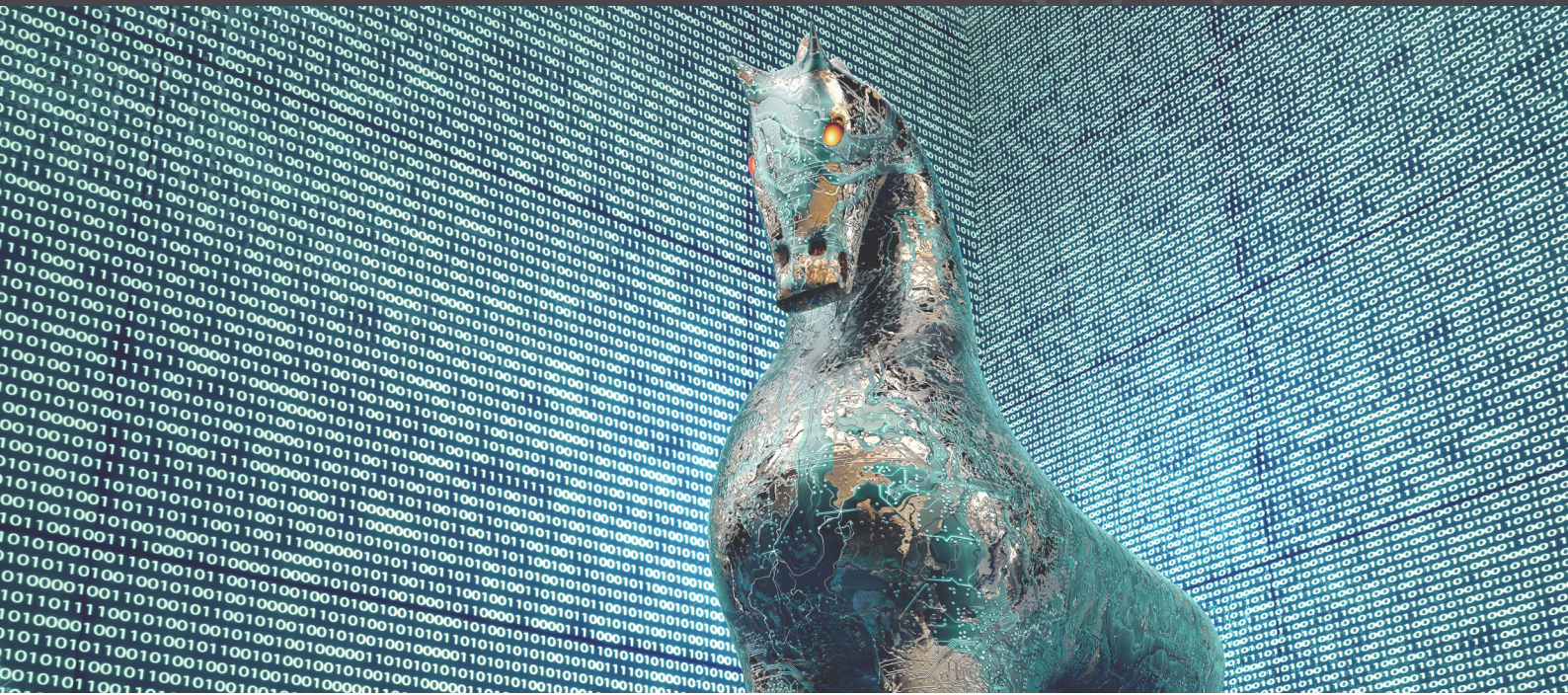
Once Ginp has infected the user's device, it scans and collects information such as: location properties, software version, installed applications, payment or banking apps, etc. Next, Ginp transmits the information it has gathered to a dedicated server controlled where analysis of the information is performed. Following the analysis, a customized attack plan is devised to target the specific financial applications the infected user has on their device. For example, a user with PayPal on their phone may be directed to a phishing page that looks and behaves just like PayPal. Likewise, for Amazon and other ecommerce websites and of course banking or credit card apps. The user gets a notification that appears to have been sent from the app they have installed on their phone, asking them to open the application.

When they do so, Ginp inserts an overlay element on top of the "legitimate" application, which looks like a login screen for the application or other webpage and asks the user to insert their credentials. Ginp is taking advantage of the "accessibility" features, which are now embedded in almost all mobile devices and operating systems, and enable users with impaired vision to view the content on their screen in various degrees of zoom-in. The content itself is not changed. Rather Ginp exploits this feature by displaying an overlay with the content as it is being viewed through a magnifying glass.

The overlay appears identical to the "official" webpages of the financial institution, and even the most experienced cybersecurity professional could be fooled. Unlike a browser-based attack, the overlay does not display the URL origin, so the user can't see that it may be malicious. When the user inserts the credentials, they are transmitted to the Ginp collection server for future use.

Ginp can also sue non-financial applications to trick the user into submitting sensitive information. For example, applications such as Google Play, also serve as a gateway for financial transactions, such as paying for applications, that also include payment information.

Recent versions of Ginp have the ability to spoof SMS messages to mimic familiar 2-factor authentication processes that send an authentication code via SMS. Ginp also gained the ability to block notifications to suppress security warnings from endpoint antivirus software that may be installed on the phone. This renders endpoint security solutions useless and allows Ginp to collect further information from social media notifications. This social media information is used to further customize attacks.



## Covid-19 Ginp Attack

**During Q2 2020, Allot Secure blocked approximately 1,000,000 instances of the Ginp malware in Spain.**

In its Covid-19 era attack, Ginp added two more features which make it even more dangerous. First, it implemented a remote access capability, which means the user's device can be spied upon in real-time, and even be controlled by the Ginp cybercriminals – including performing actions on the user's behalf without their knowledge.

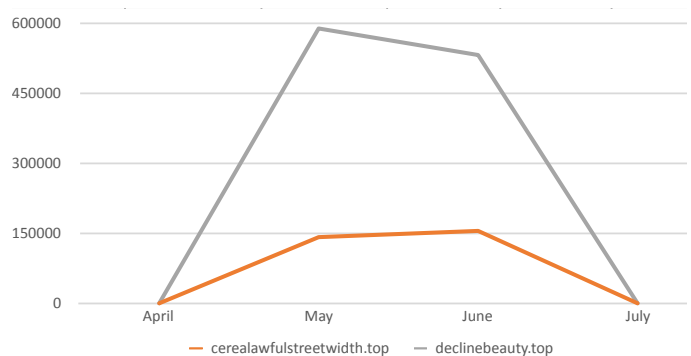
Ginp also implemented an "injection locker" ability, which can force the overlay screen to constantly appear, even after the user has inserted their credentials. This continuous display of unrequested content onscreen prevents the user from using their device, and Ginp's team can use this ability to extort the user for payment in exchange for "releasing" the screen, practically turning it into ransomware.

## Next Ginp Attack?

In mid-June 2020, IBM Trusteer claimed Ginp was responsible for close to 12% of malware infections in Android devices recorded in the 3 months prior to the publication of this data. At that time, the researchers discovered a recent version of the malware contained new fake overlays made to look like legitimate web pages of Turkish banks, therefore many in the cybersecurity community expect Ginp's next attack with target users in Turkey. So far it is unknown if such expansion was attempted and failed due to increased cybersecurity protection actions taken by Turkish entities, or that the Turkish expansion plan has not yet been activated by the malware originators. The next Ginp attack could strike anywhere.

As mentioned above, the latest Ginp attack in Spain lasted roughly two months, during May and June. During this time Allot Secure, together with Spanish service providers, blocked ~1,000,000 attempted Ginp infections.

Allot Secure Ginp Blocks





## Conclusion

### Protect Subscribers with Allot Secure

Allot Secure allows CSPs to protect their subscribers from all types of cyberthreats by offering security as a service (SECaaS) from the network. Up-to-date threat intelligence and in-line anti-virus scanning protects users from banking trojans like Ginp, and all types of malware, crypto jacking, ransomware, and IoT specific attacks such as Mirai and its variants.

Allot Secure unifies network-based security, home and business gateway security and security clients into the CSP's own branded security service. It delivers a seamless customer experience through a single interface for policy setting, reporting, and event handling.



To learn more about how service providers can increase customer satisfaction, NPS and ARPU by offering Allot Network Security Solutions, download the Telco Security Trends Report:

[\*\*How Effective are CSP Security Services for the Mass Market?\*\*](#)

or watch this video: [\*\*How Allot NetworkSecure Works.\*\*](#)