allot

See. Control. Secure.

Threat Bulletin

Banking trojans, crypto scams, and adware

March 2022

Just when you thought it was safe

In Q1 2022, the threat landscape continued to surprise us.

As usual, threats continued to rise. This past quarter, Communication Service Providers that use Allot Secure saw several interesting new threats. Let's take a look at some of what we saw.

Here are three things that we found:

- A rise and resurgence of banker trojans and other malware
- Cryptocurrency trading scams
- An explosion of adware

Just when you thought it was safe, threats that had previously been eliminated, with even the largest governments saying there is no need to worry, have since resurfaced.

Rise in banker trojans

Over the past few months, Allot researchers have identified an increase in banker trojans. A banker trojan is a malicious computer program designed to gain access to privileged information from an online banking system. Banker trojans aim to steal credentials to financial institutions.

Beating Bian

The Bian Banking Trojan was first discovered in 2019 and then went silent for a while. However, Allot security researchers have identified a rise in this trojan, with a resurgence in November 2021 and increasing since then. The Times of India even ranked this trojan as one of the 10 most dangerous mobile banking trojans of 2021.

Bian is difficult to detect because instead of placing an overlay when detecting a banking app, it obtains the banking credentials by recording the user's screen while avoiding direct communication with the C&C server. The criminals can decide when to retrieve the video with the banking information.

In addition to Bian, subscribers to CSPs using Allot Secure were also protected from other banking trojans.

Coper on the rise

Allot researchers identified several hundred thousand blocks of the Coper banking trojan. The Coper banking trojan was first discovered in Colombia, but it has spread to other parts of Latin America and has also been identified in Europe. Allot researchers identified thousands of cases among customers in Brazil. According to Dr. Web, Android.BankBot.Coper is spread by impersonating the official Bancolombia financial institution app using similar iconography and branding. Unsuspecting users than install the decoy app. Once the app is launched, the device is infected and, if permissions are granted, the app will then be able to take control of messages, install a keylogger, and much more.

The resurgence of Emotet

Allot researchers have also identified and blocked the Emotet malware. Emotet was described by EUROPOL, the European Union's law enforcement agency, as the world's most dangerous malware. They had announced that they disrupted the Emotet botnet in early January 2021.

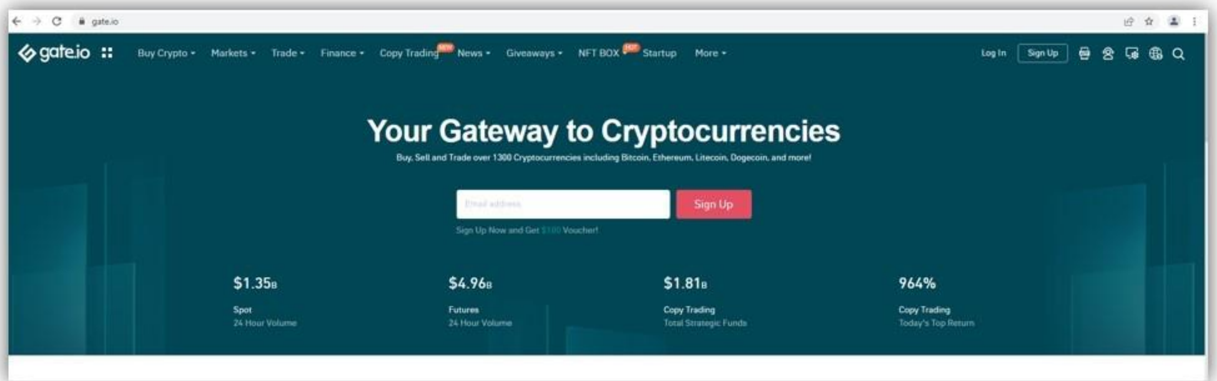
However, Allot researchers have recently identified a resurgence in Emotet. Beginning in late 2021, the botnet has seen a resurgence. Bleeping Computer previously reported that the Conti ransomware gang is behind their revival and the Emotet botnet started to slowly recreate itself in November, seeing far greater distribution via phishing campaigns beginning in January 2022. Researchers at Check

Point recently announced similar findings, noting that Emotet was the most prevalent malware in February 2022.

The fake cryptocurrency trading scam

Website spoofing is the act of creating a fake website to mislead visitors that the website is a different one. The website usually has a similar design as the real website.

For example, millions of subscribers of CSPs using Allot Secure were protected from website spoofing from a popular cryptocurrency trading site, Gate.io. According to Forbes Advisor, Gate.io “supports just about the biggest selection of crypto assets of any cryptocurrency exchange” and received 4.5 stars.



Your Gateway to Cryptocurrencies

Buy, Sell and Trade over 1300 Cryptocurrencies including Bitcoin, Ethereum, Litecoin, Dogecoin, and more!

Sign Up Now and Get $100 Voucher!

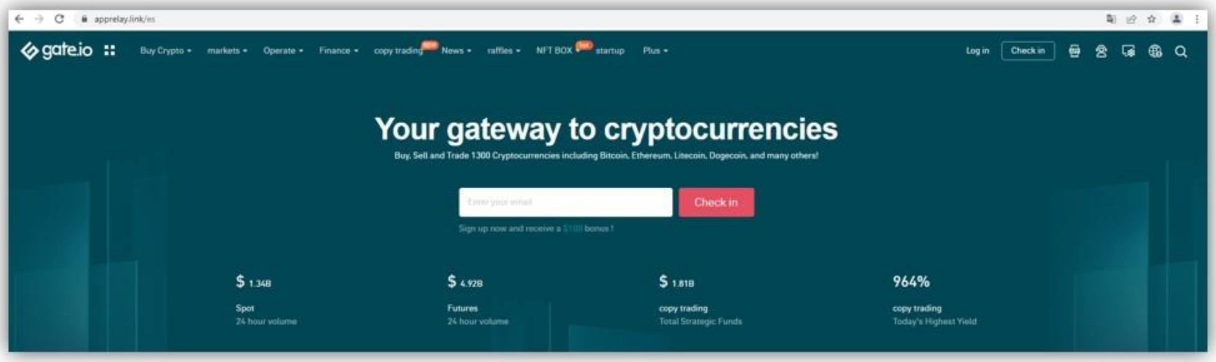
$1.35B Spot 24 Hour Volume

$4.96B Futures 24 Hour Volume

$1.81B Copy Trading Total Strategic Funds

964% Copy Trading Today's Top Return

The site’s popularity made it a target for a look-alike site so criminals can trick users into giving up their credentials.



Your gateway to cryptocurrencies

Buy, Sell and Trade 1300 Cryptocurrencies including Bitcoin, Ethereum, Litecoin, Dogecoin, and many others!

Sign up now and receive a $100 bonus !

$ 1.34B Spot 24 hour volume

$ 4.92B Futures 24 hour volume

$ 1.81B copy trading Total Strategic Funds

964% copy trading Today's Highest Yield

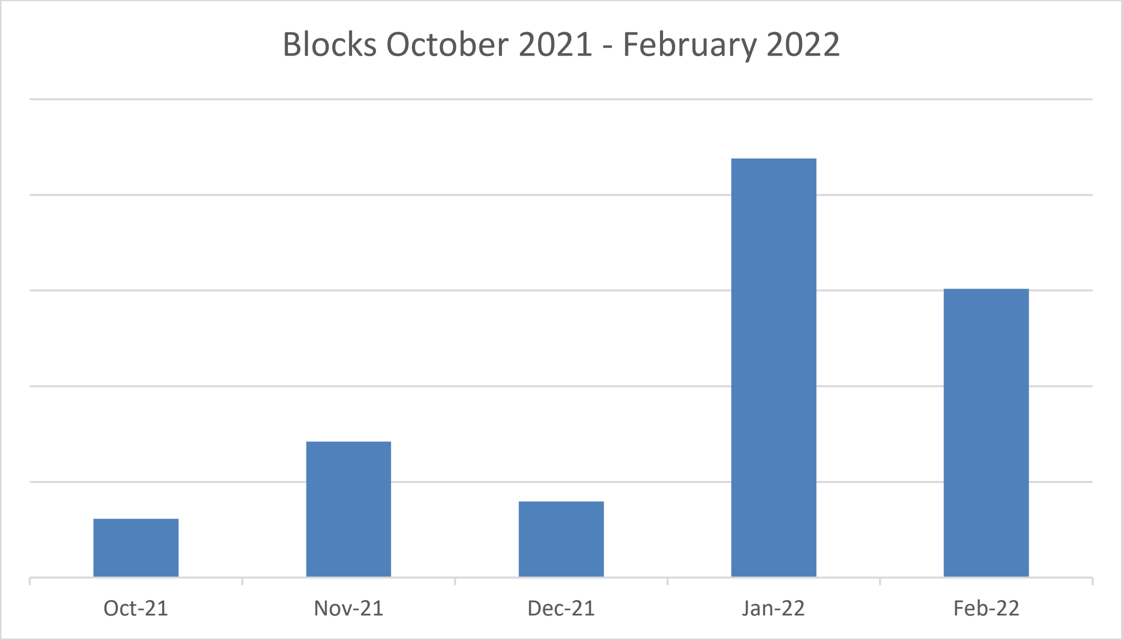
But that’s not all. During February, we saw other threats related to cryptocurrency scams, including thousands of blocks from sites that impersonate legitimate cryptocurrency sites, and will steal users’ money and crypto wallet credentials.

As the cryptocurrency market is growing and people see that as an investment opportunity, criminals don’t want to miss their chance. Crypto mining malware -- a malware attack that co-opts the target's computing resources to mine cryptocurrencies – is consistently increasing.

The explosion of adware

This past quarter also saw a rise in adware. In particular, we saw many cases of Fyben. Fyben is a type of adware, targets devices running the Android mobile operating system.

While Fyben is not a new threat, Allot security researchers identified that Fyben blocks increased 278% from November 2021 to January 2022 and, while dropping a little in February, remained high.



It is hard to know the origin of this increase but as it is related to gaming applications and December and January are months when multiple games are launched, cybercriminals could use this opportunity to takes those games and "inject" the malware on them. Therefore, people trying to download these games end on a third-party store downloading the malware instead of the original game that they wanted.

Keep your customers safe: Give them Allot Secure

There will always be new cyber threats and the old threats aren't going away. Keep your customers safe with Allot Secure.

Allot Secure is the leading Security as a Service solution for CSPs. It protects mobile devices, smart home appliances, connected business devices, and end-user devices – all with zero-touch. Provisioned and activated through the network, Allot Secure does not require any customer effort.

Besides providing peace of mind to CSP subscribers, offering Allot Secure to customers also enables CSPs to increase their ARPU, reduce customer churn, and stand out and differentiate themselves in a crowded market.

Want to learn more about Security as a Service?
We can assist.

Contact Allot.