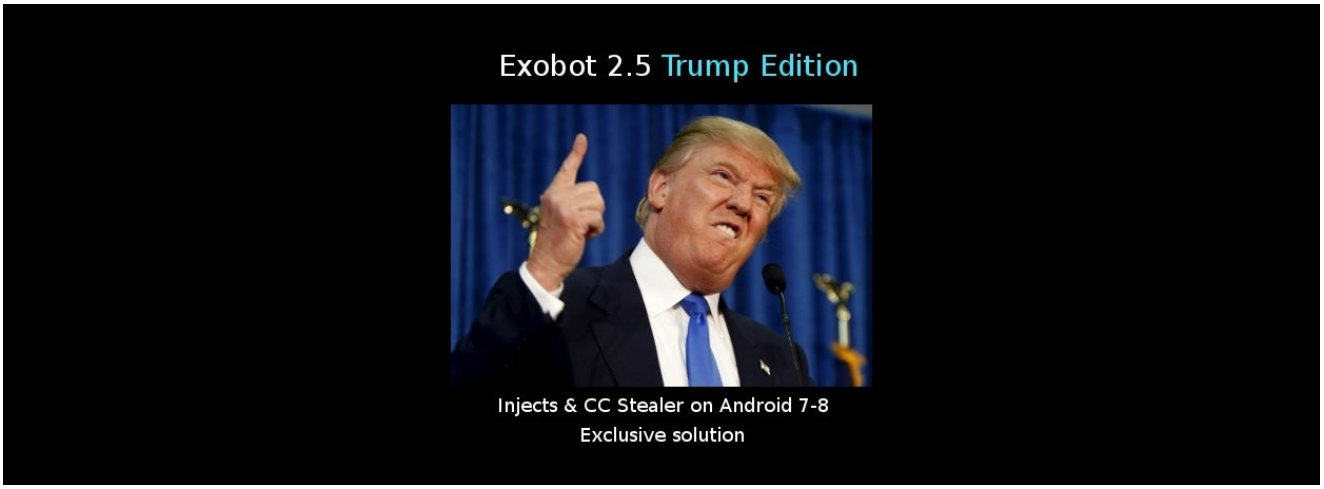
Source Code for Exobot Android Banking Trojan Leaked Online

bleepingcomputer.com/news/security/source-code-for-exobot-android-banking-trojan-leaked-online/

Catalin Cimpanu

By
Catalin Cimpanu

- July 23, 2018
- 12:15 AM
- 1



The source code of a top-of-the-line Android banking trojan has been leaked online and has since rapidly spread in the malware community, worrying researchers that a new wave of malware campaigns may be in the works.

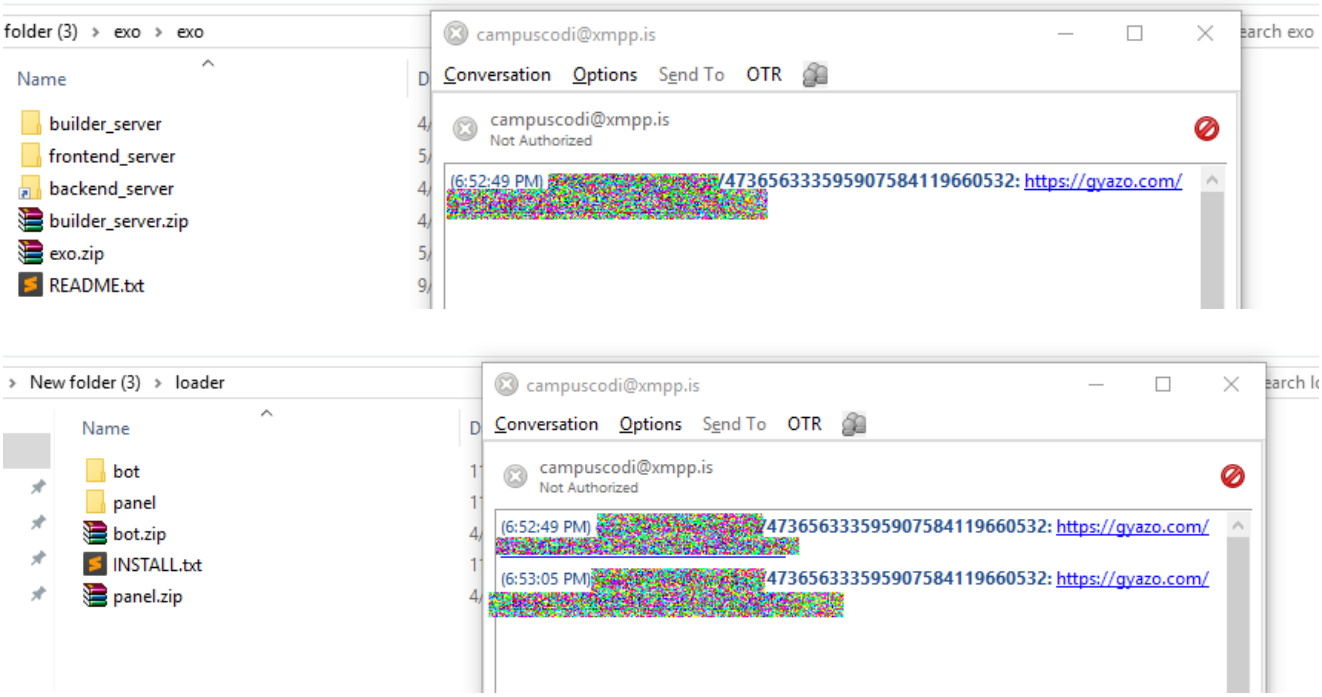
This malware's name is Exobot, an Android banking trojan that was first spotted at the end of 2016, and which its authors mysteriously abandoned by putting its source code for sale in January this year.

In day to day operations, malware authors sell monthly or weekly access to their malware in what security researchers call MaaS (Malware-as-a-Service) or CaaS (Cybercrime-as-a-Service).

But when a malware author sells the malware's entire source code, this usually means the malware author is moving to something else and doesn't want to work on it anymore. Usually, that source code leaks online after enough people buy it.

Exobot source code leaked online in May

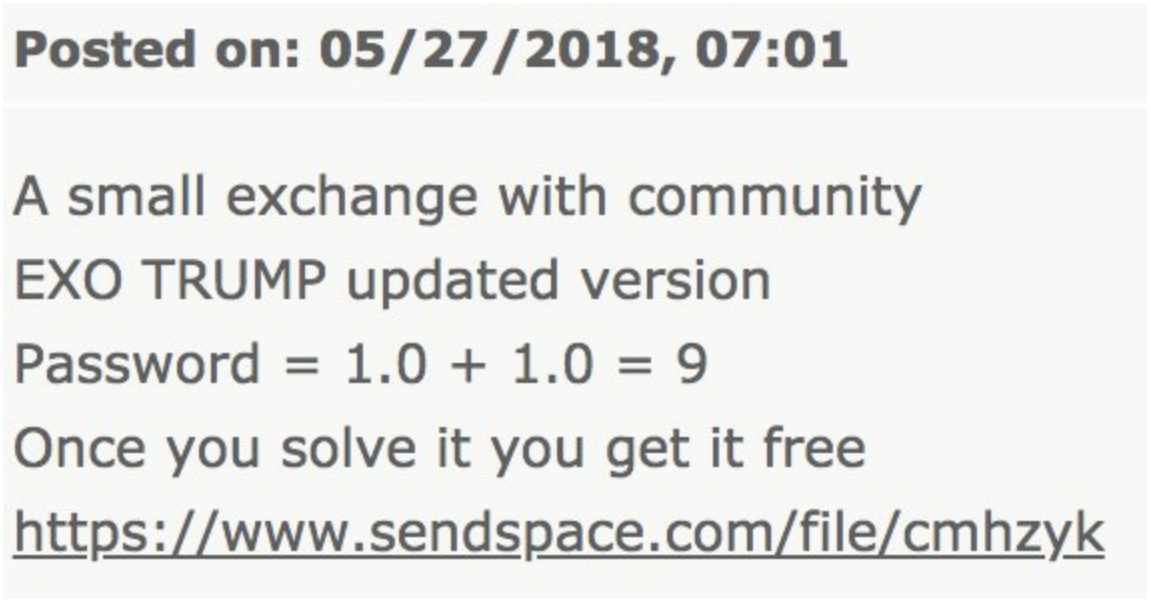
This happened many times in the past with all sorts of malware strains, and it also happened to Exobot, as last month, Bleeping Computer received a copy of this source code from an unknown individual.



Bleeping Computer has shared this source code and verified its authenticity with security researchers from ESET and ThreatFabric.

The code proved to be version 2.5 of the Exobot banking trojan, also known as the "Trump Edition," one of Exobot's last version before its original author gave up on its development.

Security researchers from ThreatFabric have told Bleeping Computer that the Exobot trojan source code we received had actually leaked online in May when one of the users who bought it from the original author decided to share it with the community.



Since then, Bleeping Computer has discovered that the Exobot source code is now being distributed on quite a few underground hacking forums.

Security researchers fear rise in Exobot campaigns

Security researchers are now afraid that the code's proliferation may lead to a surge in malware campaigns that will push malicious Android apps infected with this trojan.

But these aren't just warnings from "fearmongering" security researchers. Something like this has happened before.

In December 2016, the source code of the BankBot Android banking trojan leaked online, and it led to a massive outburst of malware campaigns pushing the trojan in 2017.

The BankBot code's availability lowered the entry barrier and financial costs for wannabe malware authors to enter the Android malware scene. Now, with Exobot being shared in the same way, security researchers are bracing for a similar surge of campaigns.

Exobot is very powerful

Cengiz Han Sahin, security researcher and spokesperson with ThreatFabric, says that Exobot is a pretty potent banking trojan, capable of infecting even smartphones running the latest Android versions, something that very few trojans can do.

"All threat actors have been working on timing injects (overlay attacks) to work on Android 7, 8, and even 9," Sahin says. "However Exobot really is something new.

"The trojan gets the package name of the foreground app without requiring any additional permissions," he says, "This is a bit buggy, still, but works in most cases."

"The interesting part here is that no Android permissions are required," Sahin adds. "All other Android banking trojans families are using the Accessibility ore Use Stats permissions to achieve the same goal and therefore require user interaction with the victim."

So not only is Exobot's source code freely accessible, but its also of pretty effective, just like the BankBot code was top-of-the-line when it was leaked in 2016. In the coming months, we may see Android malware devs slowly migrating their campaigns from BankBot to Exobot, as few will decline a "free upgrade" to a better code.

Related Articles:

Top 10 Android banking trojans target apps with 1 billion downloads

Mobile trojan detections rise as malware distribution level declines

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

SMSFactory Android malware sneakily subscribes to premium services

FluBot Android malware operation shutdown by law enforcement

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.