

# Octo2: European Banks Already Under Attack by New Malware Variant

[threatfabric.com/blogs/octo2-european-banks-already-under-attack-by-new-malware-variant](https://threatfabric.com/blogs/octo2-european-banks-already-under-attack-by-new-malware-variant)



## Jump to

Octo (ExobotCompact) is a notable malware family on the current mobile threat landscape. It dominates the tables of the number of unique samples observed by ThreatFabric in the current year.

In light of this, the discovery of a new version, named “Octo2” by its creator, could potentially shift the threat landscape and the Modus Operandi of the actors behind it. This report uncovers details about the current state of the malware family, highlights updates, and makes predictions for the future of the Octo (ExobotCompact) malware family.

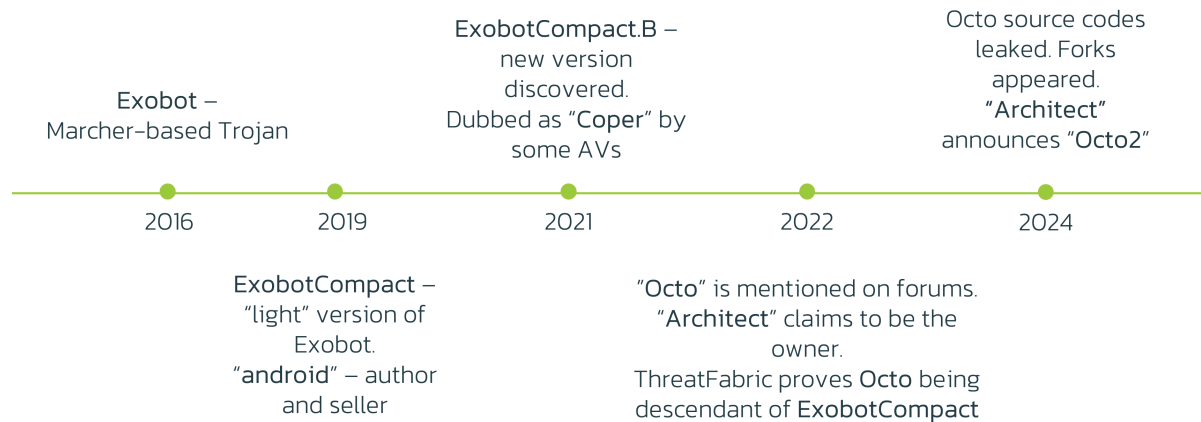
Key takeaways of the discovery:

- A new variant (named **Octo2**) of Octo, currently the most widespread malware family, has been released by the original threat actor
- The malware developers took action to increase the stability of the remote action capabilities needed for Device Takeover attacks
- New Octo2 campaigns have been spotted in European countries
- Octo2 contains sophisticated obfuscation techniques to ensure the Trojan stays undetected, including the introduction of Domain Generation Algorithm (DGA)

## From Exobot to Octo2: A Brief History of the Family

# ExobotCompact = Octo: history

Well-known player on the threat landscape



The first samples of the Exobot malware family were seen in 2016. At that time, it was a banking trojan capable of performing overlay attacks and controlling calls, SMS, and push notifications.

In 2019, a new version of Exobot called “ExobotCompact”, was promoted on underground forums as a lightweight version retaining most of the features of its predecessor.

After a break, in 2021 a new variant of ExobotCompact was discovered. Some AV vendors dubbed it “Coper”; however, ThreatFabric analysts were able to track and prove the connection with the original ExobotCompact. Furthermore, in 2022 the first mentions of a mysterious mobile malware family “Octo” appeared on underground forums. An actor with the nickname “Architect” claimed to be the owner of Octo, but showed little activity on the forums, providing only a few details about the malware itself. ThreatFabric was able to “connect the dots” and, based on the limited information shared by the owner, proved that Octo is a new name for ExobotCompact.

Since 2022, our Mobile Threat Intelligence team has observed increasing activity from Octo and its operators. More campaigns have been spotted in the wild, and more actors have gained access to this malware family, attracted by its extensive capabilities, including continuously updated remote access features.

In 2024, several notable events affected the mobile threat landscape, some related to Octo. First, **the source code of Octo was leaked**, resulting in multiple forks launched by other threat actors. The leak of the source codes was likely one of the main reasons behind the second notable event in the story of Octo: a new version, Octo2, was released by the original threat actor.

## Targeting European Countries - and More in the Future

For the past years of monitoring the activity of Octo, ThreatFabric has observed campaigns of previous variants in multiple regions all over the world. The “customers” of Octo Malware-as-a-Service were seen running campaigns targeting Europe, the USA, Canada, the Middle East, Singapore, and Australia.











When promoting the update, the owner of Octo announced that Octo2 will be available for users of Octo1 at the same price with early access. We can expect that the actors that were operating Octo1 will switch to Octo2, thus bringing it to the global threat landscape.

Our research showed that Octo2’s settings contain traces of multiple applications and apps being on the radar of the actors. This conclusion is based on the list of package names received from the C2 as a part of the initial setup as “**block\_push\_apps**” setting. It means that once Octo2 detects a push notification from one of the apps on the list, it will

intercept it and not show it to the victim. The presence of the app on the list means that it is of interest to cybercriminals, and they are already preparing to attack its users. This is likely a default setting prepared by the developers.

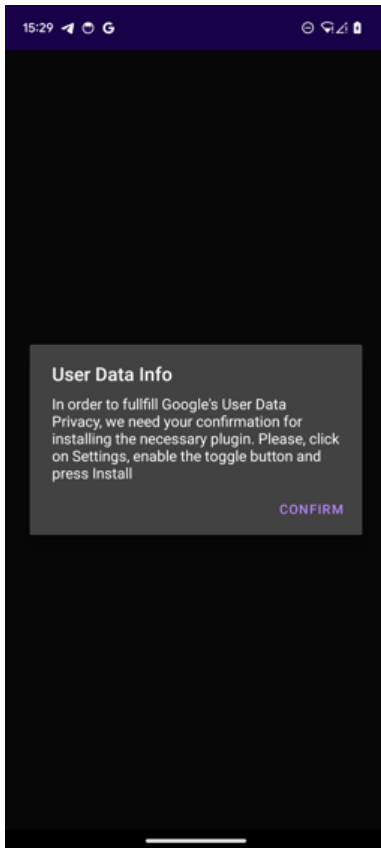
Our Threat Intelligence shows that the first samples of Octo2 discovered in the wild were seen in **Italy, Poland, Moldova,** and Hungary. These samples from the first campaigns observed were masquerading as **Google Chrome, NordVPN,** and **“Enterprise Europe Network”** applications. However, as we said previously, we can expect threat actors behind Octo2 to not limit their activity and continue targeting users of mobile banking all over the world.

## Octo2 campaigns

Icon / App name / Package name	Icon / App name / Package name
 NordVPN (com.handedfastee5) 83eea636c3f04ff1b46963688eb4bac7177e77bbc40b0d3426f5cf66a0c647ae	 Google Chrome (com.eimoverbroadcast64) c44a4a35a693037e4a2da1ff9896c9bed00dee87261b8f3334d22b3d87cfe40
 NordVPN (com.eui_connectivity3) 9256906d7dac7c2ebb9f7d5ce3a81505392e1364fb4061d011053a7e1967c3	 Google Chrome (com.adapters_gesturalaf8) 80592121882b2213e44149d3fd155c0ee9565bbc85a3a3f62db0c07693a6c1be
 NordVPN (com.handedfastee5) da37ef5fc9e3fbfe8e54fb0d52825b049795428490a276644a3b6b5e77be2d69	 Google Chrome (com.makatwatch89) fb56fce6a6e5a24d46d830e3b2df8e87e76d76e805d704436396452b78441545
 NordVPN (com.nfont_systemh) 4fb5c7cafc9eea1117fe8fe285e92789fc68d1b91c36b2ebaa73e4db32985fd	 Google Chrome (com.pipservice2_supervision) ebf146781a6b0d52c18ff72957eee3f5116c005111716596452654a75fefa11b
 Europe Enterprise (com.xsub_restore3) 6cd0fbfb088a95b239e42d139e27354abe08c6788b6083962943522a870cb98	 Google Chrome (com.handed_calculatorj7) dc3e3b541d210e0fe4122f4db10e3922ed6479cb7c12384ebc4c4a419c7ea5ca



In the Octo2 campaigns that were spotted by ThreatFabric, we observed Zombinder serving as the first stage of the installation: upon launch, Zombinder will request the installation of an additional “plugin” which is, in fact, Octo2, thus successfully bypassing Android 13+ restrictions.



*Zombinder lured the victim into allowing the installation of Octo2*

## New Features and Improvements

---

Malware developers and actors who sell their malware as a service have the same challenge as legitimate software businesses: how to differentiate their "product" from their competitors' offerings? In the case of Octo, conscious of the source code leakage, the competition is even more challenging - improve your own "product" to make it more popular than the previous version, which has now involuntarily become a competitor with a price point of zero!

It's therefore no surprise that Octo2 received several significant updates compared to previous variants. Most of the changes are focused on increasing the stability of remote control sessions while performing Device Takeover attacks, and improving **anti-detection and anti-analysis techniques**. Improvements include:

- **Increased RAT stability.**

The developers of Octo2 updated the RAT capabilities of the malware to increase the stability and decrease connection latency during remote sessions. They introduced a specific remote session setting "**SHIT\_QUALITY**" (sic) that can be specified by an operator to decrease the amount of data transmitted over the internet to C2 and thus increase the stability of the connection even on networks with a poor connection. If set, this setting will trigger Octo2 to decrease the quality of the screenshots sent to the C2 by encoding each pixel with half the usual number of bytes, capturing the image in gray tones, and decreasing the quality when converting to JPEG.

- **Improved anti-analysis and anti-detection techniques**

Octo was always known for its sophisticated and advanced anti-analysis and anti-detection techniques. As reported in our [previous blog on Octo](#), the main payload was decrypted with the use of native code, which poses challenges for manual and automated analysis, and, consequently, makes malware detection more challenging. In Octo2, the developers implemented an even more sophisticated process of malicious code obfuscation when compared to previous variants. The execution process consists of several steps, including decrypting and dynamically loading an additional native library, which is responsible for decrypting the malicious payload, generating encryption keys, and C2 domain names.

- **Communication with C2 and Domain Generation Algorithm (DGA)**

In the latest versions, Octo2 utilises a Domain Generation Algorithm (DGA) to generate the actual C2 server name. This technique allows cybercriminals to update the domain names on the fly without a need to regenerate the samples (as well as easily setting up new servers with new names after the known ones are taken down). A known limitation of DGAs is that, once the algorithm is known, researchers and AV vendors can easily predict all future domains that will be generated by cybercriminals and proactively block them. Nevertheless, the Octo2 authors decided to use this approach and came up with a proprietary date-based algorithm.

The key derivation for encrypting the data sent to the C2 was also updated: instead of a static hardcoded key, the malware generates a new key for every request to the C2. The cryptographic "Salt" is shared as a part of the request so the C2 server can derive the same key on its side to decrypt the data.

The emergence of the Octo2 variant signals future challenges for mobile banking security, as its enhanced capabilities and wider usage pose significant risks. With the original Octo malware's source code already leaked and easily accessible to various threat actors, Octo2 builds on this foundation with even more robust remote access capabilities and sophisticated obfuscation techniques. This makes it harder for security systems to detect and remove it, increasing the malware's longevity and potential impact.

## Conclusion

---

The emergence of this Octo2 variant represents a significant evolution in mobile malware, particularly in the context of banking security. With enhanced remote access functionality, sophisticated obfuscation methods, and the wide availability of its predecessor's source code, Octo2 is poised to remain a dominant force in the mobile malware landscape together with its older variants based on the leaked source code. This variant's ability to invisibly perform on-device fraud and intercept sensitive data, coupled with the ease with which it can be customised by different threat actors, raises the stakes for mobile banking users globally. As this threat continues to evolve, both users and financial institutions must remain proactive, adopting stringent security measures and continuously updating defenses to mitigate the increased risk.

## Appendix

---

### Indicators of compromise

---

Hash (SHA256)	app name	package name
83eea636c3f04ff1b46963680eb4bac7177e77bbc40b0d3426f5cf66a0c647ae	NordVPN	com.handedfastee5
6cd0fbfb088a95b239e42d139e27354abeb08c6788b6083962943522a870cb98	Europe Enterprise	com.xsusb_restore3
117aa133d19ea84a4de87128f16384ae0477f3ee9dd3e43037e102d7039c79d9	Google Chrome	com.havirtual06numberresources