

Octopus Prime: it didn't turn into a truck, but a widely spread Android botnet

 virusbulletin.com/conference/vb2024/abstracts/octopus-prime-didnt-turn-truck-widely-spread-android-botnet/

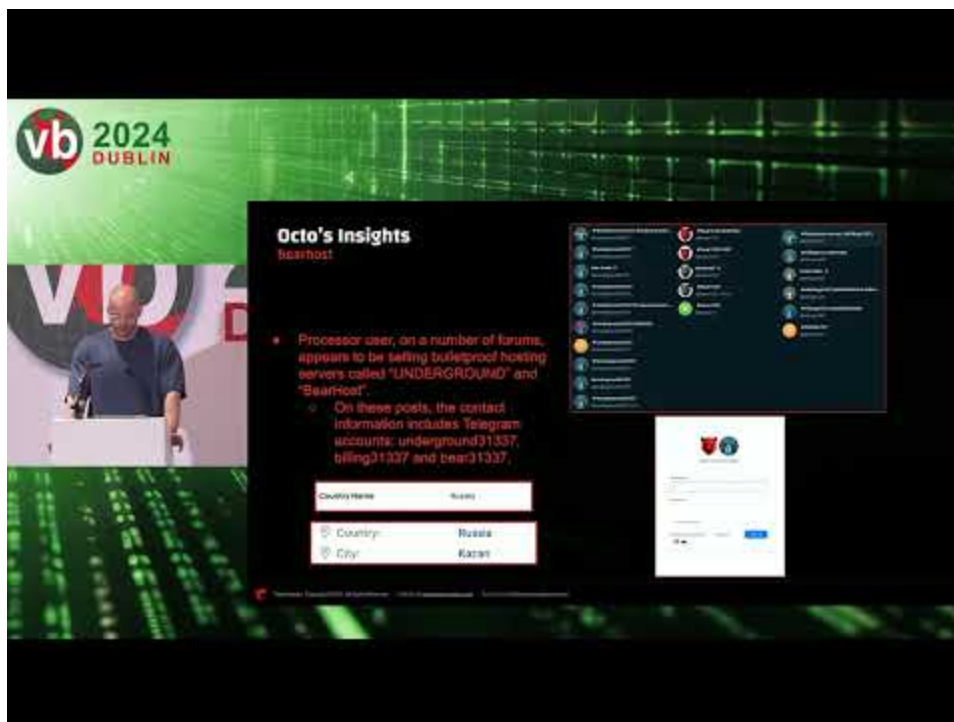
Friday 4 October 09:30 - 10:00, Red room

Thibault Seret (Team Cymru)

Coper/Octo is offered as a malware-as-a-service, where customers are provided access to a panel and builder used to coordinate and execute malware campaigns. As a result, we observe Coper/Octo being used to target many countries across the globe in campaigns crafted to 'appeal' to specific audiences.

In this presentation, we will introduce and show Octo behind the scenes: analysis of the builder, the infrastructure involved in its operation, the spreading methodologies, and the undocumented mechanisms the malware and its developer are bringing in this MaaS package.

We'll also discuss statistics on how this malware is impacting our world, professionals, and the man in the street.



[Watch Video At:](#)

https://youtu.be/H8y9d_Xkc1s

[Download paper for this talk](#)

Thibault Seret

Thibault Seret is a researcher on the Team Cymru Research Team. He is currently focusing on crimeware and APT analysis and research, reverse engineering and threat intelligence, and trying to fight against bad guys. Before joining Team Cymru, he worked as a threat researcher in McAfee's ATR team, as a cybercrime analyst in a banking institution with the mission to improve the digital forensics department, and as a CERT analyst at an IT services company where he tried to save the world with his teammate. He participates a lot in the security community and CTF competitions and is a teacher for the new generation of cyber defenders. For the Alliance!

 [@Glacijs_](https://twitter.com/Glacijs_)