VB2020: Anchor, Bazar, and the Trickbot Connection

By Cybereason Nocturnus

Archived: 2026-04-05 22:25:17 UTC

VB2020, the annual Virus Bulletin international conference "featuring the latest and best research on malware, malicious actors and threat intelligence," has gone virtual this year and will be live-streamed 30 Sept - 2 Oct, 2020. The conference is free of charge, and offers a wide selection of presentations for on-demand viewing in addition to the live sessions.

Cybereason Nocturnus Team members Daniel Frank and Lior Rochberger will be presenting a session titled, *Anchor, Bazar, and the Trickbot Connection*, examining some new developments regarding a familiar threat actor.

The Session

In March, a new loader emerged that lures its victims with double extension executables, pretending to be legitimate PDF and DOC files downloaded from Google Drive. Sound familiar? That's right, the Trickbot gang is back with a couple of new tricks up its sleeve after dropping the Anchor malware in late 2019.

In their presentation, the researchers will dive into the Trickbot gang's arsenal, focusing on the efforts made into developing two of their latter malware variants, Anchor and Bazar Loader, which emerged in 2020.

First, they will go over the Trickbot gang timeline from when they became famous in 2016 through to today, briefly reviewing their go-to tools. Next, they will review Anchor and Bazar Loader and present the development cycles and just how much the authors invested in advanced obfuscation and evasion techniques. They will show how the threat actors were determined to hinder their analysis, improving that aspect of their code from one development cycle to another.

Finally, they will dive into some of the more interesting similarities among the different malware variants presented and how these similarities point us to the conclusion that these popular malware variants were all developed by the notorious Trickbot gang.

Presenters

Daniel Frank, Senior Malware Researcher, Cybereason

With a decade in malware research, Daniel uses his expertise with malware analysis and reverse engineering to understand APT activity and commodity cybercrime attackers. Daniel has previously shared research at RSA Conference, the Microsoft Digital Crimes Consortium, and Rootcon.

Lior Rochberger, Senior Threat Researcher and Threat Hunter, cybereason

As part of the Nocturnus team at Cybereason, Lior has created procedures to lead threat hunting, reverse engineering and malware analysis teams. Lior has also been a contributing researcher to multiple threat and malware blogs including Bitbucket, Valak, Ramnit, and Racoon stealer. Prior to Cybereason, Lior led SOC operations within the Israeli Air Force.

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus
