Authorities Ramp Up Efforts to Capture the Mastermind Behind Emotet

By The Hacker News

Published: 2024-06-03 · Archived: 2026-04-06 02:11:56 UTC

Law enforcement authorities behind Operation Endgame are seeking information related to an individual who goes by the name Odd and is allegedly the mastermind behind the Emotet malware.

Odd is also said to go by the nicknames Aron, C700, Cbd748, Ivanov Odd, Mors, Morse, and Veron over the past few years, according to a video released by the agencies.

"Who is he working with? What is his current product?," the video continues, suggesting that he is likely not acting alone and may be collaborating with others on malware other than Emotet.

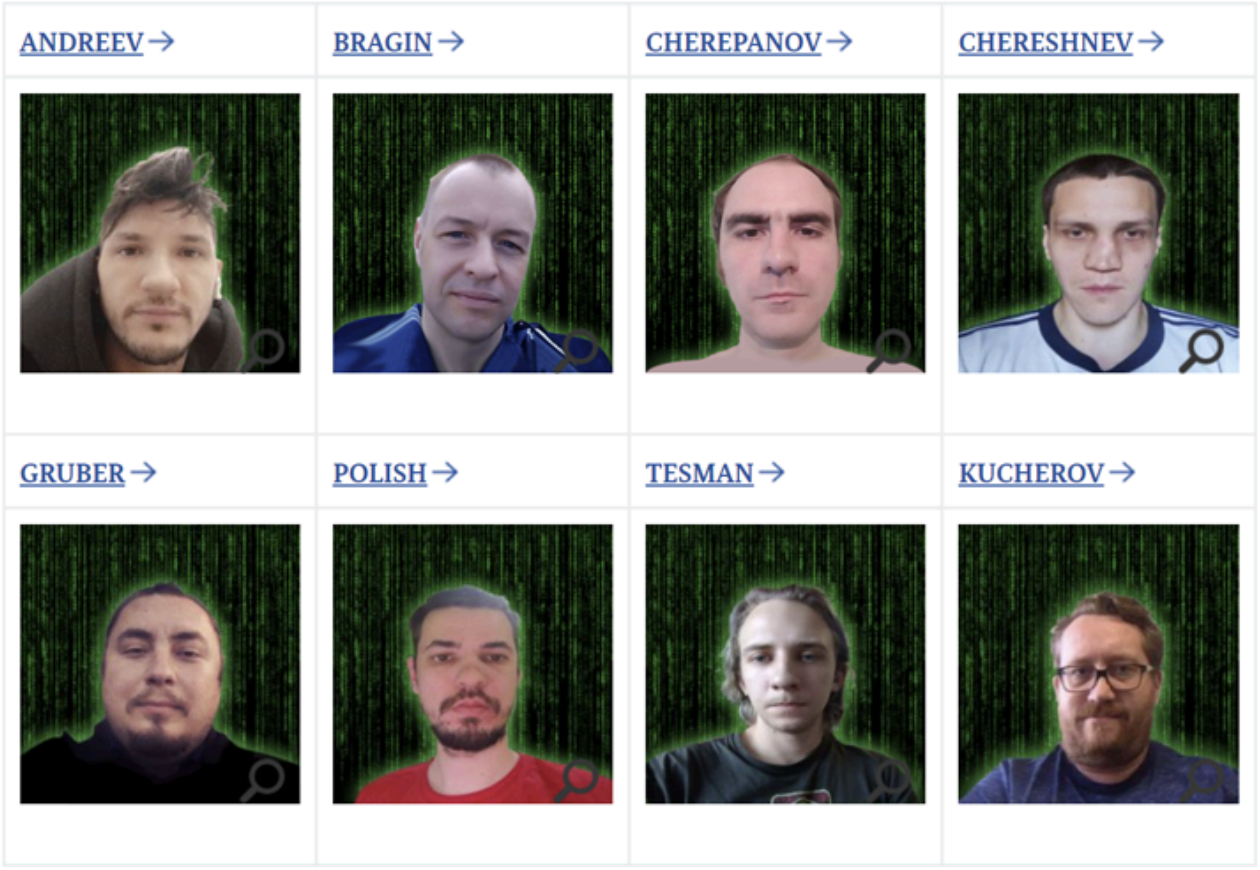
The threat actor(s) behind Emotet has been tracked by the cybersecurity community under the monikers Gold Crestwood, Mealybug, Mummy Spider, and TA542.

Originally conceived as a banking trojan, it evolved into a broader-purpose tool capable of delivering other payloads, along the lines of malware such as TrickBot, IcedID, QakBot, and others. It re-emerged in late 2021, albeit as part of low-volume campaigns, following a law enforcement operation that shutdown its infrastructure.

As recently as March 2023, attack chains distributing an updated version of the malware were found to leverage Microsoft OneNote email attachments in an attempt to bypass security restrictions. No new Emotet-related activity has been observed in the wild since the start of April 2023.

The call follows a sweeping coordination effort that saw four arrests and over 100 servers associated with malware loader operations such as IcedID, SystemBC, PikaBot, SmokeLoader, Bumblebee, and TrickBot taken down in an effort to stamp out the initial access broker (IAB) ecosystem that feeds ransomware attacks.

Germany's Federal Criminal Police Office (aka the Bundeskriminalamt) has also revealed the identities of eight cyber criminals who are believed to have played crucial roles in the SmokeLoader (aka Dofoil and Smoke) and TrickBot malware operations. They have all since been added to the E.U. Most Wanted List.



"All these malicious services were in the arsenal of such Russian cybercrime organizations as BlackBasta, Revil, Conti and helped them attack dozens of Western companies, including medical institutions," the National Police of Ukraine (NPU) said in a statement.

Cyber attacks involving the malware families have relied on compromised accounts to target victims and propagate malicious emails, with the botnet operators using stolen credentials obtained using remote access trojans (RATs) and information stealers to gain initial access into networks and organizations.

Data shared by Swiss cybersecurity firm PRODAFT with The Hacker News in the wake of the operation shows that criminal actors on underground forums like XSS.IS are on alert, with the moderator – codenamed bratva – urging others to be careful and check if their virtual private servers (VPSes) went down between May 27 and 29, 2024.

Bratva has also been found sharing the names of the eight people that the Bundeskriminalamt revealed, while noting that Operation Endgame is one of the "far-going consequences of leaked Conti [ransomware] logs."

Other actors took to the forum to wonder out loud as to who might have leaked the chats and raised the possibility of a "rat" who is working with law enforcement. They also claimed that Romania and Switzerland would not share data about criminal actors residing within their borders unless it's an "extreme threat" like terrorism.

"[The] FBI can raid anything under saying its [sic] 'terrorism," one user who goes by the alias phant0m said.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2024/06/authorities-ramp-up-efforts-to-capture.html