Oops: DanaBot Malware Devs Infected Their Own PCs

Published: 2025-05-23 · Archived: 2026-04-05 19:02:28 UTC

The U.S. government today unsealed criminal charges against 16 individuals accused of operating and selling **DanaBot**, a prolific strain of information-stealing malware that has been sold on Russian cybercrime forums since 2018. The **FBI** says a newer version of DanaBot was used for espionage, and that many of the defendants exposed their real-life identities after accidentally infecting their own systems with the malware.

DanaBot's features, as promoted on its support site. Image: welivesecurity.com.

Initially spotted in May 2018 by researchers at the email security firm **Proofpoint**, DanaBot is a malware-as-a-service platform that specializes in credential theft and banking fraud.

Today, the **U.S. Department of Justice** unsealed a criminal complaint and indictment from 2022, which said the FBI identified at least 40 affiliates who were paying between $3,000 and $4,000 a month for access to the

information stealer platform.

The government says the malware infected more than 300,000 systems globally, causing estimated losses of more than $50 million. The ringleaders of the DanaBot conspiracy are named as **Aleksandr Stepanov**, 39, a.k.a. "**JimmBee**," and **Artem Aleksandrovich Kalinkin**, 34, a.k.a. "**Onix**", both of Novosibirsk, Russia. Kalinkin is an IT engineer for the Russian state-owned energy giant **Gazprom**. His Facebook profile name is "Maffiozi."

According to the FBI, there were at least two major versions of DanaBot; the first was sold between 2018 and June 2020, when the malware stopped being offered on Russian cybercrime forums. The government alleges that the second version of DanaBot — emerging in January 2021 — was provided to co-conspirators for use in targeting military, diplomatic and non-governmental organization computers in several countries, including the United States, Belarus, the United Kingdom, Germany, and Russia.

"Unindicted co-conspirators would use the Espionage Variant to compromise computers around the world and steal sensitive diplomatic communications, credentials, and other data from these targeted victims," reads a grand jury indictment dated Sept. 20, 2022. "This stolen data included financial transactions by diplomatic staff, correspondence concerning day-to-day diplomatic activity, as well as summaries of a particular country's interactions with the United States."

The indictment says the FBI in 2022 seized servers used by the DanaBot authors to control their malware, as well as the servers that stored stolen victim data. The government said the server data also show numerous instances in which the DanaBot defendants infected their own PCs, resulting in their credential data being uploaded to stolen data repositories that were seized by the feds.

"In some cases, such self-infections appeared to be deliberately done in order to test, analyze, or improve the malware," the criminal complaint reads. "In other cases, the infections seemed to be inadvertent – one of the hazards of committing cybercrime is that criminals will sometimes infect themselves with their own malware by mistake."

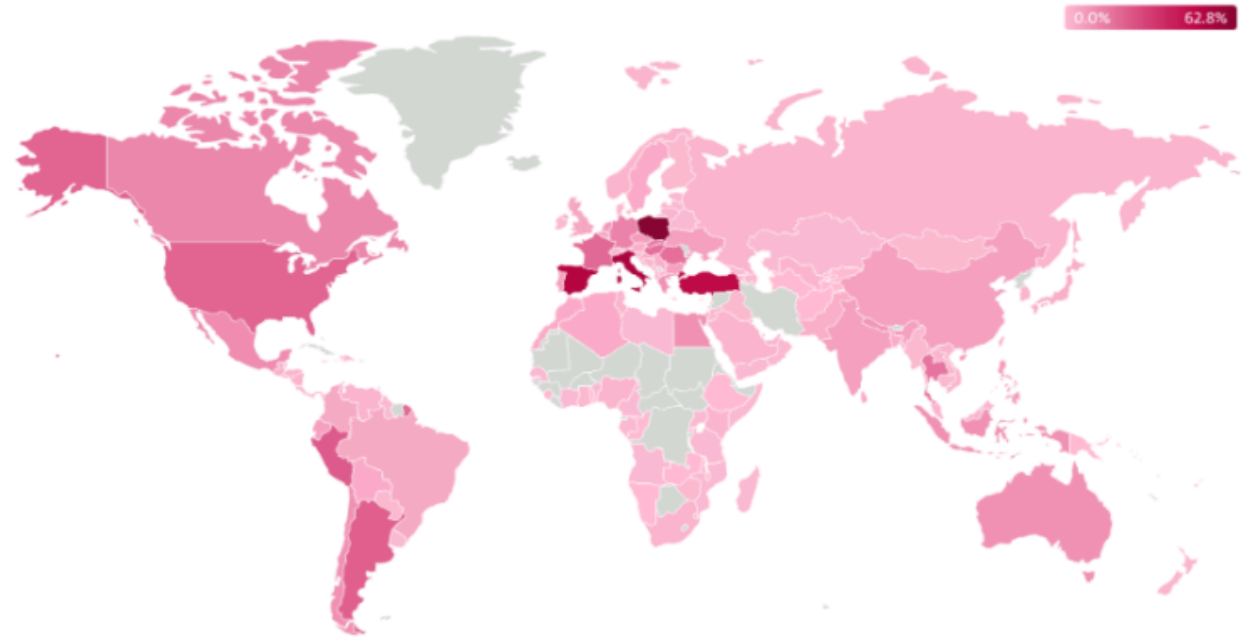

Figure 1. Worldwide Danabot detections as seen in ESET telemetry since 2018

Image: welivesecurity.com

A statement from the DOJ says that as part of today's operation, agents with the **Defense Criminal Investigative Service** (DCIS) seized the DanaBot control servers, including dozens of virtual servers hosted in the United States. The government says it is now working with industry partners to notify DanaBot victims and help remediate infections. The statement credits a number of security firms with providing assistance to the government, including **ESET**, **Flashpoint**, **Google**, **Intel 471**, **Lumen**, **PayPal**, **Proofpoint**, **Team CYMRU**, and **ZScaler**.

It's not unheard of for financially-oriented malicious software to be repurposed for espionage. A variant of the **ZeuS Trojan**, which was used in countless online banking attacks against companies in the United States and Europe between 2007 and at least 2015, was for a time diverted to espionage tasks by its author.

As detailed in this 2015 story, the author of the ZeuS trojan created a custom version of the malware to serve purely as a spying machine, which scoured infected systems in Ukraine for specific keywords in emails and documents that would likely only be found in classified documents.

The public charging of the 16 DanaBot defendants comes a day after **Microsoft** joined a slew of tech companies in disrupting the IT infrastructure for another malware-as-a-service offering — Lumma Stealer, which is likewise offered to affiliates under tiered subscription prices ranging from $250 to $1,000 per month. Separately, Microsoft filed a civil lawsuit to seize control over 2,300 domain names used by Lumma Stealer and its affiliates.

Further reading:

Danabot: Analyzing a Fallen Empire

ZScaler blog: DanaBot Launches DDoS Attack Against the Ukrainian Ministry of Defense

Flashpoint: Operation Endgame DanaBot Malware

Team CYMRU: Inside DanaBot's Infrastructure: In Support of Operation Endgame II

March 2022 criminal complaint v. Artem Aleksandrovich Kalinkin

September 2022 grand jury indictment naming the 16 defendants

---