ESET participates in operation to disrupt the infrastructure of Danabot infostealer

DUBAI , DUBAI, UNITED ARAB EMIRATES, May 27, 2025 /EINPresswire.com/ -- ESET has participated in a major infrastructure disruption of the notorious infostealer, Danabot, by the US Department of Justice, the FBI, and US Department of Defense's Defense Criminal Investigative Service. U.S. agencies were working closely with Germany's Bundeskriminalamt, the Netherlands' National Police, and the Australian Federal Police . ESET took part in the effort alongside Amazon, CrowdStrike, Flashpoint, Google, Intel471, PayPal, Proofpoint, Team Cymru and Zscaler. ESET Research, which has been tracking Danabot since 2018, contributed assistance that included providing technical analysis of the malware and its backend infrastructure, as well as identifying Danabot's C&C servers. During that period, ESET analyzed various Danabot campaigns all over the world, with Poland, Italy, Spain and Turkey historically being one of the most targeted countries. The joint takedown effort also led to the identification of individuals responsible for Danabot development, sales, administration, and more.

These law enforcement operations were conducted under Operation Endgame — an ongoing global initiative aimed at identifying, dismantling, and prosecuting cybercriminal networks. Coordinated by Europol and Eurojust, the operation successfully took down critical infrastructure used to deploy ransomware through malicious software.

"Since Danabot has been largely disrupted, we are using this opportunity to share our insights into the workings of this malware-as-a-service operation, covering the features used in the latest versions of the malware, the authors' business model, and an overview of the toolset offered to affiliates. Apart from exfiltrating sensitive data, we have observed that Danabot is also used to deliver further malware, which can include ransomware, to an already compromised system," says ESET researcher Tomáš Procházka, who investigated Danabot.

The authors of Danabot operate as a single group, offering their tool for rental to potential

affiliates, who subsequently employ it for their malicious purposes by establishing and managing their own botnets. Danabot's authors have developed a vast variety of features to assist customers with their malevolent motives. The most prominent features offered by Danabot include: the ability to steal various data from browsers, mail clients, FTP clients, and other popular software; keylogging and screen recording; real-time remote control of the victims' systems; file grabbing (commonly used for stealing cryptocurrency wallets); support for Zeus-like webinjects and form grabbing; and arbitrary payload upload and execution. Besides utilizing its stealing capabilities, ESET Research has observed a variety of payloads being distributed via Danabot over the years. Furthermore, ESET has encountered instances of Danabot being used to download ransomware onto already compromised systems.

In addition to typical cybercrime, Danabot has also been used in less conventional activities such as utilizing compromised machines for launching DDoS attacks… for example, a DDoS attack against Ukraine's Ministry of Defense soon after the Russian invasion of Ukraine.

Throughout its existence, according to ESET monitoring, Danabot has been a tool of choice for many cybercriminals and each of them has used different means of distribution. Danabot's developers even partnered with the authors of several malware cryptors and loaders, and offered special pricing for a distribution bundle to their customers, helping them with the process. Recently, out of all distribution mechanisms ESET observed, the misuse of Google Ads to display seemingly relevant, but actually malicious, websites among the sponsored links in Google search results stands out as one of the most prominent methods to lure victims into downloading Danabot. The most popular ploy is packing the malware with legitimate software and offering such a package through bogus software sites or websites falsely promising users to help them find unclaimed funds. The latest addition to these social engineering techniques are deceptive websites offering solutions for fabricated computer issues, whose only purpose is to lure victims into execution of a malicious command secretly inserted into the user's clipboard.

The typical toolset provided by Danabot's authors to their affiliates includes an administration panel application, a backconnect tool for real-time control of bots, and a proxy server application that relays the communications between the bots and the actual C&C server. Affiliates can choose from various options to generate new Danabot builds, and it's their responsibility to distribute these builds through their own campaigns.

"It remains to be seen whether Danabot can recover from the takedown. The blow will, however, surely be felt, since law enforcement managed to unmask several individuals involved in the malware's operations," concludes Procházka.

For technical overview of Danabot and insight into its operation, check out ESET Research blogpost: "Danabot: Analyzing a fallen empire" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET

ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown— securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts and blogs.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here