Operation Endgame: Global Law Enforcement Takes Down DanaBot Malware Scheme

By Flashpoint

Published: 2025-05-22 · Archived: 2026-04-05 22:55:45 UTC

Today, a federal grand jury has indicted 16 individuals, including two Russian nationals, for their alleged involvement in developing and deploying the DanaBot malware. This widespread cybercrime operation infected over 300,000 victims worldwide, caused over $50 million in damages, and facilitated fraud and ransomware, with a specific variant targeting military and government entities.

These law enforcement actions were taken in conjunction with Operation Endgame, a global law enforcement effort to dismantle cybercriminal organizations. This involved the Defense Criminal Investigative Service (DCIS) agents successfully seizing and taking down DanaBot command and control servers, including dozens hosted in the United States.

Flashpoint is proud to have contributed to this investigation as part of an alliance of government agencies and private sector partners.

> "*Pervasive malware like DanaBot harms hundreds of thousands of victims around the world, including sensitive military, diplomatic, and government entities, and causes many millions of dollars in losses. The charges and actions announced today demonstrate our commitment to eradicating the largest threats to global cybersecurity and pursuing the most malicious cyber actors, wherever they are located.*"
>
> *United States Attorney Bill Essayli*

Understanding Malware-as-a-Service (MaaS)

Malware-as-a-Service has fundamentally reshaped the cybercrime landscape by lowering the barrier to entry for even unsophisticated threat actors. Like legitimate Software-as-a-Service (SaaS) models, MaaS platforms allow cybercriminals to "rent" access to complex malware and its infrastructure, enabling them to launch attacks of their own without needing a team or technical expertise.

This model helps to create a robust illicit economy where similar MaaS tools are readily available, such as information-stealing malware or Ransomware-as-a-Service (RaaS). As such, it is critical for organizations to leverage comprehensive threat intelligence and employ robust security measures.

The DanaBot malware allegedly operated on a malware-as-a-service model, with the administrators leasing access to the botnet and support tools to client coconspirators for a fee that was typically several thousand dollars a month.

DanaBot: A Pervasive Malware-as-a-Service Threat

DanaBot's core functionality revolves around collecting sensitive information from compromised systems. This includes credentials from browsers, FTP, Secure Shell protocol (SSH), and email clients, as well as capturing data through clipboard sniffing and keylogging. It can also grab specific files and cryptocurrency wallets.

DanaBot incorporates remote access trojan (RAT) capabilities, enabling attackers to issue terminal commands, provide remote access via hidden virtual network computing (HVNC), and perform HTML injections. DanaBot also operated as a malware-as-a-service (MaaS) platform, allowing threat actors to purchase and use its capabilities.

The malware's infrastructure is typically divided into several components: a "bot" that infects target systems and performs data collection, an "OnlineServer" that manages the RAT functionalities, a "client" for processing collected logs and bot management, and a "server" that handles bot generation, packing, crypting, and command-and-control (C2) communication. DanaBot has evolved to include features like Tor fallback for C2 recovery and Jabber integration for notifications.

Beyond financial fraud, a second version of the DanaBot botnet specifically targeted computers in military, diplomatic, government, and other related entities in North America and Europe, posing a significant threat to national security.

The Power of Partnership

These law enforcement actions taken in conjunction with Operation Endgame and Operation PowerOFF, represent an ongoing coordinated effort among international law enforcement agencies aimed at dismantling and prosecuting cybercriminal organizations around the world. The investigation into DanaBot was spearheaded by the FBI's Anchorage Field Office and the Defense Criminal Investigative Service, working closely with Germany's Bundeskriminalamt (BKA), the Netherlands National Police, and the Australian Federal Police.

> *"The enforcement actions announced today, made possible by enduring law enforcement and industry partnerships across the globe, disrupted a significant cyber threat group, who were profiting from the theft of victim data and the targeting of sensitive networks. The DanaBot malware was a clear threat to the Department of Defense and our partners. DCIS will vigorously defend our infrastructure, personnel, and intellectual property."*
>
> *Special Agent in Charge, Kenneth DeChellis*

Flashpoint is honored to provide valuable assistance alongside a strong alliance of industry partners. This collaborative effort underscores the critical role of private sector intelligence and expertise in disrupting global cybercrime operations.

For a comprehensive understanding of Operation Endgame, check out the DOJ's full announcement. Flashpoint remains committed to working alongside law enforcement to provide timely and actionable intelligence that helps protect critical infrastructure and combat the evolving threat landscape.

Source: https://flashpoint.io/blog/operation-endgame-danabot-malware/