The New Release of Danabot Version 3: What You Need to Know

flashpoint.io/blog/danabot-version-3-what-you-need-to-know/

July 17, 2023

Last week, the third version of the malware toolkit Danabot was released on the high-tier Russian-language forum Exploit. Dubbed DBot v.3, this version focuses on persistence and exfiltration of useful information that can later be monetized, using social engineering in email-based threats to gather information from its victims.

How DBot v.3 works

Danabot's current infrastructure is broken into four parts:

Part 1: The bot

The first part of DBot v.3 is the bot, which is the build of Danabot that is dropped on a target's systems. The Danabot build has the following functionality:

- Stealer malware capabilities that target browsers, File Transfer Protocol (FTP), Secure Shell (SSH), and email clients.
- Clipboard sniffing capabilities which enables it to collect data from users copying information within or between applications via the clipboard.
- Keylogging capability which allows DBot v.3 to record keystrokes made by a computer user

- File and wallet grabbing
- “PostGrabber”, a form-grabbing tool
- Remote access trojan (RAT) capabilities
- HTML injections
- Web request redirecting and blocking
- Tor fallback for command and control (C2) proxy recovery
- Jabber integration for notifications

Part 2: The “OnlineServer”

The OnlineServer is a portable executable (PE) application that acts as a panel for the RAT functionality of Danabot. It does the following:

- Enables interaction with the Danabot API
- Issues terminal commands on victim systems
- Provides remote access to victims via hidden virtual network computing

Parts 3 and 4: The client and the server

The client operates as a PE application that acts as a panel to process logs collected by the bot and manage the bot.

The last component of DBot v.3 is the server, which operates the back end of the panels and handles build generation of the bots. The server is a 64-bit application with a MySQL database and has a built-in firewall. It handles the following tasks:

- Building bots
- Packing and crypting bots
- Building proxy chains for bot C2 communication
- Enabling API for handling crypting and the database

After analyzing details of the sales threads for Danabot versions 2 and 3, Flashpoint has concluded that there are no significant technical differences between the two iterations.

The most important changes of Danabot version 3

However, the most important changes from DanaTools (version 2) and DBot v.3 are its price restructuring and improved customer support. With the release of DBot v.3, threat actors have more flexibility in choosing which tools they need through new subscription structures.

The following are examples of new subscription tiers:

- Use of stealer
- Stealer, plus Hidden Virtual Network Computing (HVNC)
- Stealer and PostGrabber

- Stealer, PostGrabber, and HVNC
- Stealer, PostGrabber, HVNC, API, personal server, and personal support
- Demo of stealer, HVNC, and PostGrabber

In addition, the Danabot Tor site now offers instructions on panel setup and configuration, as well as video demonstrations and bot generation options. The restructuring and lowered barrier-of-entry will likely make DBot v.3 more accessible and appealing to threat actors.

Track and protect against malware with Flashpoint

Flashpoint analysts are currently monitoring the threat landscape for the use of Danabot version 3 bots in the wild. To learn the latest updates involving DBot v.3, in addition to other rising malware threats, sign up for a free trial.