Danabot: Analyzing a fallen empire

welivesecurity.com/en/eset-research/danabot-analyzing-fallen-empire/

ESET Research

ESET Research shares its findings on the workings of Danabot, an infostealer recently disrupted in a multinational law enforcement operation

Tomáš Procházka

22 May 2025 , 18 min. read

As announced by the US Department of Justice – the FBI and US DoD's Defense Criminal Investigative Service (DCIS) have managed to disrupt the infrastructure of the notorious infostealer, Danabot. ESET is one of the many cybersecurity companies to participate in this long-term endeavor, becoming involved back in 2018. Our contribution included providing technical analyses of the malware and its backend infrastructure, as well as identifying Danabot's C&C servers. The joint takedown effort also led to the identification of individuals responsible for Danabot development, sales, administration, and more. ESET

took part in the effort alongside with Amazon, CrowdStrike, Flashpoint, Google, Intel471, PayPal, Proofpoint, Team Cymru, Zscaler, Germany's Bundeskriminalamt, the Netherlands' National Police, and the Australian Federal Police.

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 largely been disrupted, we will use this opportunity to share our insights into the workings of this malware-as-a-service (MaaS) 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 – including ransomware – to an already compromised system.

> **Key points of the blogpost:**
>
> - ESET Research has been tracking Danabot's activity since 2018 as part of a global effort that resulted in a major disruption of the malware's infrastructure.
> - While primarily developed as an infostealer and banking trojan, Danabot also has been used to distribute additional malware, including ransomware.
> - Danabot's authors promote their toolset through underground forums and offer various rental options to potential affiliates.
> - 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 communication 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.

Background

Danabot, which belongs to a group of infostealer and/or banking malware families coded in the Delphi programming language, gained prominence in 2018 by being used in a spam campaign targeting Australian users. Since then, Danabot has expanded to other markets through various campaigns, undergone several major updates of its internals and backend infrastructure, and experienced both peaks and downturns in popularity among cybercriminals.

Throughout our monitoring since 2018, ESET has tracked and analyzed a substantial number of distinct samples and identified more than 1,000 unique C&C servers. During that period, ESET analyzed various Danabot campaigns all over the world, with Poland

historically being one of the most targeted countries, as seen in Figure 1.

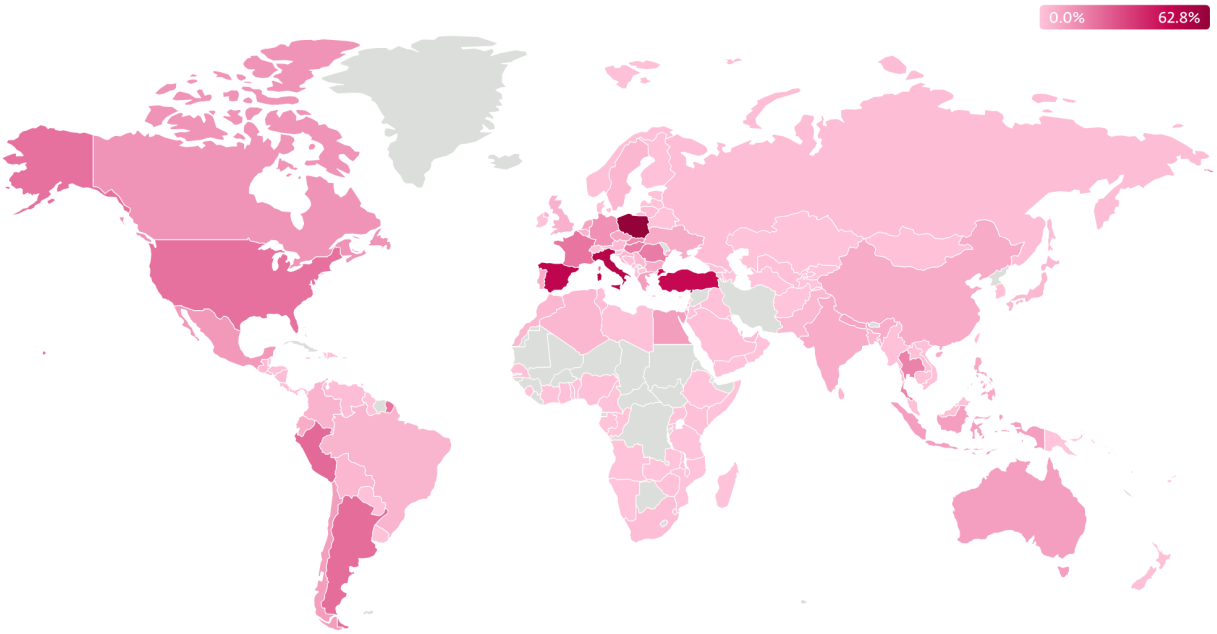

Figure 1. Worldwide Danabot detections as seen in ESET telemetry since 2018

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 was spotted by Zscaler soon after the Russian invasion of Ukraine. A very similar DDoS module to the one used in that attack was also used by a Danabot operator to target a Russian site dedicated to Arduino development. These actions were probably motivated by the affiliate's own ambitions and political motivations.

Danabot group introduction

The authors of Danabot operate as a single group, offering their tool for rent to potential affiliates, who subsequently employ it for their own malicious purposes by establishing and managing their own botnets. The authors have even set up a support page on the Tor network with detailed information about the capabilities of their tool, as depicted in Figure 2.

Figure 2. Danabot's features as promoted on its support site

To acquire new customers, Danabot is frequently promoted in underground forums by the user JimmBee, who acts as one of the main developers and administrators of the Danabot malware and its toolset. Another noteworthy person from the Danabot group is a user known in underground forums as Onix, who coadministers the Danabot infrastructure and is also responsible for sales operations.

Feature overview

Danabot's authors have developed a vast variety of features to assist customers with their malevolent objectives. 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,
- a FileGrabber command, 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, we have observed a variety of payloads being distributed through Danabot over the years, such as:

- SystemBC,
- Rescoms,
- Ursnif,
- Smokeloader,
- Zloader,
- Lumma Stealer,
- RecordBreaker,
- Latrodectus, and
- NetSupportManager remote administration tool.

Furthermore, we have encountered instances of Danabot being used to download ransomware onto already compromised systems. We can name LockBit, Buran, Crisis, and a NonRansomware variant being pushed on several occasions.

Danabot's ability to download and execute arbitrary payloads is not the only feature used to distribute additional malware. Danabot was also spotted being used as a tool to hand off control of the botnet to a ransomware operator, as reported by Microsoft Threat Intelligence in late 2023.

Distribution methods

Throughout its existence, according to our 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. Matanbuchus is an example of such a promoted loader.

Over the years, we have seen all sorts of distribution methods being used by Danabot affiliates, including:

- numerous variants of email spam campaigns,
- other malware such as Smokeloader, DarkGate, and Matanbuchus, and
- misuse of Google Ads.

Recently, out of all distribution mechanisms we saw, 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 (Figure 3) or websites falsely promising users to help them find unclaimed funds (Figure 4).

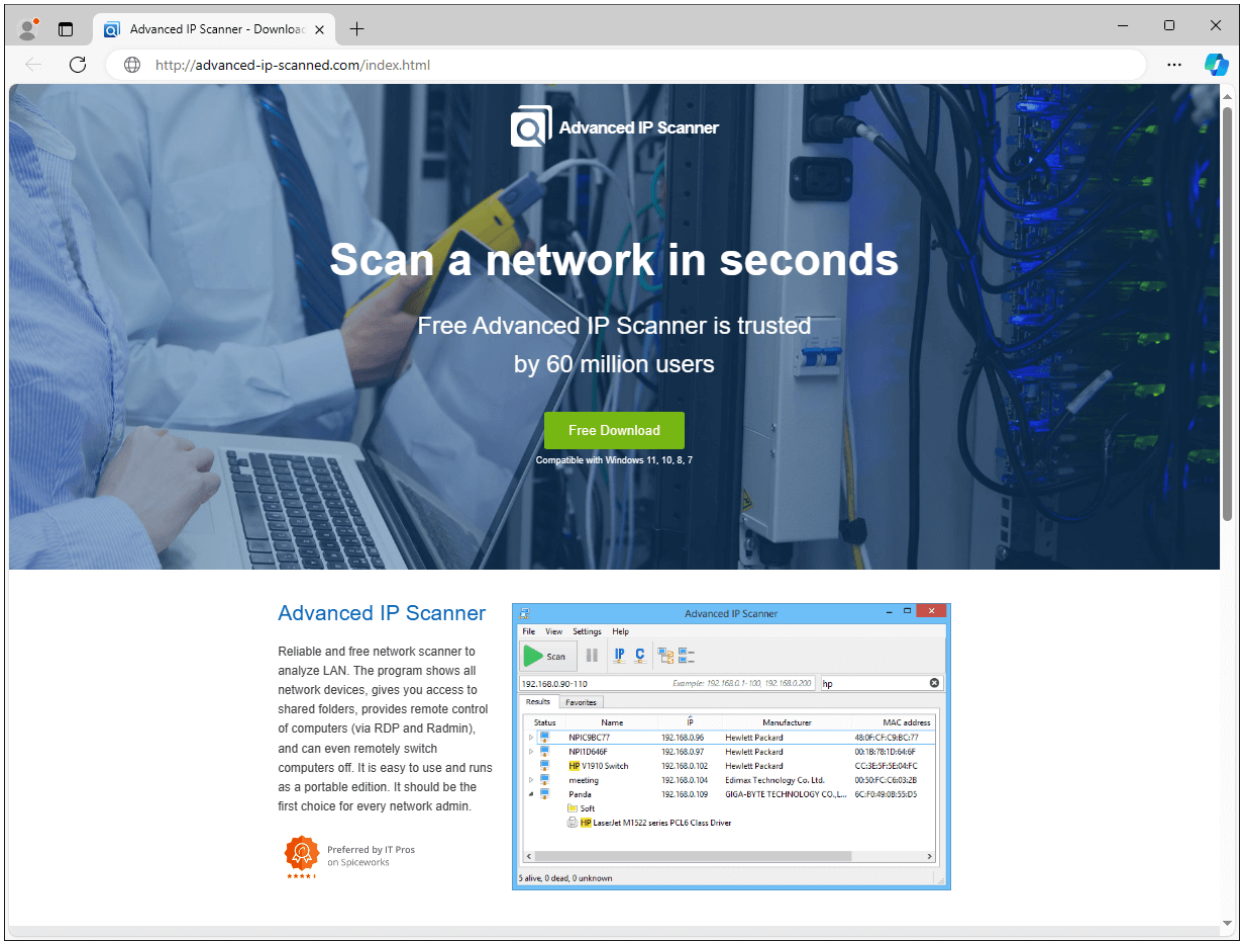

Figure 3. Fake Advanced IP Scanner website leading to Danabot compromise

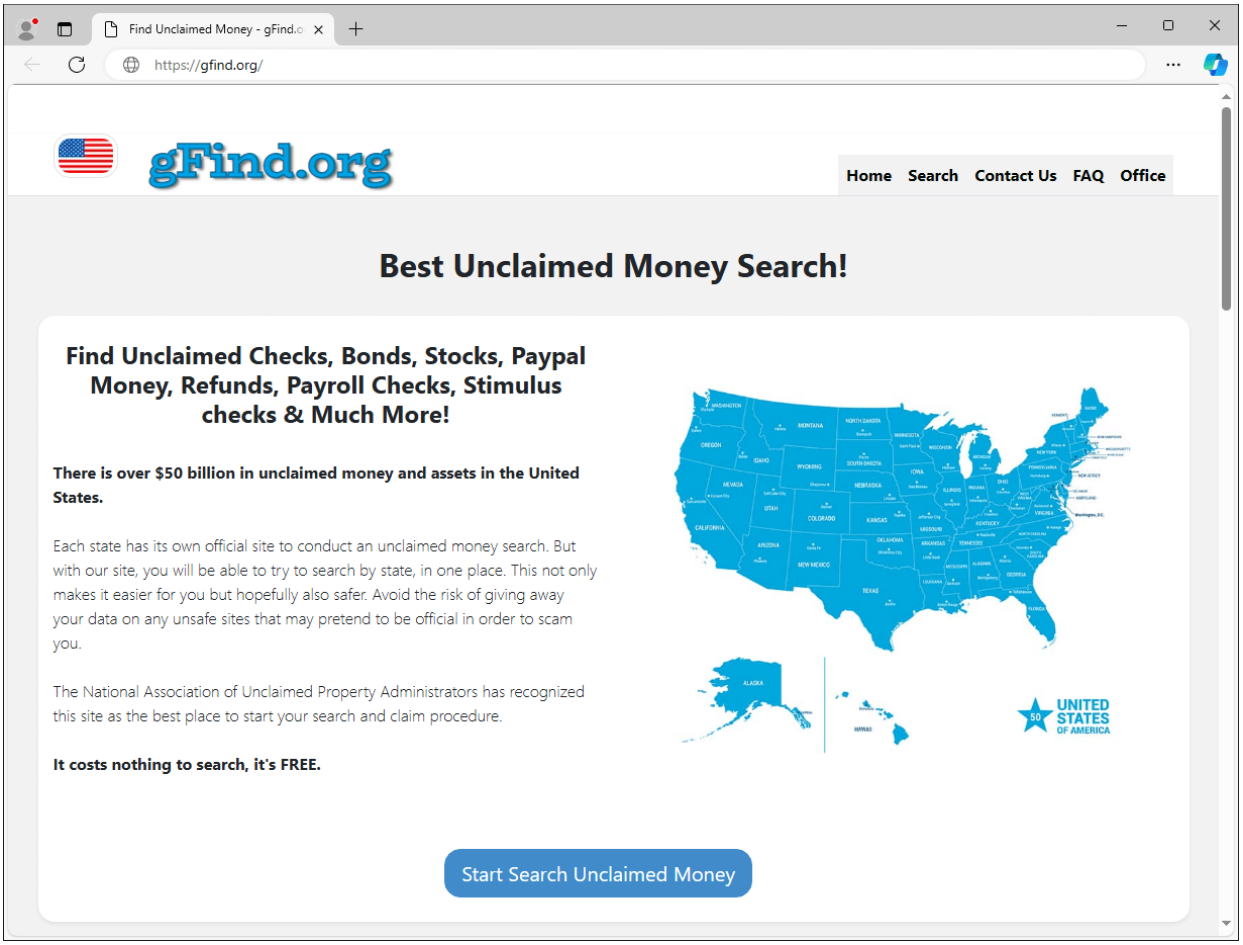

Figure 4. Fake unclaimed money search site

The latest addition to these social engineering techniques: deceptive websites offering solutions for fabricated computer issues, whose only purpose is to lure the victim into execution of a malicious command secretly inserted into the user's clipboard. An example of such a website leading to downloading of Danabot in Figure 5.

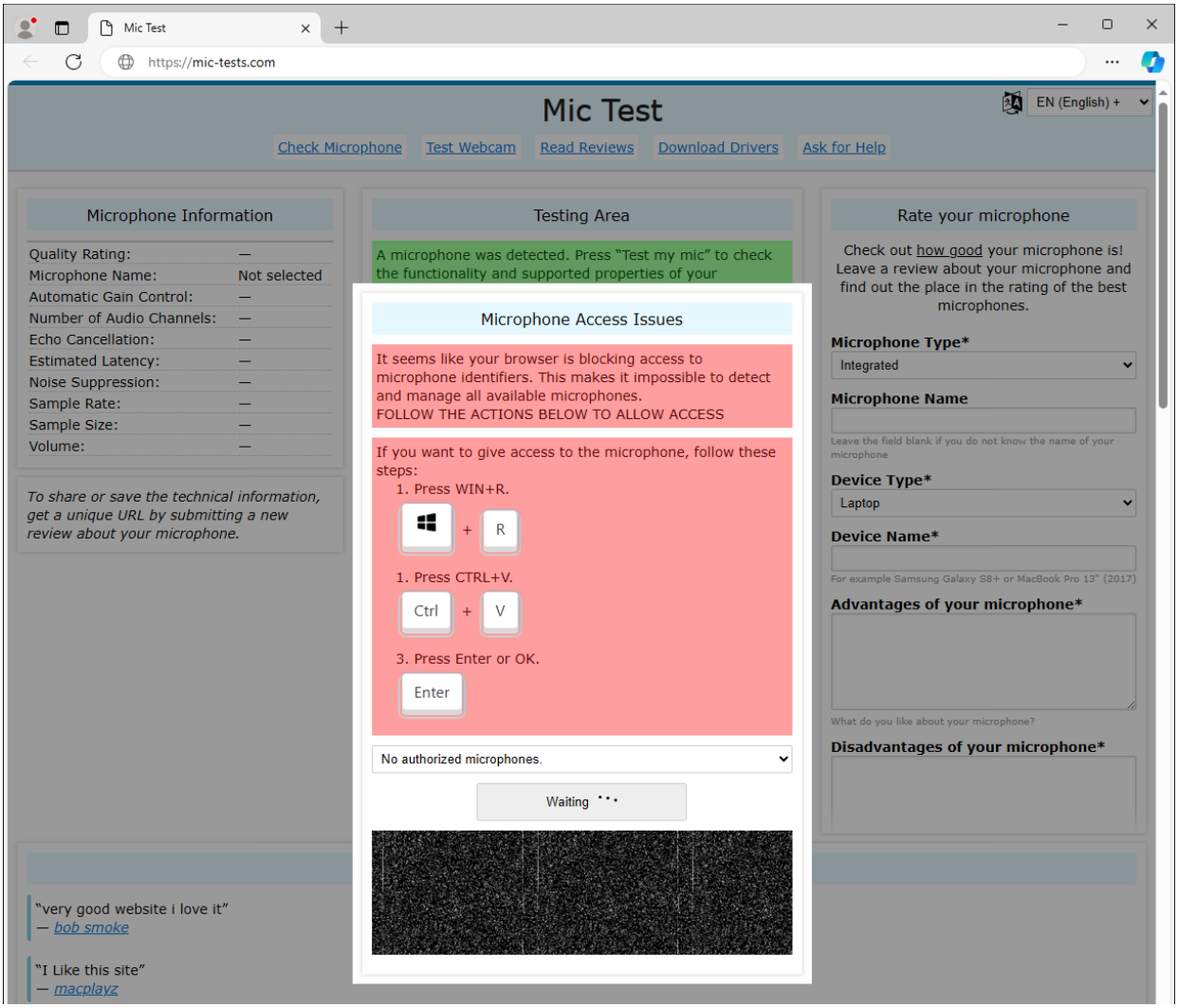

Figure 5. Website luring the victim into execution of malicious command stored in the user's clipboard

Infrastructure

Overview

Initially, Danabot's authors relied on a single centralized server to manage all bots' connections and all affiliates' data, such as command configurations and data collected from their victims. This centralized approach certainly had a negative impact on that server's performance and was more prone to possible disruptions. This is probably one of the reasons why we saw a shift in the business and infrastructure models in newer versions. In addition to renting places on their own infrastructure, Danabot's authors now offer installation of a private server, as advertised on their support site, to be operated by the affiliate (Figure 6).

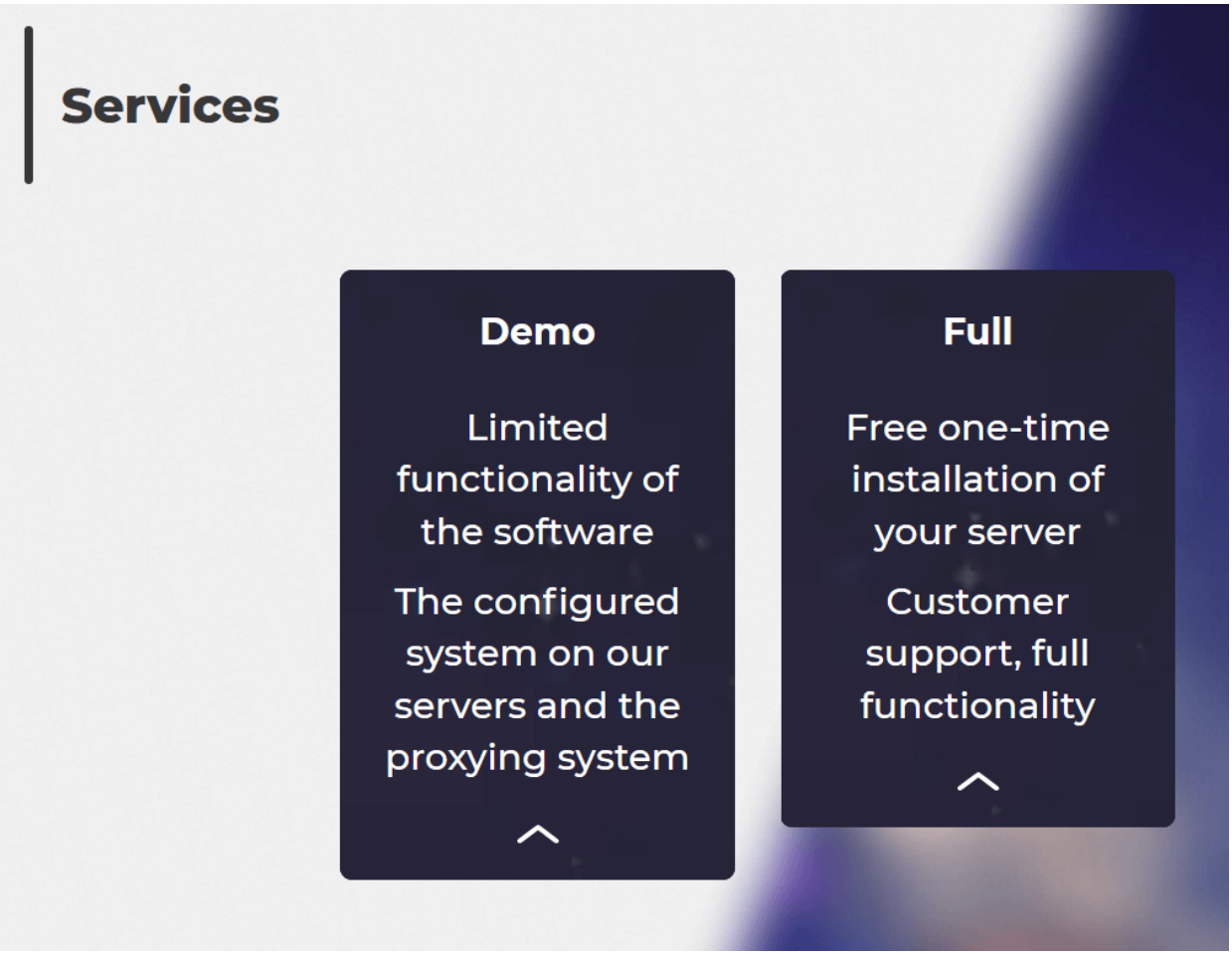

Figure 6. Basic offering on Danabot's support site

The rental options, as offered through an underground forum in July 2023, are illustrated in Figure 7.

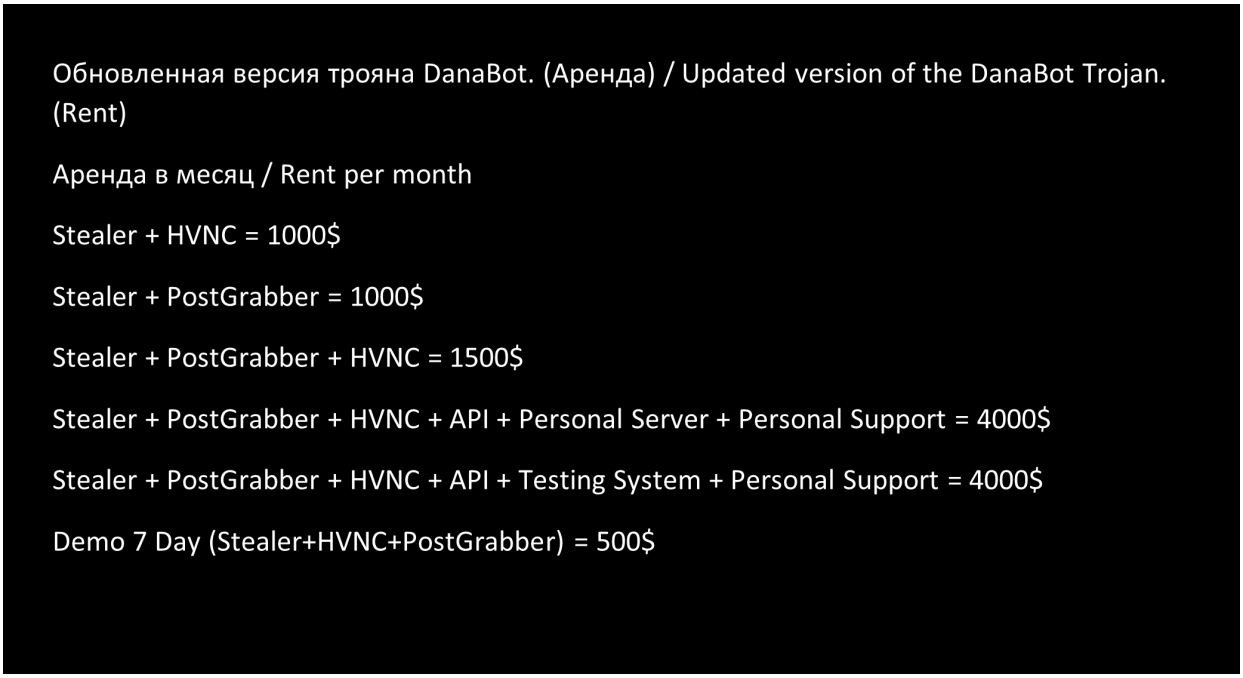

Figure 7. Price list for potential Danabot customers

It is worth mentioning that, based on our tracking, the rental of an account on the shared infrastructure controlled by Danabot's authors seems to be the most popular choice for threat actors.

When affiliates purchase a rental of one of the options, they are given tools and credentials to connect to the C&C server and manage their own botnet through an administration panel. In the following sections, we cover the different parts of the typical toolset.

C&C server application

The standalone server application comes in the form of a DLL file and acts as the brain of the botnet. It is installed on a Windows server and uses a MySQL database for data management. Bots connect to this server to transmit stolen data and receive commands issued by affiliates. Affiliates connect to this server via the administration panel application to manage their botnet. This C&C server application is available for local installation only for affiliates paying for the higher tier personal server option. Affiliates who choose to operate their botnets on Danabot's infrastructure instead are given connection details to the C&C server already set up there, and do not need to host their own C&C server.

Administration panel

The administration panel, displayed in Figure 8, is in the form of a GUI application, and represents the most important tool from the botnet operator's perspective. It allows the affiliate to connect to the C&C server and perform tasks such as:

- manage bots and retrieve statistics of the botnet,
- issue various commands and advanced configuration for bots,
- conveniently view and export data gathered from victims,
- manage the notification system and set up alerts on events triggered by bots,
- generate new Danabot builds, and
- set up a chain of proxy servers for communication between the bots and the C&C server.

We provide more details and examples of the most interesting capabilities of the administration panel in the upcoming sections.

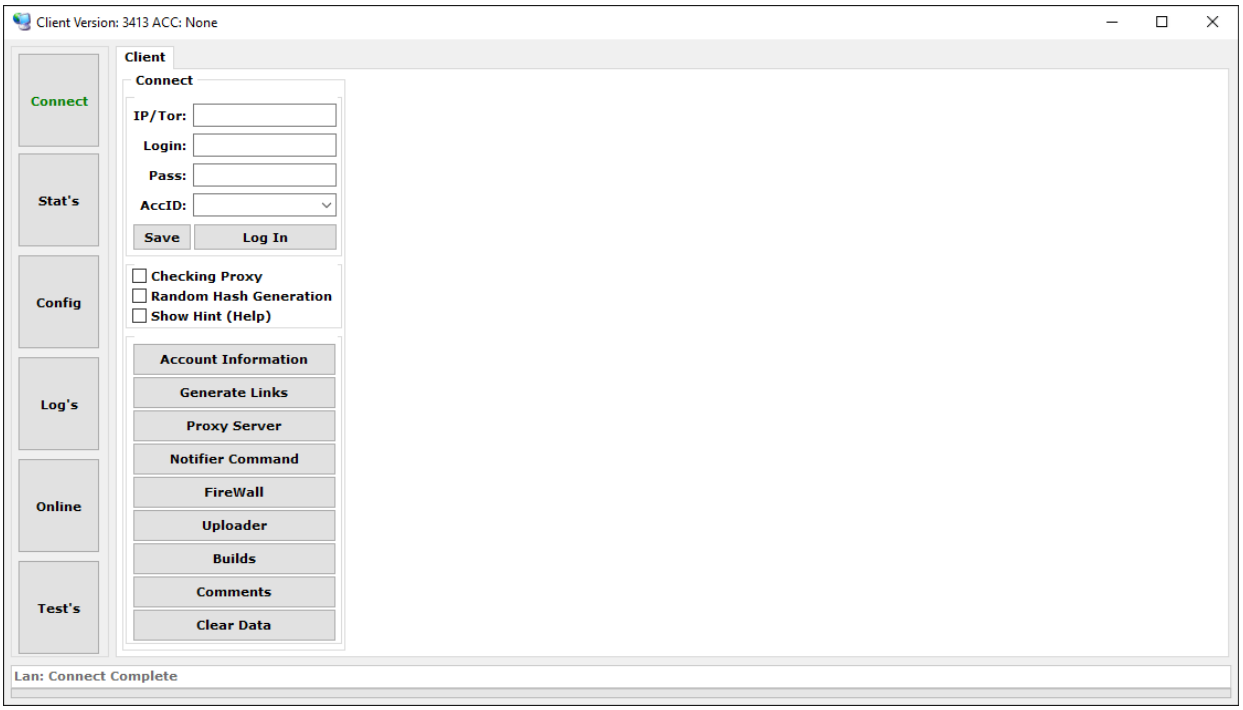

Figure 8. Administration panel overview

Backconnect tool

Another important tool for administration is the standalone utility that enables botnet operators to remotely connect to and control their online bots. Available actions for remote control, as seen in the tool, are illustrated in Figure 9. Probably the most interesting features for cybercriminals are the ability to see and control the victim's computer via a remote desktop connection and to perform reconnaissance of the file system using the built-in file manager.

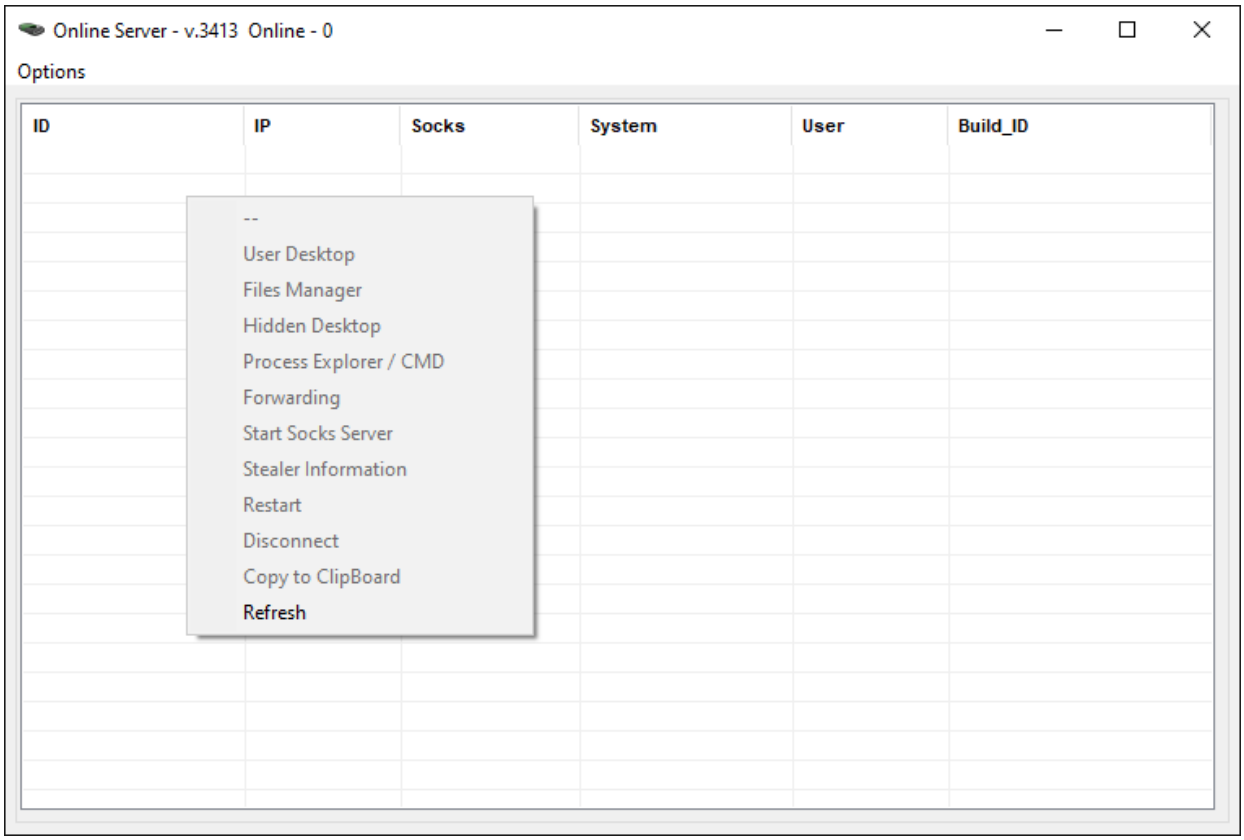

Figure 9. Features of the backconnect utility

Proxy server application

Bots typically do not connect to the main C&C server directly, but rather use a chain of proxies to relay the traffic and hide the location of the real backend C&C. To facilitate this strategy, Danabot's authors provide a proxy server application, available for both Windows and Linux systems. Figure 10 shows the usage message from the Linux version of this simple proxy server application. Besides using proxies, bots can be configured to communicate with the server through the Tor network in case all proxy chains become unavailable. An optional downloadable Tor module is then used for such communication.

```
test@debian:~/proxy$ ./proxy
Userspace TCP proxy.
Usage:
  ./proxy <local_ip:local_port> <dest_ip:dest_port> [-d] [-o] [-b]
Options:
  -d              run in background
  -o              accept IPv6 connections only for IPv6 listener
  -b              base address to port mapping mode
  -p <pidfile>    write PID to file
```

Figure 10. Usage message from the Linux version of the proxy server application

Affiliates also frequently utilize this proxy server application as an intermediary between their administration panel and the C&C server to further enhance their anonymity. When everything is put together, the typical infrastructure may look as shown in Figure 11.

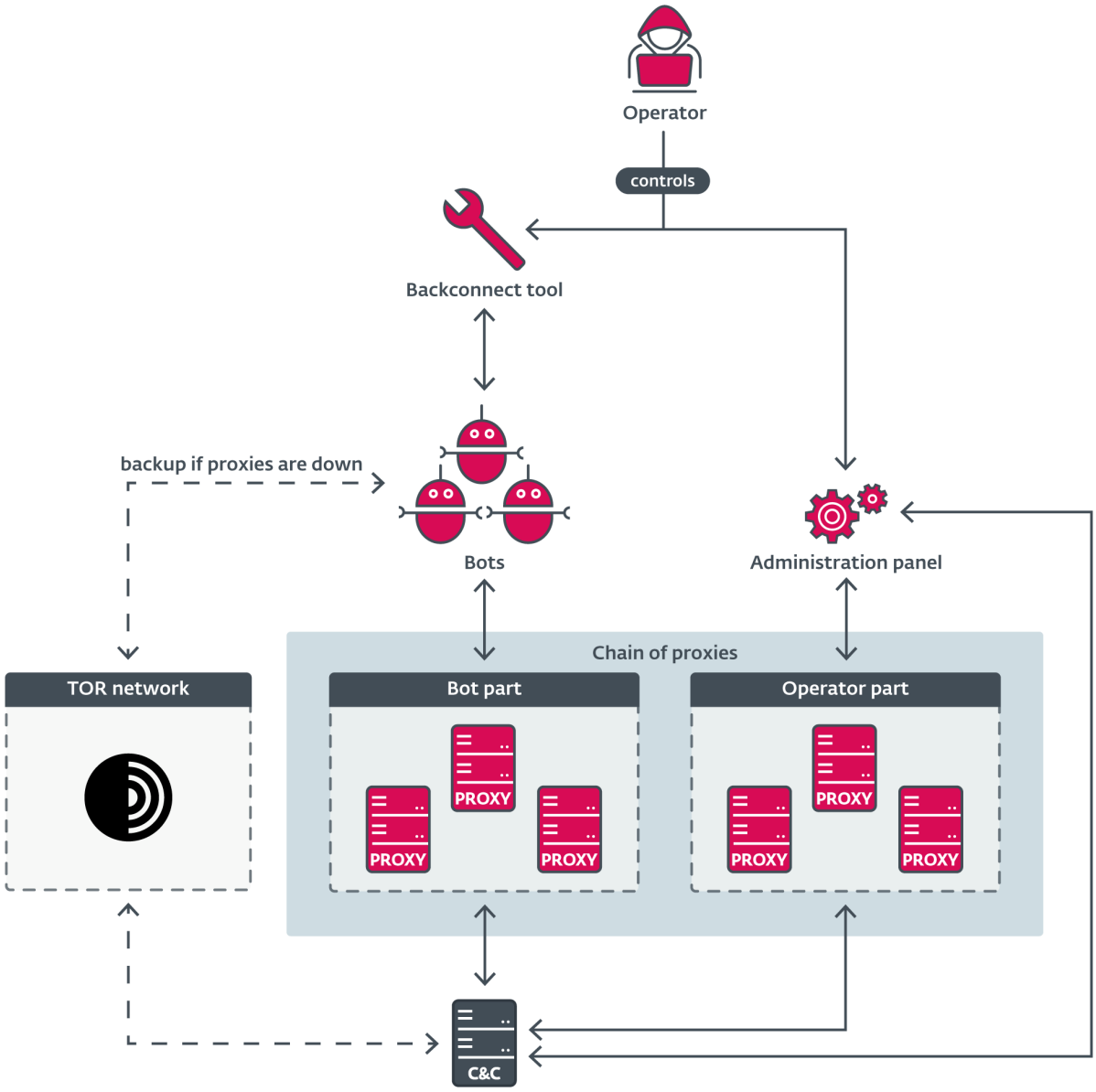

Figure 11. Example of typical Danabot infrastructure

Internals

Communication

Danabot employs its own proprietary C&C communication protocol with its data encrypted using AES-256. Generated AES session keys, unique for every message, are then further encrypted using RSA key pairs, securing the whole communication. It's worth mentioning that there have been several updates to the communication protocol and the packet structure over time.

The current packet data structure of the typical command, before it is encrypted, looks as shown in Table 1 . We would like to point out that most of the fields are only used during the first request in the communication loop to authenticate the bot, and are left unset in the subsequent commands.

Table 1. Packet structure used in Danabot communication

Offset	Size (bytes)	Description
0x00	0x04	Size of the packet.
0x04	0x08	Random value.
0x0C	0x08	Sum of the two values above.
0x14	0x04	Account ID used to differentiate affiliates in the previous versions. This field contains a random value in newer versions.
0x18	0x04	Command.
0x1C	0x04	Subcommand.
0x20	0x04	Danabot version.
0x24	0x04	IsUserAdmin flag.
0x28	0x04	Process integrity level.
0x2C	0x04	OS architecture x86/x64.
0x30	0x04	Encoded Windows version.
0x34	0x04	Time zone bias as a DWORD value.
0x38	0x04	Unknown bytes; set to 0 in the current versions.
0x3C	0x04	Tor active flag.
0x40	0x04	Unknown bytes; set to 0 in the current versions.
0x44	0x18	Padding null bytes.
0x5C	0x21	Bot ID Delphi string (a string preceded by a length byte).
0x7D	0x21	Build ID hardcoded Delphi string.
0x9E	0x21	MD5 checksum of concatenated Account ID, Bot ID, and Build ID strings.
0xBF	0x29	Command dependent string used in some commands complemented by its CRC-32 and a string size.

Offset	Size (bytes)	Description
0xE8	0xDF	Padding null bytes.

The newest versions of Danabot also add, to further disguise its communication, a random amount of seemingly junk bytes to the end of the packet structure before it is encrypted. It's worth mentioning that Danabot authors do not always follow the best coding practices and the addition of this random number of bytes was done by resizing of the original memory buffer allocated to hold the packet structure instead of clearing or initializing this newly acquired space. This led to unintentionally including surrounding memory regions of the process into the data packet being sent from the bot to the server and, more importantly, vice versa. These appended memory regions captured and decrypted from the server-to-bot communication sometimes contained interesting information from the server's process memory and gave researchers valuable insight into Danabot's infrastructure and its users. This bug was introduced in 2022 and was fixed in the latest versions of Danabot in February 2025.

Further details about the communication and its encryption were already covered by various researchers, and we won't dive into it more in this blogpost.

Builds

Botnet operators have multiple options for generating new Danabot builds to distribute to their victims. To the best of our knowledge, while the operator may configure the build process and desired output through the administration panel application, the build process itself is performed on the Danabot authors' servers. After generating the selected build, the operator receives download links for the builds and becomes responsible for their distribution in a campaign.

Figure 12 shows an example of a build configuration window and available options, such as the C&C server list to be configured in the final binary file, various obfuscation methods, build bitness, etc.

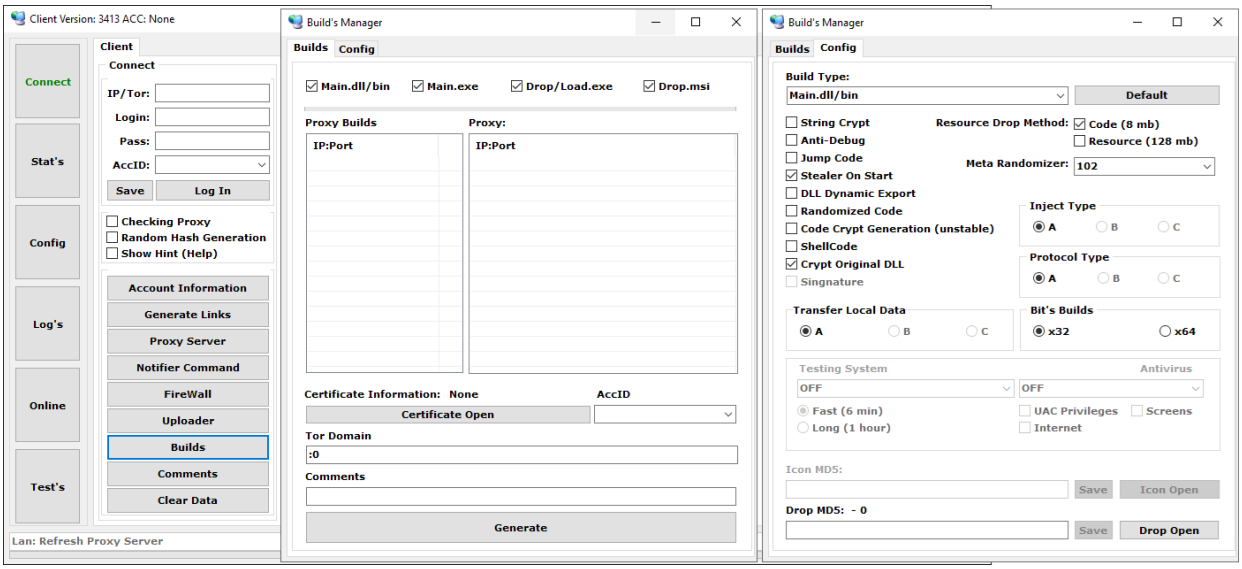

Figure 12. Build options menu from the Administration panel application

Danabot currently offers four basic payload types, described in Table 2.

Table 2. Variants of available builds

Payload type	Description
Main.dll	Generates a sole main component in the form of a DLL to be distributed and loaded via rundll32.exe or regsvr32.exe.
Main.exe	Generates a loader in the form of an EXE that may contain the abovementioned main component DLL or download it from one of the configured C&C servers.
Drop.exe	Generates a dropper with an embedded main component DLL to be dropped to disk.
Drop.msi	Generates an MSI package with an embedded main component DLL to be loaded.

Commands configuration

A botnet operator can issue an advanced configuration to the bots through the administration panel. Bots are then ordered to perform various commands according to the instructions received. Figure 13 shows an example of such a command configuration.

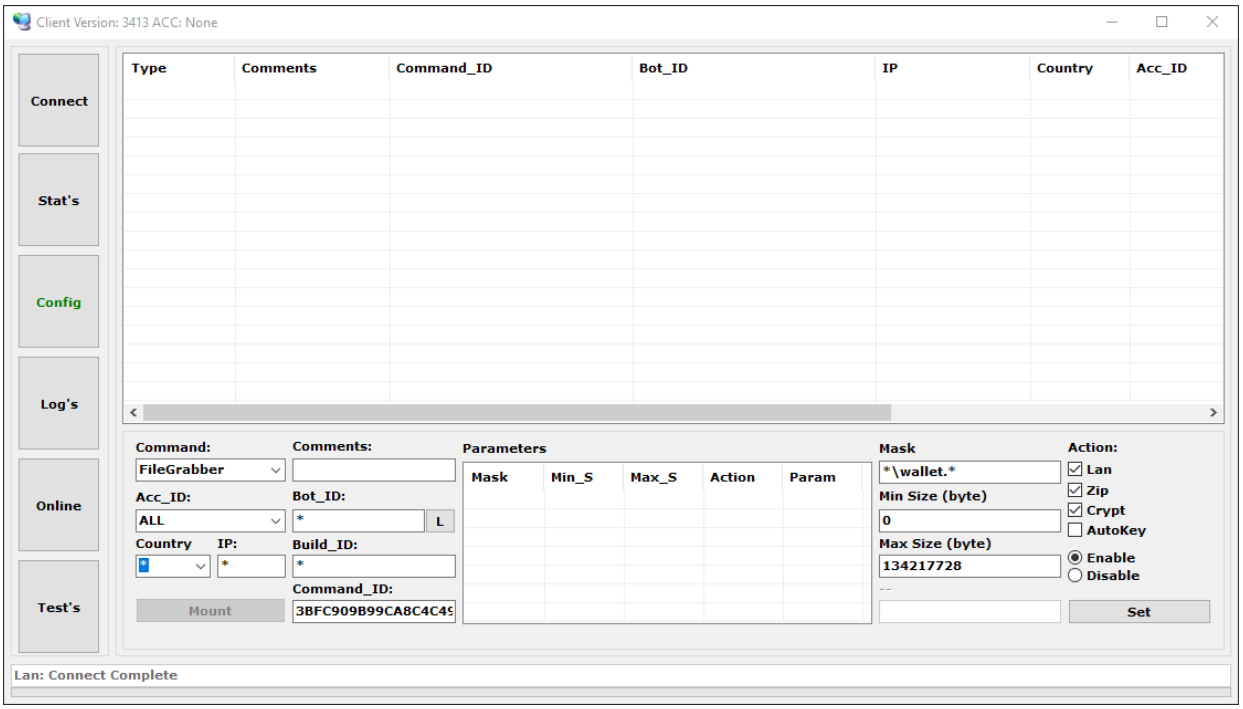

Figure 13. Dynamic configuration options for the FileGrabber *command*

Table 3 lists the available commands that can be issued. Each task has its own specific options to further accommodate the operator's needs.

Table 3. Available commands

Command	Description
Video	Record a video of the selected application or website.
KeyLogger	Capture keystrokes from the selected application.
PostFilter	Grab information from certain websites' forms.
WebInject	Allow Zeus-like webinjects on certain loaded websites to alter their function.
Redirect	Allow redirection of certain URLs.
Block	Block access to configured URLs.
Screens	Take screenshots of a selected application or website at certain intervals.
Alerts	Allow notifications to be sent to a selected Jabber account on a configurable event.
Uninstall	Uninstall the bot from the system.
UAC	Provide support for privilege escalation.

Command	Description
FileGrabber	Allow certain files to be uploaded to the C&C if found on the victim's hard disk.
TorActive	Enable loading of a Tor module and allow connection via the Tor network if all C&C servers are inaccessible.
Stealer	Enable/disable the stealer functionality and set its update interval.
TimeOut	Set interval for the bot to contact its C&C server.
Install	Configure the bot's installation on the system and its persistence.
Exclusion	Set exclusions in Windows Defender or Windows Firewall for a selected process.
ConfigSave	Save the bot's configuration before its termination.
HideProcess	Hide the bot's process.
CoreProtect	Allow the main component to be injected into an additional process.

Additional payloads

Danabot also provides the capability to download and execute further executable files. This feature allows the botnet operator to configure the installation of additional malware to the compromised system, as mentioned earlier. Figure 14 shows available options for this feature in the administration panel application.

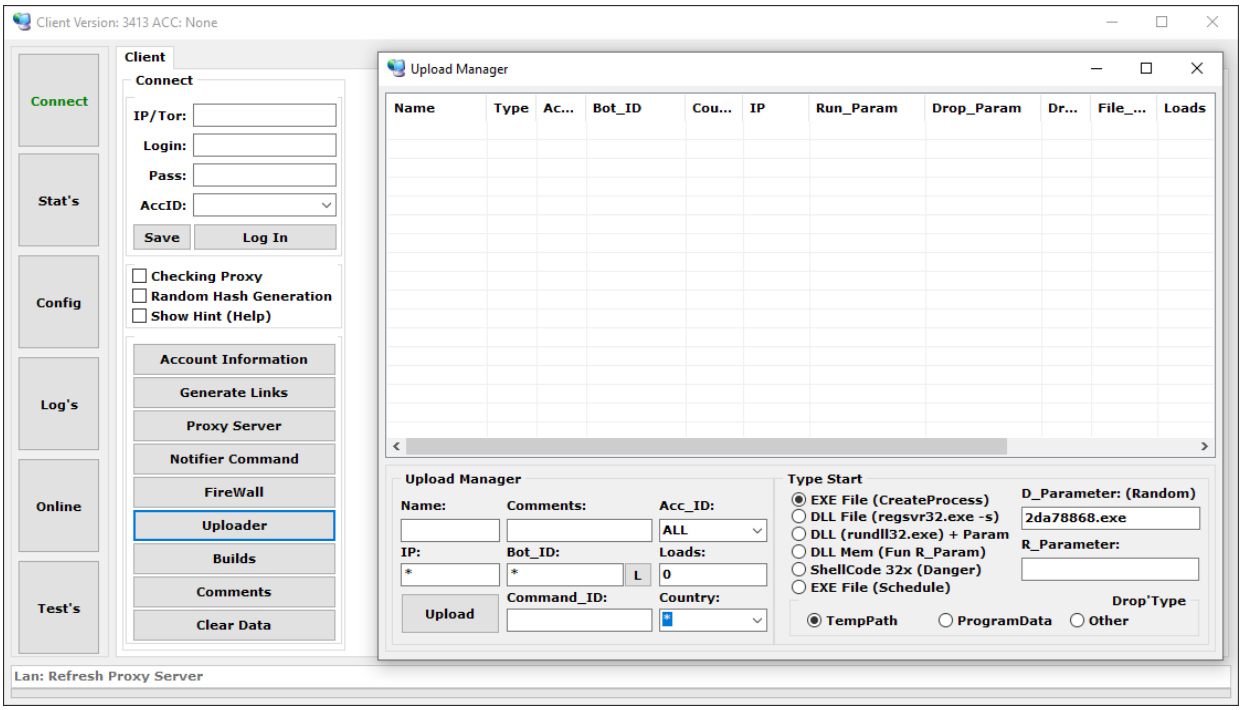

Figure 14. Options for an additional payload configuration

Conclusion

Danabot is a large-scale MaaS operation distributing a wide array of tools for the malware affiliates' disposal. Our investigation of this infostealer, which started in 2018, resulted in the analysis of Danabot's toolset provided in this blogpost. The efforts of the authorities and several cybersecurity companies, ESET included, led to the disruption of the malware's infrastructure. 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.

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

IoCs

Files

SHA-1	Filename	Detection	Description
6D361CD9ADBF1630AF7B323584168E0CBD9315FB	N/A	Win32/Spy.Danabot.X	Loader of the main component (version 4006).

SHA-1	Filename	Detection	Description
A7475753CB865AEC8DC4A6CEA27F2AA594EE25E8	N/A	Win32/Spy.Danabot.O	Main component (version 4006).
787EAB54714F76099EC350E029154ADFD5EDF079	N/A	Win32/Spy.Danabot.AC	Dropper component (version 3272).
17B78AD12B1AE1C037C5D39DBE7AA0E7DE4EC809	1c0e7316.exe	MSIL/Kryptik.AMBV	Lockbit payload (variant Black) distributed by Danabot.

Network

IP	Domain	Hosting provider	First seen	Details
212.18.104[.]245	N/A	GLOBAL CONNECTIVITY SOLUTIONS LLP	2025-03-25	Danabot proxy C&C server
212.18.104[.]246	N/A	GLOBAL CONNECTIVITY SOLUTIONS LLP	2025-03-25	Danabot proxy C&C server
34.16.215[.]110	N/A	Google LLC	2024-10-10	Danabot proxy C&C server
34.65.116[.]208	N/A	Google LLC	2024-10-10	Danabot proxy C&C server
34.168.100[.]35	N/A	Google LLC	2024-11-27	Danabot proxy C&C server
N/A	advanced-ip-scanned.com	N/A	2023-08-21	Deceptive website used in Danabot distribution
N/A	gfind.org	N/A	2022-06-15	Deceptive website used in Danabot distribution
N/A	mic-tests.com	N/A	2024-12-07	Deceptive website used in Danabot distribution

MITRE ATT&CK techniques

This table was built using version 17 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583.003	Acquire Infrastructure: Virtual Private Server	Danabot operators use VPS in their infrastructure.
	T1583.004	Acquire Infrastructure: Server	Danabot operators acquire multiple servers for C&C communication.
	T1587.001	Develop Capabilities: Malware	Danabot authors have developed custom malware tools.
	T1608.001	Stage Capabilities: Upload Malware	Danabot operators upload other malware to their infrastructure for further spreading.
	T1583.008	Acquire Infrastructure: Malvertising	Malvertising is a popular method of Danabot distribution.
Initial Access	T1566.001	Phishing: Spearphishing Attachment	Phishing is a common method used for distribution.
Execution	T1106	Native API	Dynamic Windows API resolution is used by Danabot.
	T1204.001	User Execution: Malicious Link	Luring users into downloading Danabot via a malicious link is a popular distribution choice.
	T1204.002	User Execution: Malicious File	Danabot is often distributed as a file to be opened by the user.
Privilege Escalation	T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Several methods are used by Danabot to bypass User Account Control.
Defense Evasion	T1027.007	Obfuscated Files or Information: Dynamic API Resolution	Danabot uses hashing for dynamic API resolution.
	T1055.001	Process Injection: Dynamic-link Library Injection	Danabot has the ability to inject itself into other processes.

Tactic	ID	Name	Description
	T1218.007	System Binary Proxy Execution: Msiexec	An MSI package is one of the possible distribution methods.
	T1218.010	System Binary Proxy Execution: Regsvr32	regsvr32.exe can be used to execute the main Danabot module.
	T1218.011	System Binary Proxy Execution: Rundll32	rundll32.exe can be used to execute the main Danabot module.
	T1656	Impersonation	Danabot uses impersonation in its phishing campaigns.
Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Danabot has the ability to steal various data from browsers.
	T1539	Steal Web Session Cookie	Danabot can steal cookies.
Discovery	T1010	Application Window Discovery	Danabot can be configured to steal data based on the active window.
	T1217	Browser Information Discovery	Data, such as browsing history, can be gathered by Danabot.
	T1083	File and Directory Discovery	Danabot can be configured to gather certain files from the compromised file system.
	T1057	Process Discovery	Danabot can enumerate running processes on a compromised system.
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol	Danabot operators can use the remote desktop module to access compromised systems.
	T1021.005	Remote Services: VNC	VNC is one of the supported features for controlling a compromised system.
Collection	T1056.001	Input Capture: Keylogging	Keylogging is one of Danabot's features.

Tactic	ID	Name	Description
	T1560.002	Archive Collected Data: Archive via Library	Danabot can use zlib and ZIP to compress collected data.
	T1560.003	Archive Collected Data: Archive via Custom Method	Collected data is further encrypted using AES and RSA cyphers.
	T1119	Automated Collection	Danabot can be configured to collect various data automatically.
	T1185	Browser Session Hijacking	Danabot can perform AitB attacks via webinjects.
	T1115	Clipboard Data	Danabot can collect information stored in the clipboard.
	T1005	Data from Local System	Danabot can be configured to search for sensitive data on a local file system.
	T1113	Screen Capture	Danabot can be configured to capture screenshots of applications and web pages.
	T1125	Video Capture	Danabot can capture video from the compromised system.
Command and Control	T1132.001	Data Encoding: Standard Encoding	Traffic between bot and C&C server is compressed using ZIP and zlib.
	T1001.001	Data Obfuscation: Junk Data	Junk bytes are added to data to be sent between bot and C&C server.
	T1573.001	Encrypted Channel: Symmetric Cryptography	AES-256 is used as one of the encryption methods of C&C communication.
	T1573.002	Encrypted Channel: Asymmetric Cryptography	RSA is used as one of the encryption methods of C&C communication.
	T1008	Fallback Channels	The Tor module can be used as a fallback channel in case all regular C&C servers are not responding.
	T1095	Non-Application Layer Protocol	Danabot uses its own custom TCP protocol for communication.

Tactic	ID	Name	Description
	T1571	Non-Standard Port	Danabot can communicate on any port.
	T1090.003	Proxy: Multi-hop Proxy	A chain of proxy servers is used to hide the location of the real C&C server.
	T1219	Remote Access Software	Danabot has support for remote access.
Exfiltration	T1020	Automated Exfiltration	Danabot can be configured to gather various data from a compromised system.
	T1030	Data Transfer Size Limits	Danabot can be configured to avoid sending large files from a compromised system.
	T1041	Exfiltration Over C2 Channel	Gathered data is exfiltrated through standard C&C communication.
Impact	T1498	Network Denial of Service	Danabot employed a module to perform various DDoS attacks.

Let us keep you up to date

Sign up for our newsletters