DanaBot control panel revealed | Proofpoint US

By March 13, 2019 Dennis Schwarz and Proofpoint Threat Insight Team

Published: 2019-03-13 · Archived: 2026-04-02 10:37:37 UTC

Overview

Proofpoint researchers discovered and reported on the DanaBot banking malware in May 2018 [1]. In our October 2018 update [2], we speculated that DanaBot may be set up as a “malware as a service” in which one threat actor controls a global command and control (C&C) panel and infrastructure system and then sells access to other threat actors known as affiliates. Affiliates then target and distribute DanaBot malware as they see fit. While analyzing a component of this infrastructure, we discovered an interesting graphical client application that we believe to be a control panel used by affiliates to access the global C&C system. Once logged on to the system, they can configure and build their DanaBot malware; access infected devices; and sift through any stolen data including credentials, financial account information, and more.

Control Panel Application

Our current theory is that when an affiliate buys access to the DanaBot system, they are given the control panel application described here and a user account to the global C&C system.

Like the malware, the control panel is written in the Delphi programming language. It has a compilation date of “2019-02-04 22:33:42” and an internal name of “Client.exe”. The application is mostly a graphical frontend in which inputs are formatted as commands that are sent to a backend C&C server for processing. Once processed, the C&C server sends back the results, which are then displayed by the application.

Figures 1 through 6 give a tour of the main components of the control panel. While a valid login is required to send and receive data to and from the backend C&C server, the figures still illustrate some of the potential actions a DanaBot affiliate can execute via the control panel:

- Login to a backend C&C server (Figure 1)
- Build new DanaBot malware (Figure 2)
- See various statistics from infected devices (Figure 3)
- Configure various aspects of the malware (e.g., video recording of the screen, keylogging, and webinjects) (Figure 4)
- Search and view stolen information (e.g., credentials and financial account information) (Figure 5)
- Operate on infected devices (e.g., search for files, download files, execute commands, take a screenshot, and open a VNC session) (Figure 6)

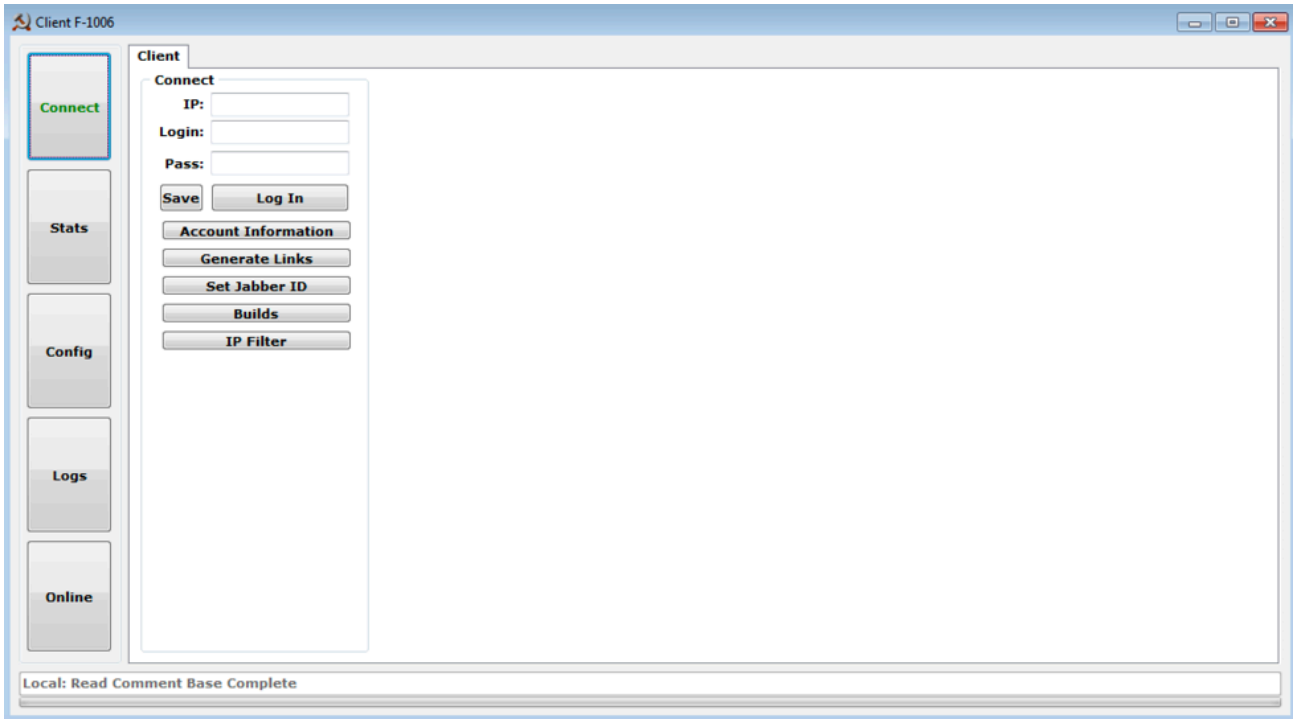

Figure 1: Control panel "Connect" tab

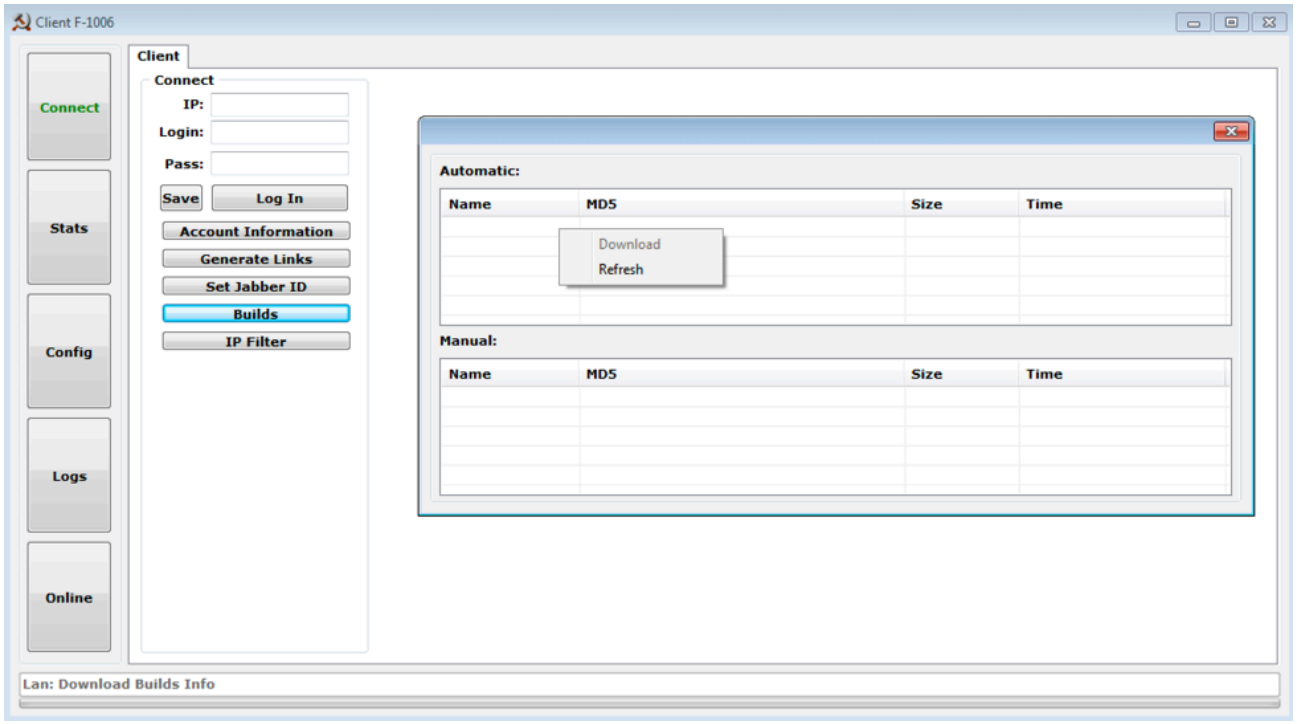

Figure 2: Control panel "Builds" button

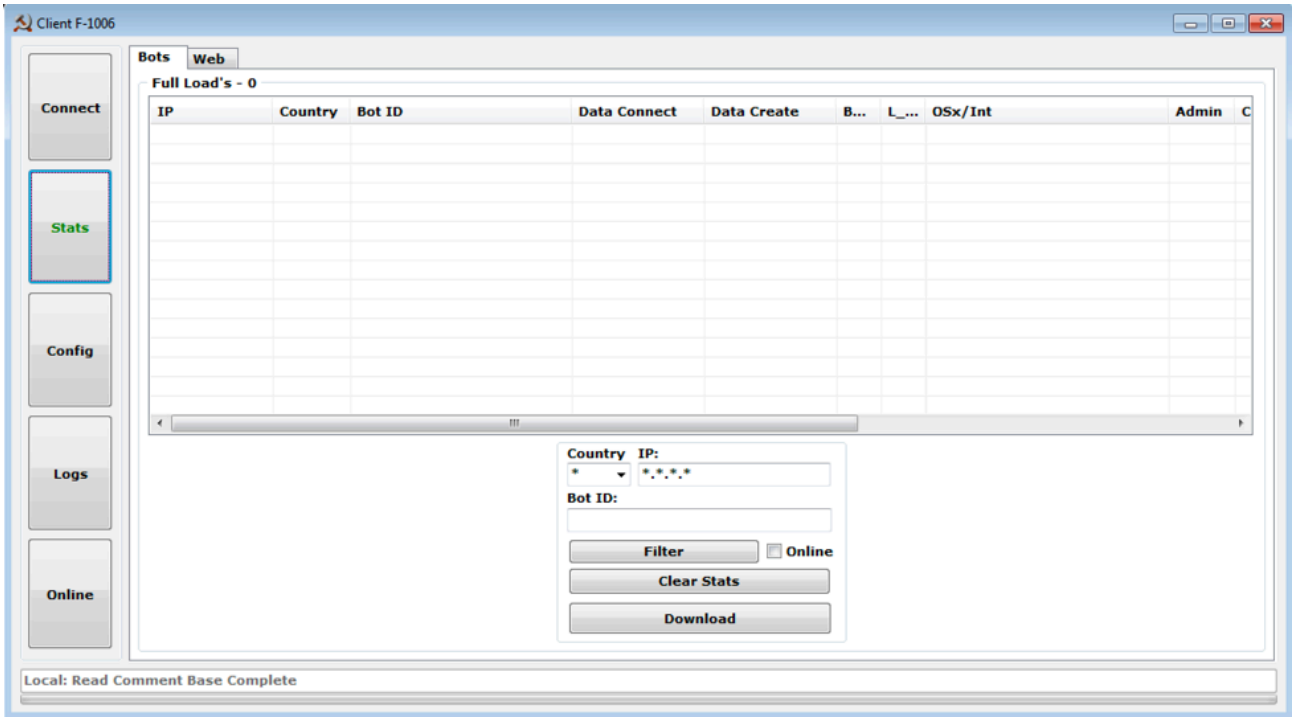

Figure 3: Control panel "Stats" tab

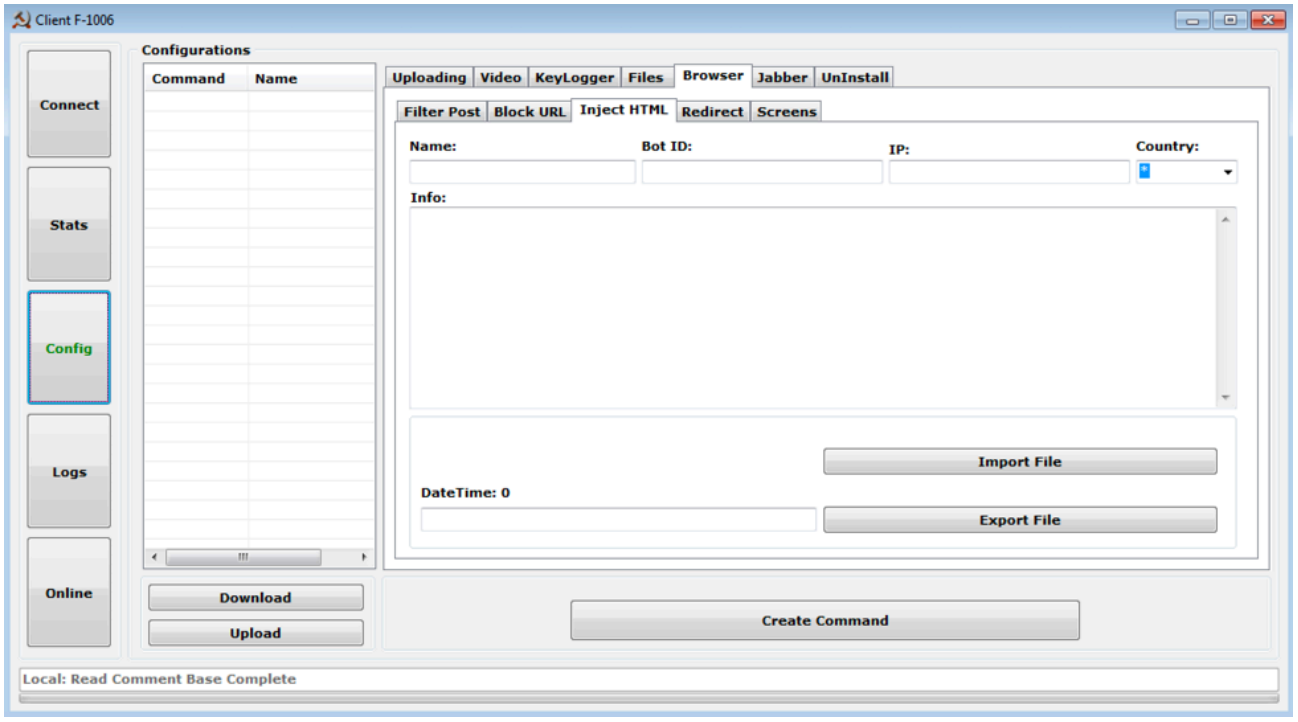

Figure 4: Control panel "Config" tab

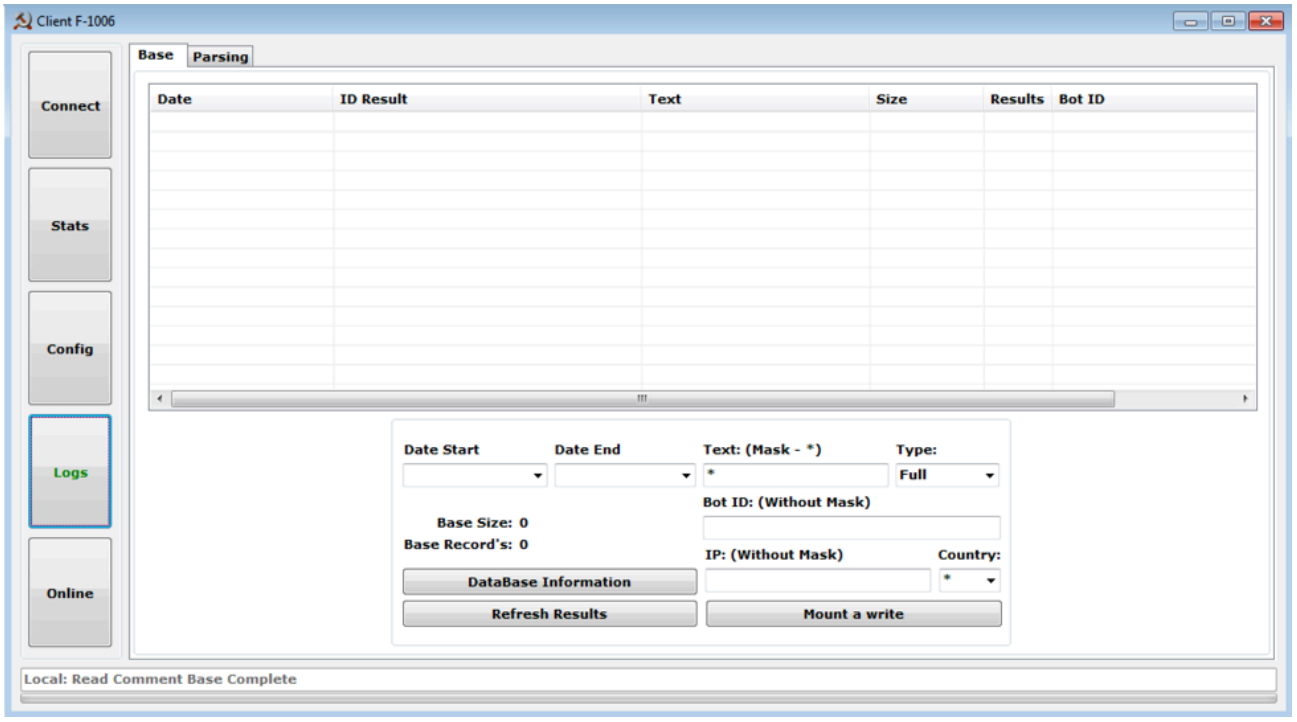

Figure 5: Control panel "Logs" tab

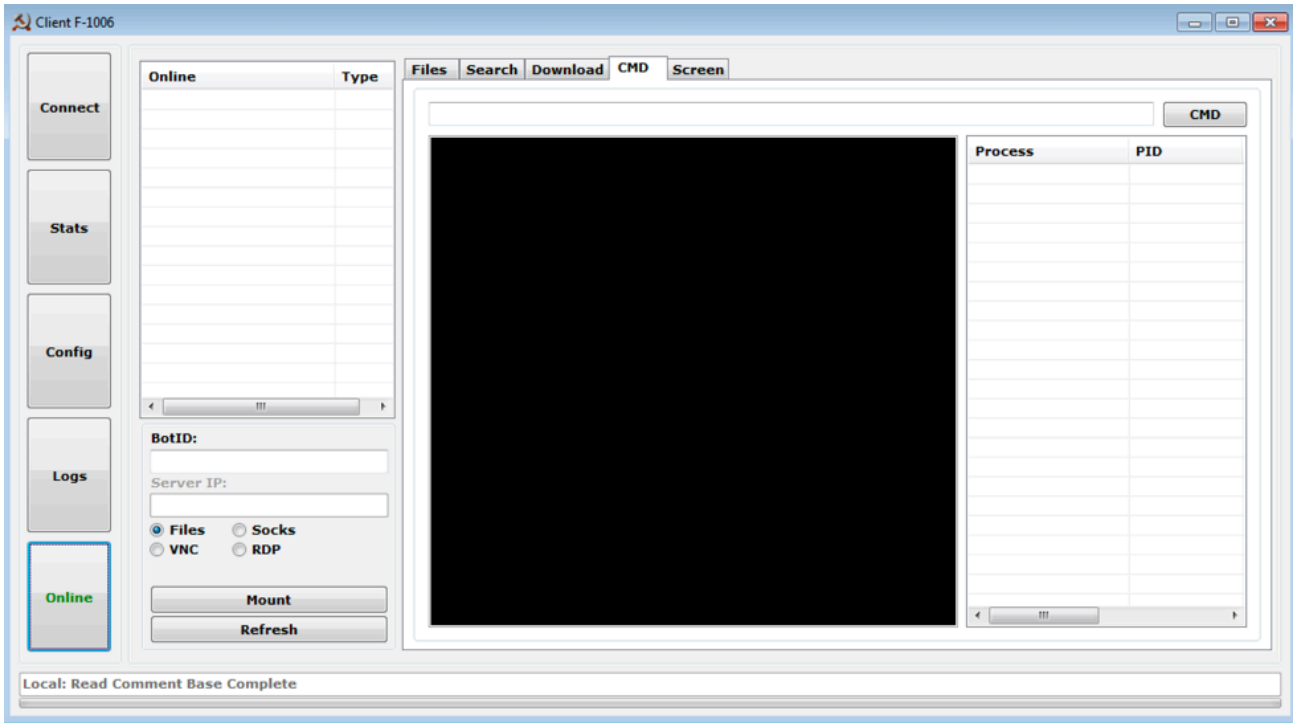

Figure 6: Control panel "Online" tab

Association with DanaBot Malware

In addition to finding the control panel application on infrastructure closely tied to DanaBot, two other significant pieces of evidence tie this control panel application to the DanaBot malware:

- C&C protocol overlap

- Shared RSA public key

In February 2019, a new version of the DanaBot malware was spotted in the wild that contained a new C&C protocol. ESET researchers were the first to notice the update and published a blog post [3] detailing the changes. Since then all of the DanaBot affiliates into which we have visibility have switched to this new version.

Using ESET's post as background, we can compare and contrast the network communications used in the control panel application (traffic generated when trying to login to a C&C server - Figure 7) and the C&C protocol used in the malware (initial beacon - Figure 8).

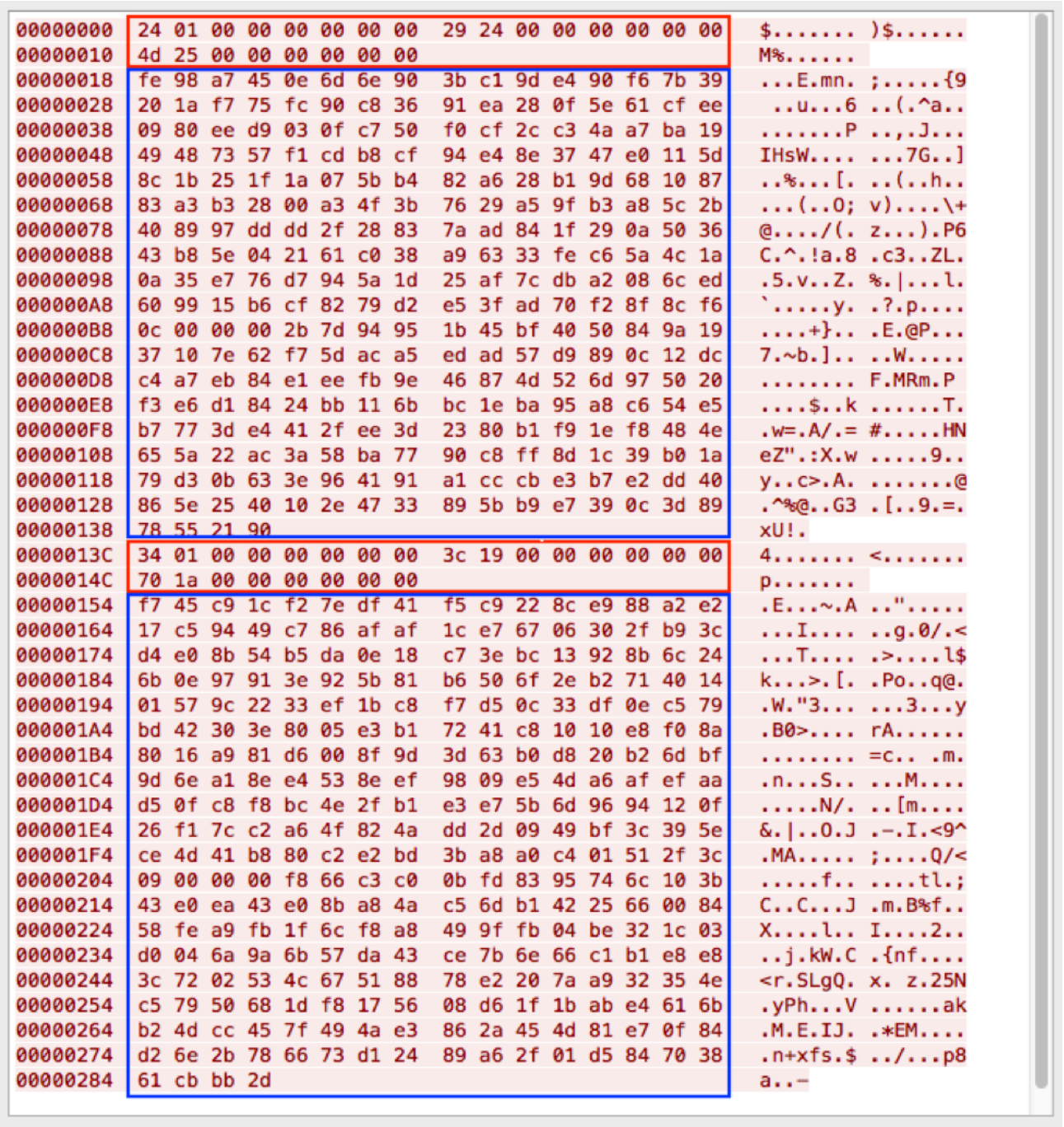

Figure 7: Control panel "login" request

Figure 8: DanaBot malware "initial beacon"

In both figures we can see two sets of communications each containing a 24-byte header (highlighted in red) followed by encrypted data (highlighted in blue).

The header contains:

- Offset 0x0: length of data (QWORD)
- Offset 0x8: random value (QWORD)
- Offset 0x10: random value + length of data (QWORD)

The encrypted data sections are composed of 3 pieces:

- AES-256 encrypted data using a randomly generated key
- Padding length (DWORD)
- The randomly generated AES key that has been RSA encrypted using an embedded RSA public key

In the first set of communications, the AES encrypted data contains a second RSA public key that is generated by the control panel application and malware. This second RSA key is used to decrypt data sent back from the C&C server.

The second set of communications contains the initial commands “login command” for the control panel application and “initial beacon” for the malware. Both commands use a 167-byte structure and share many common fields as shown in Table 1. Some fields that only appear to apply to the malware such as architecture and process integrity are set to zero in the control panel.

Field	**Control Panel Application**	**DanaBot Malware**
Length	167	167
Random value	8931	8499
Random value + length	9098	8666
Affiliate ID	0	5
Command	101	300
Argument	1006*	0
Random value 2	35786	14697
Unknown	0	0
Architecture	0	64
Windows version	0	610760110

Unknown	0	0
Is admin	0	1
Process integrity	0	12288
Unknown	0	1
Unknown	0	0
Username/archive key**	test_user	BB0B8678649F818C3A8F360098FD8874
Password/nonce 1***	test_pass	9AA088954D476D58590AC5B40543AF3C
nonce***/nonce 2***	701011CE5A3BBBC4A5901A19BF19A706	AF9DE6B708E347F5A8F77E2EAF29E75F

* Control panel version
** A key used to decrypt an archive of components sent from the C&C server to the malware
*** The malware and control panel use something we call “nonces”. They can also be considered a type of checksum. In general they are MD5 hash values of various fields and hard coded constants added together.

Table 1: Control panel “login” command vs. DanaBot malware “initial beacon” command

The second major feature that the control panel application and malware have in common is an embedded RSA public key used for encrypting AES session keys in the C&C protocol:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCyJo2aXOQNP+KeAnWlpOiuMk5W
l1An5GorPHqEyFAlRyv6sEylQDjAuSLGsy2LCvKmuzx2AFQ+3IMfqFf3JacY1HmY
WuiL1V+R910TohM+6hnLnWx7JNbfzB3S7D1JC/WNUwlVv5NnIIX1i+zIW5BTanU1
```

```
yQ97xjvokjvZHCHe2wIDAQAB
```

```
-----END PUBLIC KEY-----
```

This RSA public key has actually been used in all of the DanaBot malware samples we have observed since the upgrade in February. It is part of the reason we suspect that there is a single global C&C panel with which all affiliate malware communicates.

In addition to the overlapping C&C protocol and shared RSA key, the code in both the control panel and the malware share the same structure and style.

Conclusion

A stand-alone binary application through which affiliates access malware control panels is unusual, with malware developers generally opting for web-based control panels. Several factors, however, suggest that the application described here is used by DanaBot affiliates to build and configure their malware and then to access victim devices.

In either case, it is usually a careless OPSEC mistake by a threat actor or an intentional “leak” of the malware that exposes the control panel. Once exposed, however, they tend to provide useful insights into malware campaigns and a perspective usually hidden to defenders.

References

[1] https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0

[2] https://www.proofpoint.com/us/threat-insight/post/danabot-gains-popularity-and-targets-us-organizations-large-campaigns

[3] https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
d7ef48545457cbe791ed23c178551e4b17f0964a9e9ef7d0badda9f3e8c594f3	SHA256	DanaBot Control Panel
8327931a5d2430526862d789b9654c9c8da7bc64519d210a93e4720aac7ccaa0	SHA256	DanaBot Malware (Affiliate 5) used for comparison

---

Source: https://www.proofpoint.com/us/threat-insight/post/danabot-control-panel-revealed