DanaBot control panel revealed

proofpoint.com/us/threat-insight/post/danabot-control-panel-revealed

March 13, 2019

Blog
Threat Insight
DanaBot control panel revealed

March 13, 2019 Dennis Schwarz and Proofpoint Threat Insight Team

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.

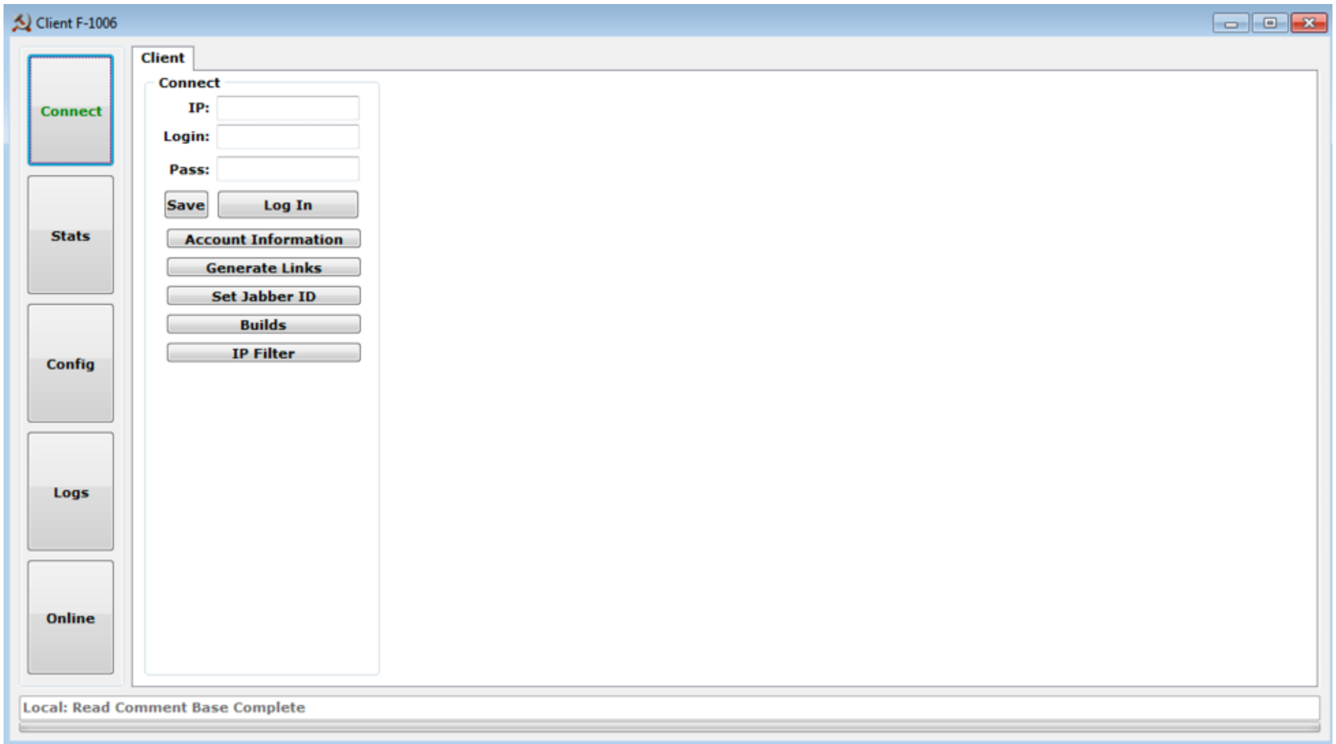
Control Panel Application

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.

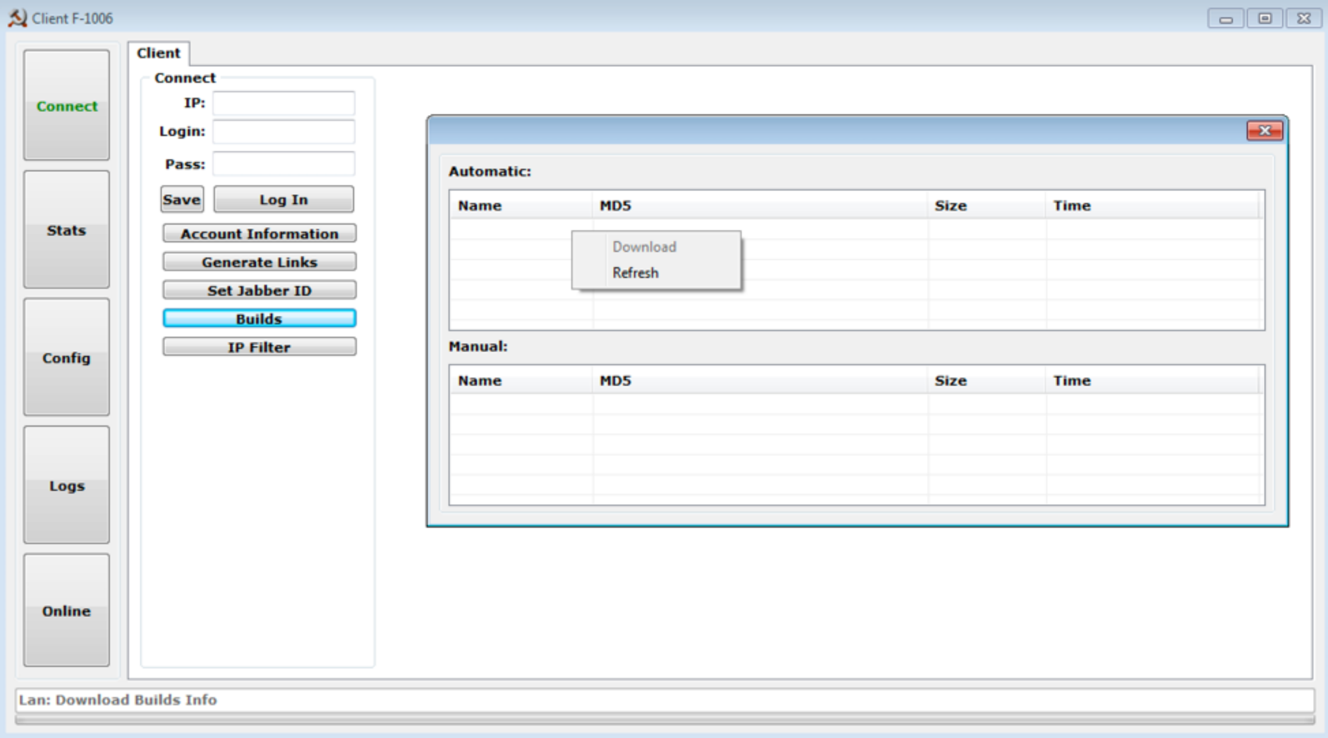
Figures 1 through 6 give a tour of the main components of the control panel. While a valid login is required to send and receive data to and from the backend C&C server, the figures still illustrate some of the potential actions a DanaBot affiliate can execute via the control panel:

- 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)



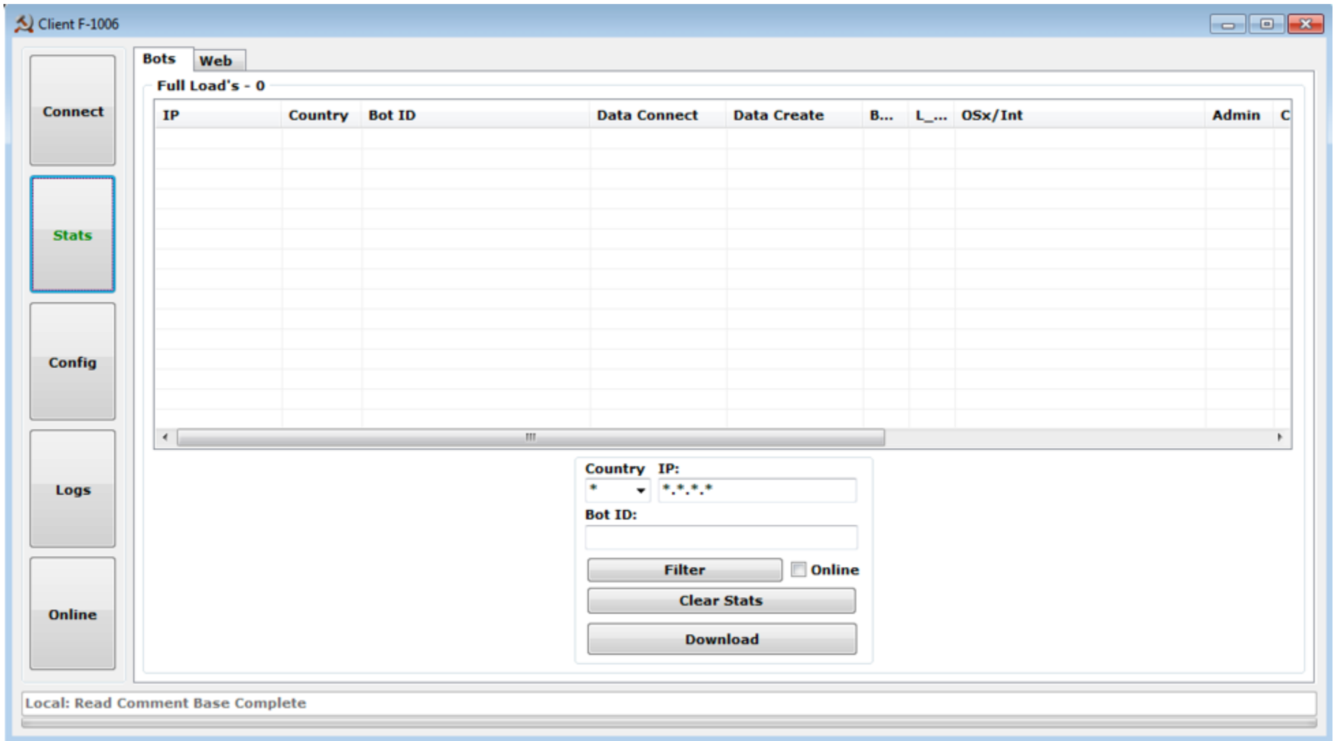
Local: Read Comment Base Complete

Figure 1: Control panel "Connect" tab



Lan: Download Builds Info

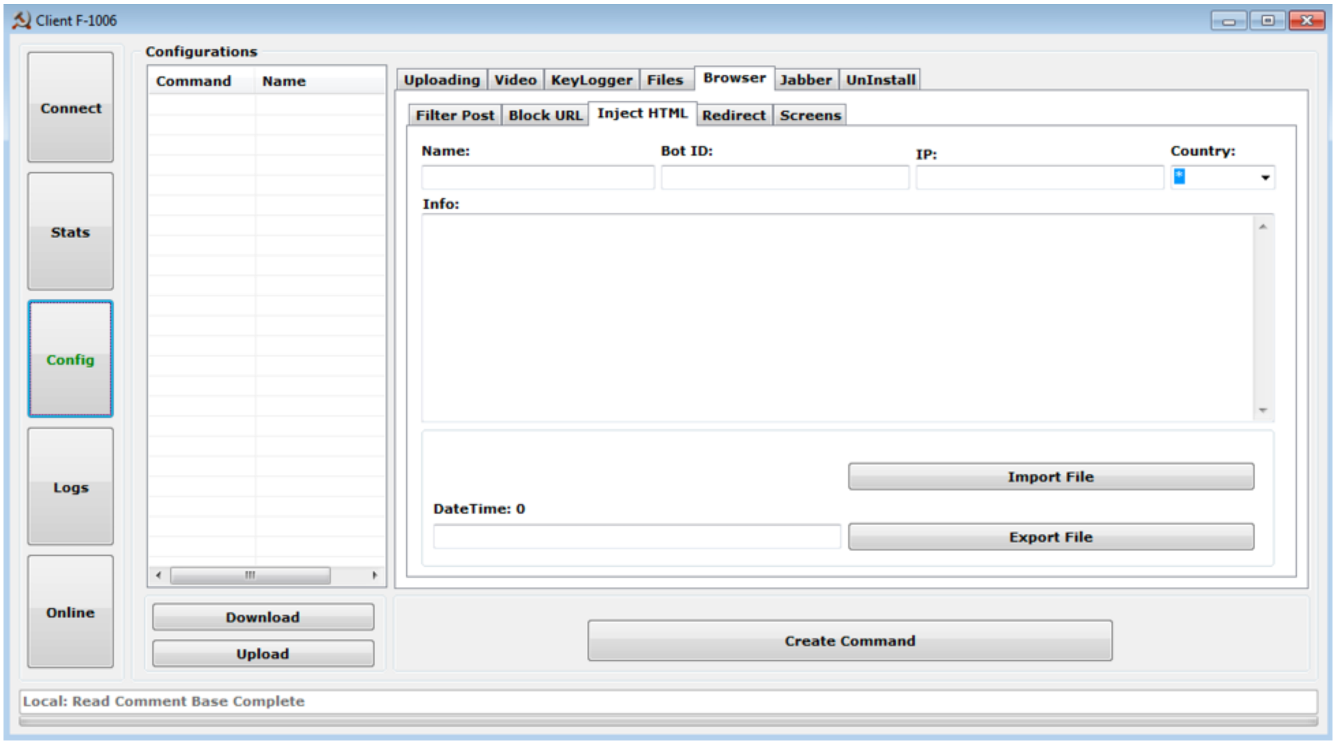
Figure 2: Control panel "Builds" button



Country: * IP: *.*.*.*

Local: Read Comment Base Complete

Figure 3: Control panel “Stats” tab

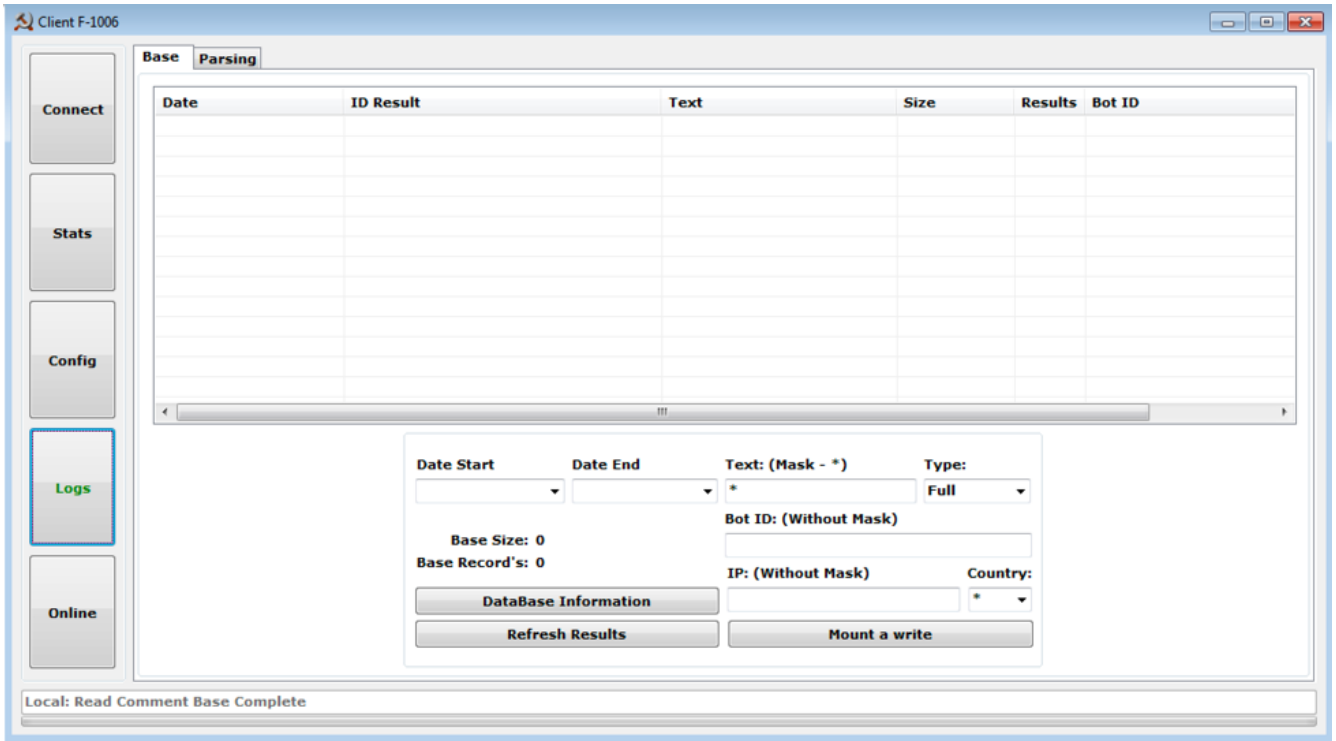


Country: *

DateTime: 0

Local: Read Comment Base Complete

Figure 4: Control panel “Config” tab



Text: (Mask - *) *

Type: Full

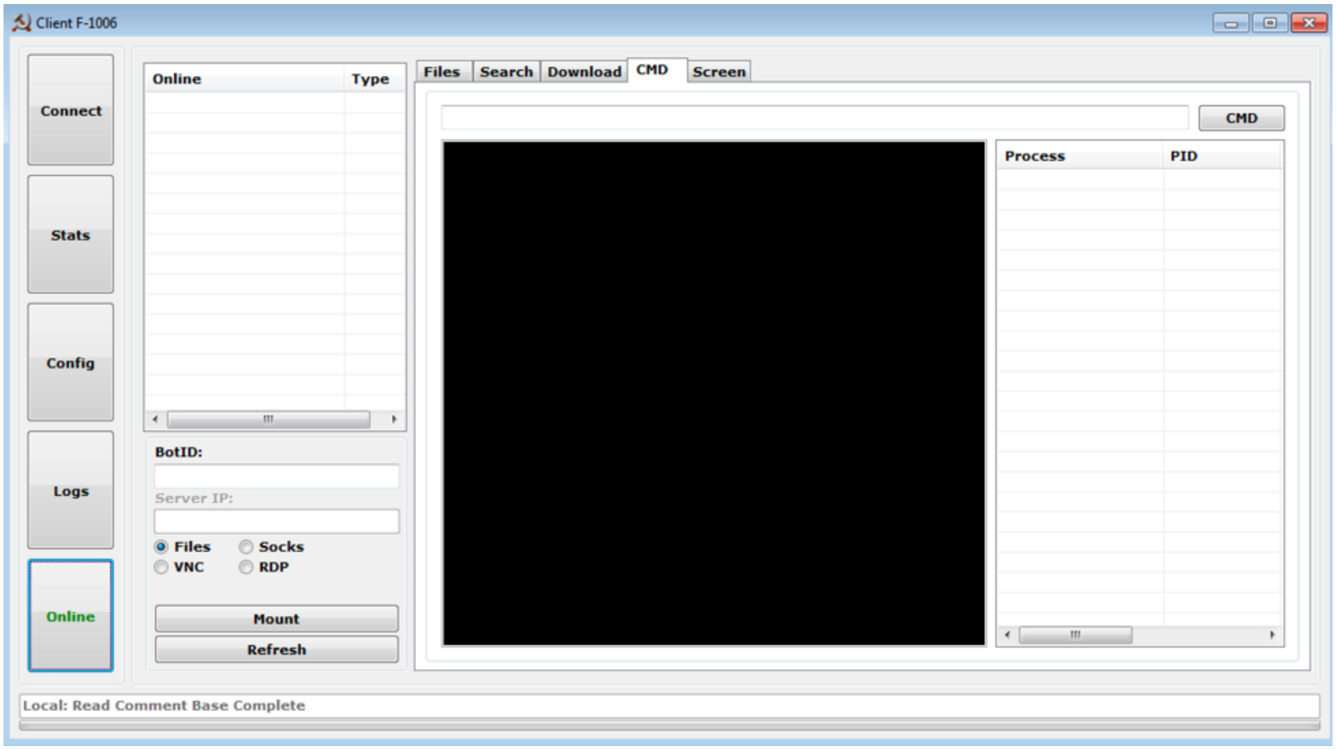
Base Size: 0

Base Record's: 0

Country: *

Local: Read Comment Base Complete

Figure 5: Control panel "Logs" tab



● Files ○ Socks
○ VNC ○ RDP

Local: Read Comment Base Complete

Figure 6: Control panel "Online" tab

Association with DanaBot Malware

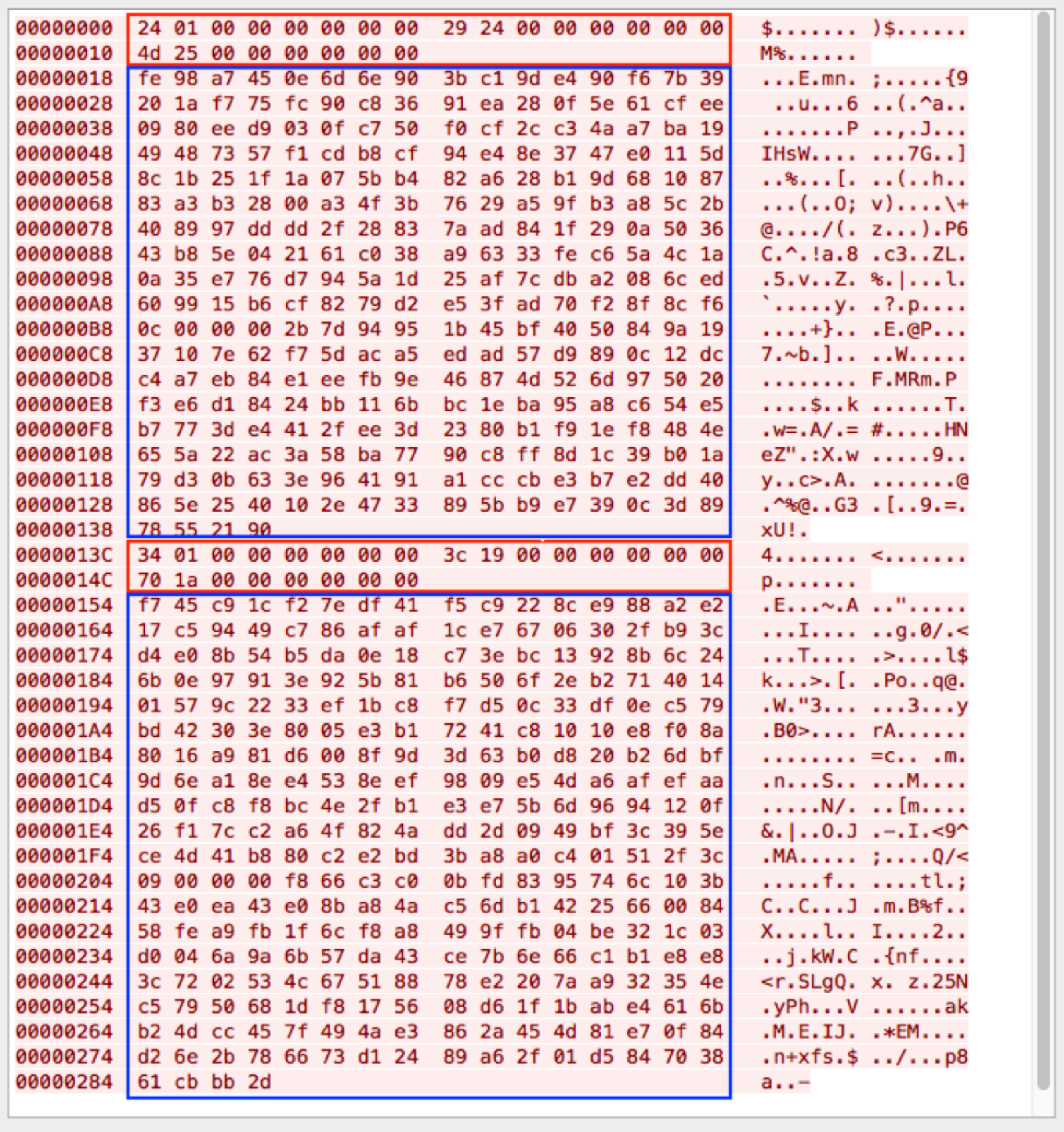
In addition to finding the control panel application on infrastructure closely tied to DanaBot, two other significant pieces of evidence tie this control panel application to the DanaBot malware:

- C&C protocol overlap

- Shared RSA public key

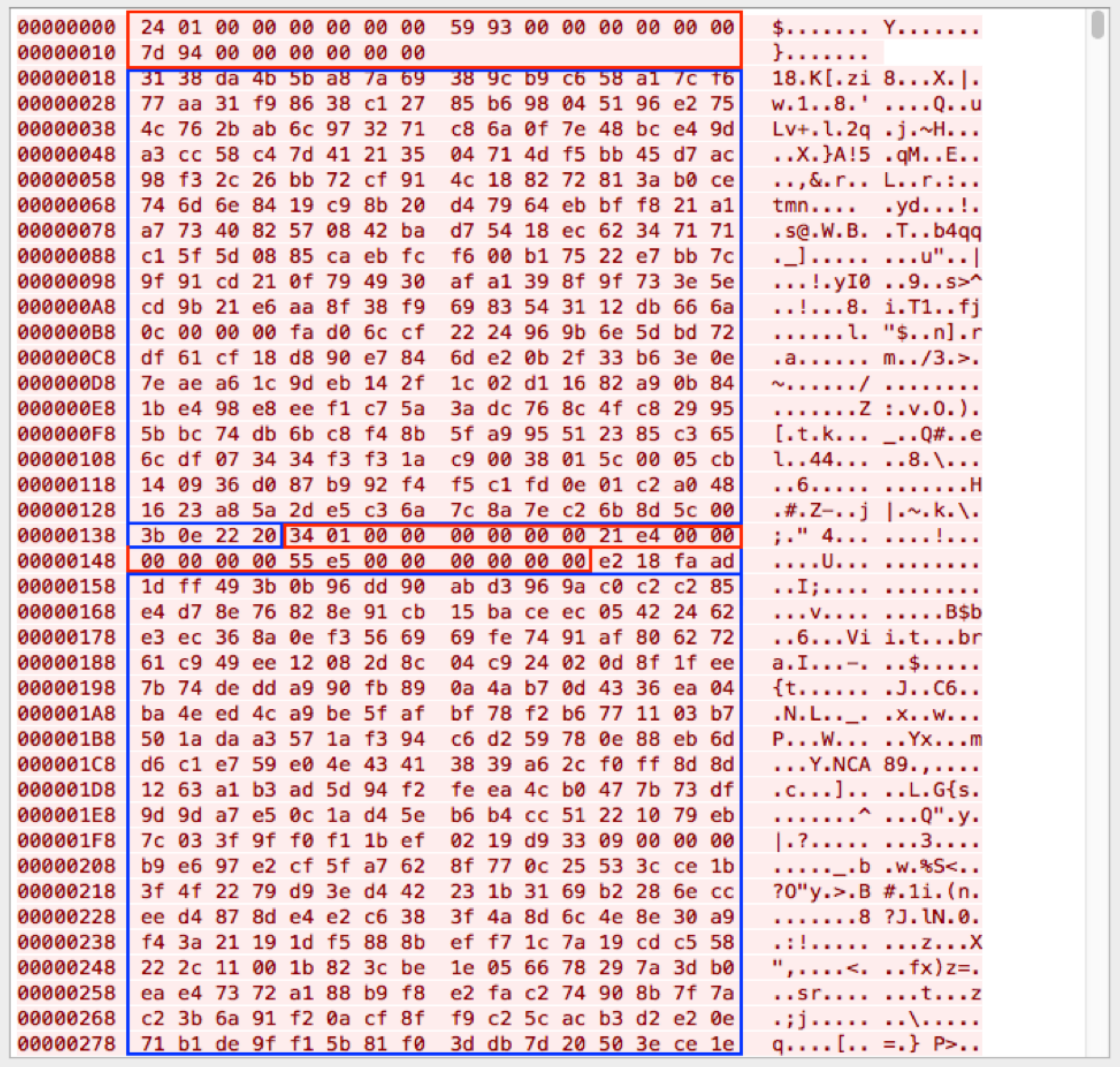
In February 2019, a new version of the DanaBot malware was spotted in the wild that contained a new C&C protocol. ESET researchers were the first to notice the update and published a blog post [3] detailing the changes. Since then all of the DanaBot affiliates into which we have visibility have switched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



```
00000000  24 01 00 00 00 00 00 00  29 24 00 00 00 00 00 00   $....... )$......
00000010  4d 25 00 00 00 00 00 00                            M%......
00000018  fe 98 a7 45 0e 6d 6e 90  3b c1 9d e4 90 f6 7b 39   ...E.mn. ;.....{9
00000028  20 1a f7 75 fc 90 c8 36  91 ea 28 0f 5e 61 cf ee    ..u...6 ..(.^a..
00000038  09 80 ee d9 03 0f c7 50  f0 cf 2c c3 4a a7 ba 19   .......P ..,.J...
00000048  49 48 73 57 f1 cd b8 cf  94 e4 8e 37 47 e0 11 5d   IHsW.... ...7G..]
00000058  8c 1b 25 1f 1a 07 5b b4  82 a6 28 b1 9d 68 10 87   ..%...[. ..(..h..
00000068  83 a3 b3 28 00 a3 4f 3b  76 29 a5 9f b3 a8 5c 2b   ...(..O; v)....\+
00000078  40 89 97 dd dd 2f 28 83  7a ad 84 1f 29 0a 50 36   @..../(. z...).P6
00000088  43 b8 5e 04 21 61 c0 38  a9 63 33 fe c6 5a 4c 1a   C.^.!a.8 .c3..ZL.
00000098  0a 35 e7 76 d7 94 5a 1d  25 af 7c db a2 08 6c ed   .5.v..Z. %.|...l.
000000A8  60 99 15 b6 cf 82 79 d2  e5 3f ad 70 f2 8f 8c f6   `.....y. .?.p....
000000B8  0c 00 00 00 2b 7d 94 95  1b 45 bf 40 50 84 9a 19   ....+}.. .E.@P...
000000C8  37 10 7e 62 f7 5d ac a5  ed ad 57 d9 89 0c 12 dc   7.~b.].. ..W.....
000000D8  c4 a7 eb 84 e1 ee fb 9e  46 87 4d 52 6d 97 50 20   ........ F.MRm.P 
000000E8  f3 e6 d1 84 24 bb 11 6b  bc 1e ba 95 a8 c6 54 e5   ....$..k ......T.
000000F8  b7 77 3d e4 41 2f ee 3d  23 80 b1 f9 1e f8 48 4e   .w=.A/.= #.....HN
00000108  65 5a 22 ac 3a 58 ba 77  90 c8 ff 8d 1c 39 b0 1a   eZ".:X.w .....9..
00000118  79 d3 0b 63 3e 96 41 91  a1 cc cb e3 b7 e2 dd 40   y..c>.A. .......@
00000128  86 5e 25 40 10 2e 47 33  89 5b b9 e7 39 0c 3d 89   .^%@..G3 .[..9.=.
00000138  78 55 21 90                                        xU!.
0000013C  34 01 00 00 00 00 00 00  3c 19 00 00 00 00 00 00   4....... <.......
0000014C  70 1a 00 00 00 00 00 00                            p.......
00000154  f7 45 c9 1c f2 7e df 41  f5 c9 22 8c e9 88 a2 e2   .E...~.A ..".....
00000164  17 c5 94 49 c7 86 af af  1c e7 67 06 30 2f b9 3c   ...I.... ..g.0/.<
00000174  d4 e0 8b 54 b5 da 0e 18  c7 3e bc 13 92 8b 6c 24   ...T.... .>....l$
00000184  6b 0e 97 91 3e 92 5b 81  b6 50 6f 2e b2 71 40 14   k...>.[. .Po..q@.
00000194  01 57 9c 22 33 ef 1b c8  f7 d5 0c 33 df 0e c5 79   .W."3... ...3...y
000001A4  bd 42 30 3e 80 05 e3 b1  72 41 c8 10 10 e8 f0 8a   .B0>.... rA......
000001B4  80 16 a9 81 d6 00 8f 9d  3d 63 b0 d8 20 b2 6d bf   ........ =c.. .m.
000001C4  9d 6e a1 8e e4 53 8e ef  98 09 e5 4d a6 af ef aa   .n...S.. ...M....
000001D4  d5 0f c8 f8 bc 4e 2f b1  e3 e7 5b 6d 96 94 12 0f   .....N/. ..[m....
000001E4  26 f1 7c c2 a6 4f 82 4a  dd 2d 09 49 bf 3c 39 5e   &.|..O.J .-.I.<9^
000001F4  ce 4d 41 b8 80 c2 e2 bd  3b a8 a0 c4 01 51 2f 3c   .MA..... ;....Q/<
00000204  09 00 00 00 f8 66 c3 c0  0b fd 83 95 74 6c 10 3b   .....f.. ....tl.;
00000214  43 e0 ea 43 e0 8b a8 4a  c5 6d b1 42 25 66 00 84   C..C...J .m.B%f..
00000224  58 fe a9 fb 1f 6c f8 a8  49 9f fb 04 be 32 1c 03   X....l.. I....2..
00000234  d0 04 6a 9a 6b 57 da 43  ce 7b 6e 66 c1 b1 e8 e8   ..j.kW.C .{nf....
00000244  3c 72 02 53 4c 67 51 88  78 e2 20 7a a9 32 35 4e   <r.SLgQ. x. z.25N
00000254  c5 79 50 68 1d f8 17 56  08 d6 1f 1b ab e4 61 6b   .yPh...V ......ak
00000264  b2 4d cc 45 7f 49 4a e3  86 2a 45 4d 81 e7 0f 84   .M.E.IJ. .*EM....
00000274  d2 6e 2b 78 66 73 d1 24  89 a6 2f 01 d5 84 70 38   .n+xfs.$ ../...p8
00000284  61 cb bb 2d                                        a..-
```

Figure 7: Control panel "login" request



```
00000000  24 01 00 00 00 00 00 00  59 93 00 00 00 00 00 00   $....... Y.......
00000010  7d 94 00 00 00 00 00 00                            }.......
00000018  31 38 da 4b 5b a8 7a 69  38 9c b9 c6 58 a1 7c f6   18.K[.zi 8...X.|.
00000028  77 aa 31 f9 86 38 c1 27  85 b6 98 04 51 96 e2 75   w.1..8.' ....Q..u
00000038  4c 76 2b ab 6c 97 32 71  c8 6a 0f 7e 48 bc e4 9d   Lv+.l.2q .j.~H...
00000048  a3 cc 58 c4 7d 41 21 35  04 71 4d f5 bb 45 d7 ac   ..X.}A!5 .qM..E..
00000058  98 f3 2c 26 bb 72 cf 91  4c 18 82 72 81 3a b0 ce   ..,&.r.. L..r.:..
00000068  74 6d 6e 84 19 c9 8b 20  d4 79 64 eb bf f8 21 a1   tmn....  .yd...!.
00000078  a7 73 40 82 57 08 42 ba  d7 54 18 ec 62 34 71 71   .s@.W.B. .T..b4qq
00000088  c1 5f 5d 08 85 ca eb fc  f6 00 b1 75 22 e7 bb 7c   ._]..... ...u"..|
00000098  9f 91 cd 21 0f 79 49 30  af a1 39 8f 9f 73 3e 5e   ...!.yI0 ..9..s>^
000000A8  cd 9b 21 e6 aa 8f 38 f9  69 83 54 31 12 db 66 6a   ..!...8. i.T1..fj
000000B8  0c 00 00 00 fa d0 6c cf  22 24 96 9b 6e 5d bd 72   ......l. "$..n].r
000000C8  df 61 cf 18 d8 90 e7 84  6d e2 0b 2f 33 b6 3e 0e   .a...... m../3.>.
000000D8  7e ae a6 1c 9d eb 14 2f  1c 02 d1 16 82 a9 0b 84   ~....../ ........
000000E8  1b e4 98 e8 ee f1 c7 5a  3a dc 76 8c 4f c8 29 95   .......Z :.v.O.).
000000F8  5b bc 74 db 6b c8 f4 8b  5f a9 95 51 23 85 c3 65   [.t.k... _..Q#..e
00000108  6c df 07 34 34 f3 f3 1a  c9 00 38 01 5c 00 05 cb   l..44... ..8.\...
00000118  14 09 36 d0 87 b9 92 f4  f5 c1 fd 0e 01 c2 a0 48   ..6..... .......H
00000128  16 23 a8 5a 2d e5 c3 6a  7c 8a 7e c2 6b 8d 5c 00   .#.Z-..j |.~.k.\.
00000138  3b 0e 22 20 34 01 00 00  00 00 00 00 21 e4 00 00   ;." 4... ....!...
00000148  00 00 00 00 55 e5 00 00  00 00 00 00 e2 18 fa ad   ....U... ........
00000158  1d ff 49 3b 0b 96 dd 90  ab d3 96 9a c0 c2 c2 85   ..I;.... ........
00000168  e4 d7 8e 76 82 8e 91 cb  15 ba ce ec 05 42 24 62   ...v.... .....B$b
00000178  e3 ec 36 8a 0e f3 56 69  69 fe 74 91 af 80 62 72   ..6...Vi i.t...br
00000188  61 c9 49 ee 12 08 2d 8c  04 c9 24 02 0d 8f 1f ee   a.I...-. ..$.....
00000198  7b 74 de dd a9 90 fb 89  0a 4a b7 0d 43 36 ea 04   {t...... .J..C6..
000001A8  ba 4e ed 4c a9 be 5f af  bf 78 f2 b6 77 11 03 b7   .N.L.._. .x..w...
000001B8  50 1a da a3 57 1a f3 94  c6 d2 59 78 0e 88 eb 6d   P...W... ..Yx...m
000001C8  d6 c1 e7 59 e0 4e 43 41  38 39 a6 2c f0 ff 8d 8d   ...Y.NCA 89.,....
000001D8  12 63 a1 b3 ad 5d 94 f2  fe ea 4c b0 47 7b 73 df   .c...].. ..L.G{s.
000001E8  9d 9d a7 e5 0c 1a d4 5e  b6 b4 cc 51 22 10 79 eb   .......^ ...Q".y.
000001F8  7c 03 3f 9f f0 f1 1b ef  02 19 d9 33 09 00 00 00   |.?..... ...3....
00000208  b9 e6 97 e2 cf 5f a7 62  8f 77 0c 25 53 3c ce 1b   ....._.b .w.%S<..
00000218  3f 4f 22 79 d9 3e d4 42  23 1b 31 69 b2 28 6e cc   ?O"y.>.B #.1i.(n.
00000228  ee d4 87 8d e4 e2 c6 38  3f 4a 8d 6c 4e 8e 30 a9   .......8 ?J.lN.0.
00000238  f4 3a 21 19 1d f5 88 8b  ef f7 1c 7a 19 cd c5 58   .:!..... ...z...X
00000248  22 2c 11 00 1b 82 3c be  1e 05 66 78 29 7a 3d b0   ",....<. ..fx)z=.
00000258  ea e4 73 72 a1 88 b9 f8  e2 fa c2 74 90 8b 7f 7a   ..sr.... ...t...z
00000268  c2 3b 6a 91 f2 0a cf 8f  f9 c2 5c ac b3 d2 e2 0e   .;j..... ..\.....
00000278  71 b1 de 9f f1 5b 81 f0  3d db 7d 20 50 3e ce 1e   q....[.. =.} P>..
```

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

Subscribe to the Proofpoint Blog