DanaBot updated with new C&C communication

welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/

February 7, 2019

ESET researchers have discovered new versions of the DanaBot Trojan, updated with a more complicated protocol for C&C communication and slight modifications to architecture and campaign IDs

ESET Research
7 Feb 2019 - 12:00PM

ESET researchers have discovered new versions of the DanaBot Trojan, updated with a more complicated protocol for C&C communication and slight modifications to architecture and campaign IDs

The fast-evolving, modular Trojan DanaBot has undergone further changes, with the latest version featuring an entirely new communication protocol. The protocol, introduced to DanaBot at the end of January 2019, adds several layers of encryption to DanaBot's C&C communication.

Besides the changes in communication, DanaBot's architecture and campaign IDs have also been modified.

The evolution of DanaBot

After being discovered in May 2018 as part of Australia-targeted spam campaigns, DanaBot has had an eventful time since, appearing in malspam campaigns in Poland, Italy, Germany, Austria and Ukraine, as well as in the United States. The European campaigns have seen the Trojan expanding its capabilities with new plugins and spam-sending features.

In ESET telemetry on January 25, 2019, we noticed unusual DanaBot-related executables. Upon further inspection, these binaries were, indeed, revealed to be DanaBot variants, but using a different communication protocol to communicate with the C&C server. Starting January 26, 2019, DanaBot operators stopped building binaries with the old protocol.

At the time of writing, the new version is being distributed under two scenarios:

- As “updates” delivered to existing DanaBot victims
- Via malspam in Poland

The new communication protocol

In the communication protocol used before January 25, packets were not encrypted in any way, as seen in Figure 1.

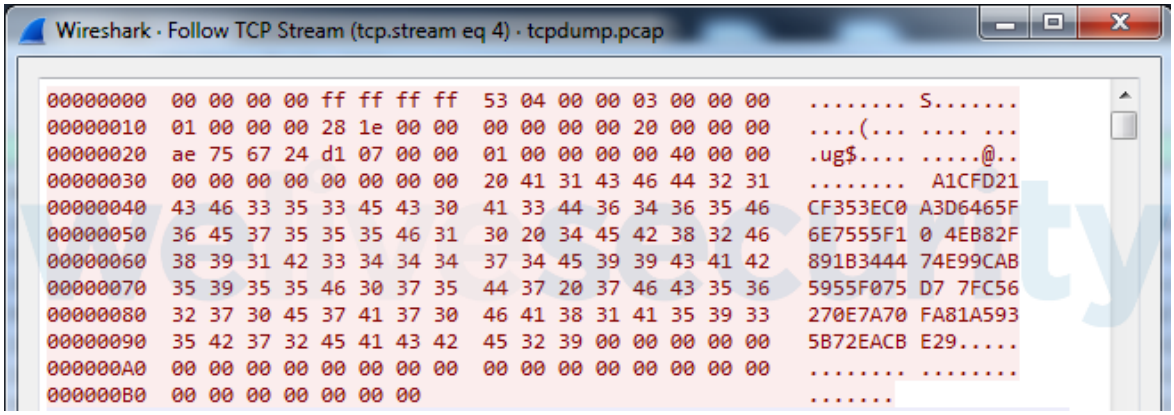

Figure 1 – Packet capture showing the old protocol with data in plaintext

Following the latest changes, DanaBot uses the AES and RSA encryption algorithms in its C&C communication. The new communication protocol is complicated, with several encryption layers being used, as seen in Figure 2.

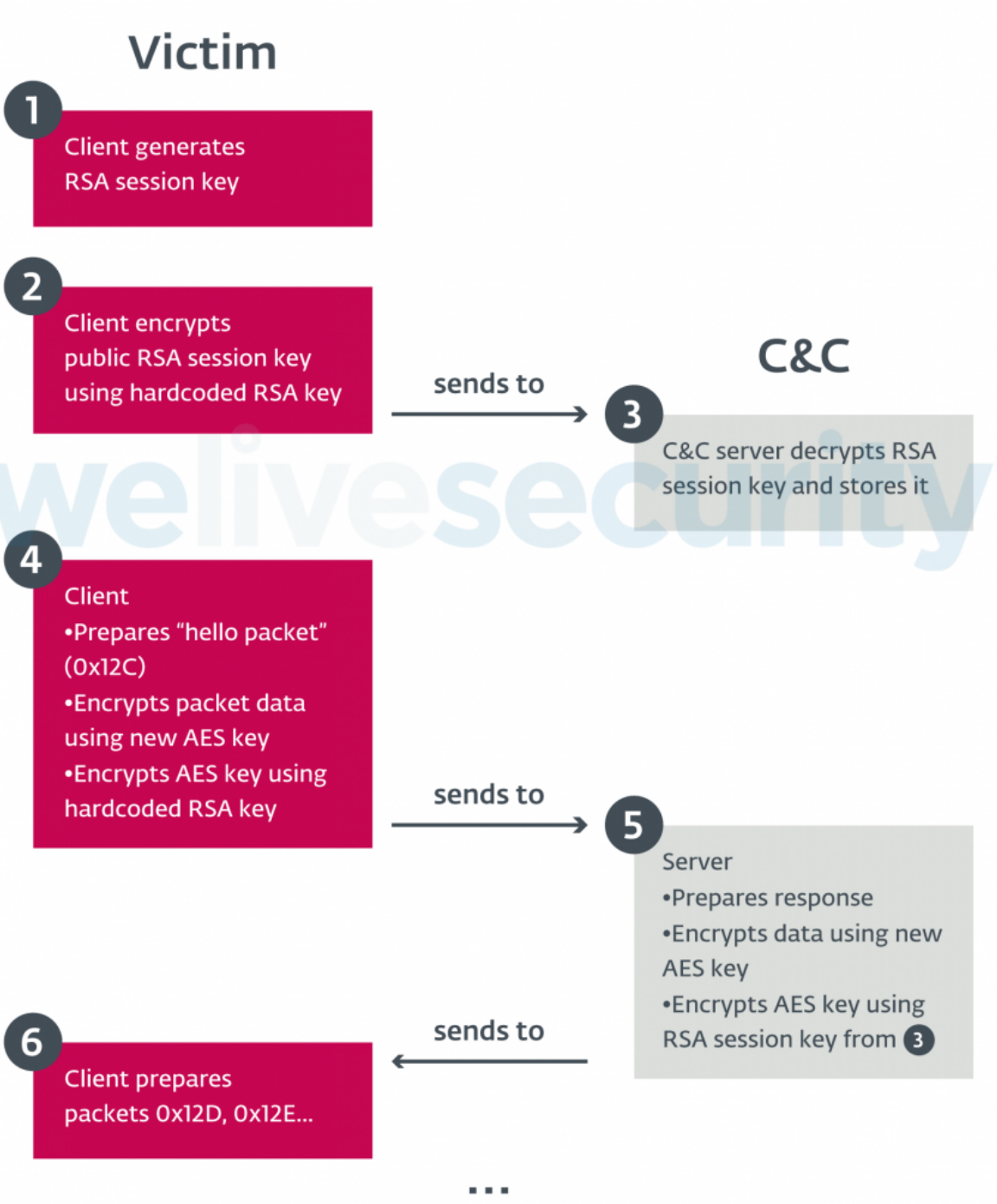

Figure 2 – A diagram of DanaBot's new communication protocol

These changes break existing network-based signatures and make it more difficult to write new rules for Intrusion Detection and Prevention Systems. Also, without access to the corresponding RSA keys, it is impossible to decode sent or received packets; thus PCAP files from cloud-based analysis systems (such as ANY.RUN) become unusable for researchers.

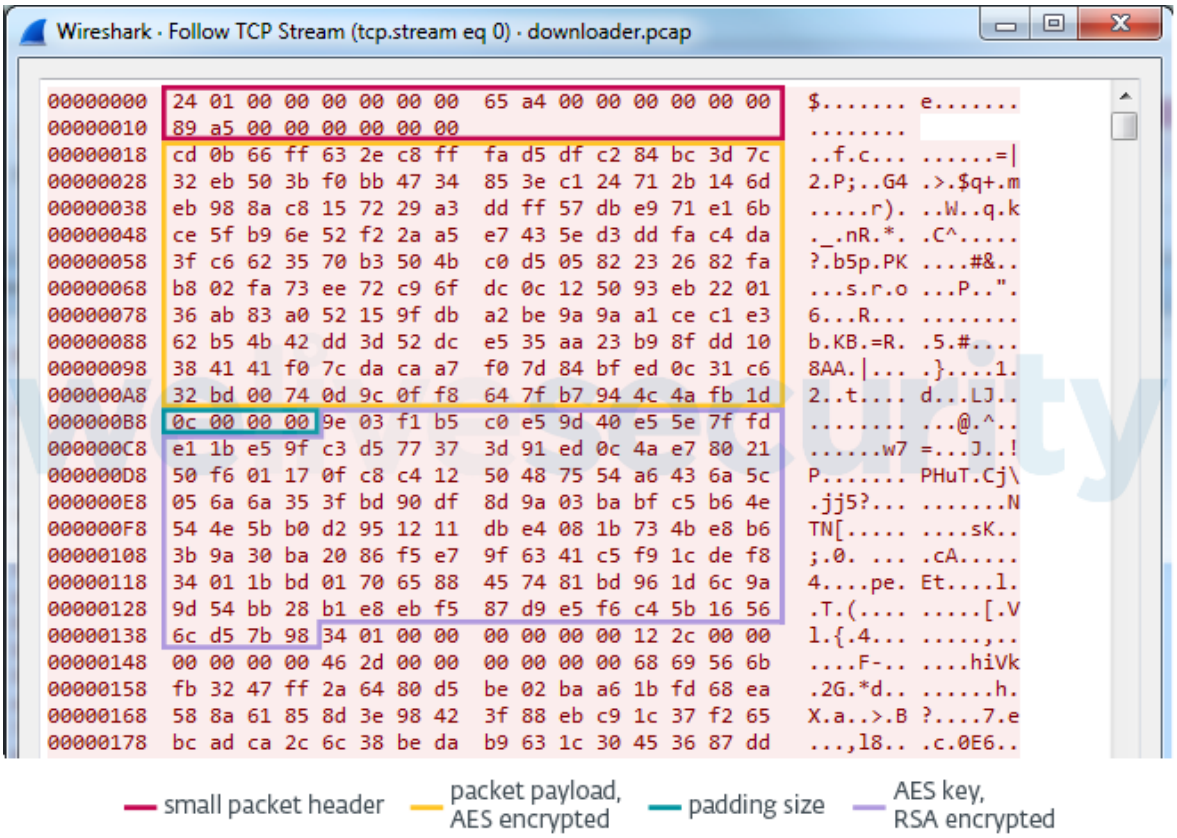

Figure 3 – Packet capture with the new communication protocol in place

Each packet sent by the client has a 24 (0x18)-byte header:

Offset	Size (bytes)	Meaning
0x0	0x8	Size of the data after this header
0x8	0x8	Random value
0x10	0x8	Sum of first two fields

For each packet, the header is followed by AES-encrypted packet data, then a 4-byte value indicating AES padding size, and finally the RSA-encrypted AES key. Each packet is encrypted with a different AES key.

Server responses use the same format. Unlike in previous versions, packet data in server responses does not follow any specific layout (with some exceptions).

Packet data layout

Former packet data layout was detailed by Proofpoint in October 2018. In the latest version of DanaBot, the layout is slightly modified, as seen in Figure 4.

Previous layout

Offset	Size (bytes)	Meaning
0x0	0x4	Random values (stack junk)
0x4	0x4	Hardcoded -1
0x8	0x4	Command ID
0xC	0x4	Campaign ID
0x10	0x4	Hardcoded 1
0x14	0x4	Random value
0x18	0x4	Unknown counter variable
0x1C	0x4	System architecture
0x20	0x4	Windows version information
0x24	0x4	Command parameter (0/32/64)
0x28	0x4	Admin status
0x2C	0x4	Process integrity level
0x30	0x8	Payload length
0x38	0x21	Client ID
0x59	0x21	Command dependent
0x7A	0x21	Checksum
0x9B	0x1C	Junk

New layout

Offset	Size (bytes)	Meaning
0x0	0x4	Size of the packet header (0xA7)
0x4	0x8	Random value
0xC	0x8	Sum of first 2 fields
0x14	0x4	Campaign ID
0x18	0x4	Command ID
0x1C	0x4	Command parameter (0/32/64)
0x20	0x4	Random value
0x24	0x4	Unknown counter variable
0x28	0x4	System architecture
0x2C	0x4	Windows version information
0x30	0x4	Command dependent (0/0x3E9)
0x34	0x4	Admin status
0x38	0x4	Process integrity level
0x3C	0x8	Payload length
0x44	0x21	Client ID
0x65	0x21	Command dependent
0x86	0x21	Checksum

Legend:
different field
same field in a different position
same field in the same position

Figure 4 – Comparison of packet data layout in DanaBot's previous and latest version

Changes in DanaBot architecture

Besides the changed communication protocol, DanaBot has also undergone some changes in architecture. The previous versions of DanaBot included a component that downloaded and executed the main module. The main module then downloaded and executed plugins and configurations.

The latest version shifts both these responsibilities to a new loader component, which is used to download all plugins along with the main module. Persistence is achieved by registering the loader component as a service.

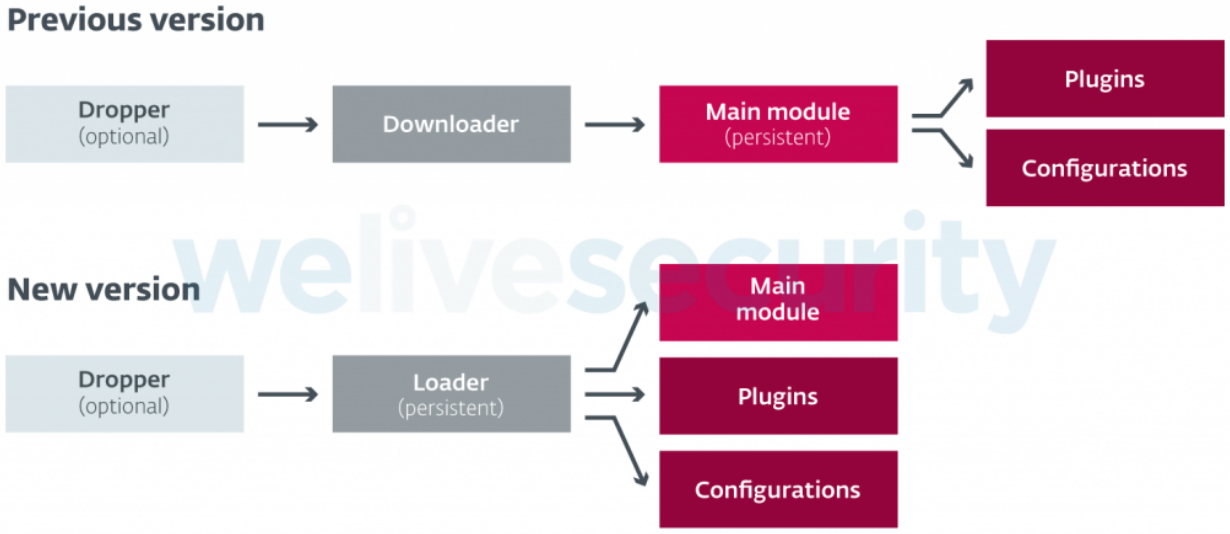

Figure 5 – Comparison of architecture in DanaBot's previous and latest version

Commands

According to our analysis, the loader component uses the following commands:

- 0x12C – Hello. First command sent by client to server
- 0x12D – Download 32/64-bit launcher component
- 0x12E – Request list of plugins and configuration files
- 0x12F – Download plugin/configuration files

Downloaded plugins and configuration files are encrypted using an AES key derived from the Client ID. In addition to that, plugins are compressed in ZIP format using LZMA compression, whereas configuration files are compressed using zlib.

Commands with ID numbers 0x130 – 0x134 are sent by the main module:

- 0x130 – Upload collected information to C&C server (e.g., screenshot of a victim's computer; system information)
- 0x131 – Upload collected information to C&C server (e.g., list of files on the victim's hard disk)
- 0x132 – Ask C&C server for further commands; there are around 30 available commands typical of backdoors, including launching plugins, gathering detailed system information and modifying files on client system
- 0x133 – Update C&C server list via Tor proxy
- 0x134 – Exact purpose unknown; most likely used for communication between plugins and C&C

Changes in campaign IDs

Previous research has suggested that DanaBot is distributed under various "affiliate" or "campaign" IDs.

In the previous version of DanaBot, almost 20 different campaign IDs were used. In the latest version, campaign IDs have changed slightly. As of February 5, 2019, we are seeing the following IDs in the wild:

- **ID=2** appears to be a test version, serving a limited number of configuration files and no webinjects
- **ID=3** is being actively spread, targeting users in both Poland and Italy, serving all configuration files and webinjects for both Polish and Italian targets
- **ID=5** serves configuration files for Australian targets
- **ID=7** is being spread only in Poland, serving webinjects for Polish targets
- **ID=9** appears to be another test version, with limited spread and no specific targeting, serving a limited number of configuration files and no webinjects

Conclusion

In 2018, we observed DanaBot expanding in both distribution and functionality. The beginning of 2019 has seen the Trojan undergo "internal" changes, indicating active development by its authors. The latest updates suggest the authors are making an effort to evade detection at the network level, and possibly paying attention to published research and making changes to stay ahead of defenders.

ESET systems detect and block all DanaBot components and plugins under detection names listed in the IoCs section.

This research was carried out by Kaspars Osis, Tomáš Procházka and Michal Kolář.

Indicators of Compromise (IoCs)

C&C servers used by the new version of DanaBot

- 84.54.37[.]102
- 89.144.25[.]243
- 89.144.25[.]104
- 178.209.51[.]211
- 185.92.222[.]238
- 192.71.249[.]51

Webinject and redirect servers

- 47.74.249[.]106
- 95.179.227[.]160
- 185.158.249[.]144

Example hashes

Note that since new builds of DanaBot's components are released regularly, we provide just a sampling of hashes.

Component	SHA-1	ESET detection name
Dropper	98C70361EA611BA33EE3A79816A88B2500ED7844	Win32/TrojanDropper.Danabot.O
Loader (x86), campaign ID=3	0DF17562844B7A0A0170C9830921C3442D59C73C	Win32/Spy.Danabot.L
Loader (x64), campaign ID=3	B816E90E9B71C85539EA3BB897E4F234A0422F85	Win64/Spy.Danabot.G
Loader (x86), campaign ID=9	5F085B19657D2511A89F3172B7887CE29FC70792	Win32/Spy.Danabot.I
Loader (x64), campaign ID=9	4075375A08273E65C223116ECD2CEF903BA97B1E	Win64/Spy.Danabot.F
Main module (x86)	28139782562B0E4CAB7F7885ECA75DFCA5E1D570	Win32/Spy.Danabot.K
Main module (x64)	B1FF7285B49F36FE8D65E7B896FCCDB1618EAA4B	Win64/Spy.Danabot.C

Plugins

Plugin	SHA-1	ESET detection name
RDPWrap	890B5473B419057F89802E0B6DA011B315F3EF94	Win32/Spy.Danabot.H
Stealer (x86)	E50A03D12DDAC6EA626718286650B9BB858B2E69	Win32/Spy.Danabot.C
Stealer (x64)	9B0EC454401023DF6D3D4903735301BA669AADD1	Win64/Spy.Danabot.E
Sniffer	DBFD8553C66275694FC4B32F9DF16ADEA74145E6	Win32/Spy.Danabot.B
VNC	E0880DCFCB1724790DFEB7DFE01A5D54B33D80B6	Win32/Spy.Danabot.D
TOR	73A5B0BEE8C9FB4703A206608ED277A06AA1E384	Win32/Spy.Danabot.G

7 Feb 2019 - 12:00PM