DanaBot тепер використовує новий протокол з’єднання з C&C

ESET НАСОЛОДЖУЙСЯ БЕЗПЕКОЮ

Дослідники ESET виявили нові версії троянської програми DanaBot з більш складним протоколом для зв'язку з командним сервером (C&C) та незначними змінами в архітектурі та ідентифікаторах (ID) кампанії.

Модульний троян DanaBot продовжує вдосконалюватися. Зокрема в останній версії модульного трояна використовується абсолютно новий протокол з'єднання. Протокол, застосований наприкінці січня 2019 року, додає декілька рівнів шифрування до з'єднання DanaBot із командним сервером.

Крім цього, у новій версії змінено архітектуру DanaBot та ідентифікатори кампанії.

Еволюція DanaBot

Після виявлення в травні 2018 року в рамках спам-кампаній, спрямованих на Австралію, троян DanaBot почав поширюватися в Польщі, Італії, Німеччині, Австрії та Україні, а також у США. У європейських кампаніях DanaBot розширює свої можливості за допомогою нових модулів і функцій для поширення спаму.

За результатами аналізу даних телеметрії 25 січня 2019 року спеціалісти ESET зафіксували незвичайні виконувані файли, пов'язані з DanaBot. Після подальшої перевірки ці бінарні файли, дійсно, виявилися варіантами DanaBot, однак вони використовують інший протокол для зв'язку з командним сервером. Із 26 січня 2019 року оператори DanaBot припинили створювати бінарні файли з старим протоколом.

На момент написання матеріалу нова версія розповсюджується за двома сценаріями:

1. Як «оновлення», які застосовуються уже існуючим жертвам DanaBot
2. Через поширення шкідливого спаму у Польщі

Новий протокол з'єднання

У протоколі з'єднання, який використовувався до 25 січня, пакети не були зашифровані жодним способом, як показано на Рис. 1.

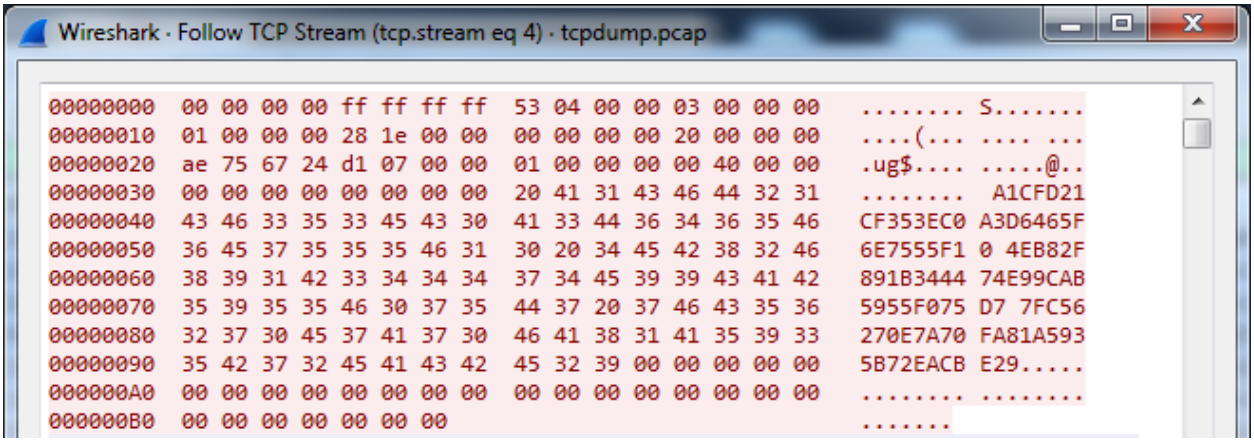

Рис. 1 – Старий протокол із даними у відкритому тексті

Після останніх змін DanaBot використовує алгоритми шифрування AES та RSA у своєму з’єднанні з командним сервером. Новий протокол з'єднання є достатньо складним та володіє кількома рівнями шифрування, як показано на Рис. 2.

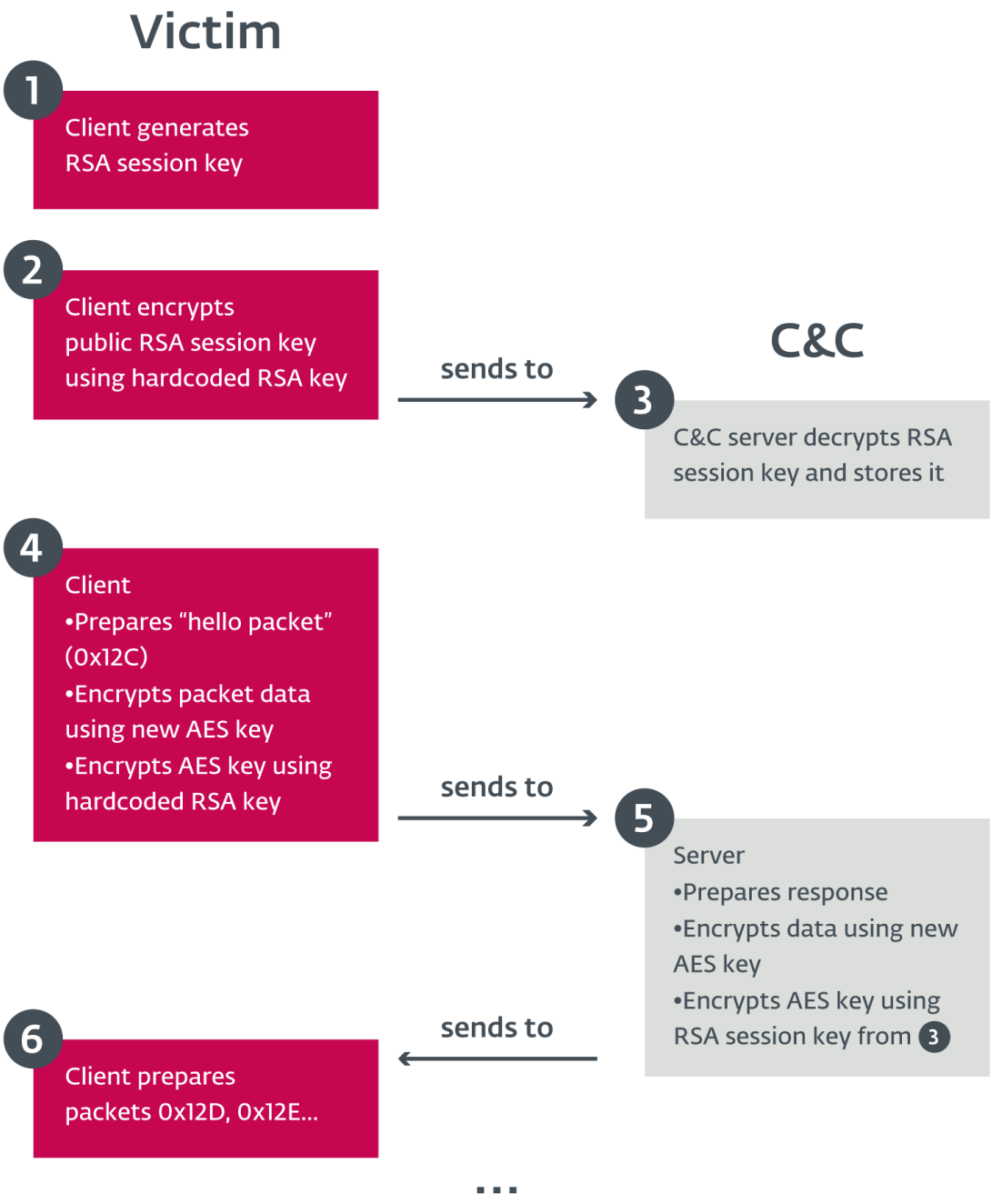

Рис. 2 – Новий протокол з’єднання DanaBot

Ці зміни порушують існуючі підписи на основі мережі і ускладнюють написання нових правил для систем виявлення та запобігання вторгнень. Також, без доступу до відповідних ключів RSA, неможливо декодувати відправлені або прийняті пакети; таким чином, файли PCAP із систем на основі хмарного аналізу (наприклад, ANY.RUN) стають непридатними для дослідників.

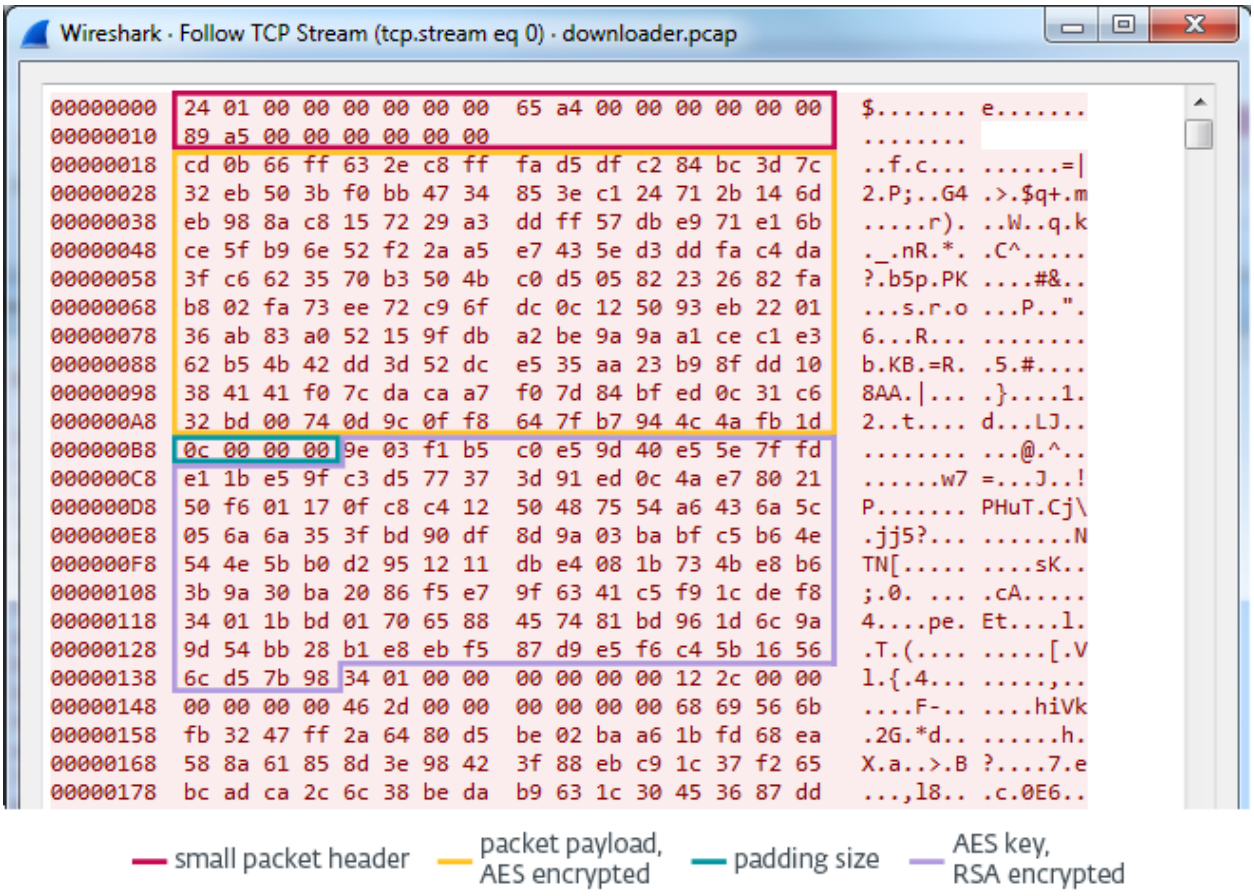

Рис. 3 – Пакет з новим протоколом з'єднання

Кожен пакет, надісланий клієнтом, має 24 (0x18)-байтовий заголовок:

Зміщення	**Розмір (байти)**	**Значення**
0x0	0x8	Розмір даних після цього заголовка
0x8	0x8	Випадкове значення
0x10	0x8	Сума перших двох полів

Для кожного пакету заголовок супроводжується зашифрованими AES пакетними даними, потім 4-байтовим значенням, яке вказує розмір заповнення AES, та зашифрованим RSA AES ключем. Кожен пакет шифрується за допомогою іншого AES ключа.

Відповіді сервера надсилаються в однаковому форматі. На відміну від попередніх версій, дані пакетів у відповідях сервера не відповідають жодному шаблону (з деякими винятками).

Макет пакетних даних

Попередній макет пакетних даних був деталізований Proofpoint у жовтні 2018 року. В останній версії DanaBot, макет трохи змінений, як показано на Рис. 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

Рис. 4 – Порівняння пакетних даних у попередній і останній версії DanaBot

Зміни в архітектурі DanaBot

Крім зміненого протоколу з'єднання, DanaBot також має певні зміни в архітектурі. У попередніх версіях DanaBot був компонент, який завантажував і виконував основний модуль. Потім основний модуль завантажував і запускав плагіни і конфігурації.

У останній версії ці дії виконує новий компонент завантажувача, який використовується для завантаження всіх плагінів разом з основним модулем. Стійкість досягається шляхом реєстрації компонента завантажувача як сервісу.

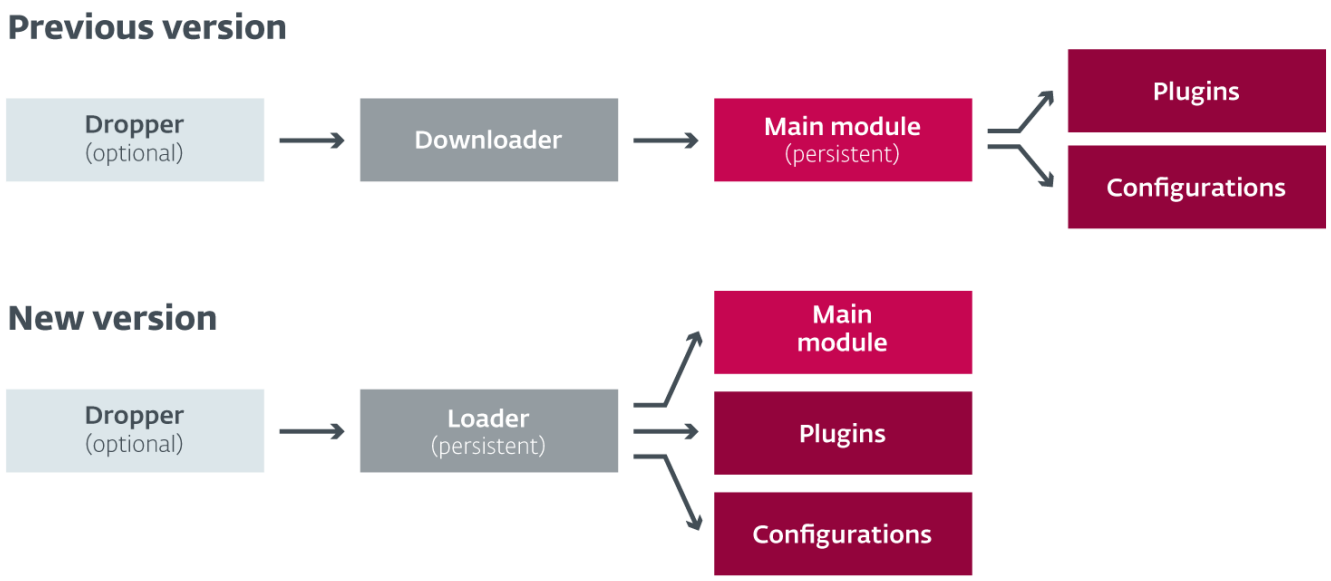

Рис. 5 – Порівняння архітектури в попередній і останній версії DanaBot

Команди

Відповідно до аналізу спеціалістів ESET компонент завантажувача використовує такі команди:

- 0x12C — Привіт. Перша команда, яку клієнт надсилає на сервер
- 0x12D — Завантажити 32/64-бітний компонент запуску
- 0x12E — Запит списку плагінів та файлів конфігурації
- 0x12F — Завантажити файли плагіни/файли конфігурацій

Завантажені плагіни та файли конфігурацій шифруються за допомогою ключа AES, отриманого з ідентифікатора клієнта. На додаток до цього, плагіни архівуються у форматі ZIP за допомогою стиснення LZMA, тоді як файли налаштування стискаються за допомогою zlib.

Команди з номерами ідентифікаторів 0x130 - 0x134 надсилаються основним модулем:

- 0x130 — завантаження зібраної інформації на командний сервер (наприклад, знімок екрана комп'ютера жертви; інформація про систему).
- 0x131 — завантаження зібраної інформації на командний сервер (наприклад, список файлів на жорсткому диску жертви)
- 0x132 — запит на командний сервер подальших команд; існує близько 30 доступних команд, типових для бекдорів, включаючи запуски плагінів, збирання детальної інформації про систему та зміна файлів у системі клієнта.
- 0x133 — оновлення списку командних серверів через проксі-сервер Tor.
- 0x134 — точна ціль невідома, найімовірніше використовується для зв'язку між плагінами та командним сервером.

Зміни в ідентифікаторах (ID) кампанії

Попередні дослідження показали, що DanaBot поширюється під різними ідентифікаторами (ID).

У попередній версії DanaBot було використано майже 20 різних ідентифікаторів кампанії. У останній версії трояна ідентифікатори кампанії дещо змінилися. Станом на 5 лютого 2019 року спеціалісти ESET виявили у реальному середовищі наступні ідентифікатори (ID).

- **ID=2** — тестова версія, яка обслуговує обмежену кількість файлів конфігурації та не містить модулів та пакетів, які вводять код HTML або JavaScript у вміст перед відображенням у веб-браузері.
- **ID=3** — активно розповсюджується, спрямована на користувачів Польщі та Італії, обслуговує всі файли конфігурацій, а також модулі чи пакети, які вводять код HTML або JavaScript у вміст перед відображенням у веб-браузері та спрямовані та польських та італійських користувачів.
- **ID=5** — файли конфігурацій, спрямованих на Австралію.
- **ID=7** — розповсюджується тільки в Польщі та обслуговує модулі чи пакети, які вводять код HTML або JavaScript у вміст перед відображенням у веб-браузері та спрямовані тільки на польських користувачів.
- **ID=9** — імовірно, є іншою тестовою версією з обмеженим поширенням та без певного спрямування, обслуговує обмежену кількість файлів налаштування та не містить жодних модулів чи пакетів, які вводять код HTML або JavaScript у вміст перед відображенням у веб-браузері.

Висновок

У 2018 році спеціалісти ESET зафіксували вдосконалення функціоналу та зростання рівня поширення трояна DanaBot. У 2019 році активна розробка шкідливої програми продовжилася. За допомогою вдосконалень зловмисники намагаються уникнути виявлення на рівні мережі, а також, ймовірно, приховати діяльність загрози після публікації попередніх досліджень.

Продукти ESET виявляють і блокують усі компоненти та плагіни DanaBot з назвами виявлень, перелічених нижче.

Ідентифікатори компрометації (IoC)

Командні сервери, які використовує нова версія 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

Модулі чи пакети, які вводять код HTML або JavaScript у вміст перед відображенням у веб-браузері, а також сервери перенаправлення

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

Приклади хешів

Зверніть увагу, оскільки нові списки компонентів DanaBot з'являються регулярно, нижче наведено лише приклади хешів.

Компонент	**SHA-1**	**Назва виявлення ESET**
Завантажувальний модуль	98C70361EA611BA33EE3A79816A88B2500ED7844	Win32/TrojanDropper.Danabot.O
Завантажувач (x86), ID=3	0DF17562844B7A0A0170C9830921C3442D59C73C	Win32/Spy.Danabot.L
Завантажувач (x64), ID=3	B816E90E9B71C85539EA3BB897E4F234A0422F85	Win64/Spy.Danabot.G
Завантажувач (x86), ID=9	5F085B19657D2511A89F3172B7887CE29FC70792	Win32/Spy.Danabot.I
Завантажувач (x64), ID=9	4075375A08273E65C223116ECD2CEF903BA97B1E	Win64/Spy.Danabot.F
Головний модуль (x86)	28139782562B0E4CAB7F7885ECA75DFCA5E1D570	Win32/Spy.Danabot.K
Головний модуль (x64)	B1FF7285B49F36FE8D65E7B896FCCDB1618EAA4B	Win64/Spy.Danabot.C

Плагіни

Плагін	**SHA-1**	**Назва виявлення ESET**
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