АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET обнаружила новые версии трояна DanaBot

08 февраля 2019 года

Быстро развивающийся модульный троян DanaBot подвергся новым изменениям. В версии, выпущенной в конце января 2019 года, реализован совершенно новый коммуникационный протокол, добавляющий несколько уровней шифрования в коммуникацию трояна и его C&C-сервера. Помимо этого, была изменена архитектура DanaBot и идентификаторы кампаний.

Эволюция DanaBot

После обнаружения в мае 2018 года в составе спам-кампании, нацеленной на Австралию, DanaBot фигурировал в ряде других атак, включая спам-кампанию в Польше, Италии, Германии, Австрии и Украине, а также США. В европейских кампаниях функциональность трояна была расширена с помощью новых плагинов и возможностей рассылки спама.

25 января мы обнаружили в данных телеметрии необычные исполняемые файлы, связанные с DanaBot. В ходе дальнейшей проверки выяснилось, что эти бинарные файлы действительно являются версиями DanaBot, но для связи с C&C-сервером они используют иной протокол связи. С 26 января операторы трояна остановили сборку бинарных файлов со старым протоколом.

На момент написания поста новая версия DanaBot распространялась по двум сценариям:

1) В качестве «обновлений», доставляемых жертвам DanaBot;
2) Посредством спам-рассылки (в Польше).

Новый коммуникационный протокол

В протоколе, который использовался до 25 января, пакеты не были зашифрованы, как показано на рисунке 1.

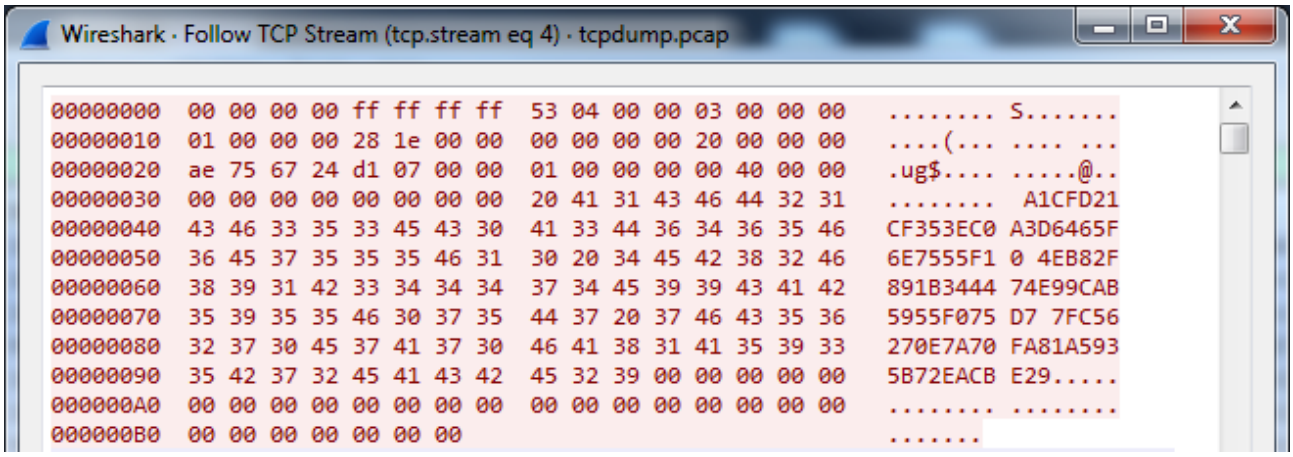

Рисунок 1. Перехват пакета, показывающий старый протокол с данными в незашифрованном виде

После доработки DanaBot использует в коммуникации с C&C-сервером алгоритмы шифрования AES и RSA. Новый протокол связи более сложен, поскольку использует несколько уровней шифрования, как показано на рисунке ниже.

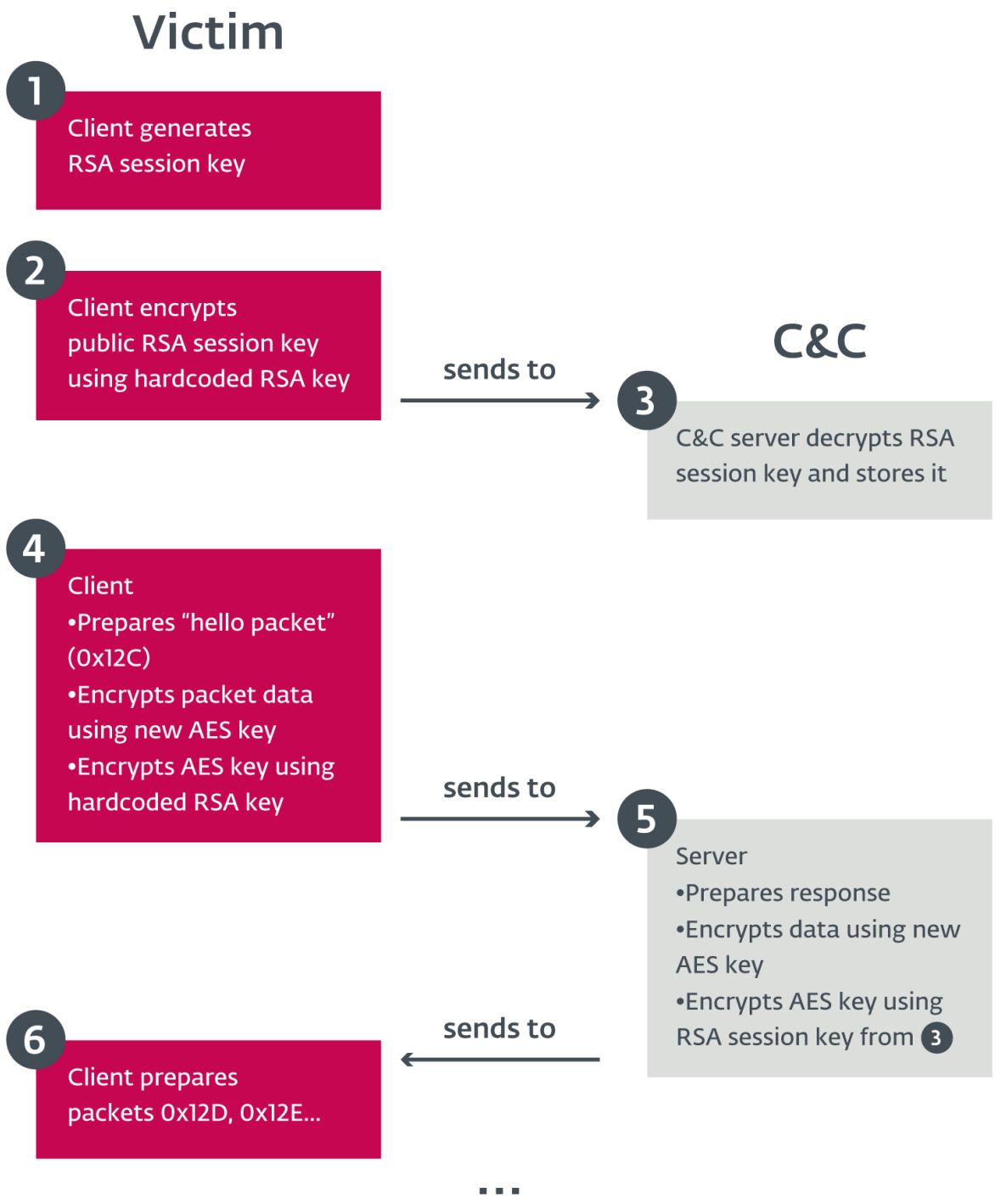

Рисунок 2. Схема нового коммуникационного протокола DanaBot

Эти изменения позволяют избежать детектирования с применением существующих сетевых сигнатур и затрудняют написание новых правил для систем обнаружения и предотвращения вторжений. Кроме того, без доступа к соответствующим ключам RSA невозможно декодировать отправленные или полученные пакеты; таким образом, файлы PCAP из облачных систем анализа (таких как ANY.RUN) непригодны для исследования.

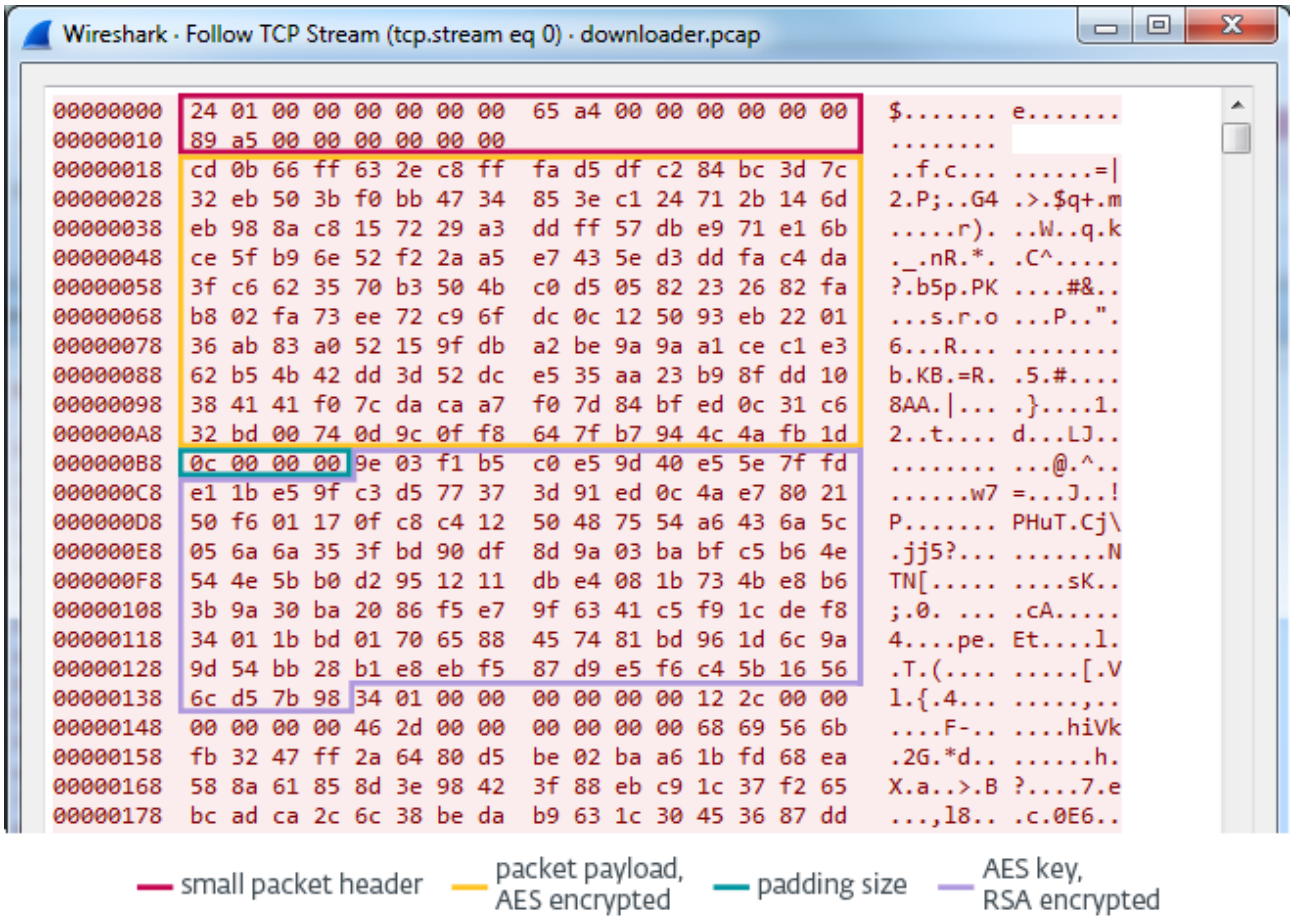

Рисунок 3. Захват пакета с новым коммуникационным протоколом

Каждый пакет, отправляемый клиентом, имеет 24 (0x18)-байтный заголовок:

Смещение	Размер (в байтах)	Значение
0x0	0x8	Размер данных после этого заголовка
0x8	0x8	Случайное значение
0x10	0x8	Сумма первых двух полей

Для каждого пакета за заголовком следуют данные пакета, зашифрованные AES, затем 4-байтовое значение, указывающее размер сдвига AES, и далее ключ AES, зашифрованный RSA. Все пакеты зашифрованы разными ключами AES.

Ответы сервера используют тот же формат. В отличие от предыдущих версий, данные пакета в ответах сервера не соответствуют какой-то определенной структуре (за некоторыми исключениями).

Структура пакета данных

Прежняя структура данных пакета была детально описана Proofpoint в октябре 2018 года. В последней версии DanaBot эта схема немного изменена, как показано на рисунке ниже.

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

Рисунок 4. Сравнение структуры данных пакета в старой и новой версиях DanaBot

Изменения архитектуры DanaBot

Помимо протокола связи, в DanaBot несколько изменена архитектура. Предыдущие версии трояна включали компонент, который скачивал и выполнял основной модуль. Затем основной модуль загружал и выполнял плагины и конфигурации.

В последней версии эти функции выполняет новый загрузчик, который используется для скачивания всех плагинов вместе с основным модулем. Персистентность обеспечивается путем регистрации компонента загрузчика в качестве службы.

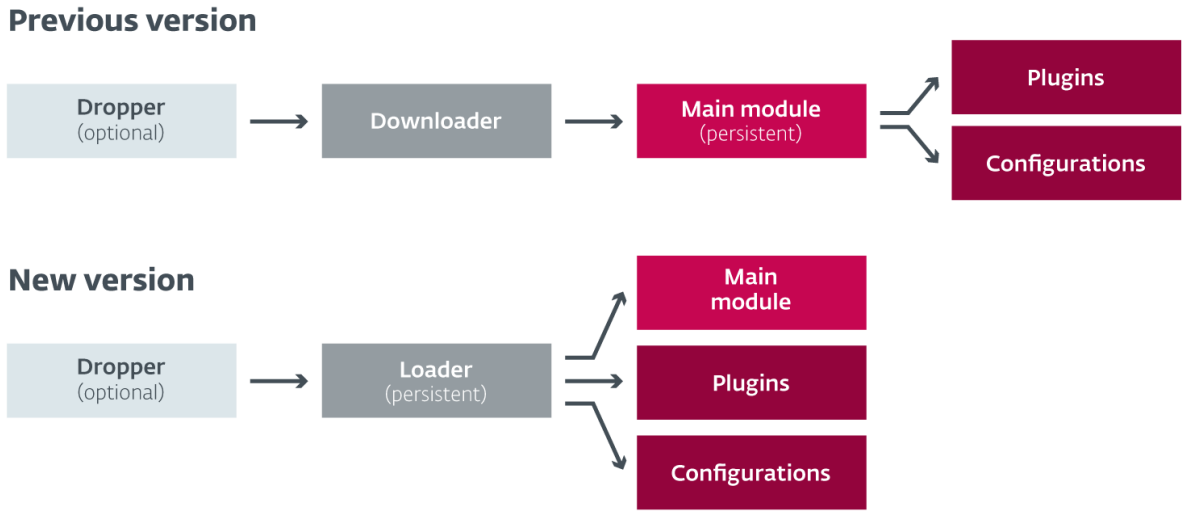

Рисунок 5. Сравнение архитектуры старой и новой версий DanaBot

Команды

Согласно анализу, компонент загрузчика использует следующие команды:
— 0x12C – Hello. Первая команда, отправляемая с клиента на сервер
— 0x12D – загрузить 32/64-битный компонент средства запуска
— 0x12E – запросить список плагинов и файлов конфигурации
— 0x12F – загрузить плагины/файлы конфигурации

Загруженные плагины и файлы конфигурации зашифрованы с ключом AES, полученным из идентификатора клиента. В дополнение к этому плагины архивируются в формате ZIP с использованием сжатия LZMA, в то время как файлы конфигурации – с использованием zlib. Команды с ID 0x130–0x134 отправляются основным модулем:

— 0x130 – передать собранную информацию на C&C-сервер (например, снимок экрана компьютера жертвы; системные данные)
— 0x131 – передать собранную информацию на C&C-сервер (например, список файлов на жестком диске зараженного компьютера)
— 0x132 – запросить у C&C-сервера дальнейшие команды. Есть порядка 30 команд, типичных для бэкдоров, включая запуск плагинов, сбор системной информации и изменение файлов в клиентской системе
— 0x133 – обновить список C&C-серверов через прокси Tor
— 0x134 – точное назначение неизвестно, скорее всего, используется для связи между плагинами и C&C-сервером

Изменение идентификаторов кампании

Предыдущее исследование показало, что DanaBot распространяется под разными ID.

В предыдущей версии DanaBot использовалось около 20 идентификаторов кампании. В последней версии идентификаторы изменились незначительно. По состоянию на 5 февраля 2019 года мы наблюдаем следующие ID:

— ID=2 по видимости, тестовая версия, обслуживающая незначительное число файлов конфигурации, без веб-инжектов
— ID=3 активно распространяется, ориентирован на пользователей в Польше и Италии, обслуживает все файлы конфигурации и веб-инжекты для польских и итальянских целей
— ID=5 обслуживает файлы конфигурации для австралийских целей
— ID=7 распространяется только в Польше, обслуживает веб-инжекты для польских целей
— ID=9 по видимости, также является тестовой версией с ограниченным распространением и без специального таргетинга, обслуживает ограниченное число файлов конфигурации, без веб-инжектов

Выводы

В 2018 году мы наблюдали развитие DanaBot с точки зрения распространения и функциональности. В начале 2019 года троян подвергся «внутренним» изменениям, указывающим на активную работу его создателей. Последние обновления предполагают, что создатели DanaBot прилагают усилия, чтобы избежать обнаружения на сетевом уровне. Не исключено, что авторы трояна обращают внимание на публикуемые исследования, чтобы оперативно вносить изменения в код, опережая разработчиков продуктов для безопасности.

Продукты ESET детектируют и блокируют все компоненты и плагины DanaBot. Имена детектирования приведены в следующем разделе.

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Индикаторы компрометации (IoCs)

C&C-серверы, используемые новой версией 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

Серверы для веб-инжекта и редиректа

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

Примеры хешей

Новые сборки DanaBot выходят регулярно, поэтому мы можем предоставить только часть хешей:
Дроппер 98C70361EA611BA33EE3A79816A88B2500ED7844 Win32/TrojanDropper.Danabot.O
Загрузчик (x86), ID=3 0DF17562844B7A0A0170C9830921C3442D59C73C Win32/Spy.Danabot.L
Загрузчик (x64), ID=3 B816E90E9B71C85539EA3BB897E4F234A0422F85 Win64/Spy.Danabot.G
Загрузчик (x86), ID=9 5F085B19657D2511A89F3172B7887CE29FC70792 Win32/Spy.Danabot.I
Загрузчик (x64), ID=9 4075375A08273E65C223116ECD2CEF903BA97B1E Win64/Spy.Danabot.F
Основной модуль (x86) 28139782562B0E4CAB7F7885ECA75DFCA5E1D570 Win32/Spy.Danabot.K
Основной модуль (x64) B1FF7285B49F36FE8D65E7B896FCCDB1618EAA4B Win64/Spy.Danabot.C

Плагины

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