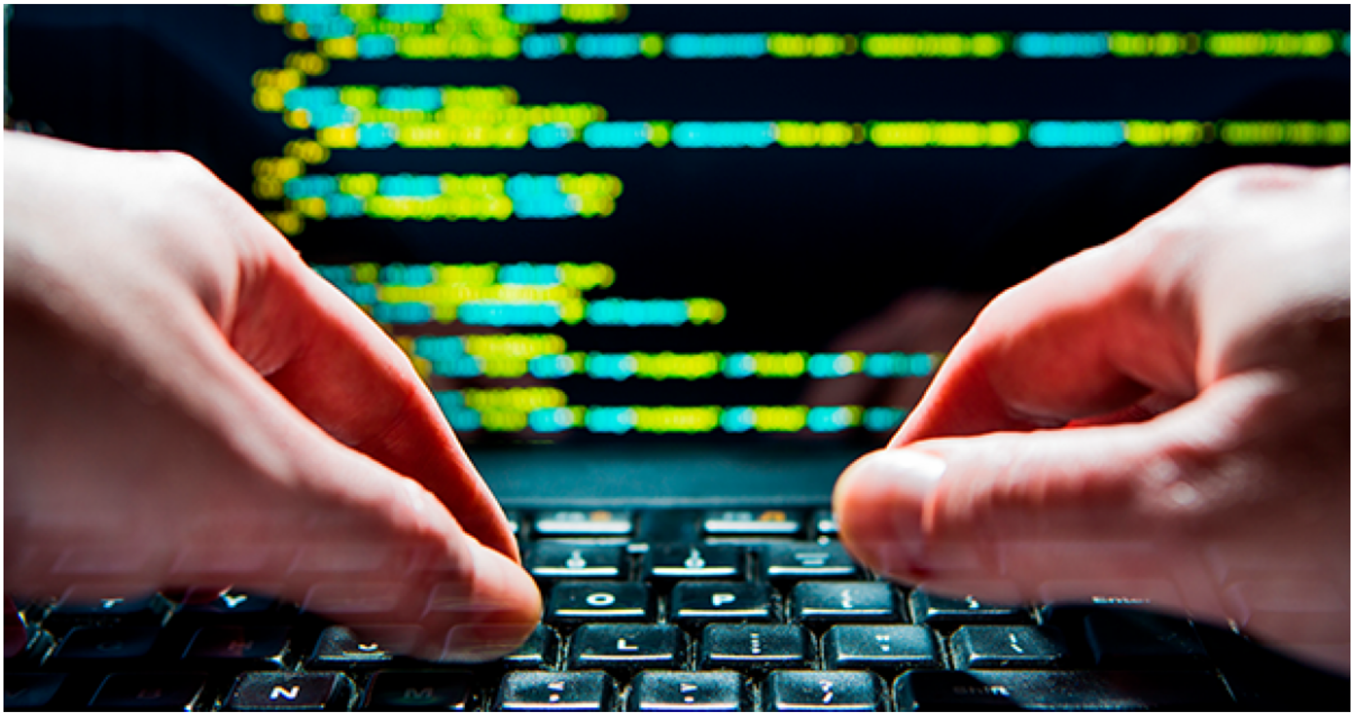
Nightmare on Tor Street: Ursnif variant Dreambot adds Tor functionality

proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality

August 29, 2016



Blog
Threat Insight
Nightmare on Tor Street: Ursnif variant Dreambot adds Tor functionality

August 25, 2016 Proofpoint Staff

Introduction

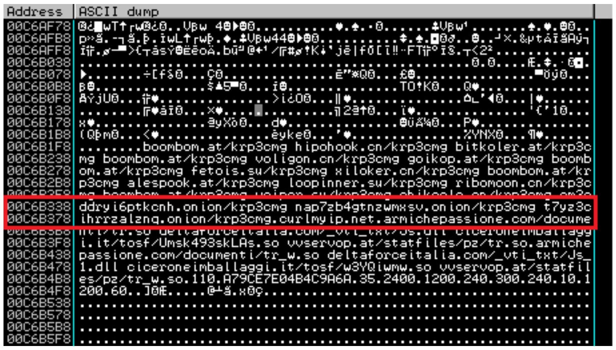
One of the most active banking Trojans that we have observed recently in email and exploit kits is one often referred to as Ursnif or Gozi ISFB [6]. Thanks to Frank Ruiz from FoxIT InTELL, we know that the actor developing one of its variants since 2014 has named this variant Dreambot. The Dreambot malware is actively evolving, and recent samples in particular caught our attention for their addition of Tor communication capability, as well as peer-to-peer (P2P) functionality. Dreambot is currently spreading via numerous exploit kits as well as through email attachments and links.

It should be noted that while Dreambot is one of the most active and prevalent Ursnif variants, there are other active forks including “IAP” [5]. The Gozi ISFB source has been leaked, making way for additional development efforts.

Analysis

The Dreambot malware is still in active development and over the last few months we have seen multiple versions of it spreading in the wild. The Tor-enabled version of Dreambot has been active since at least July 2016, when we first observed the malware successfully download the Tor client and connect to the Tor network. Today, many Dreambot samples include this functionality, but few use it as their primary mode of communication with their command and control (C&C) infrastructure. However, in the future this feature may be utilized much more frequently, creating additional problems for defenders.

For this analysis, we looked at version 2.14.845, which has a configuration that differs from the others Dreambot versions in that the domain generation algorithm (DGA) is not used: therefore, the DGA variables and parameters are missing. The following is an example of decrypted configuration data with sections of interest highlighted in red.



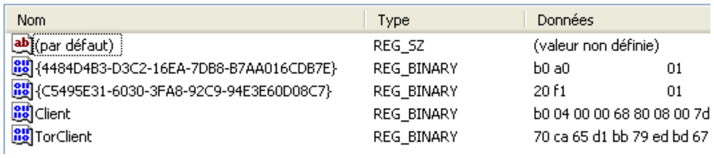
```
Address |ASCII dump
00C6AF78 @¿█wT↑┌w@¿0..Vβw 4☻►00..........♥.♠.·0......‡Vβw¹........♠.♥.00..
00C6AFB8 p»ã.¬┐ã.þ.ïwL↑┌wþ.♦.‡Vβw44☻►00..........‡.♠.◘0∂..☻..┘×.&µtÂÏãÂÿ┐
00C6AFF8 ï╬.ø─▀>{┬âsÝ☻ËëòÄ.bü╝@♦¹/╔#ø!K↓'jë|fõ[ï‼·FT╬°ÏS.┬<2²............
00C6B038 .............................................0.0....Æ.‡.·0◘.
00C6B078 ►.......÷[f§0...Ç0...............ë"*Q0...£☻...............▀ôÿ0...
00C6B0B8 β☻................$▲5▀0...ï☻...............TO!K0...Q♥...............
00C6B0F8 ÅÝjU0...╬♥..................>i¿O0...‖♥...............⌂∟'◄0...|♥.....
00C6B138 .........╔♦âÏ0...×♥.....▒..........╗2ª↑0...ï♥.................'{'10...
00C6B178 ×♥.................ªyXõ0...d♥.................☻üÅ%0...P♥..............
00C6B1B8 (Qþm0...<♥..................êyke0...'♥.................%YNX0...¶♥......
00C6B1F8 ........boombom.at/krp3cmg hipohook.cn/krp3cmg bitkoler.at/krp3c
00C6B238 mg boombom.at/krp3cmg voligon.cn/krp3cmg goikop.at/krp3cmg boomb
00C6B278 om.at/krp3cmg fetois.su/krp3cmg xiloker.cn/krp3cmg boombom.at/kr
00C6B2B8 p3cmg alespook.at/krp3cmg loopinner.su/krp3cmg ribomoon.cn/krp3c
00C6B2F8 mg boombom.at/krp3cmg voipon.su/krp3cmg chikoolo.cn/krp3cmg om3c
00C6B338 ddryi6ptkcnh.onion/krp3cmg nap7zb4gtnzwmxsv.onion/krp3cmg t7yz3c
00C6B378 ihrrzalznq.onion/krp3cmg.curlmyip.net.armichepassione.com/docume
00C6B3B8 nti/tr.so deltaforceitalia.com/_vti_txt/Js.dll ciceroneimballagg
00C6B3F8 i.it/tosf/Umsk493skLAs.so vvservop.at/statfiles/pz/tr.so.armiche
00C6B438 passione.com/documenti/tr_w.so deltaforceitalia.com/_vti_txt/Js_
00C6B478 1.dll ciceroneimballaggi.it/tosf/w3YQiwmw.so vvservop.at/statfil
00C6B4B8 es/pz/tr_w.so.110.A79CE7E04B4C9A6A.35.2400.1200.240.300.240.10.1
00C6B4F8 200.60..]0Æ.....@┴ã.x0ç..........................................
00C6B538 ................................................................
00C6B578 ................................................................
00C6B5B8 ................................................................
00C6B5F8 ................................................................
```

Figure 1: Decrypted configuration data used by Dreambot

There are three types of URLs present in the decrypted configuration. The first type of URL listed in the configuration data is used for the plain HTTP (that is, non-Tor) communication with C&C servers. The bot reports to the C&C server using the typical request pattern: for example, the initial checkin to the C&C server is in the form of: cfg_url + “/images/” + encoded_data + (.jpeg|.gif|.bmp).

The second type of URL that appears in the configuration data (highlighted in red box in Fig. 1) are the .onion C&C addresses. They are the default choice for the bot and work in the same way the plain HTTP C&C’s do, except that all communication is encrypted and tunneled over Tor.

The third set of URLs is used to download the Tor client. We believe the client is decrypted using the configuration serpent key [7]. When the Tor client is retrieved, the bot creates a registry key named “TorClient” in the registry subfolder to store its data. This subfolder is located in HKCU\\Software\AppDataLow\Software\Microsoft\{random guid}. This key contains the path to the client, which is dropped in the %TMP% folder, with a filename using the pattern [A-F0-9]{4}.bin.

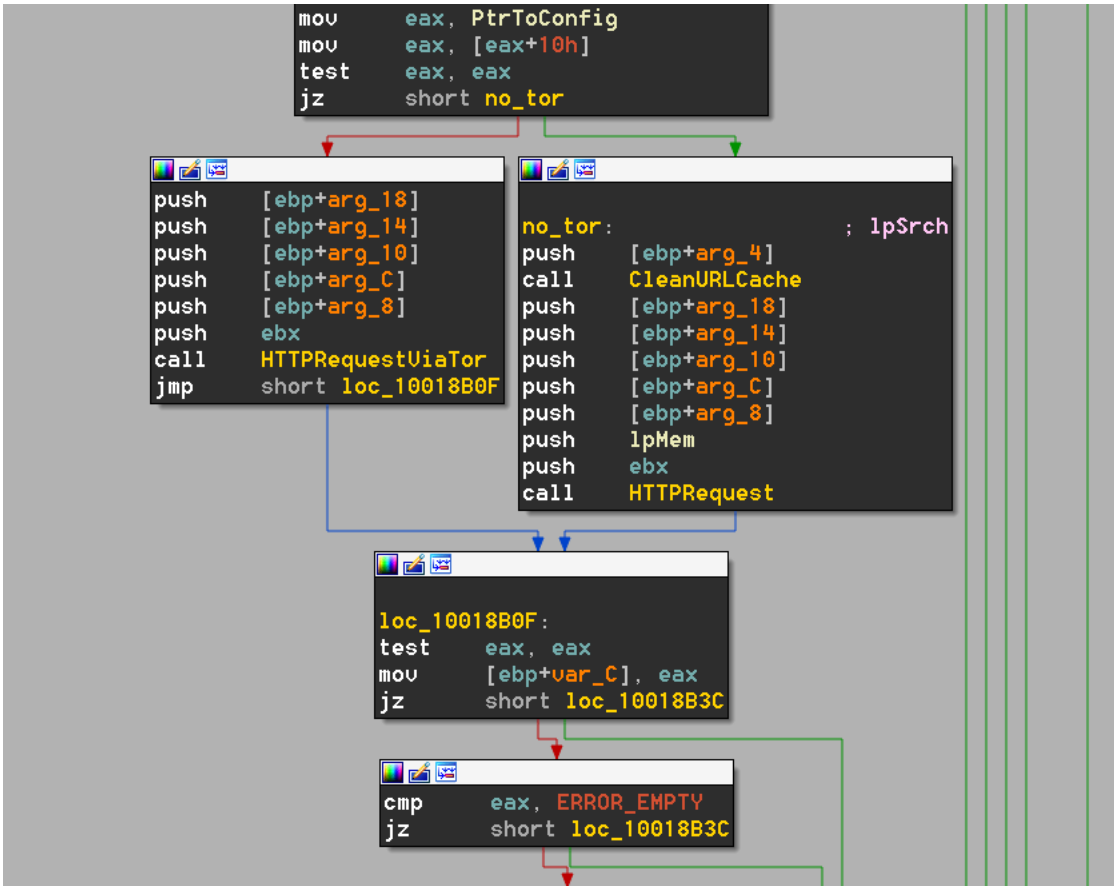


Nom	Type	Données
ab (par défaut)	REG_SZ	(valeur non définie)
{4484D4B3-D3C2-16EA-7DB8-B7AA016CDB7E}	REG_BINARY	b0 a0 01
{C5495E31-6030-3FA8-92C9-94E3E60D08C7}	REG_BINARY	20 f1 01
Client	REG_BINARY	b0 04 00 00 68 80 08 00 7d
TorClient	REG_BINARY	70 ca 65 d1 bb 79 ed bd 67

Figure 2: TorClient registry key

The registry key value is easy to decrypt, as the XOR-based algorithm [8] is reused in much of the code (e.g., for decryption of the strings in the .bss section). The 4-byte key is generated at runtime based on the TOKEN_USER value XORed with 0xE8FA7DD7.

For the two types of POST HTTP requests (Tor and non-Tor), the configuration includes a check of the Tor flag (here at eax+10). If this flag is set, Dreambot sends both the C&C checkins and the data upload requests using Tor.



```
mov     eax, PtrToConfig
mov     eax, [eax+10h]
test    eax, eax
jz      short no_tor
```

```
push    [ebp+arg_18]
push    [ebp+arg_14]
push    [ebp+arg_10]
push    [ebp+arg_C]
push    [ebp+arg_8]
push    ebx
call    HTTPRequestViaTor
jmp     short loc_10018B0F
```

```
no_tor:                           ; lpSrch
push    [ebp+arg_4]
call    CleanURLCache
push    [ebp+arg_18]
push    [ebp+arg_14]
push    [ebp+arg_10]
push    [ebp+arg_C]
push    [ebp+arg_8]
push    lpMem
push    ebx
call    HTTPRequest
```

```
loc_10018B0F:
test    eax, eax
mov     [ebp+var_C], eax
jz      short loc_10018B3C
```

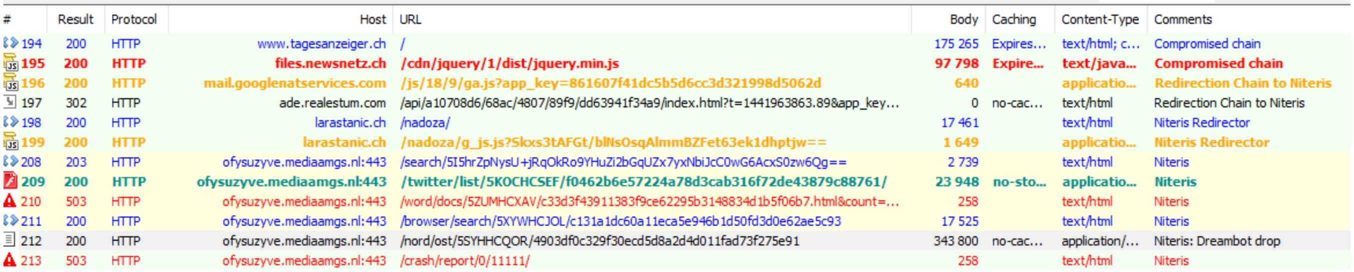
```
cmp     eax, ERROR_EMPTY
jz      short loc_10018B3C
```

Figure 3: Configuration flags for communicating via Tor

In addition to the Dreambot with Tor functionality, we have observed a P2P-enabled versions (e.g. version 2.15.798) that has been around considerably longer. Spread alongside the other variants this version utilizes the usual DGA or hard-coded addresses as well as what appears to be a peer-to-peer protocol to communicate. This functionality needs an additional IP in the configuration that delivers the nodes list. This protocol operates over TCP and UDP and uses a custom packet format. Due to the addition of this functionality, the client code surface is almost twice as big as that of the Tor version. We are still investigating the functionality and will not go into deeper detail at this time.

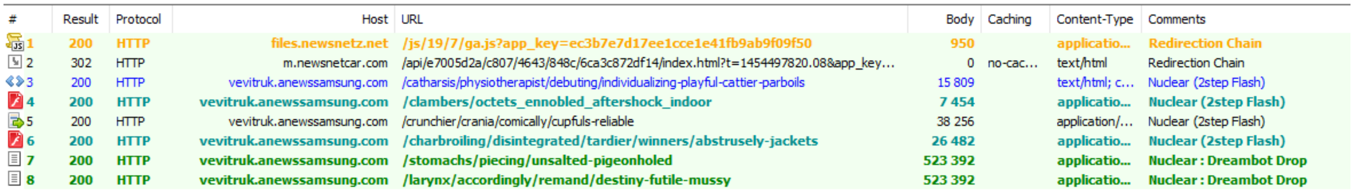
Exploit Kit Campaigns

One early interesting example of Dreambot delivery came from an instance of the Niteris exploit kit. Several months after that, we spotted the same redirection chain but instead to an undocumented 2-step flash Nuclear Pack. This particular Nuclear Pack behaved similarly to Spartan EK from the same coder in which an initial flash payload acted as a filter before sending the exploit and payload to end users. GooNky and AdGholas actors also commonly used Angler EK to deliver Dreambot while Angler was still highly active. Figures 4-7 show these infection chains.



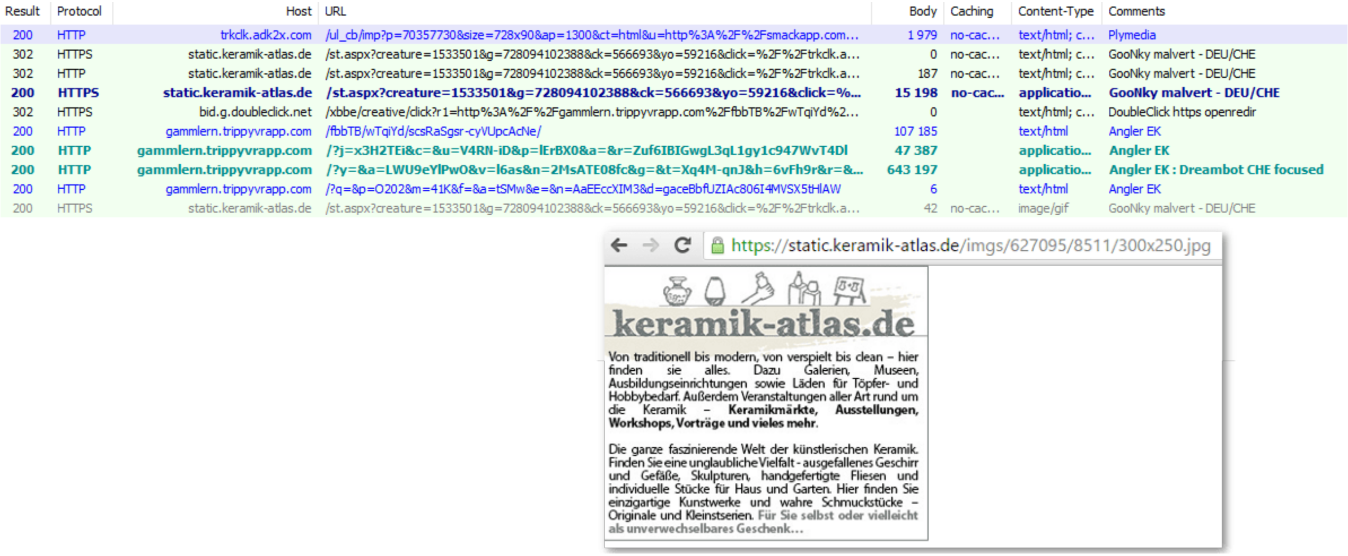
#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Comments
194	200	HTTP	www.tagesanzeiger.ch	/	175 265	Expires...	text/html; c...	Compromised chain
195	200	HTTP	files.newsnetz.ch	/cdn/jquery/1/dist/jquery.min.js	97 798	Expire...	text/java...	Compromised chain
196	200	HTTP	mail.googlenatservices.com	/js/18/9/ga.js?app_key=861607f41dc5b5d6cc3d321998d5062d	640		applicatio...	Redirection Chain to Niteris
197	302	HTTP	ade.realestum.com	/api/a10708d6/68ac/4807/89f9/dd63941f34a9/index.html?t=1441963863.89&app_key...	0	no-cac...	text/html	Redirection Chain to Niteris
198	200	HTTP	larastanic.ch	/nadoza/	17 461		text/html	Niteris Redirector
199	200	HTTP	larastanic.ch	/nadoza/g_js.js?Skxs3tAFGt/blNsOsqAlmmBZFet63ek1dhptjw==	1 649		applicatio...	Niteris Redirector
208	203	HTTP	ofysuzyve.mediaamgs.nl:443	/search/5I5hrZpNysU+jRqOkRo9YHuZi2bGqUZx7yxNbiJcC0wG6AcxS0zw6Qg==	2 739		text/html	Niteris
209	200	HTTP	ofysuzyve.mediaamgs.nl:443	/twitter/list/5KOCHCSEF/f0462b6e57224a78d3cab316f72de43879c88761/	23 948	no-sto...	applicatio...	Niteris
210	503	HTTP	ofysuzyve.mediaamgs.nl:443	/word/docs/5ZUMHCXAV/c33d3f43911383f9ce62295b3148834d1b5f06b7.html&count=...	258		text/html	Niteris
211	200	HTTP	ofysuzyve.mediaamgs.nl:443	/browser/search/5XYWHCJOL/c131a1dc60a11eca5e946b1d50fd3d0e62ae5c93	17 525		text/html	Niteris
212	200	HTTP	ofysuzyve.mediaamgs.nl:443	/nord/ost/5SYHHCQOR/4903df0c329f30ecd5d8a2d4d011fad73f275e91	343 800	no-cac...	application/...	Niteris: Dreambot drop
213	503	HTTP	ofysuzyve.mediaamgs.nl:443	/crash/report/0/11111/	258		text/html	Niteris

Figure 4: 09-11-2015 - Compromised AdAgency with high volume traffic chain to Niteris [4]



#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Comments
1	200	HTTP	files.newsnetz.net	/js/19/7/ga.js?app_key=ec3b7e7d17ee1cce1e41fb9ab9f09f50	950		applicatio...	Redirection Chain
2	302	HTTP	m.newsnetcar.com	/api/e7005d2a/c807/4643/848c/6ca3c872df14/index.html?t=1454497820.08&app_key...	0	no-cac...	text/html	Redirection Chain
3	200	HTTP	vevitruk.anewssamsung.com	/catharsis/physiotherapist/debuting/individualizing-playful-cattier-parboils	15 809		text/html; c...	Nuclear (2step Flash)
4	200	HTTP	vevitruk.anewssamsung.com	/clambers/octets_ennobled_aftershock_indoor	7 454		applicatio...	Nuclear (2step Flash)
5	200	HTTP	vevitruk.anewssamsung.com	/crunchier/crania/comically/cupfuls-reliable	38 256		application/...	Nuclear (2step Flash)
6	200	HTTP	vevitruk.anewssamsung.com	/charbroiling/disintegrated/tardier/winners/abstrusely-jackets	26 482		applicatio...	Nuclear (2step Flash)
7	200	HTTP	vevitruk.anewssamsung.com	/stomachs/piecing/unsalted-pigeonholed	523 392		applicatio...	Nuclear : Dreambot Drop
8	200	HTTP	vevitruk.anewssamsung.com	/larynx/accordingly/remand/destiny-futile-mussy	523 392		applicatio...	Nuclear : Dreambot Drop

Figure 5: 02-03-2016 - Same redirection chain but instead redirecting to an undocumented 2-step Flash Nuclear Pack [6]



Result	Protocol	Host	URL	Body	Caching	Content-Type	Comments
200	HTTP	trkclk.adk2x.com	/ul_cb/imp?p=70357730&size=728x90&ap=1300&ct=html&u=http%3A%2F%2Fsmackapp.com...	1 979	no-cac...	text/html; c...	Plymedia
302	HTTPS	static.keramik-atlas.de	/st.aspx?creature=1533501&g=728094102388&ck=566693&yo=59216&click=%2F%2Ftrkclk.a...	0	no-cac...	text/html; c...	GooNky malvert - DEU/CHE
302	HTTP	static.keramik-atlas.de	/st.aspx?creature=1533501&g=728094102388&ck=566693&yo=59216&click=%2F%2Ftrkclk.a...	187	no-cac...	text/html; c...	GooNky malvert - DEU/CHE
200	HTTPS	static.keramik-atlas.de	/st.aspx?creature=1533501&g=728094102388&ck=566693&yo=59216&click=%...	15 198	no-cac...	applicatio...	GooNky malvert - DEU/CHE
302	HTTPS	bid.g.doubleclick.net	/xbbe/creative/click?r1=http%3A%2F%2Fgammlern.trippyvrapp.com%2FfbbTB%2FwTqiYd%2...	0		text/html; c...	DoubleClick https openredir
200	HTTP	gammlern.trippyvrapp.com	/fbbTB/wTqiYd/scsRaSgsr-cyVUpcAcNe/	107 185		text/html	Angler EK
200	HTTP	gammlern.trippyvrapp.com	/?j=x3H2TEi&c=&u=V4RN-iD&p=lErBX0&a=&r=Zuf6IBIGwgL3qL1gy1c947WvT4Dl	47 387		applicatio...	Angler EK
200	HTTP	gammlern.trippyvrapp.com	/?y=&a=LWU9eYlPwO&v=l6as&n=2MsATE08fc&g=&t=Xq4M-qnJ&h=6vFh9r&r=&...	643 197		applicatio...	Angler EK : Dreambot CHE focused
200	HTTP	gammlern.trippyvrapp.com	/?q=&p=O202&m=41K&f=&a=tSMw&e=&n=AaEEccXIM3&d=gaceBbfUZIAc806I4MVSX5tHlAW	6		text/html	Angler EK
200	HTTPS	static.keramik-atlas.de	/st.aspx?creature=1533501&g=728094102388&ck=566693&yo=59216&click=%2F%2Ftrkclk.a...	42	no-cac...	image/gif	GooNky malvert - DEU/CHE

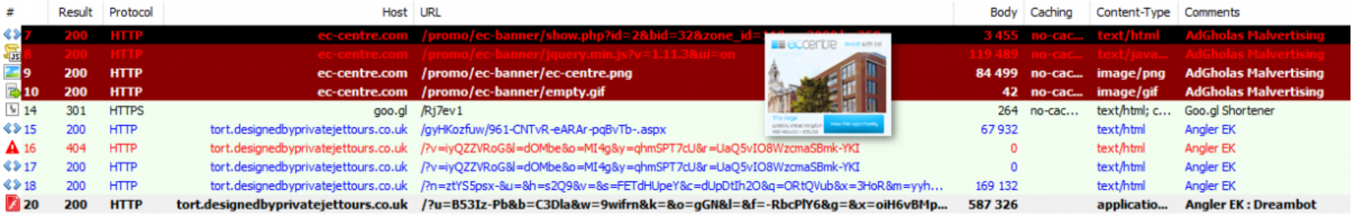
https://static.keramik-atlas.de/imgs/627095/8511/300x250.jpg

keramik-atlas.de

Von traditionell bis modern, von verspielt bis clean – hier finden sie alles. Dazu Galerien, Museen, Ausbildungseinrichtungen sowie Läden für Töpfer- und Hobbybedarf. Außerdem Veranstaltungen aller Art rund um die Keramik – **Keramikmärkte, Ausstellungen, Workshops, Vorträge und vieles mehr**.

Die ganze faszinierende Welt der künstlerischen Keramik. Finden Sie eine unglaubliche Vielfalt - ausgefallenes Geschirr und Gefäße, Skulpturen, handgefertigte Fliesen und individuelle Stücke für Haus und Garten. Hier finden Sie einzigartige Kunstwerke und wahre Schmuckstücke – Originale und Kleinstserien. **Für Sie selbst oder vielleicht als unverwechselbares Geschenk...**

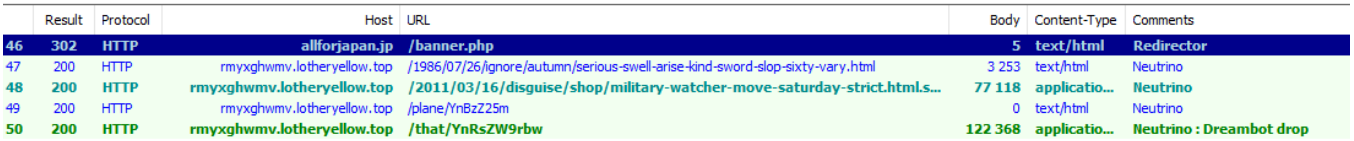
Figure 6: 04-11-2016 - Malvertising run by GooNky in Switzerland



#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Comments
7	200	HTTP	ec-centre.com	/promo/ec-banner/show.php?id=2&bid=32&zone_id=	3 455	no-cac...	text/html	AdGholas Malvertising
8	200	HTTP	ec-centre.com	/promo/ec-banner/jquery.min.js?v=1.11.3&ui=on	119 489	no-cac...	text/java...	AdGholas Malvertising
9	200	HTTP	ec-centre.com	/promo/ec-banner/ec-centre.png	84 499	no-cac...	image/png	AdGholas Malvertising
10	200	HTTP	ec-centre.com	/promo/ec-banner/empty.gif	42	no-cac...	image/gif	AdGholas Malvertising
14	301	HTTPS	goo.gl	/Rj7ev1	264	no-cac...	text/html; c...	Goo.gl Shortener
15	200	HTTP	tort.designedbyprivatejettours.co.uk	/gyHKozfuw/961-CNTvR-eARAr-pqBvTb-.aspx	67 932		text/html	Angler EK
16	404	HTTP	tort.designedbyprivatejettours.co.uk	/?v=iyQZZVRoG&l=dOMbe&o=MI4g&y=qhmSPT7cU&r=UaQ5vIO8WzcmaSBmk-YKI	0		text/html	Angler EK
17	200	HTTP	tort.designedbyprivatejettours.co.uk	/?v=iyQZZVRoG&l=dOMbe&o=MI4g&y=qhmSPT7cU&r=UaQ5vIO8WzcmaSBmk-YKI	0		text/html	Angler EK
18	200	HTTP	tort.designedbyprivatejettours.co.uk	/?n=ztYS5psx-&u=&h=s2Q9&v=&s=FETdHUpeY&c=dUpDtIh2O&q=ORtQVub&x=3HoR&m=yyh...	169 132		text/html	Angler EK
20	200	HTTP	tort.designedbyprivatejettours.co.uk	/?u=B53Iz-Pb&b=C3Dla&w=9wifrn&k=&o=gGN&l=&f=-RbcPlY6&g=&x=oiH6vBMp...	587 326		applicatio...	Angler EK : Dreambot

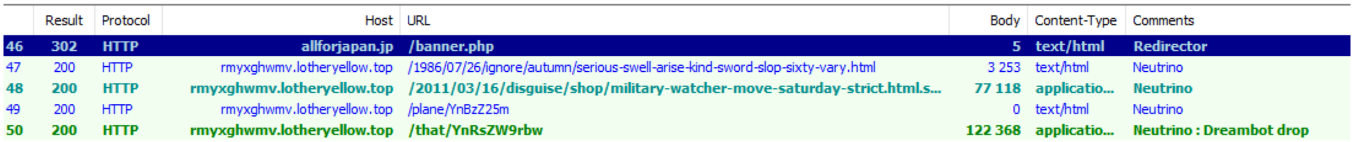
Figure 7: 05-10-2016 - Malvertising run by AdGholas in Switzerland

Figure 8 shows Dreambot delivery in a Japan-focused malvertising campaign using Neutrino EK while Figure 9 shows a recent sample of Dreambot as a secondary payload via the EITest and the Smokebot Trojan. In the latter example, we can see this instance of Dreambot is using Tor to connect to C&C infrastructure.



	Result	Protocol	Host	URL	Body	Content-Type	Comments
46	302	HTTP	allforjapan.jp	/banner.php	5	text/html	Redirector
47	200	HTTP	rmyxghwmv.lotheryellow.top	/1986/07/26/ignore/autumn/serious-swell-arise-kind-sword-slop-sixty-vary.html	3 253	text/html	Neutrino
48	200	HTTP	rmyxghwmv.lotheryellow.top	/2011/03/16/disguise/shop/military-watcher-move-saturday-strict.html.s...	77 118	applicatio...	Neutrino
49	200	HTTP	rmyxghwmv.lotheryellow.top	/plane/YnBzZ25m	0	text/html	Neutrino
50	200	HTTP	rmyxghwmv.lotheryellow.top	/that/YnRsZW9rbw	122 368	applicatio...	Neutrino : Dreambot drop

Figure 8: 07-09-2016 - Japan-focused malvertising based on the redirector's domain



	Result	Protocol	Host	URL	Body	Content-Type	Comments
46	302	HTTP	allforjapan.jp	/banner.php	5	text/html	Redirector
47	200	HTTP	rmyxghwmv.lotheryellow.top	/1986/07/26/ignore/autumn/serious-swell-arise-kind-sword-slop-sixty-vary.html	3 253	text/html	Neutrino
48	200	HTTP	rmyxghwmv.lotheryellow.top	/2011/03/16/disguise/shop/military-watcher-move-saturday-strict.html.s...	77 118	applicatio...	Neutrino
49	200	HTTP	rmyxghwmv.lotheryellow.top	/plane/YnBzZ25m	0	text/html	Neutrino
50	200	HTTP	rmyxghwmv.lotheryellow.top	/that/YnRsZW9rbw	122 368	applicatio...	Neutrino : Dreambot drop

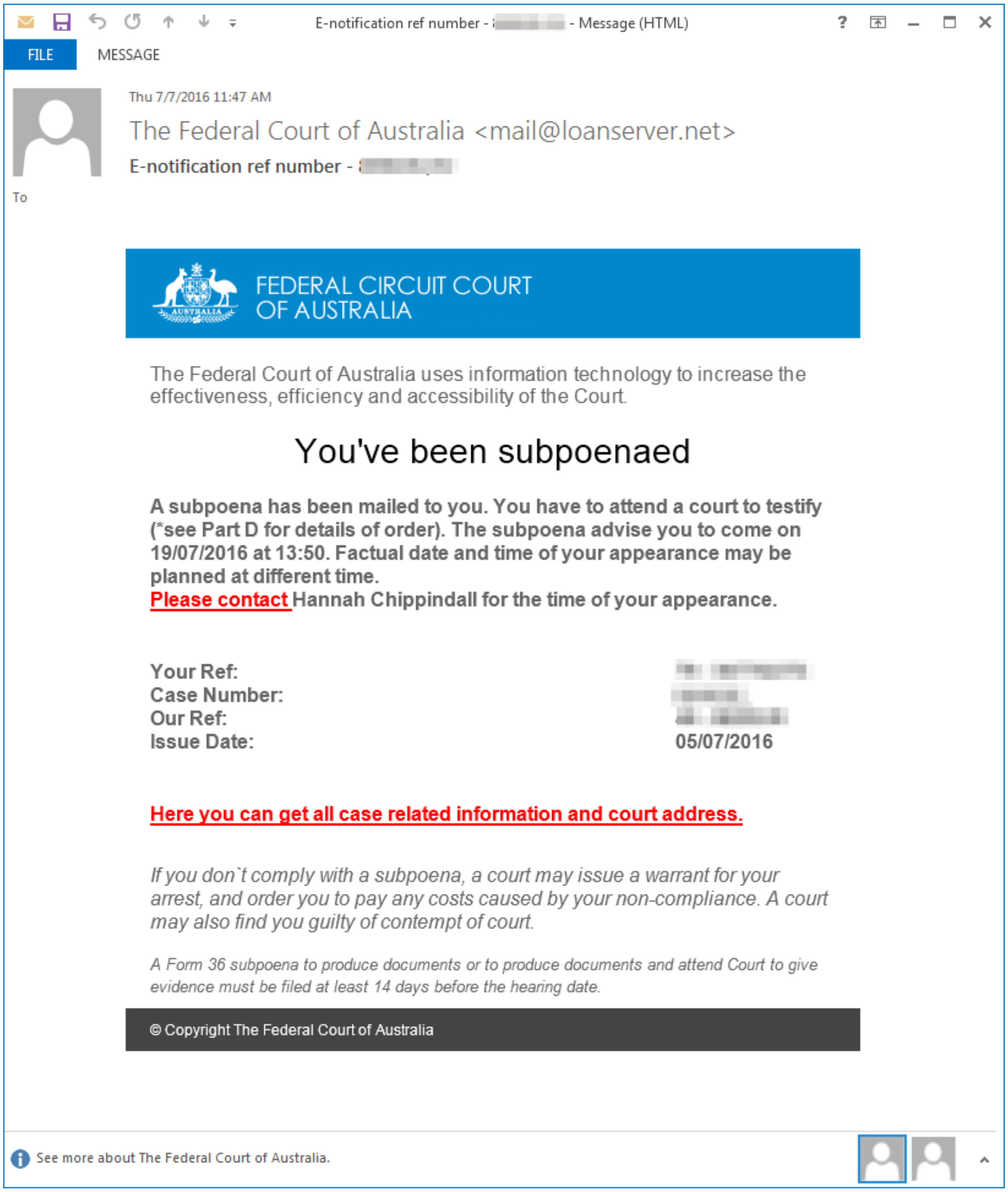
Figure 9: 08-15-2016 - EITest infection chain into Smokebot loading an instance of Dreambot using Tor to connect to C&C

Email Campaigns

Dreambot has been actively distributed via email in 2016. We have noted campaigns targeting various regions including Australia, Italy, Switzerland, United Kingdom, United States, Poland, and Canada. These campaigns have ranged from thousands to hundreds of thousands of malicious email messages. We show few examples of these campaigns using links or document attachments leading to the installation of

Dreambot.

In the first example, the actor used a lure claiming the recipient had been subpoenaed by the Federal Court of Australia. If the user were to follow the link they would be greeted by a web page purporting to be the official court site. If the user then followed the instructions, they would be led to a download of a zipped JavaScript file that, when executed, led to a Dreambot download.



Thu 7/7/2016 11:47 AM

The Federal Court of Australia <mail@loanserver.net>

E-notification ref number - [redacted]

FEDERAL CIRCUIT COURT
OF AUSTRALIA

The Federal Court of Australia uses information technology to increase the effectiveness, efficiency and accessibility of the Court.

You've been subpoenaed

A subpoena has been mailed to you. You have to attend a court to testify (*see Part D for details of order). The subpoena advise you to come on 19/07/2016 at 13:50. Factual date and time of your appearance may be planned at different time.
Please contact Hannah Chippindall for the time of your appearance.

Your Ref:	[redacted]
Case Number:	[redacted]
Our Ref:	[redacted]
Issue Date:	**05/07/2016**

Here you can get all case related information and court address.

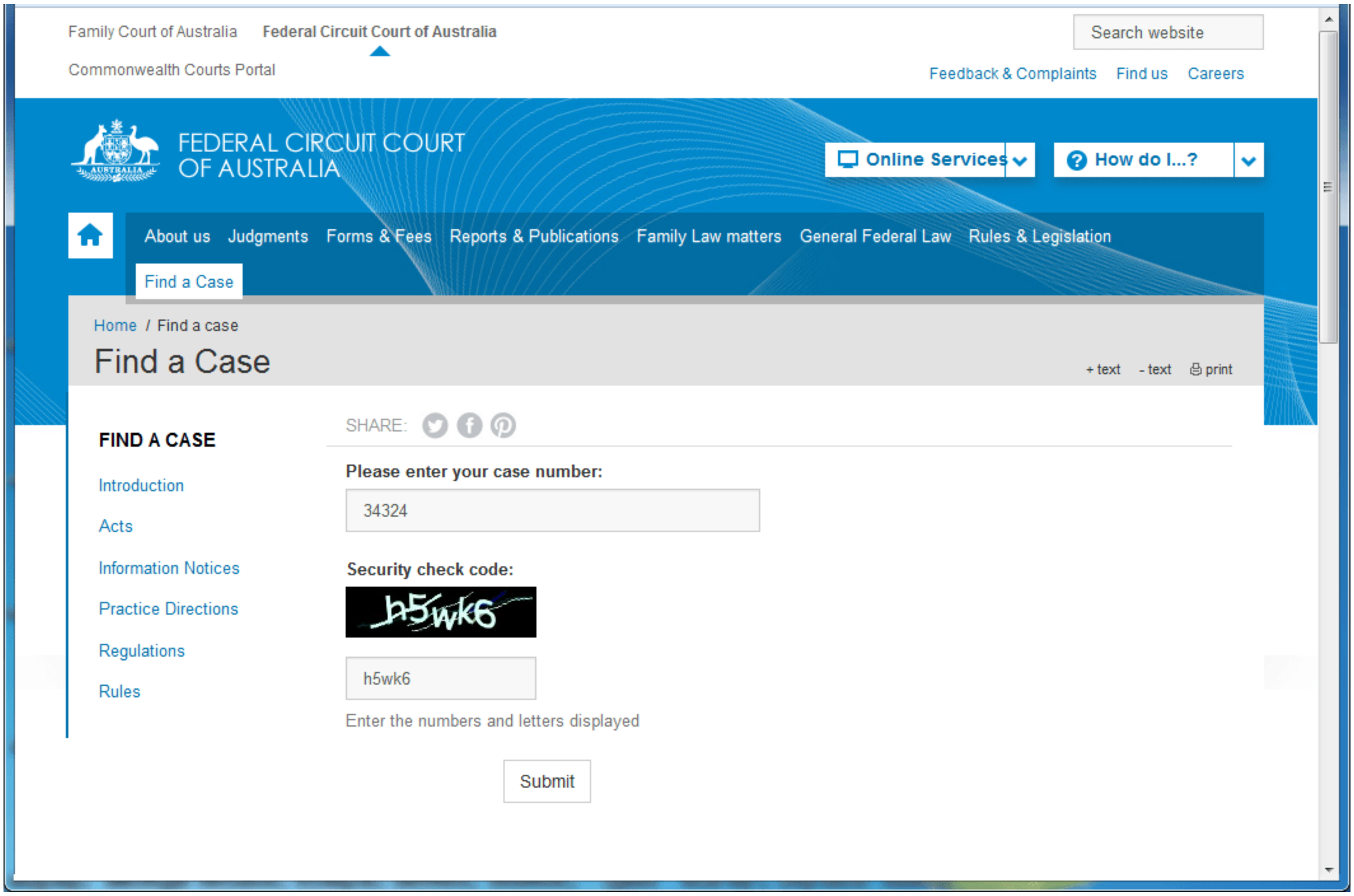
If you don`t comply with a subpoena, a court may issue a warrant for your arrest, and order you to pay any costs caused by your non-compliance. A court may also find you guilty of contempt of court.

A Form 36 subpoena to produce documents or to produce documents and attend Court to give evidence must be filed at least 14 days before the hearing date.

© Copyright The Federal Court of Australia

See more about The Federal Court of Australia.

Figure 10: 07-08-2016 - Message used to distribute Dreambot in Australia



Find a Case

FIND A CASE

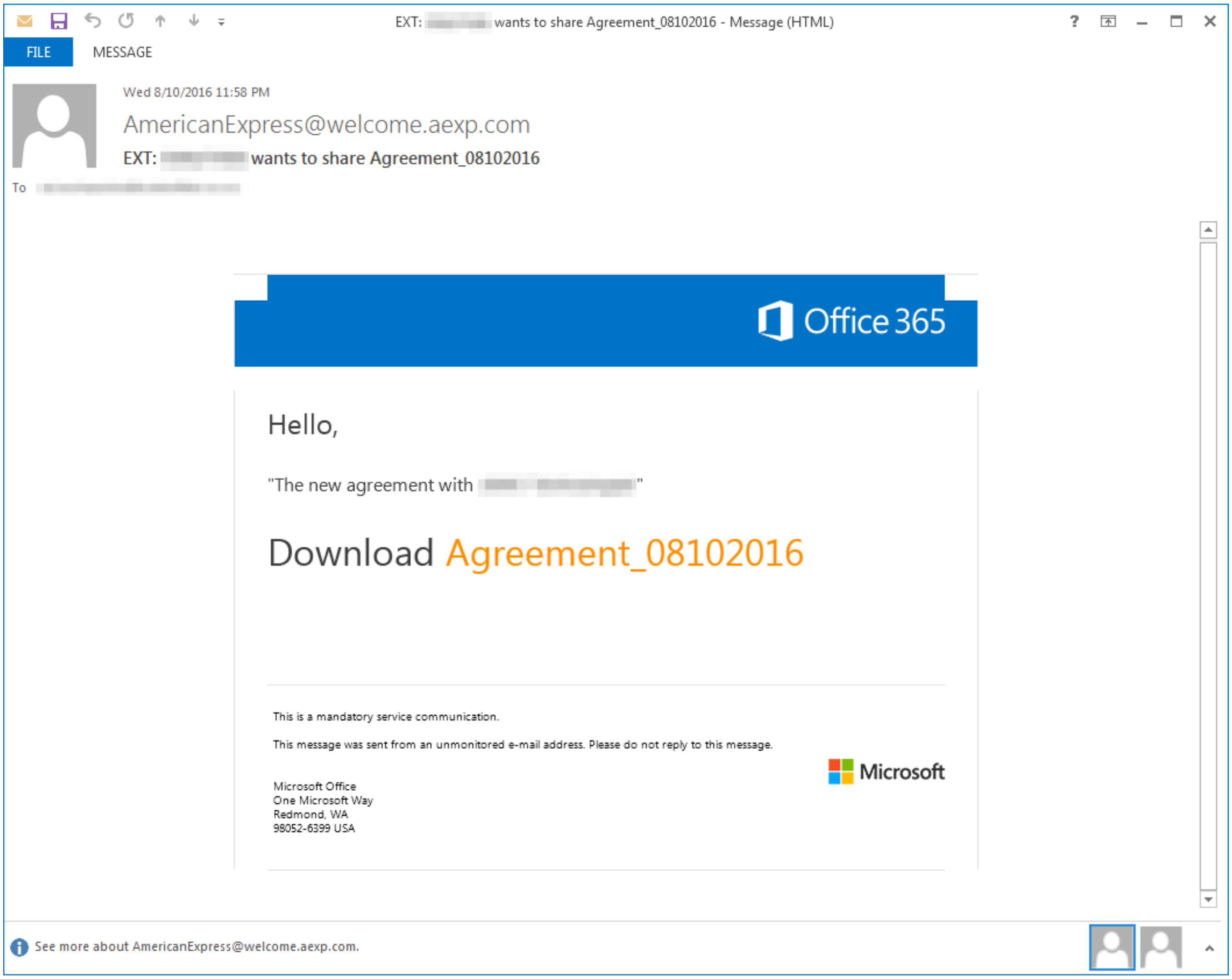
Please enter your case number: 34324

Security check code: h5wk6

Enter the numbers and letters displayed

Figure 11: 07-08-2016 - Fake court website leading to the download of Dreambot

In the next example, users in Australia were targeted with an email pretending be associated with Microsoft and Office365. The link in the email led directly to a zipped JavaScript downloader hosted on Microsoft Sharepoint; opening the file would install DreamBot. (Proofpoint researchers notified Microsoft about the hosted malware).



EXT: [redacted] wants to share Agreement_08102016 - Message (HTML)

Wed 8/10/2016 11:58 PM

AmericanExpress@welcome.aexp.com

EXT: [redacted] wants to share Agreement_08102016

To [redacted]

Office 365

Hello,

"The new agreement with [redacted]"

Download Agreement_08102016

This is a mandatory service communication.

This message was sent from an unmonitored e-mail address. Please do not reply to this message.

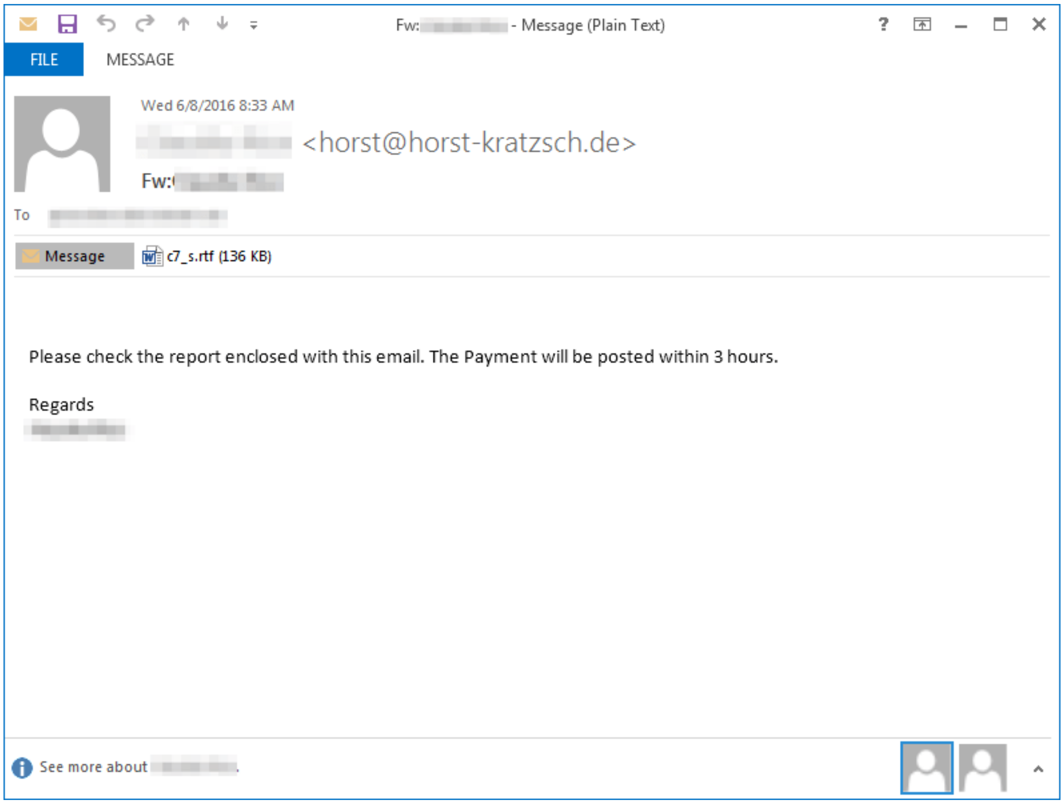
Microsoft Office
One Microsoft Way
Redmond, WA
98052-6399 USA

Microsoft

See more about AmericanExpress@welcome.aexp.com.

Figure 12: 08-11-2016 - Message used to distribute Dreambot in Australia via Microsoft SharePoint

In the following example, users in the United States received messages with attachments purporting to contain a record of a payment. The Microsoft Word document attachment contained malicious macros that, if enabled, downloaded Dreambot.



Fw: [redacted] - Message (Plain Text)

Wed 6/8/2016 8:33 AM

[redacted] <horst@horst-kratzsch.de>

Fw: [redacted]

To [redacted]

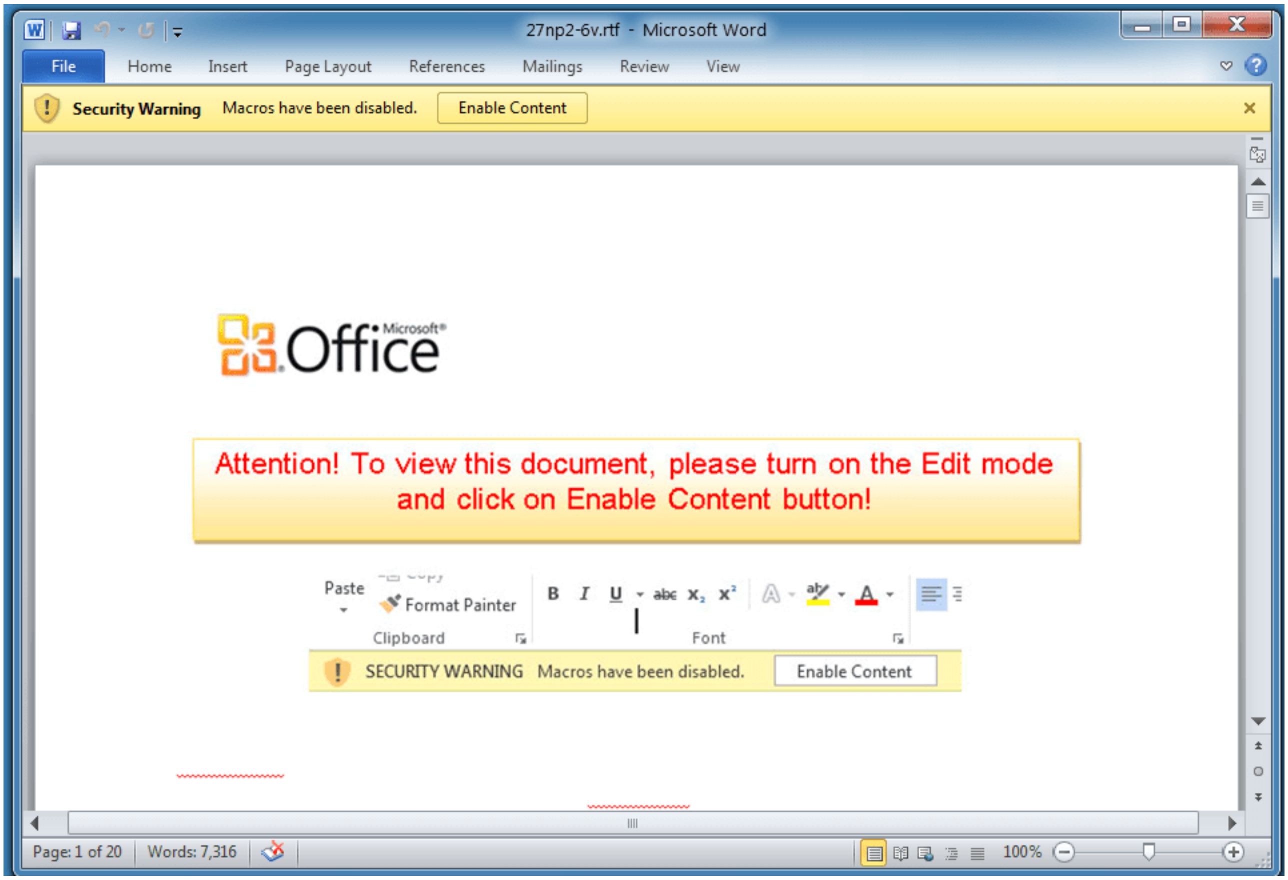
Message c7_s.rtf (136 KB)

Please check the report enclosed with this email. The Payment will be posted within 3 hours.

Regards
[redacted]

See more about [redacted].

Figure 13: 06-08-2016 - Message used to distribute Dreambot in the United States



27np2-6v.rtf - Microsoft Word

Security Warning Macros have been disabled. Enable Content

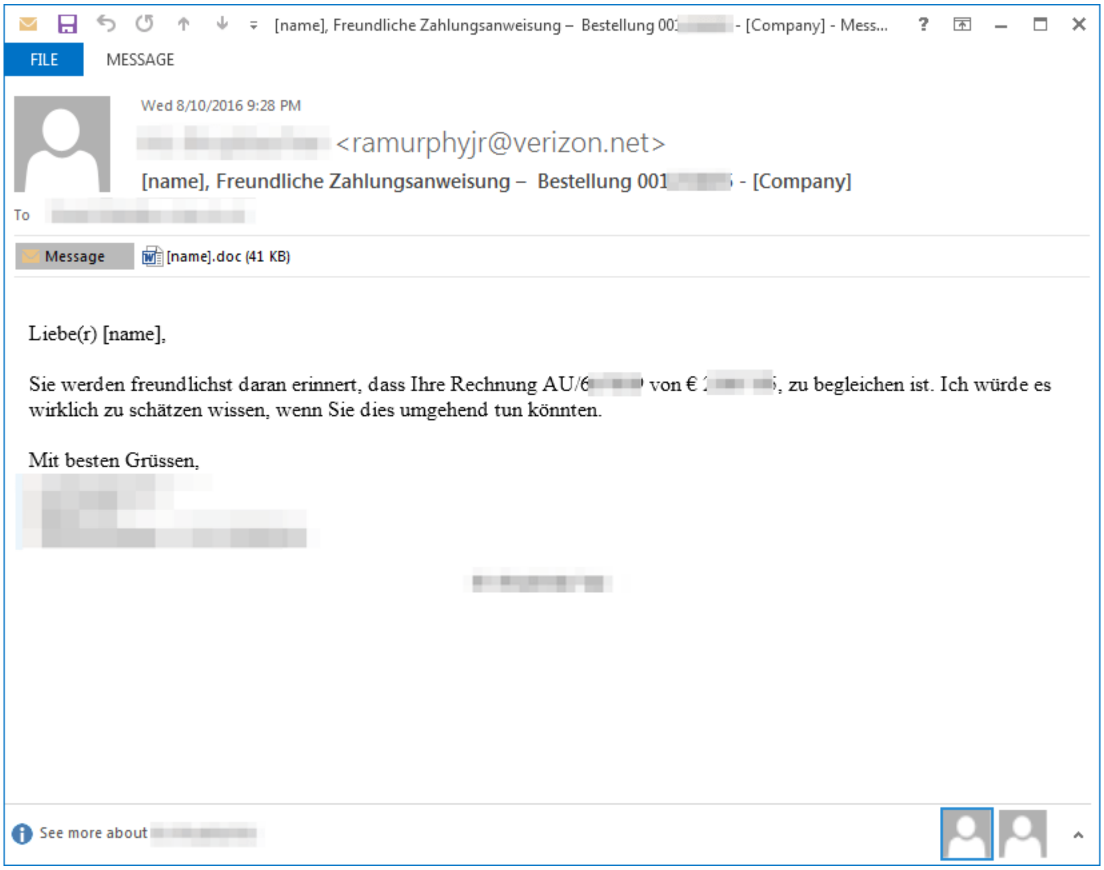
Attention! To view this document, please turn on the Edit mode and click on Enable Content button!

SECURITY WARNING Macros have been disabled. Enable Content

Page: 1 of 20 Words: 7,316 100%

Figure 14: 07-08-2016 - Microsoft Word attachment with malicious macros used to deliver Dreambot in the United States

In the next campaign, users in Switzerland received personalized messages in German containing their name and company name, claiming to attach an invoice for an order. The Microsoft Word attachment contained macros that, if enabled, would download Dreambot.



[name], Freundliche Zahlungsanweisung – Bestellung 00[redacted] - [Company] - Mess...

Wed 8/10/2016 9:28 PM

[redacted] <ramurphyjr@verizon.net>

[name], Freundliche Zahlungsanweisung – Bestellung 001[redacted] - [Company]

To [redacted]

[name].doc (41 KB)

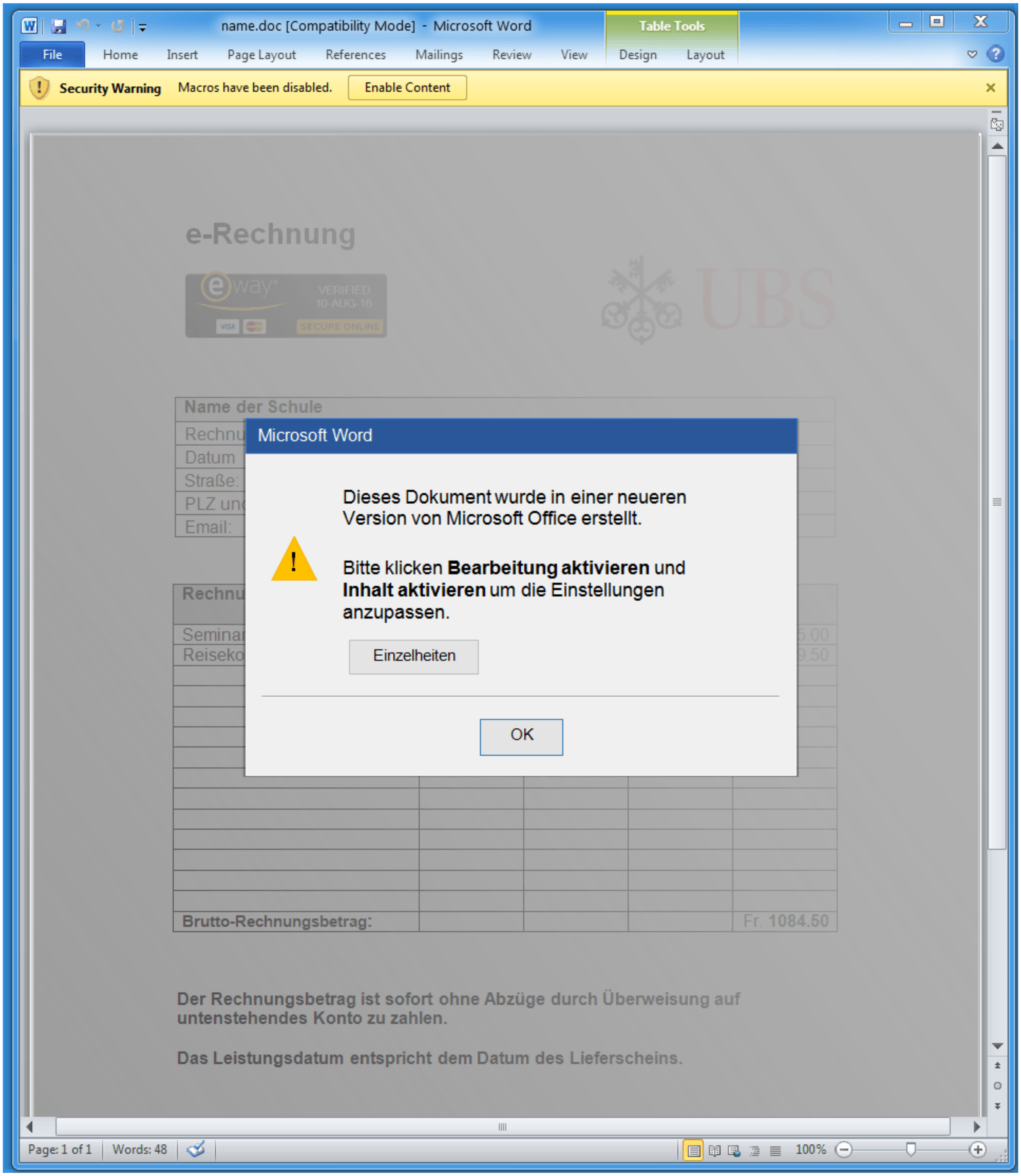
Liebe(r) [name],

Sie werden freundlichst daran erinnert, dass Ihre Rechnung AU/6[redacted] von € [redacted], zu begleichen ist. Ich würde es wirklich zu schätzen wissen, wenn Sie dies umgehend tun könnten.

Mit besten Grüssen,
[redacted]

[redacted]

Figure 15: 08-10-2016 - Message distributing Dreambot in Switzerland



Security Warning Macros have been disabled.

e-Rechnung

Name der Schule
Rechnu
Datum
Straße:
PLZ und
Email:

Rechnu				
Seminar				5.00
Reiseko				9.50
Brutto-Rechnungsbetrag:				Fr. 1084.50

Der Rechnungsbetrag ist sofort ohne Abzüge durch Überweisung auf untenstehendes Konto zu zahlen.

Das Leistungsdatum entspricht dem Datum des Lieferscheins.

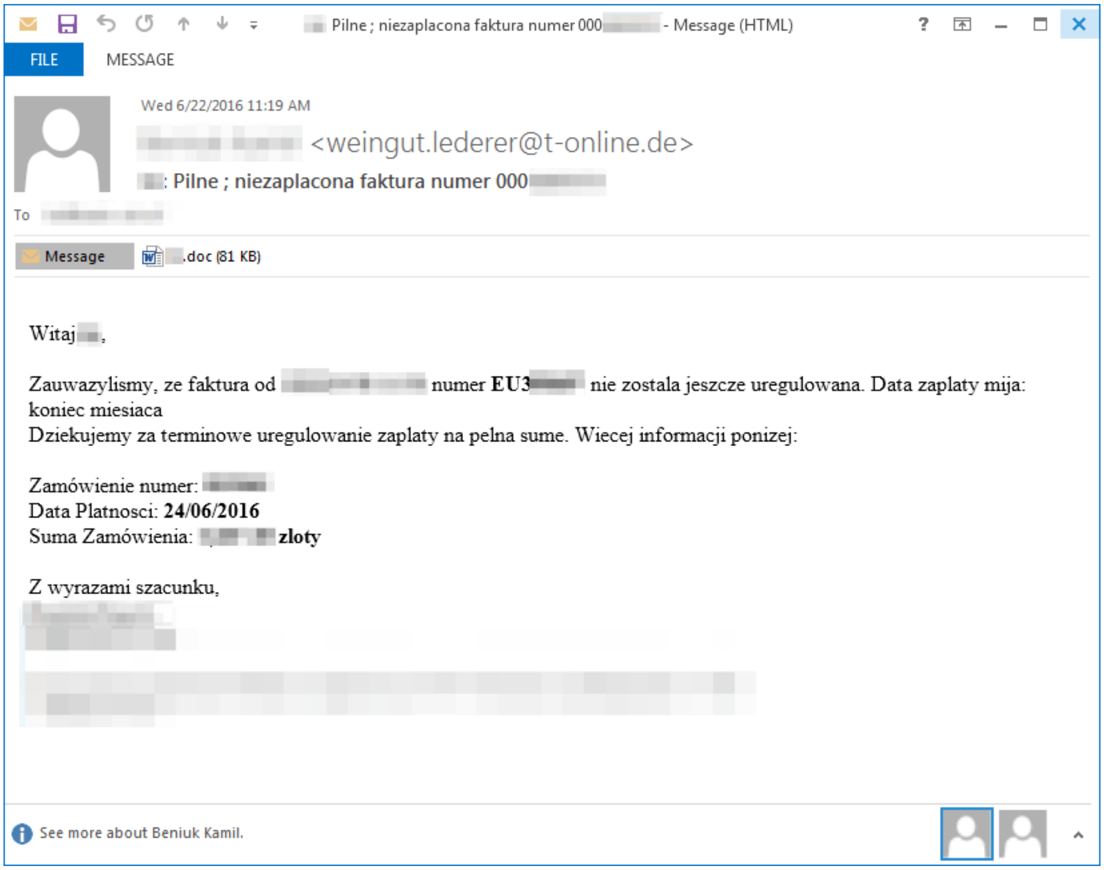
Microsoft Word

Dieses Dokument wurde in einer neueren Version von Microsoft Office erstellt.

Bitte klicken **Bearbeitung aktivieren** und **Inhalt aktivieren** um die Einstellungen anzupassen.

Figure 16: 08-10-2016 - Microsoft Word attachment used to deliver Dreambot in Switzerland

In another example, users in Poland were sent a personalized message using their name with a fake invoice document attachment for one of their purchases. The Microsoft Word attachments contained macros that, if enabled, would download Dreambot.



[redacted] Pilne ; niezaplacona faktura numer 000[redacted] - Message (HTML)
FILE
MESSAGE

Wed 6/22/2016 11:19 AM

[redacted] <weingut.lederer@t-online.de>

[redacted]: Pilne ; niezaplacona faktura numer 000[redacted]

To [redacted]

[redacted].doc (81 KB)

Witaj [redacted],

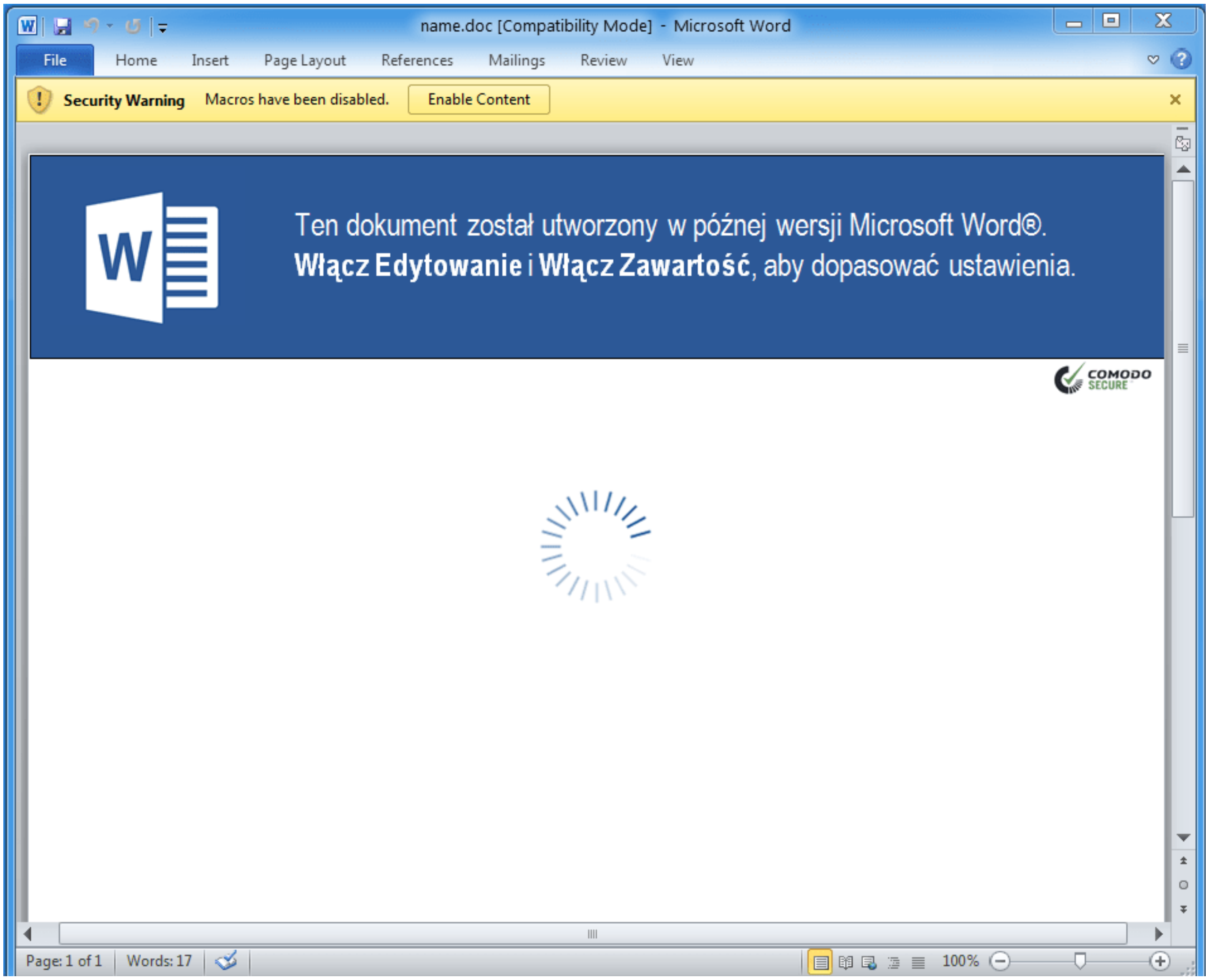
Zauwazylismy, ze faktura od [redacted] numer **EU3**[redacted] nie zostala jeszcze uregulowana. Data zaplaty mija: koniec miesiaca
Dziekujemy za terminowe uregulowanie zaplaty na pelna sume. Wiecej informacji ponizej:

Zamówienie numer: [redacted]
Data Platnosci: **24/06/2016**
Suma Zamówienia: [redacted] **zloty**

Z wyrazami szacunku,
[redacted]

See more about Beniuk Kamil.

Figure 17: 06-22-2016 - Message used to distribute Dreambot in Poland



Ten dokument został utworzony w późnej wersji Microsoft Word®.
Włącz Edytowanie i **Włącz Zawartość**, aby dopasować ustawienia.

Figure 18: 06-22-2016 - Microsoft Word attachment used to distribute Dreambot in Poland

Conclusion

Dreambot is one of the most active banking Trojans we have seen recently, with distribution vectors across a variety of exploit kits and both malicious document attachment and URL-based email campaigns. Often referred to as Ursnif and Gozi ISFB, Dreambot is being distributed in countries around the world and is under active development. In particular, we have observed samples with C&C communications enabled over both Tor and P2P. For Tor-enabled versions in particular, Dreambot activity on infected machines can be especially hard to detect at the network level, creating new challenges for defenders and IT organizations alike.

We will continue to monitor Dreambot and its growing list of capabilities as the banking Trojan landscape evolves.

References

Indicators of Compromise (IOC’s)

Payloads delivered by Exploit Kits:

Hash	Date	Description	Vector
a14d9ad2b03dd5f6360139f2772a303066ed292c51b0777cbece7b92d4a9e62c	2015-09-11	Dreambot	Chain of Compromise to Niteris
1448a395e741a419e5e7abb3f3bc2e6c46588823f093c93c695fffe0a69c17ee	2016-04-11	Dreambot	GooNky Malvert into Angler
e06b753aa98e1b8fdc7c8ee1cbd07f5d46b2bbf88ebc8d450c8f24c6e79520a4	2016-05-10	Dreambot	AdGholas Malvertising into Angler

bd3c470fc6999212373c2c31b08d9944d4bee3baf79bd75a233743ad64845481	2016-05-10	Dreambot	EITest chain into Angler
54405a8cfa557b33e5a1e0c5b69433fce900c96a34496949da501c844b0e7919	2016-06-03	Dreambot (P2P)	
1dca7b73070679b796a2318c6e11ed0bb65bf66e5cc782b475bb43d735915e6c	2016-06-03	Dreambot	EITest chain into Angler
0d6014f1d2487230c3bb38f31d2742577f84fd2f2e0d97be5fb9cf28b7ab6de9	2016-07-09	Dreambot	Malvertising to Neutrino
f70a7b04a475c7140049ec586eb3f7c7a3480ddaac53c15db4905915e9dea52b	2016-07-20	Dreambot	EITest chain into Neutrino
8664c68d5c1ef72f32485c61704ce4fb350c95952a17908908a420443b411414	2016-07-20	Dreambot	Undocumented actor into Neutrino
c25b56c5ea2d0af3cf6057f974f1c3a06845ab41f61c8895aaaad55aafaeed7e	2016-08-12	Dreambot	Undocumented actor into RIG
04ea4e0417f1f49bc349efe7ee07c0bdf145a98dd7358610f598395246b4c433	2016-08-15	Dreambot	Undocumented actor into RIG
54405a8cfa557b33e5a1e0c5b69433fce900c96a34496949da501c844b0e7919	2016-08-15	Dreambot	EITest chain into RIG
8aa2442fb7a489d0c7f50a2220e0fd4ead270ff812edc3721a49eec5784a1ad6	2016-08-15	Dreambot (tor)	EITest chain into RIG into Smokebot
446a639371b060de0b4edaa8789f101eaeae9388b6389b4c852cd8323ec6757c	2016-08-15	Smokebot	EITest chain into RIG
396bd75514ab92e007917c1d136f1993466c0913a532af58386ccb99d5f60ef3	2016-08-24	IAP	Malvertising into RIG

Payloads delivered by Email:

Hash/Link
0edde27c90bbb55d80b89a2ce0baa21feb69a1420dbb1a15059b6bdfde994fde
[hxxp://easypagemachine[.]com/kshf[.]jpg]
2720d7cc899337adf5f021eeddb313f4317fc46f9c6e83bde9f47458b2d955e7
6e0da9199f10ff5bd6d2f4e5309cde2332d534cbb3364e15cb0f7873455e0eb5
[hxxp//safiidesign[.]com/winword[.]bin]
7e0bf604d3ab673a519feb5d5375f0f88cf46e7cd1d3aa301b1b9fb722e9cef7

[hxxp://pechat-suveniri[.]com/mam5pcan8wynct/hwd7popy[.]php]
0195bf393584b203334c4ca3934e72e388e8e579cde35fa8db892d2ee306dc16
[hxxp://ue-craft[.]ru/1ryvq8owo/rukdl1[.]exe]
84bc2608707859a0643be642128b351757dc1f43f5b0a88b5448764dfc23487d
b6d6fc672f8b45eed0e88601dea2390e7d0dc01e63840ab840613dd3d6939ad7
[hxxp://one99two[.]com/cgi/office16[.]bin]
85f68545c6d98dd6a6a00859ec136d8a8fd06c20ce189e39ce78f6685da40d4e
[hxxps://searchfinancial-my[.]sharepoint[.]com/personal/tariq_searchfinancial_com_au/_layouts/15/guestaccess[.]aspx?guestaccesstoken=4GPoi4OBx0cZ%2bhMi6vHvpfR1vqc9vmqwU6WuwK6%2b7U8%3d&docid=0ec6abef70a134e70978ed191c8364229&rev=1]
414b3cbc230768d9930e069cb0b73173fe9951e82486f0d6524addf49052d5ad
[hxxp://www[.]wizardwebhosting[.]com/css/header[.]css]
3cde892a8faddd4aaf90e8455698719516ab96ea6d116af21353c08375d457b9

Select ET Signatures that would fire on such traffic:

2021813 || ET TROJAN Ursnif Variant CnC Beacon
2021829 || ET TROJAN Ursnif Variant CnC Beacon 4
2022970 || ET TROJAN Ursnif Variant CnC Beacon 6
2018789 || ET POLICY TLS possible TOR SSL traffic
Multiple || ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group **

Subscribe to the Proofpoint Blog