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

Adrian Korczak
Head of Network Security
Methods Team
NASK - Research and
Academic Computer
Network
adrian.korczak@nask.pl
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

Sample execution

Current behavior analysis (automatic systems + analyst)

Long term observation (analyst)
System architecture
- External snapshots
- CPU usage limitation
- Emails never leave the sandbox environment
- Network bandwidth limited
- External snapshots
- CPU usage limitation
- Emails never leave the sandbox environment
- Network bandwidth limited
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

- 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": [
        "caziudah.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",
        "huvanauy.me",
        "wiuhlaav.mobi",
        "dieetamax.name",
        "zuimabra.us",
        "ufqeubeb.biz",
        "piqaialas.net"
    ],
    "DGA_family": "DGArchive_unknown",
    "domains_count": 8
}
```
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
<table>
<thead>
<tr>
<th>Protocol</th>
<th>DNS commands</th>
<th>SMTP commands</th>
<th>DNS commands</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tofsee</td>
<td>DNS</td>
<td>DNS_PTR, DNS_MX, DNS_A, DNS_AAAA</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Tofsee</td>
<td>SMTP</td>
<td>EHLO, MAIL, RCPT, DATA, QUIT, HELO</td>
<td>-</td>
<td>53</td>
</tr>
<tr>
<td>Tofsee</td>
<td>TLS/SSL</td>
<td>-</td>
<td>-</td>
<td>443</td>
</tr>
<tr>
<td>Tofsee</td>
<td>HTTP</td>
<td>-</td>
<td>GET</td>
<td>80</td>
</tr>
<tr>
<td>Tofsee</td>
<td>UNKNOWN/NOT_IMPLEMENTED</td>
<td>-</td>
<td>-</td>
<td>483, 42, 7, 8, 88, 7</td>
</tr>
</tbody>
</table>
Network Traffic analyzer - SMTP characteristics

Tofsee abused SMTP ports

- Port 25: 25
- Port 427: 427
- Port 26: 26
- Port 587: 587

Emotet abused SMTP ports

- Port 25: 25
- Port 587: 587
- Port 26: 26
- Port 2525: 2525

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.
<table>
<thead>
<tr>
<th>From</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Peyton&quot; <a href="mailto:jxjauhxo@tel.ru">jxjauhxo@tel.ru</a></td>
<td>Bet you'll never find better offer for Viagra.</td>
</tr>
<tr>
<td>&quot;Khloe&quot; <a href="mailto:sqmrtako@tel.ru">sqmrtako@tel.ru</a></td>
<td>Viagra - your main equipment for love adventures.</td>
</tr>
<tr>
<td>&quot;Elliana&quot; <a href="mailto:rvkelizns@tel.ru">rvkelizns@tel.ru</a></td>
<td>All the power of lust with best ED remedy. Viagra.</td>
</tr>
<tr>
<td>&quot;Melody&quot; <a href="mailto:pminxgtzlm@tel.ru">pminxgtzlm@tel.ru</a></td>
<td>More firmness with Viagra. Bet you won't find cheaper.</td>
</tr>
</tbody>
</table>

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/A1uoUj1b7?i=2DByk

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/A1uoB8DD742wVnk
<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Know &lt;IKnow1000168.com&gt;</td>
<td>I <a href="mailto:know@yahoo.com">know@yahoo.com</a></td>
<td>I recorded you - 091592</td>
</tr>
<tr>
<td>I Know &lt;IKnow1108536.com&gt;</td>
<td>I <a href="mailto:know@hotmail.com">know@hotmail.com</a></td>
<td>I recorded you - xtort97</td>
</tr>
<tr>
<td>I Know &lt;IKnow662956.com&gt;</td>
<td>I <a href="mailto:know@hotmail.com">know@hotmail.com</a></td>
<td>You got recorded - armyp3540</td>
</tr>
<tr>
<td>I Know &lt;IKnow0700705.com&gt;</td>
<td><a href="mailto:99999@yahoo.ca">99999@yahoo.ca</a></td>
<td>Video of you - 22334455</td>
</tr>
</tbody>
</table>

Content:

"Hey, I know your password is: [REDACTED] Your 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". My 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. I collected all your private data and I RECORDED YOU (through your webcam) SATISFYING YOURSELF! After that I removed my malware to not leave any traces. I 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! Only you can prevent me from doing this and only I can help you out in this situation. Transfer exactly 900$ with the current bitcoin (BTC) price to my bitcoin address. It's a very good offer, compared to all that horrible shit that will happen if I publish everything! You can easily buy bitcoin here: www.paxful.com, www.coingate.com, www.coinbase.com, or check for bitcoin ATM near you, or Google for other exchanger. You 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. My bitcoin address is: 1LyC6ss5B2nIF3VWRBTVZFEzxsweyPGQ. Copy and paste my address, it's (cAs
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.cn

Source: urlscan.io

ПРИМЕТЕ НАШИ ПОЗДРАВЛЕНИЯ!
Вы выиграли денежный приз!

http://stolotoo.vip/yN26JY

-----

Global Lending Partners

Source: urlscan.io
2019-10-15 - #malspam pushing #Shade (#Troldeh) #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...

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 #Troldeh
A few js dropper distribution urls: pastebin.com/raw/FB5Fvv90

https://twitter.com/malware_traffic/status/1184520519275728899
### SPAM analysis - Emotet

<table>
<thead>
<tr>
<th>imf_from</th>
<th>imf_to</th>
<th>mail_analysis.urls</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Askullogist.co&quot;&lt;@pci-connector.com&gt;</td>
<td>ASKUL LOGIST&lt;@askullogist.com&gt;</td>
<td><a href="http://www.askullogist.co.jp">www.askullogist.co.jp</a></td>
</tr>
<tr>
<td>&quot;Askullogist.co&quot;&lt;valmeca.ru&gt;</td>
<td>shi&lt;@askullogist.co.jp&gt;</td>
<td><a href="http://www.askullogist.co.jp">www.askullogist.co.jp</a></td>
</tr>
<tr>
<td>&quot;Askullogist.co&quot;&lt;grandsuhahotel.com&gt;</td>
<td></td>
<td><a href="http://www.askullogist.co.jp">www.askullogist.co.jp</a></td>
</tr>
</tbody>
</table>

### File metadata

<table>
<thead>
<tr>
<th>Filename</th>
<th>WRX-110119-112819.doc</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
<td>41a597173b1df6bf33f6fa1d456b4f93</td>
</tr>
</tbody>
</table>
### SPAM analysis - Emotet

<table>
<thead>
<tr>
<th>sandbox_malware_family</th>
<th>email_content_text.content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emotet</td>
<td>Gentile Cliente, abbiamo notato una fattura non paga ta sull'ultima fattura 095601797285877164-Scadenza-13/1 0/2019 di 63,22 € la società ENEL informa che il serv izio energia sarà sospeso dal 15/1</td>
</tr>
<tr>
<td></td>
<td>20eb81c0fe6446323ff6c56636401564eb63658e</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: 095601797285877164.doc</td>
<td>7b7a97231a8bf1f0563cc0fb295372aa</td>
</tr>
<tr>
<td>Size: 219648</td>
<td>89d48d08bea2f68bffc2c148f415d474c73c9df1e5a2862173213449381f65cf</td>
</tr>
</tbody>
</table>
Gentile Cliente, abbiamo notato una fattura non pagata sull’ultima fattura № <var 0> di <var 1> € la società ENEL informa che il servizio energia problema reinviamo la fattura Cordiali saluti, <var 2> Enel Energia <var 3>
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
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://adserver.afilol/pl/red_fi/1405/1/5555/62476/fraud/0/0/0063ce6b7-6aa9-4055-9674-80e5d8235f97/0/?l=https%3a%2f%2fad.doubleclick.net%2fddm%2ftrackclk%2fN2004.1937504GRUPAZPR.PL%2fB8502102.247049999%3bdc_trk_aid%3d443615273%3bdc_trk_cid%3d116400487%3bdc_lat%3d%3bdc_rdid%3d%3btag_for_child_directed_treatment%3d%3bfua%3d%3fhtps%3a%2f%2fwww.leroymerlin.pl%2fhydraulika%2fkanalizacja-wewnetrzna%2fsyfony%2fkorek-click-clack-brodzikowy-wannowy-wirquin%2cp245313%2cl675.html%3futm_source%3dgrupazpr.pl%2futm_medium%3dfeed%2futm_content%3dfeed%2futm_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
Command to grab password from Chrome browser

- In next commands: PuTTY, RDP
### Lethic - tracking changes in behavior with HTTPS

<table>
<thead>
<tr>
<th>Dst IP / Country</th>
<th>Dst Port</th>
<th>Databases / Bytes</th>
<th>Packets</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>31.13.92.36</td>
<td>443</td>
<td>3,673</td>
<td>8</td>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
</tr>
<tr>
<td>IE</td>
<td></td>
<td>4,105</td>
<td></td>
<td></td>
</tr>
<tr>
<td>157.240.20.19</td>
<td>443</td>
<td>132,173</td>
<td>26</td>
<td>scontent-frt3-2.xx.fbcdn.net</td>
</tr>
<tr>
<td>US</td>
<td></td>
<td>133,577</td>
<td></td>
<td></td>
</tr>
<tr>
<td>157.240.20.19</td>
<td>443</td>
<td>15,620</td>
<td>13</td>
<td>external-frt3-2.xx.fbcdn.net</td>
</tr>
<tr>
<td>US</td>
<td></td>
<td>16,322</td>
<td></td>
<td></td>
</tr>
<tr>
<td>172.217.168.238</td>
<td>443</td>
<td>1,268</td>
<td>7</td>
<td>clients4.google.com</td>
</tr>
<tr>
<td>US</td>
<td></td>
<td>1,645</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31.13.92.10</td>
<td>443</td>
<td>2,299</td>
<td>24</td>
<td>edge-chat.facebook.com</td>
</tr>
<tr>
<td>IE</td>
<td></td>
<td>3,595</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- Tracking behavior with classification of HTTP requests
- Created request fingerprinting mechanism to group the messages
Tracking HTTP - Emotet and Trickbot on one machine

POST /ktwl [redacted] HTTP/1.1
Referer: http://95.219.199.225/ktwl [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

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

--[redacted]
Content-Disposition: form-data; name="proclist"
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 checks 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
Emotet change in URL

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

POST /HP5X HTTP/1.1
Referer: http://190.97.30.167/HP5X
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
Feeding external systems

- Extracting static configuration
- Decoding C&C exchange
- Artifacts extraction (webinjests, dlls)
Static configuration extraction

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

<table>
<thead>
<tr>
<th>Family</th>
<th>danabot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config type</td>
<td>static</td>
</tr>
<tr>
<td>+ campaign_const</td>
<td>785342789</td>
</tr>
<tr>
<td>+ campaign_id</td>
<td>7</td>
</tr>
<tr>
<td>+ rsa_key</td>
<td>8gIAAAAkAABSU9ExAAQAAAABQQQ0b31Ec2TuS6DvGew/JXVqU5Bby0yL9UqZ50/VQ1Tj_</td>
</tr>
<tr>
<td>+ type</td>
<td>danabot</td>
</tr>
<tr>
<td>+ urls</td>
<td>[&quot;138.167.173.24&quot;, &quot;73.114.1.155&quot;, &quot;45.172.198.33&quot;, &quot;188.88.36.122&quot;,...</td>
</tr>
<tr>
<td>Upload time</td>
<td>Thu, 03 Oct 2019 18:26:42 GMT</td>
</tr>
</tbody>
</table>
Extracting artifacts from PCAP files

```
{'pwhpya': 'fgbcbjvaq', 'soft': '1', 'version': '217027', 'empty response
>>> inject
{'ihsv': 'jvalpxo', 'soft': '1', 'version': '217027', 'use empty response
>>> task
{'rpojdb': 'sul', 'soft': '1', 'version': '217027', 'user empty response
>>> inject
{'fpg': 'wymednl', 'soft': '1', 'version': '217027', 'use empty response
>>> task
{'etwwmm': 'guks', 'soft': '1', 'version': '217027', 'user empty response
>>> inject
{'odbb': 'kkjnsib', 'soft': '1', 'version': '217027', 'use
```
- 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

<table>
<thead>
<tr>
<th>Filename</th>
<th>Black_Friday_Promo.doc</th>
</tr>
</thead>
<tbody>
<tr>
<td>File size</td>
<td>199587</td>
</tr>
<tr>
<td>File type</td>
<td>Composite Document File V2 Document, Little Endian, Os: WindkSnke Harting, Template: Normal.dotm, Revision Number: 1, Nam Nov 29 07:04:00 2019, Last Saved Time/Date: Fri Nov 29 07:04:00 Characters: 340, Security: 0</td>
</tr>
<tr>
<td>md5</td>
<td>63e6a22df803a30e5be520f1b75fbbf</td>
</tr>
<tr>
<td>sha1</td>
<td>140f2a9d47f5d5c71899afdf0e1e03cee3840d12</td>
</tr>
<tr>
<td>sha256</td>
<td>f4355df85abdb94ef49e8053d1a04cfcc06798088f0d9c99b30</td>
</tr>
</tbody>
</table>

- 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

Found emotet distribution urls:
- [http://www.mobiextend.com/New_website/mZUOdoa/](http://www.mobiextend.com/New_website/mZUOdoa/)
- [http://www.onlineboutiquelc.com/wp-includes/EDoZV/](http://www.onlineboutiquelc.com/wp-includes/EDoZV/)
- [https://www.cirugiurologica.com/wp-content/SX/](https://www.cirugiurologica.com/wp-content/SX/)
- [https://isella.edu.uir.ac.id/sitemapxml/F9i/](https://isella.edu.uir.ac.id/sitemapxml/F9i/)
- [https://hssc.co.uk/tmp/kp4/](https://hssc.co.uk/tmp/kp4/)
Summary
## Similar systems

<table>
<thead>
<tr>
<th>Project name</th>
<th>Description</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://github.com/jbremer/long">https://github.com/jbremer/long</a> cuckoo</td>
<td>Cuckoo Sandbox fork for longterm analysis</td>
<td>LTS is agentless, with own instrumentation and analyses</td>
</tr>
<tr>
<td><a href="https://www.stratosphereips.org">https://www.stratosphereips.org</a></td>
<td>Bare-metal hosts with continuous execution</td>
<td>LTS - virtualized environment, periodical execution, other monitoring systems</td>
</tr>
<tr>
<td>BotWatcher - T. Barabosch et al.</td>
<td>Monitoring of memory dumps and network traffic to infer malware behavior and reconstruct it</td>
<td>LTS equipped with less sophisticated analyses, focused on longer periods of monitoring and more operational outputs</td>
</tr>
</tbody>
</table>
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 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, psroki1,
Krzysztof Andrusiak, Mateusz Goniprowski
Tracking botnets with Long Term Sandboxing