Why Them?
Extracting Intelligence about Target Selection from Zeus Financial Malware

Samaneh Tajalizadehkhoob
Hadi Asghari
Carlos Gañán
Michel van Eeten
Economics of Cybersecurity Group, Delft University of Technology

Outline

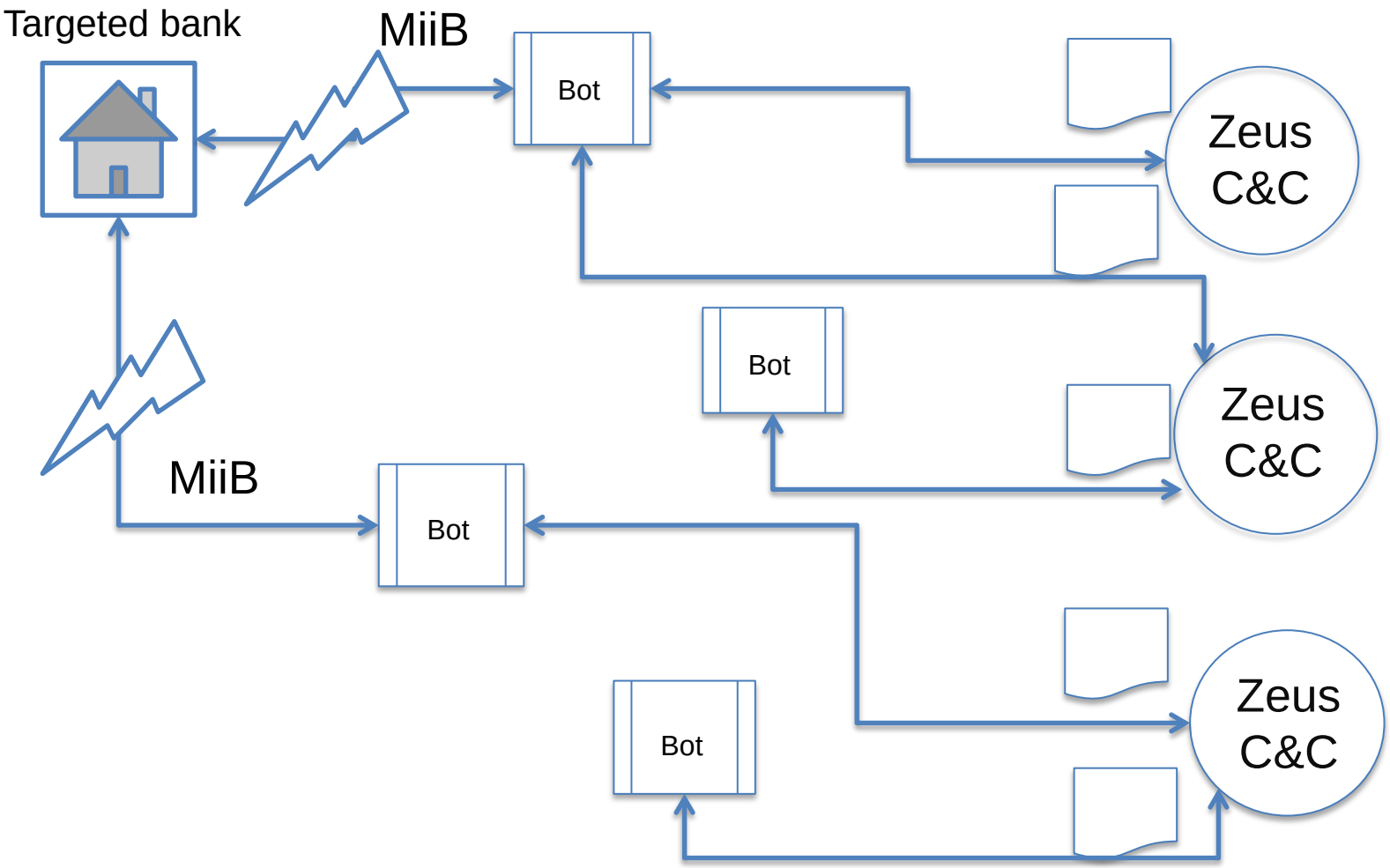
1. Problem of online banking fraud
2. Zeus malware
3. Capturing attackers' instructions from infected machines
4. Extracting intelligence from the instructions (targets, inject code)
5. Who is being targeted?
6. Do bigger targets attract more attacks?
7. How fast do attackers explore new targets?
8. Did the sudden availability of Zeus source code increase attacks?
9. How does inject code evolve?
10. Conclusion

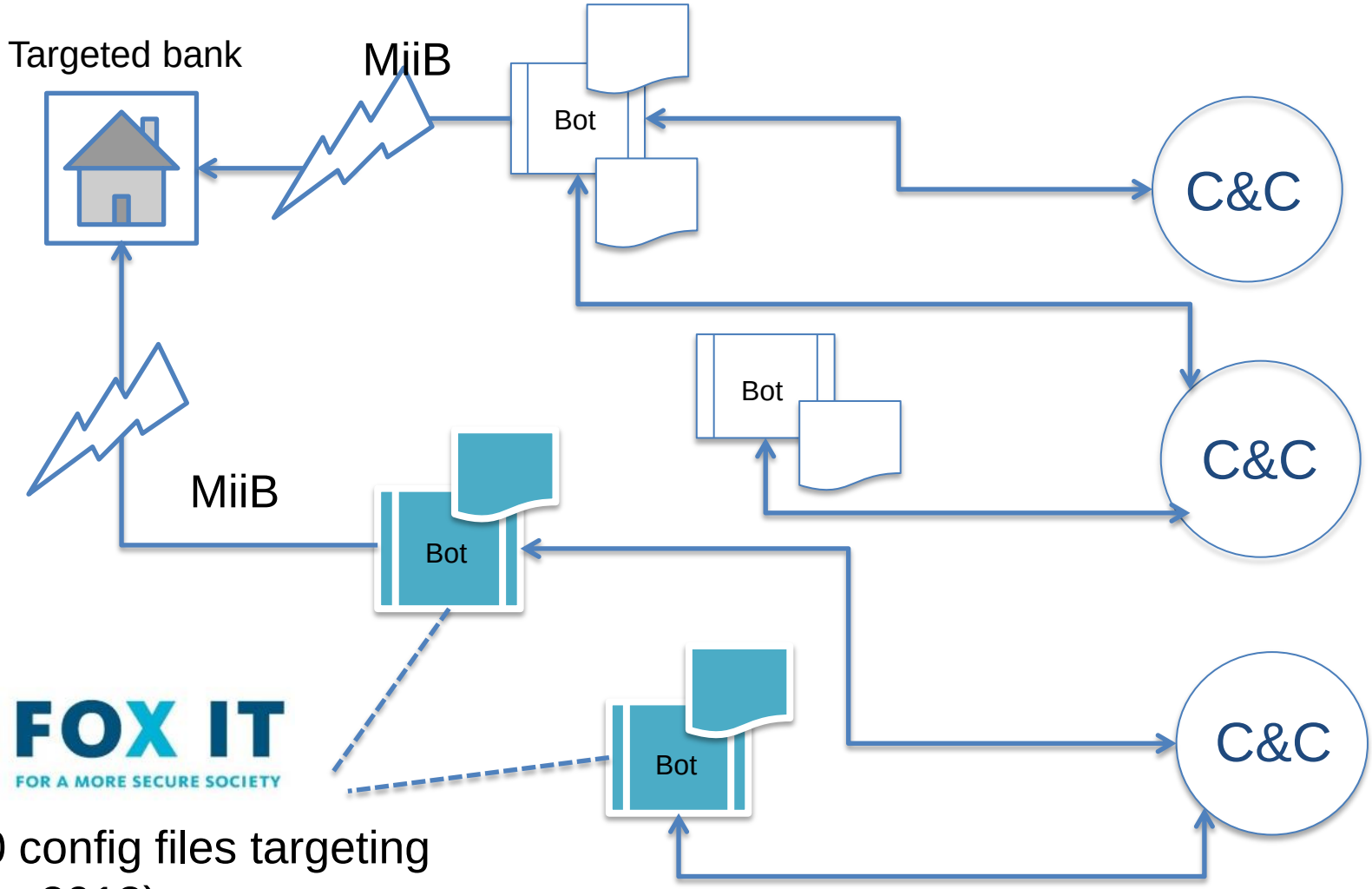
Online banking fraud

- Fraud statistics for the Single European Payment area are around €800 million (European Central Bank, 2014)
- Different banks with different properties are targeted around the world
- No clear patterns have been found till now
- Little information is published about the targeted domains
- Even when the information exists, it is incomplete and under/over counted

Outline

1. Problem of online banking fraud
2. Zeus malware
3. Capturing attackers' instructions from infected machines
4. Extracting intelligence from the instructions (targets, inject code)
5. Who is being targeted?
6. Do bigger targets attract more attacks?
7. How fast do attackers explore new targets?
8. Did the sudden availability of Zeus source code increase attacks?
9. How does attack code evolve?
10. Conclusion


Targeted bank
MiiB
Bot
Zeus
C&C
Bot
Zeus
C&C
MiiB
Bot
Bot
Zeus
C&C



FOX IT
FOR A MORE SECURE SOCIETY

11,000 config files targeting
(2009 - 2013)

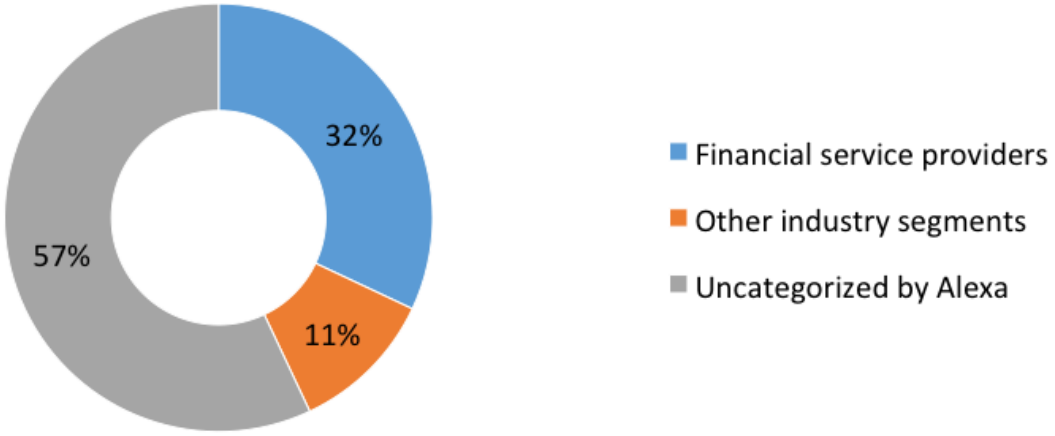
```
Mask 0x64
 Target URL          : "https://www.signatureny.web-access.com/signat/cgi-bin/*
 data_before
  <FORM NAME="login_form" METHOD=post action="
 data_after
  "
 data_inject
  https://www.signatureny.web-access.com/signat/cgi-bin/welcome.cgi

 data_before
  <FORM NAME="login_form"*>
 data_after

 data_inject
  <input type="hidden" name="injtoken" value="data">

 data_before
  name="SecurityCode">*</tr>
 data_after
 Mask 0x24
 Target URL          : "https://www.signatureny.web-access.com/signat/cgi-bin/welcome.cgi
 Do   fake if form contains: "*injtoken*
 data_before
  <HTML>
 data_after
  </HTML>
 data_inject
  <head>
 <title>Cash management website is currently unavailable</title>
 <img src="https://www.signatureny.web-access.com/signat/images/HC/loginban.gif"><br><br>
 <h2>Due to system maintenance, online banking will be unavailable for 24 hours. Please try to access this page at
a later point or if you have any questions contact our technical support desk at 1-888-236-0232. .</h2>
 </center>
 </body>


 Mask 0x64
 Target URL          : "https://*treasury.pncbank.com/*/login.ht
 data_before
  <head>
 data_after

 data_inject
  <script type="text/javascript" src="https://ajax.googleapis.com/ajax/libs/jquery/1.3.2/jquery.min.js"></script>
 <link rel="stylesheet" type="text/css"
href="https://ajax.googleapis.com/ajax/libs/jqueryui/1.7.1/themes/start/ui.all.css" />
 {
```

Outline

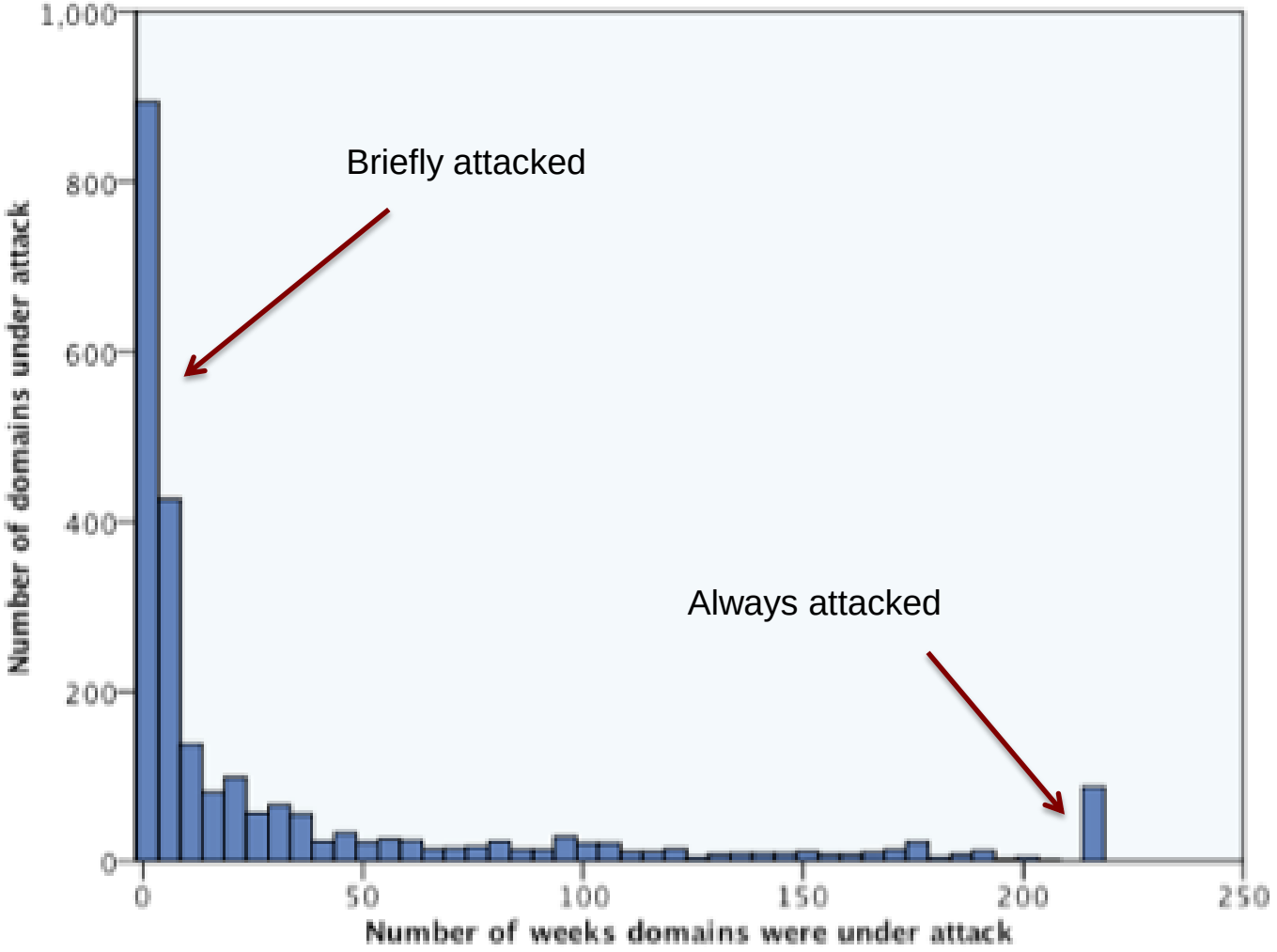
1. Problem of online banking fraud
2. Zeus malware
3. Capturing attackers' instructions from infected machines
4. Extracting intelligence from the instructions (targets, inject code)
5. Who is being targeted?
6. Do bigger targets attract more attacks?
7. How fast do attackers explore new targets?
8. Did the sudden availability of Zeus source code increase attacks?
9. How does attack code evolve?
10. Conclusion

Targeted domains

- Between January 2009 and March 2013, 2,131 unique botnets were in operation (based on different encrypted command and control channels)
- These botnets targeted 2,412 unique domains – via 14,870 unique URLs
- Located in 92 countries
- Over 74% of the targets are financial service providers



Attack persistence

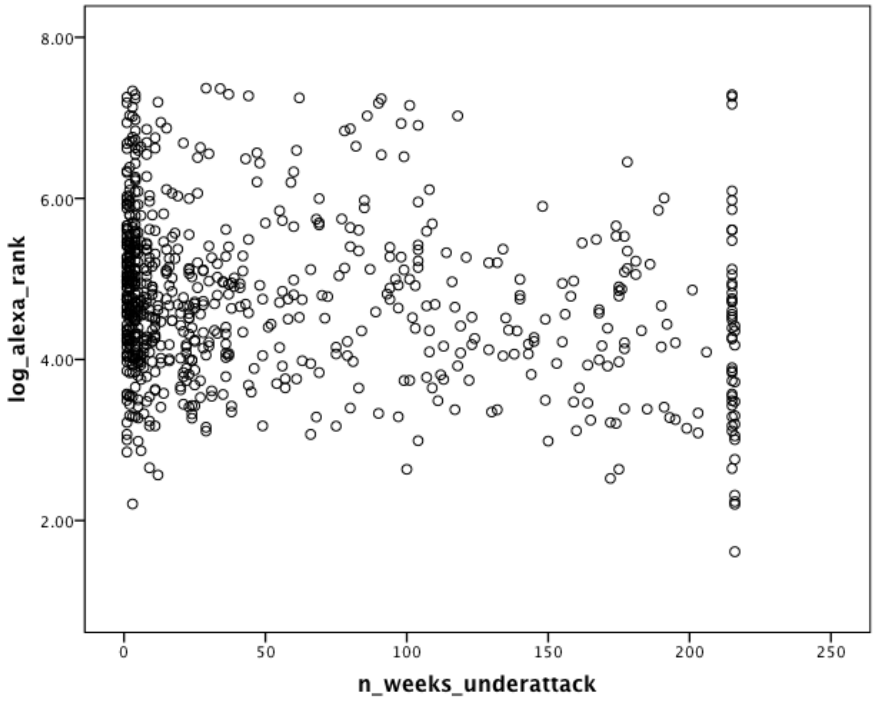


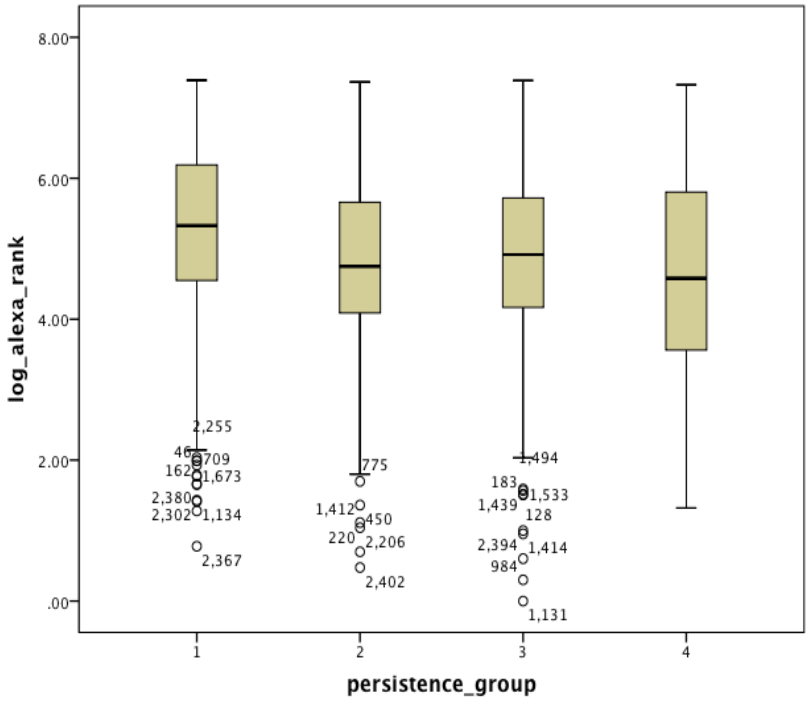
Outline

1. Problem of online banking fraud
2. Zeus malware
3. Capturing attackers' instructions from infected machines
4. Extracting intelligence from the instructions (targets, inject code)
5. Who is being targeted?
6. Do bigger targets attract more attacks?
7. How fast do attackers explore new targets?
8. Did the sudden availability of Zeus source code increase attacks?
9. How does attack code evolve?
10. Conclusion

Is target popularity related to its size?

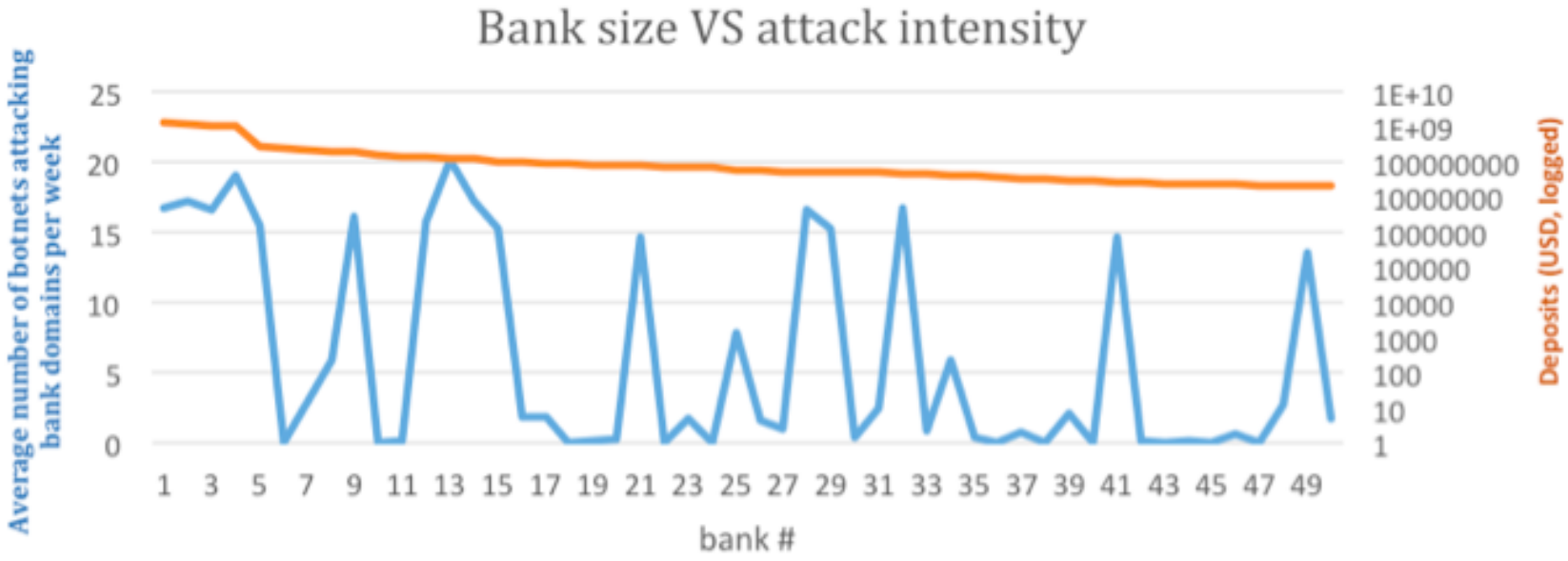
- Minor, but significant relationship between the size of a domain (measured by Alexa ranking) and the persistence of attacks





Is target popularity related to its size?

- United States: out of around 6,500 financial institutions with online presence, only 175 have been targeted
- Almost all of the larger banks (48 of the top 50) are attacked
- Size acts as a threshold for being attacked; it does not predict attack intensity

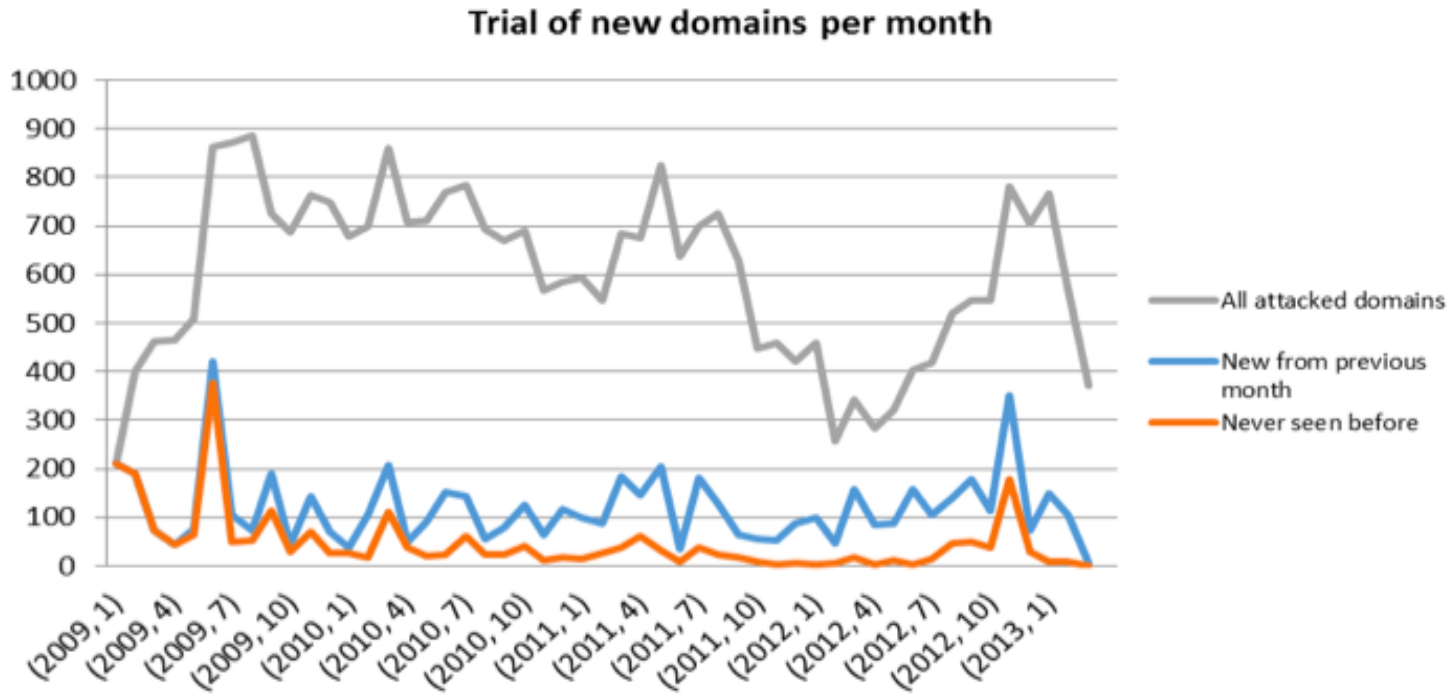


Outline

1. Problem of online banking fraud
2. Zeus malware
3. Capturing attackers' instructions from infected machines
4. Extracting intelligence from the instructions (targets, inject code)
5. Who is being targeted?
6. Do bigger targets attract more attacks?
7. How fast do attackers explore new targets?
8. Did the sudden availability of Zeus source code increase attacks?
9. How does attack code evolve?
10. Conclusion

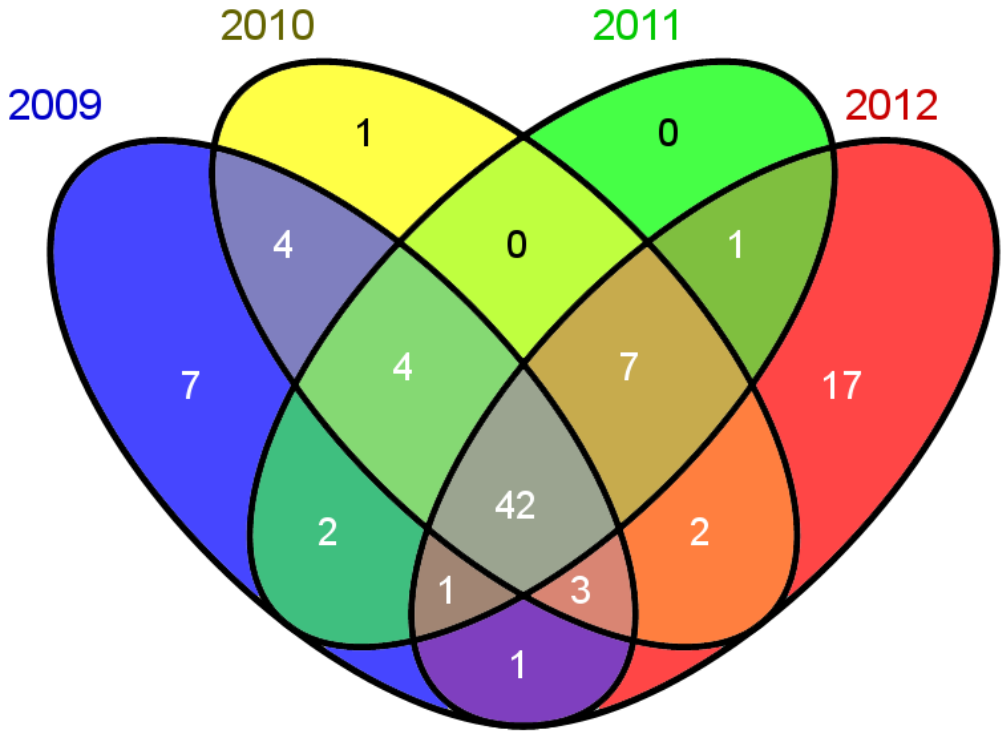
Trial of new targets

- Average of 601attacked domains per month by Zeus malware
- Average of 112 of these are new domains each month
- There is a relatively stable ceiling in the peaks of overall attacked domains, as well as in the trial and error for new targets



Trial of new targets

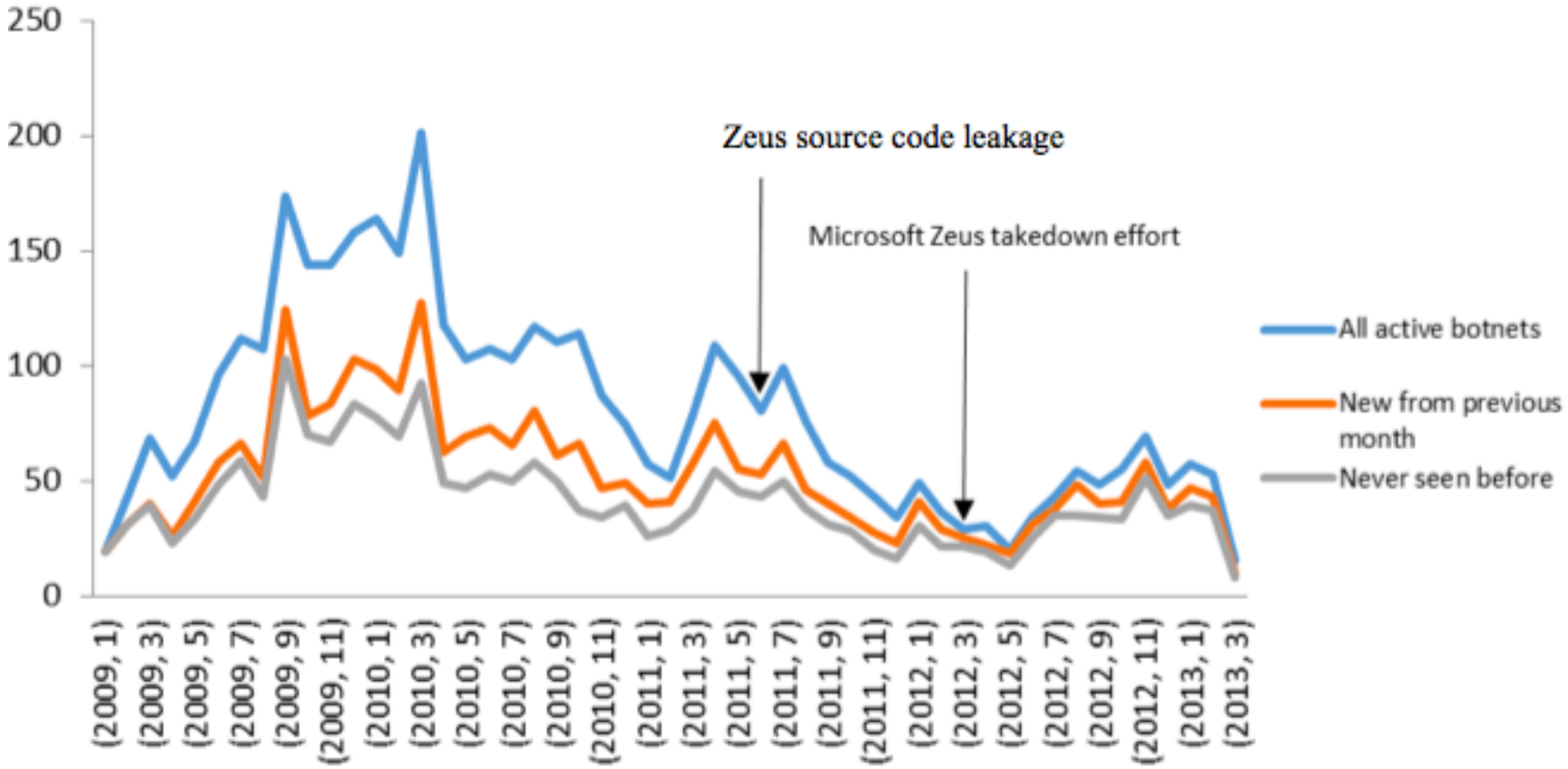
- Seeking new targets across a larger area
- In 2012, 17 new countries were targeted, but 18 countries from the previous years were no longer being attacked



Outline

1. Problem of online banking fraud
2. Zeus malware
3. Capturing attackers' instructions from infected machines
4. Extracting intelligence from the instructions (targets, inject code)
5. Who is being targeted?
6. Do bigger targets attract more attacks?
7. How fast do attackers explore new targets?
8. Did the sudden availability of Zeus source code increase attacks?
9. How does attack code evolve?
10. Conclusion

Number of active botnets

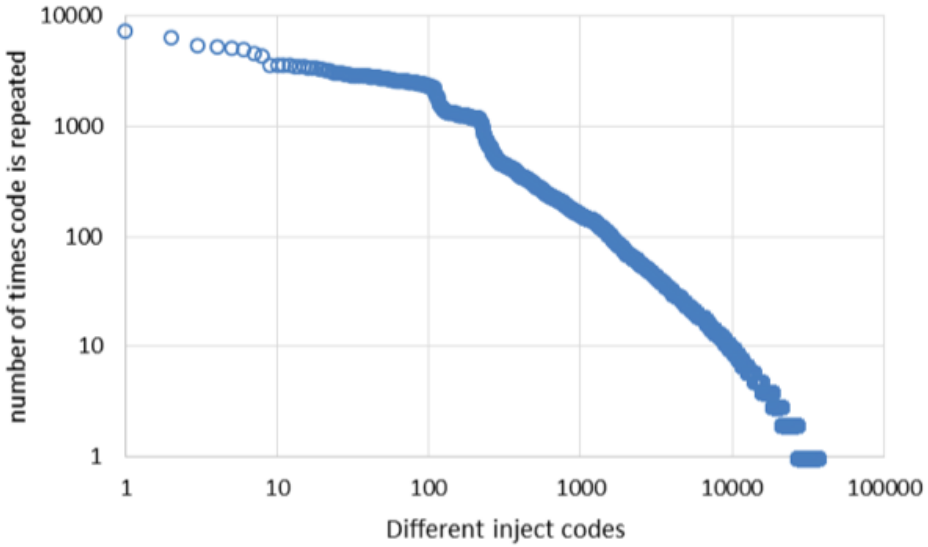


Outline

1. Problem of online banking fraud
2. Zeus malware
3. Capturing attackers' instructions from infected machines
4. Extracting intelligence from the instructions (targets, inject code)
5. Who is being targeted?
6. Do bigger targets attract more attacks?
7. How fast do attackers explore new targets?
8. Did the sudden availability of Zeus source code increase attacks?
9. How does attack code evolve?
10. Conclusion

Inject code development over time

- 1.1m target URLs with ‘inject’ codes
- On average, each inject code is repeated 27 times; 43% repeated over 1,000 times, and just 1% appears once!
- Across all Zeus botnets and attackers, code similarity is over 90% from one attack to the next. 97% per URL per botnet
- This suggests sharing, stealing or selling code across attackers



Outline

1. Problem of online banking fraud
2. Zeus malware
3. Capturing attackers' instructions from infected machines
4. Extracting intelligence from the instructions (targets, inject code)
5. Who is being targeted?
6. Do bigger targets attract more attacks?
7. How fast do attackers explore new targets?
8. Did the sudden availability of Zeus source code increase attacks?
9. How does attack code evolve?
10. Conclusion

Conclusions

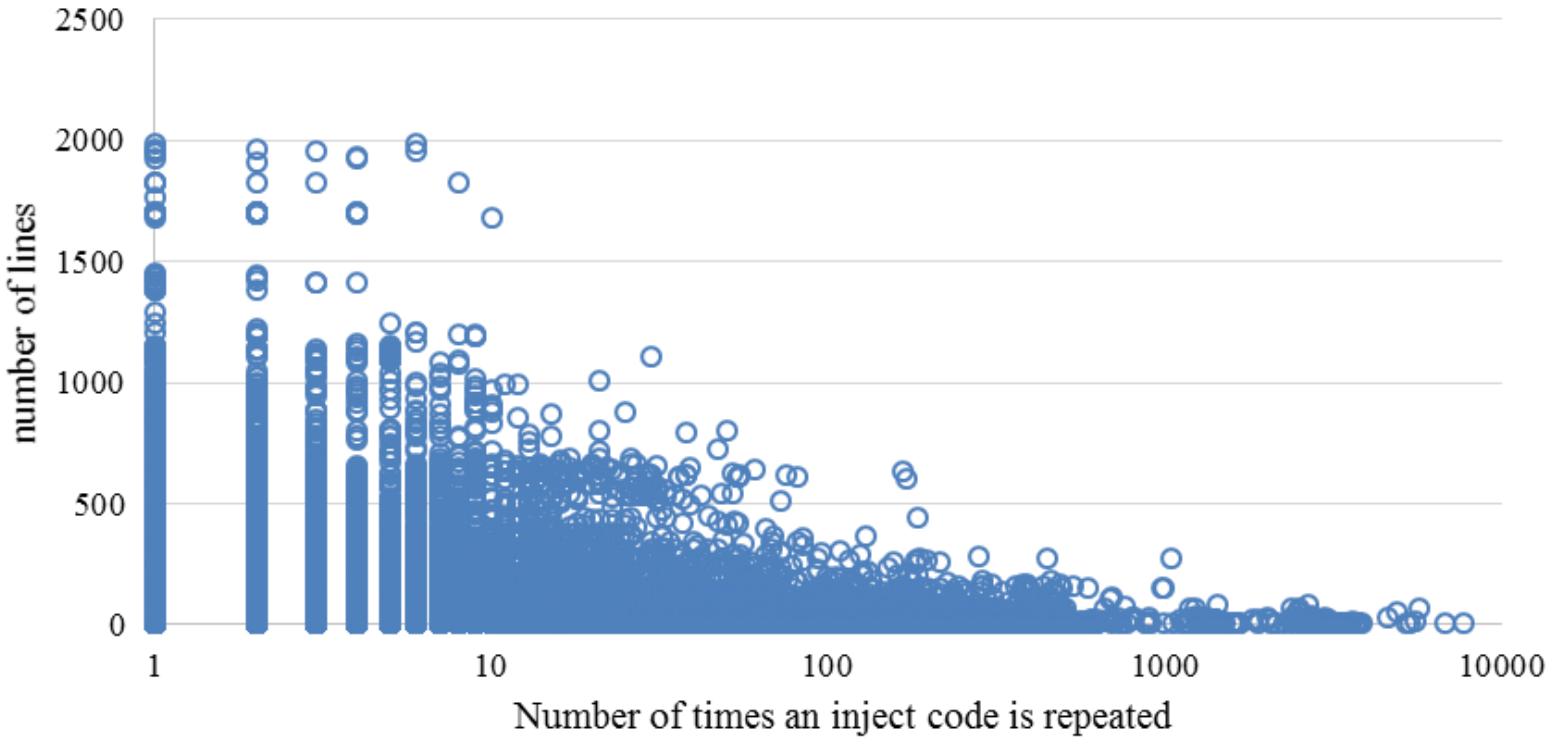
- Although Zeus inject code was highly reused and Zeus source code became openly available, the criminal market of Zeus-based attacks did not expand as theory and experts predicted

- Mitigating financial fraud might be more effective by allocating resources away from fighting freely available attacker resources

Questions?

Backup

Inject Code Size vs. Repetition



Summary

- Not every Financial Service Provider is equally popular among criminals
- Size is a threshold for getting attacked, but does not predict the intensity
- Attack persistence varies widely. Half the domains are targeted briefly, mostly likely in search of new targets
- Attack (and defense!) is less dynamic than often presumed

Summary

- The underground market for bots and malware may have lower economic entry barriers for criminals and reduced costs in the value chain of attacks, but it has not increased attack volume (number of botnets) or the number of targets
- Attack ceiling suggests other bottlenecks in the criminal value chain, such as in cash out operations and mule recruitment
- Defense should focus on these bottlenecks, not only on reducing abundant attacker resources (i.e., bots, malware and injects)

Next steps

- Map security properties of attacked services (e.g., authentication mechanism)
- Study interaction among attack and defense (e.g., deterrence, waterbed effect?)
- Statistically model factors that determine fraud levels in countries
- Identify most cost-effective countermeasures

- Attacks to the same URL are more than 90% similar, no matter the length of the inject; this suggests code sharing, stealing or selling (inject-code-as-a-service) among criminals

Questions

- What type of domains are targeted via ZeuS?
- Are some financial services targeted more often than other? Why?
- How are new targets identified over time?
- What is the impact on attack volume of attack code becoming more easily availabe over time?
- How quickly does attack code (web injects) develop over time?

```
WebInjects:

set_url */my.ebay.com/*CurrentPage=MyeBayPersonalInfo* <FLAG_GET><FLAG_LOG>
data_before
   Registered email address</td>*<img*>
data_after
  </td>
data_inject
  e-mail:


set_url *.ebay.com/*eBayISAPI.dll?* <FLAG_GET><FLAG_LOG>
data_before
  (<a href="http://feedback.ebay.com/ws/eBayISAPI.dll?ViewFeedback&*">
data_after
  </a>
data_inject
  Feedback:


set_url https://www.us.hsbc.com/* <FLAG_GET><FLAG_LOG>
data_before
  <table cellspacing="0" summary="page layout">
data_after
  </table>
```