Threat monitoring: a national CERT perspective

Paweł Pawliński

CERT Polska / NASK

pawel.pawlinski@cert.pl

MNSEC 2017

Ulaanbaatar, 2017-09-28

Agenda

1 Overview

2 Sensors

3 Drive-by attacks

4 Malware

5 Conclusions

CERT.PL: quick introduction

- Established in 1996
- Constituency:
  - population of Poland: 38M
  - internet users: 28M
  - no gov networks
- Part of NASK:
  - research institute
  - **.pl** registry
  - software development
  - ISP
  - …
- Member of FIRST, TF-CSIRT, APWG, …

Goal: situational awareness

- Goals of adversaries
- Techniques & tools used by attackers
- Indicators of Compromise for defense
- Trends in attacks
- Targets / Victims
- . . . and more.

Agenda

1 Overview

2 Sensors

3 Drive-by attacks

4 Malware

5 Conclusions

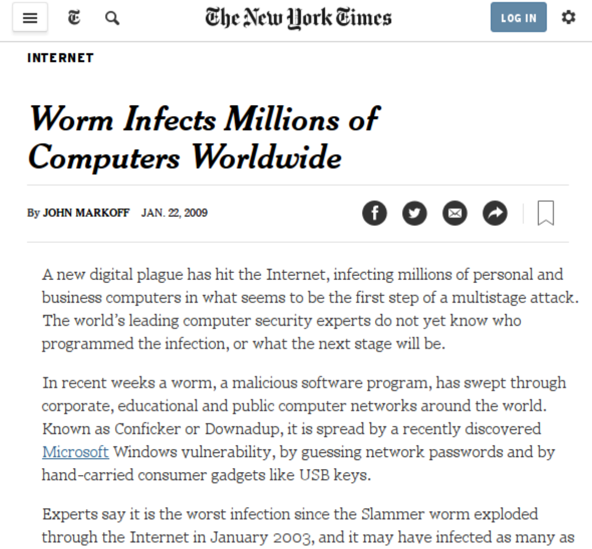
Landscape in early 2000s

- 2001-07-15 Code Red
- 2001-09-11 Nimda
- 2003-01-25 SQL Slammer
- 2003-08-11 Blaster
- 2004-01-26 MyDoom
- 2004-04-12 Sasser

ARAKIS monitoring system

- Project started in 2006
- Distributed sensor network
- Server-side honeypots
- Automatic traffic analysis
- IDS signature generation (machine learning)

November 2008: Conficker



The New York Times

INTERNET

Worm Infects Millions of Computers Worldwide

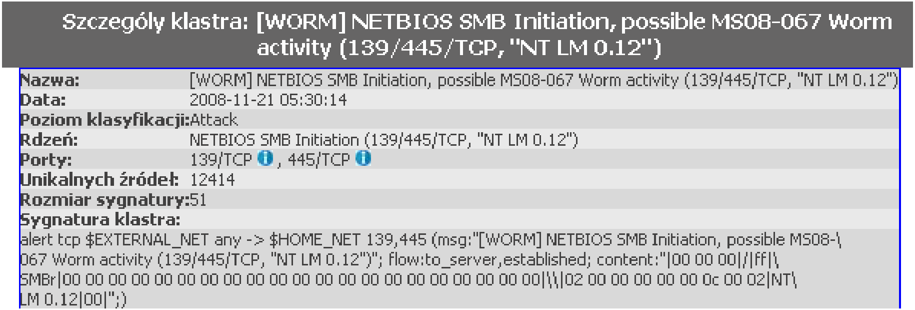
By JOHN MARKOFF JAN. 22, 2009

A new digital plague has hit the Internet, infecting millions of personal and business computers in what seems to be the first step of a multistage attack. The world's leading computer security experts do not yet know who programmed the infection, or what the next stage will be.

In recent weeks a worm, a malicious software program, has swept through corporate, educational and public computer networks around the world. Known as Conficker or Downadup, it is spread by a recently discovered Microsoft Windows vulnerability, by guessing network passwords and by hand-carried consumer gadgets like USB keys.

Experts say it is the worst infection since the Slammer worm exploded through the Internet in January 2003, and it may have infected as many as

November 2008: Conficker



Szczegóły klastra: [WORM] NETBIOS SMB Initiation, possible MS08-067 Worm activity (139/445/TCP, "NT LM 0.12")

Nazwa:	[WORM] NETBIOS SMB Initiation, possible MS08-067 Worm activity (139/445/TCP, "NT LM 0.12")
Data:	2008-11-21 05:30:14
Poziom klasyfikacji:	Attack
Rdzeń:	NETBIOS SMB Initiation (139/445/TCP, "NT LM 0.12")
Porty:	139/TCP, 445/TCP
Unikalnych źródeł:	12414
Rozmiar sygnatury:	51

Sygnatura klastra:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139,445 (msg:"[WORM] NETBIOS SMB Initiation, possible MS08-\
067 Worm activity (139/445/TCP, "NT LM 0.12")"; flow:to_server,established; content:"|00 00 00|/|ff|\
SMBr|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|\\|02 00 00 00 00 00 0c 00 02|NT\
LM 0.12|00|";)
```

■ ■ ■

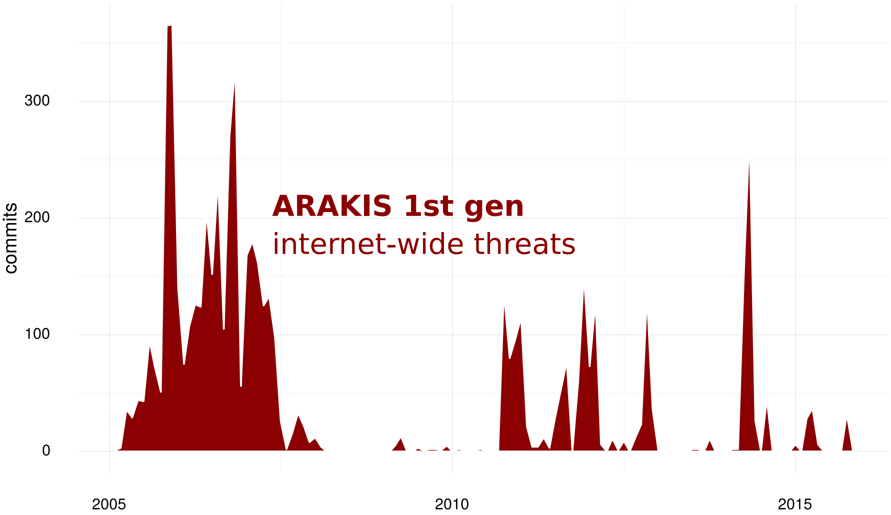
Landscape in 2010s

- Scanners
- Scanners
- Scanners
- . . .
- 2011-08-26 Morto
- 2012-04-23 Carna Botnet
- . . .
- Scanners
- Scanners
- Scanners
- . . .

Results

- Automated analysis works
- Generated signatures: possibly high-impact
- Sources of scanning: low-impact
  - approx 1% from Poland
  - value?
- Other anomalies detected: too much noise
- Problem: distribution

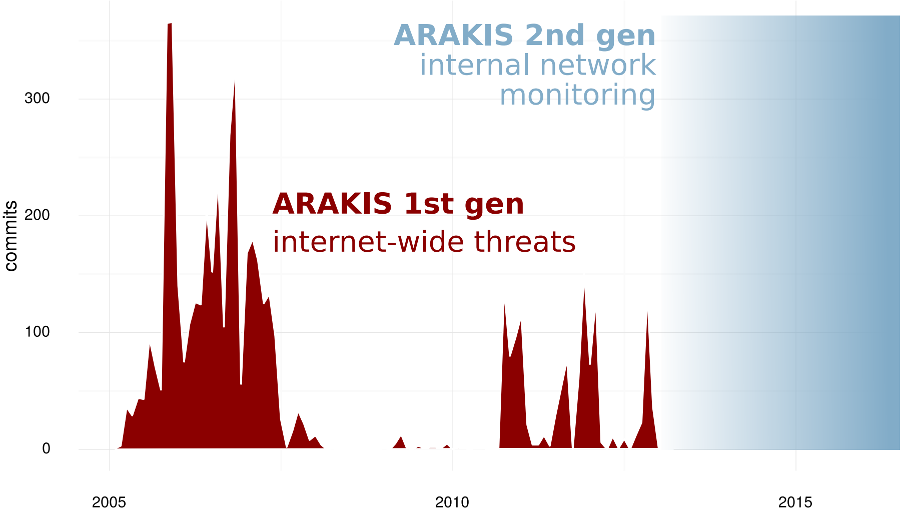
ARAKIS: development history



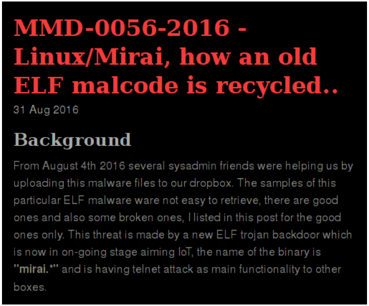
ARAKIS 1st gen

internet-wide threats

ARAKIS: development history



August 2016 – . . .

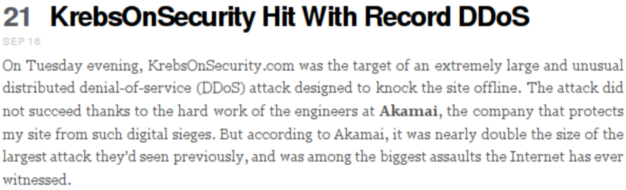


MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled..

31 Aug 2016

Background

From August 4th 2016 several sysadmin friends were helping us by uploading this malware files to our dropbox. The samples of this particular ELF malware ware not easy to retrieve, there are good ones and also some broken ones, I listed in this post for the good ones only. This threat is made by a new ELF trojan backdoor which is now in on-going stage aiming IoT, the name of the binary is **"mirai.*"** and is having telnet attack as main functionality to other boxes.

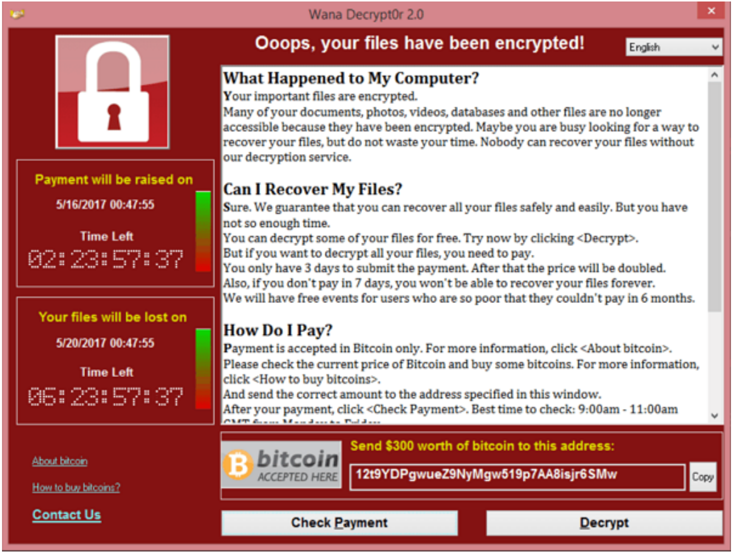


21 KrebsOnSecurity Hit With Record DDoS

SEP 16

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

May 2017



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Agenda

1 Overview

2 Sensors

3 Drive-by attacks

4 Malware

5 Conclusions

Landscape in 2000s

- Exploiting web browsers known but still not popular
- 2004 first client-side honeypots developed
- 2006 first exploit kits

Honeyspider Network

- Goal: detect drive-by downloads at medium scale
  - identify victims (possibly high-profile)
  - share malicious URLs
- Hybrid client honeypots
  - low-interaction = emulated (crawlers)
  - high-interaction = real Windows/Linux system
- Project started in 2007

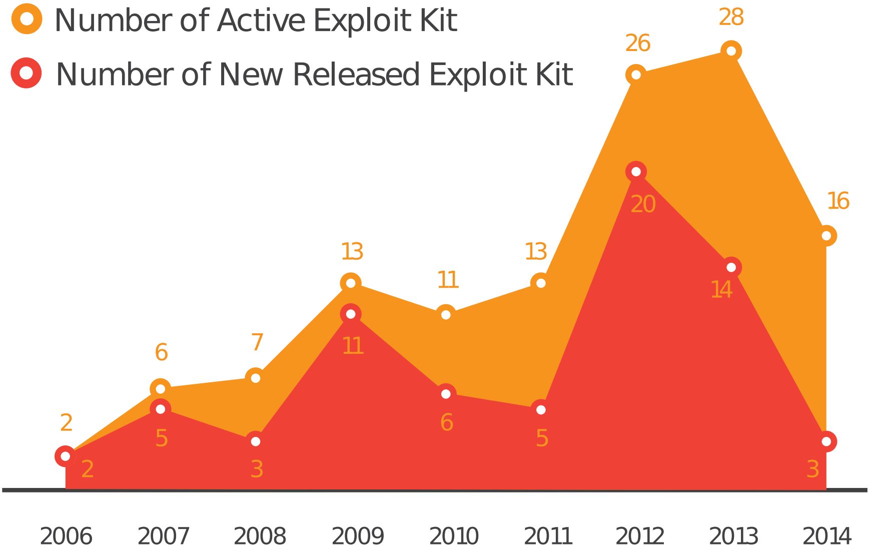
Honeyspider Network

Prototype detects malicious domains in the wild!

What next?

Honeyspider Network 2

- Goal 1: fix reliability
- Goal 2: scalability / performance
- Flexible framework
- Multiple specialized analyzers

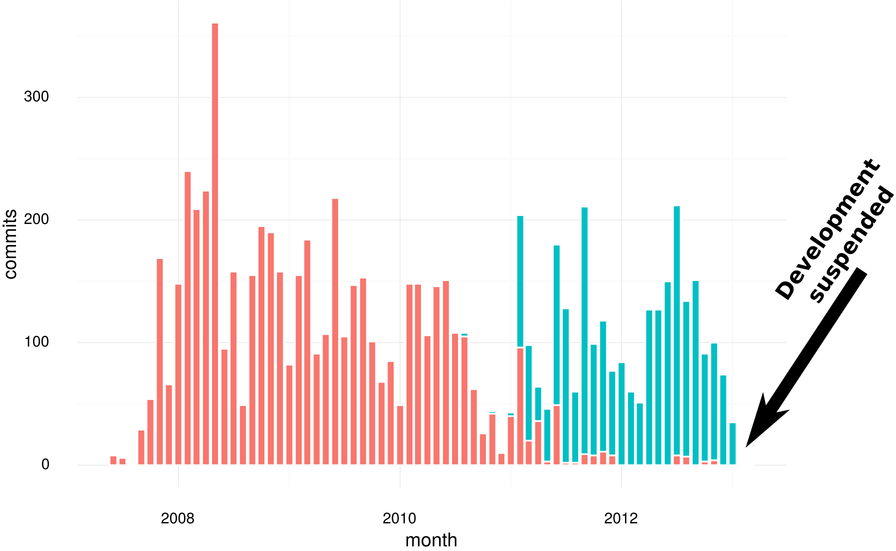


Trend Micro, *Evolution of exploit kits*

Results

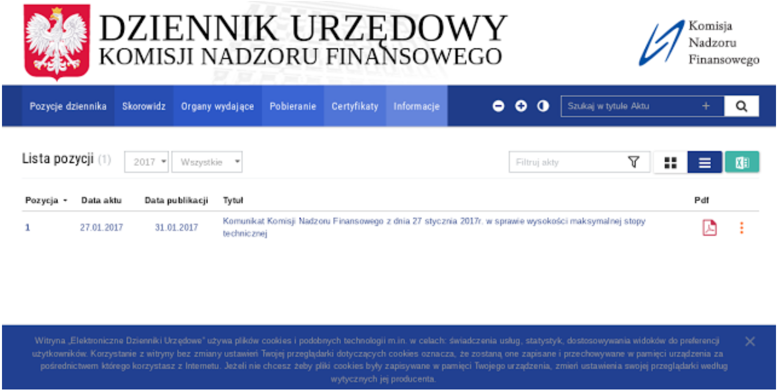
- Early successes
- Threat evolved faster than we did
- Problem: insufficient detection method
- Small-scale deployment only
- What worked: detecting changes in websites

Honeyspider Network: development history



...

November 2016



DZIENNIK URZĘDOWY
KOMISJI NADZORU FINANSOWEGO

Lista pozycji (1) 2017 Wszystkie Filtruj akty

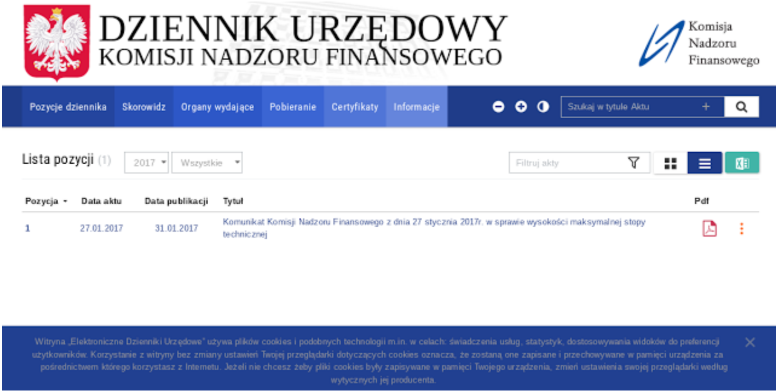
Pozycja	Data aktu	Data publikacji	Tytuł	Pdf
1	27.01.2017	31.01.2017	Komunikat Komisji Nadzoru Finansowego z dnia 27 stycznia 2017r. w sprawie wysokości maksymalnej stopy technicznej	

Witryna „Elektroniczne Dzienniki Urzędowe" używa plików cookies i podobnych technologii m.in. w celach: świadczenia usług, statystyk, dostosowywania widoków do preferencji użytkowników. Korzystanie z witryny bez zmiany ustawień Twojej przeglądarki dotyczących cookies oznacza, że zostaną one zapisane i przechowywane w pamięci urządzenia za pośrednictwem którego korzystasz z Internetu. Jeżeli nie chcesz żeby pliki cookies były zapisywane w pamięci Twojego urządzenia, zmień ustawienia swojej przeglądarki według wytycznych jej producenta.

Redirects:

```
http://sap.misapor.ch/vishop/view.jsp?pagenum=1
https://www.eye-watch.in/design/fancybox/Pnf.action
```

November 2016



Pozycja	Data aktu	Data publikacji	Tytuł	Pdf
1	27.01.2017	31.01.2017	Komunikat Komisji Nadzoru Finansowego z dnia 27 stycznia 2017r. w sprawie wysokości maksymalnej stopy technicznej	

Witryna „Elektroniczne Dzienniki Urzędowe" używa plików cookies i podobnych technologii m.in. w celach: świadczenia usług, statystyk, dostosowywania widoków do preferencji użytkowników. Korzystanie z witryny bez zmiany ustawień Twojej przeglądarki dotyczących cookies oznacza, że zostaną one zapisane i przechowywane w pamięci urządzenia za pośrednictwem którego korzystasz z Internetu. Jeżeli nie chcesz żeby pliki cookies były zapisywane w pamięci Twojego urządzenia, zmień ustawienia swojej przeglądarki według wytycznych jej producenta.

More details tomorrow: Irek Parafjańczuk (Team Cymru)
Who is behind the recent attack on Polish banking systems

Agenda

1 Overview

2 Sensors

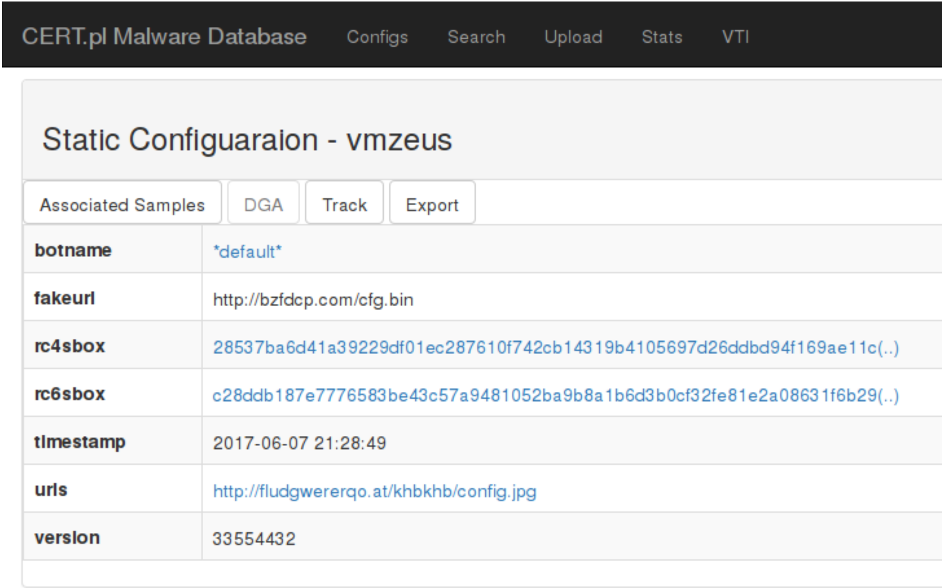
3 Drive-by attacks

4 Malware

5 Conclusions

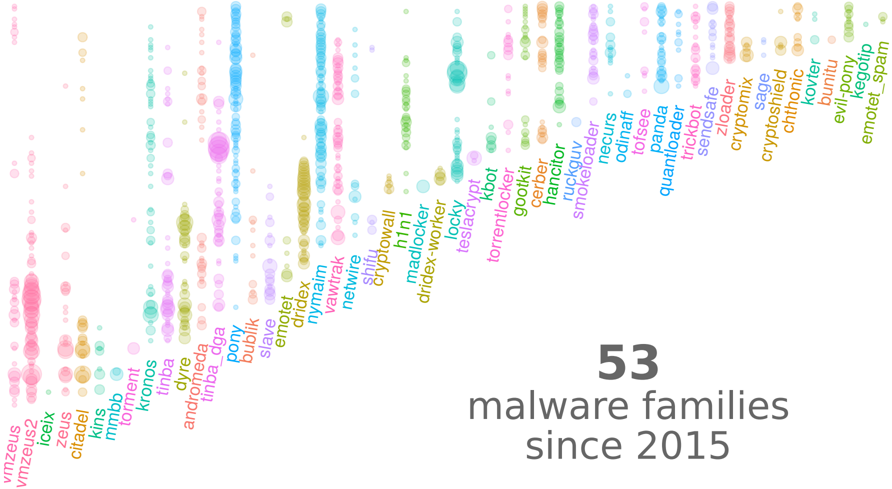
Automating malware analysis

- Malware: the most visible problem
- Many samples, few families, different configurations
- Idea: automate configuration extraction



Static Configuaraion - vmzeus

botname	*default*
fakeurl	http://bzfdcp.com/cfg.bin
rc4sbox	28537ba6d41a39229df01ec287610f742cb14319b4105697d26ddbd94f169ae11c(..)
rc6sbox	c28ddb187e7776583be43c57a9481052ba9b8a1b6d3b0cf32fe81e2a08631f6b29(..)
timestamp	2017-06-07 21:28:49
urls	http://fludgwererqo.at/khbkhb/config.jpg
version	33554432

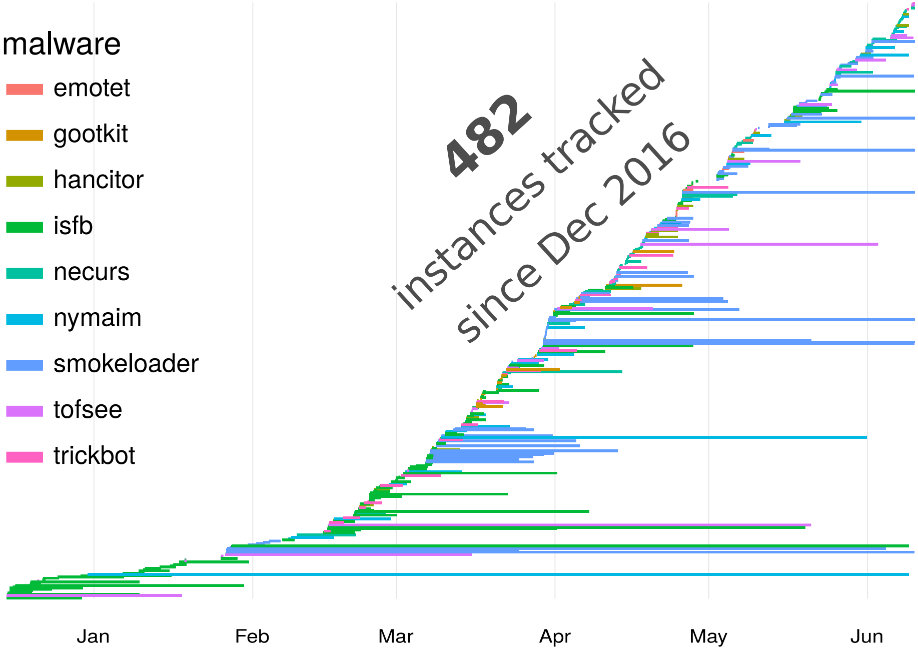


53

malware families
since 2015

Going one step further

- Malware configuration can be dynamic
- Idea: talk with botnet controllers



482
instances tracked
since Dec 2016

Results

- Actually relevant information:
  - botmasters’ activity
  - IoCs
- Challenge: distribution (again)
- approx 20% n6 users download IoCs regularly

Agenda

1 Overview

2 Sensors

3 Drive-by attacks

4 Malware

5 Conclusions

Conclusions

- Monitoring: **collect** → **analyze** → **distribute**
- Difficult to build
- Research parts are fun regardless
- Do not forget about low-hanging fruit
- Complex solution ≠ actionable output or high-impact
- Avoid drowning in software development or system maintenance

Interested?

- Malware analysis service: pawel.pawlinski@cert.pl
- Free data feeds: n6@cert.pl
- Have something to share? Tell us!

Thank you for your attention.

Part of this research has been supported by the European Union Horizon 2020 programme under grant agreement No. 700176 (SISSDEN). The opinions expressed in this presentation are those of the authors and do not necessarily reflect the views of the European Commission.