Modern Malwares...

... Only a few clicks away from you!

Xavier Mertens - Principal Security Consultant

"We worried for decades about WMDs – Weapons of Mass Destruction. Now it is time to worry about a new kind of WMDs – Weapons of Mass Disruption."
(John Mariotti)

whoami

- Xavier Mertens, again!

Agenda

- **Introduction**
- How to fight?
- Quick wins
- Real time analysis
- Solutions
- Limitations
- Conclusions

Let's Avoid This!

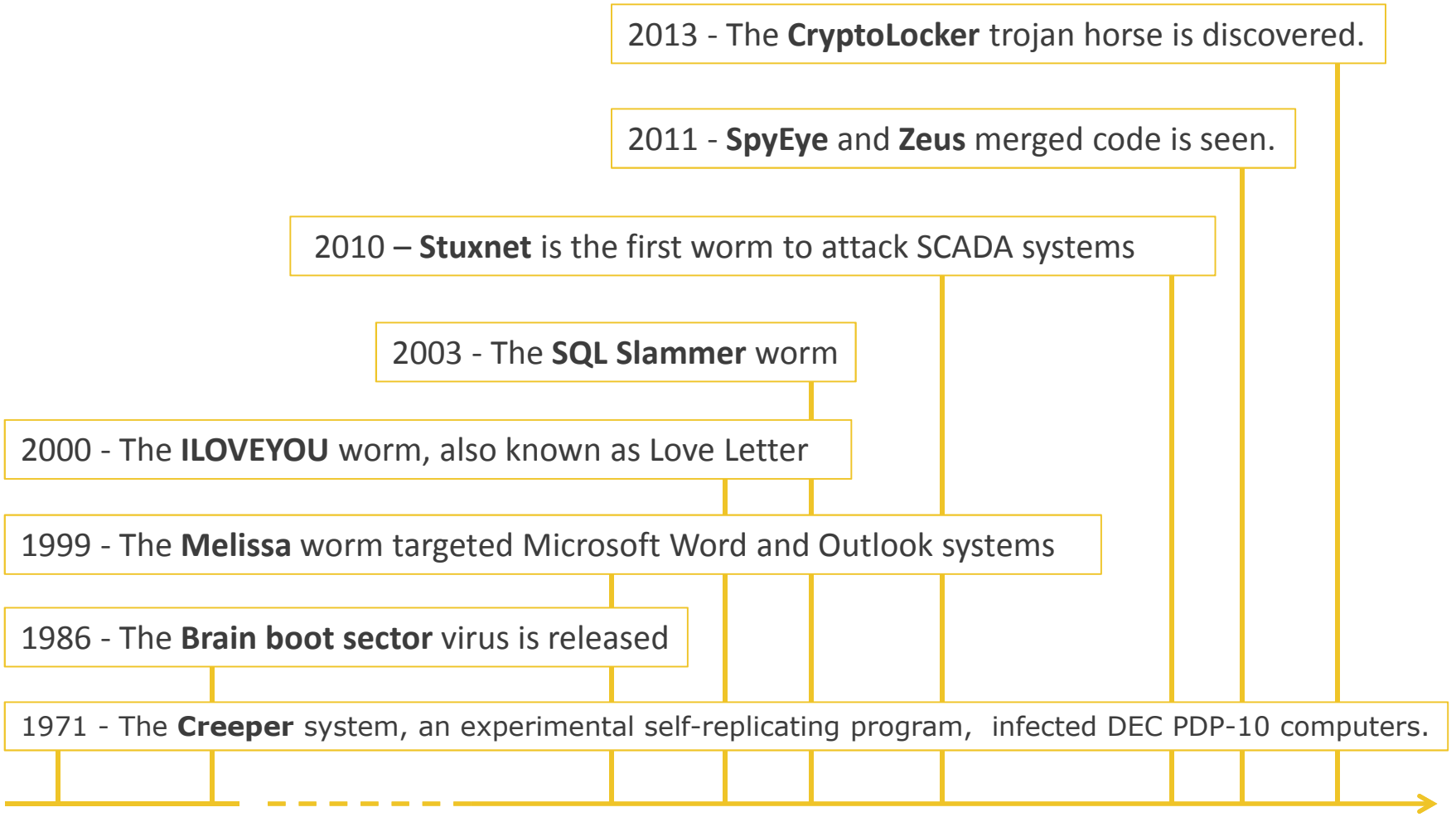

Cryptolocker 2.0
Your personal files are encrypted
Info
Your important files were encrypted on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.
Encryption was produced using unique public key RSA-4096 generated for this computer. To decrypt files, you need to obtain private key.
The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.
To retrieve the private key, you need to pay 0.5 bitcoins.
Click proceed to payment to obtain private key.
Any attempt to remove or damage this software will lead to immediate private key destruction by server.
Your files will be lost without payment on:
11/24/2013 3:16:34 PM
See files
<< Back
Proceed to payment >>

Me? Breached?

- In 66% of investigated incidents, detection was a matter of **months** or even more
- 69% of data breaches are discovered by **third** parties

(Source: Verizon DBIR 2012)

Malicious Code is not New



2014?

Fridge sends spam emails as attack hits smart gadgets…

2014?

"Target" PoS were compromised…

2014?

Yahoo! ads network compromised to redirect users to malicious websites

“Malware?”

“A malware, or malicious code, is defined as software or firmware intended to perform an unauthorized process that will have an adverse impact on **confidentiality**, **integrity** and **availability** of an information system.”

Understanding Threats

- Attack actors
  - $$$
  - Espionage (industrial or political)
  - Hacktivism
- Attack vectors
  - Mainly: HTTP / SMTP
  - Local access (USB – CIFS)
  - Interactions with humans

“WMP”

“Weapon of Mass Pwnage”

Backdoors in Software

Backdoors in Software

Golden Tips

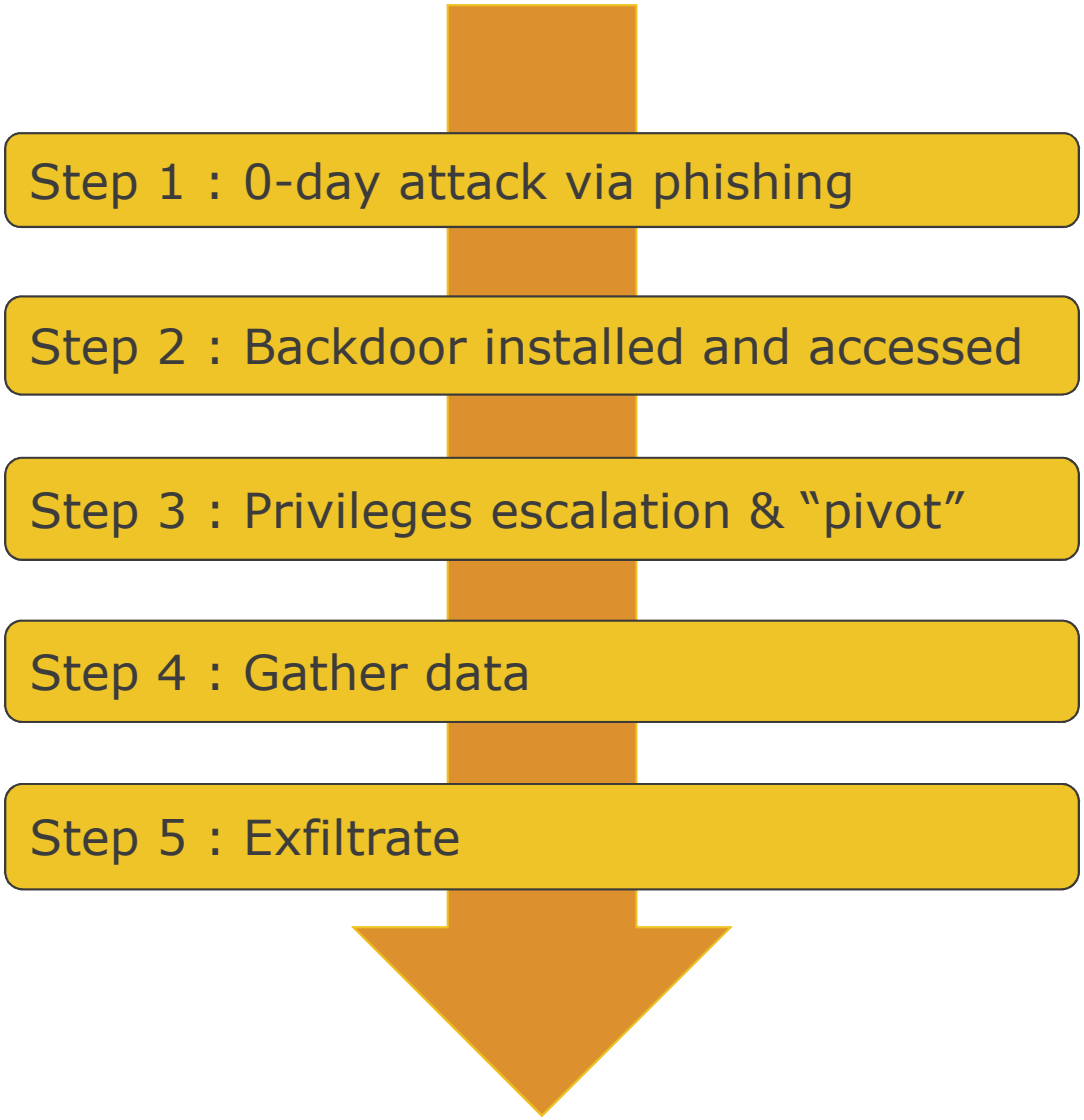
- Always download from official repositories
- Always cross-check the MD5/SHA1 hash
- Deploy in a lab

Bulk VS. Targeted

- Bulk attacks use a well-known vulnerability in a piece of software
  Ex: CVE-2012-4681
- Lot of computers infected, low revenue
- Massive pwnage

- Targeted attacks uses a 0-day vulnerability in a piece of software
  Ex: CVE-2011-0609
- Limited amount of victims but potentially huge revenue

Easy as 1, 2, 3, … 4, 5!



Callbacks...

- A malware without C&C communications is useless...
- Callbacks are used to phone home
  - To send interesting data
  - To ask for what to do?

Below the Radar...

- Callbacks must be stealthy
  - Obfuscated, encrypted and look “very common”
- Multiple channels
  - JPEG images
  - Twitter
  - Tor
  - Google Drive
  - ... Theoretically any web 2.0 app!

Agenda

- Introduction
- **How to fight?**
- Quick wins
- Real time analysis
- Solutions
- Limitations
- Conclusions

Step 1 – Infection

- Rogue e-mails
  - Security awareness
  - Limit / scan attachments
- Malicious websites
  - Can be your favourite website visited daily → Scan web traffic
- Trust nobody
- Prevent the “click-o-mania”

Step 2 - Malware Behavior

- Alter the OS
  - Create/alter files
  - Create/kill processes
  - Wait for events
  - Work stealthy
- Network flow
  - Contact the C&C

Step 3 – Escalation & Pivot

- Hardening
  - Restrict users privileges
  - Uses OS security features
- Network segmentation
  - Don’t put all your eggs in the same bag

Step 4 – Data Are Valuable

- Protect your data
  - Encrypt them
  - Restrict access to them
    - Data at rest
    - Data in motion
    - Data in use

Step 5 – Exfiltration

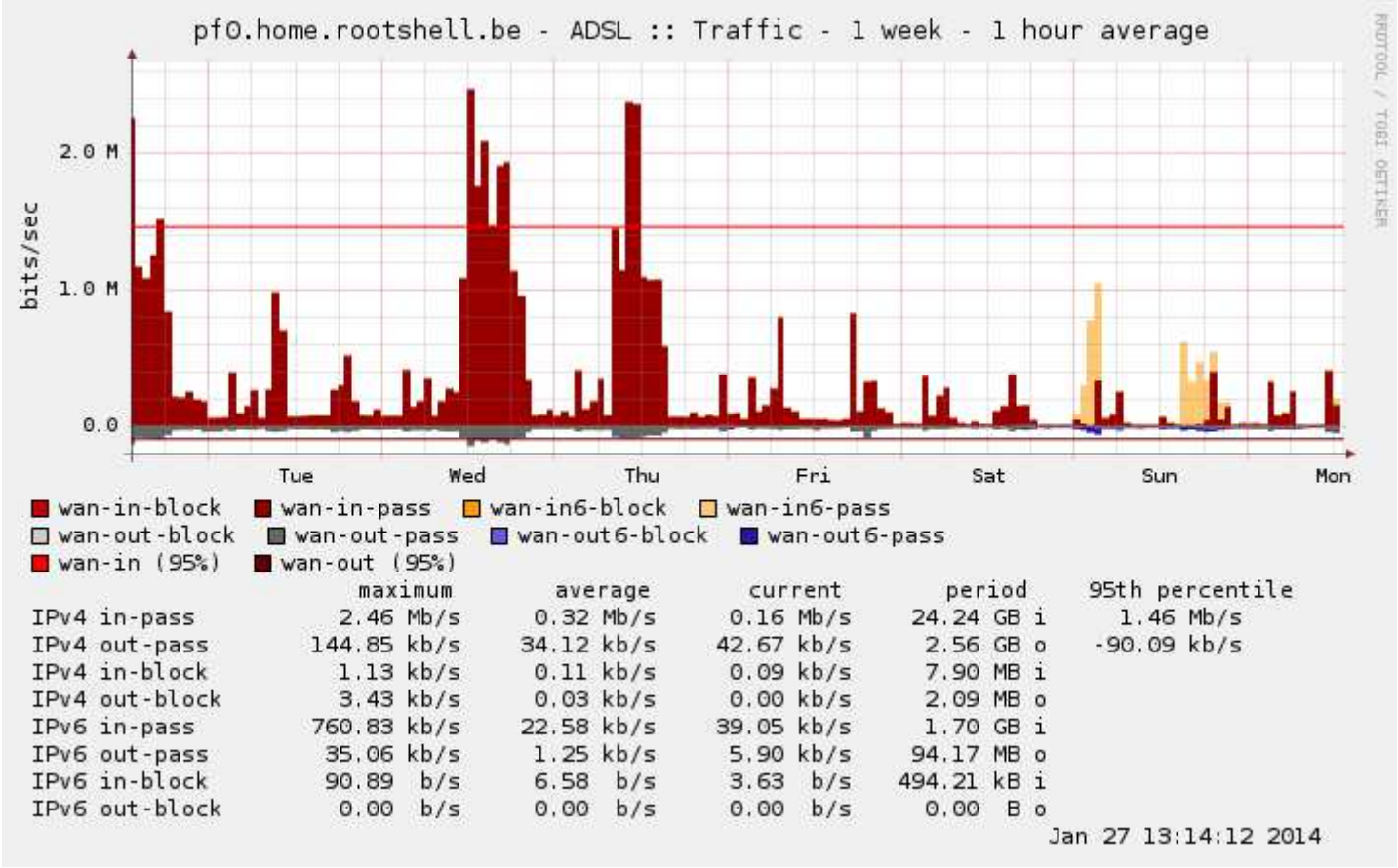
- Classify data
- Network flows

Due Diligence

Agenda

- Introduction
- How to fight?
- **Quick wins**
- Real time analysis
- Solutions
- Limitations
- Conclusions

RRD


pf0.home.rootshell.be - ADSL :: Traffic - 1 week - 1 hour average
bits/sec
2.0 M
1.0 M
0.0
Tue
Wed
Thu
Fri
Sat
Sun
Mon
wan-in-block
wan-in-pass
wan-in6-block
wan-in6-pass
wan-out-block
wan-out-pass
wan-out6-block
wan-out6-pass
wan-in (95%)
wan-out (95%)
maximum
average
current
period
95th percentile
IPv4 in-pass 2.46 Mb/s 0.32 Mb/s 0.16 Mb/s 24.24 GB i 1.46 Mb/s
IPv4 out-pass 144.85 kb/s 34.12 kb/s 42.67 kb/s 2.56 GB o -90.09 kb/s
IPv4 in-block 1.13 kb/s 0.11 kb/s 0.09 kb/s 7.90 MB i
IPv4 out-block 3.43 kb/s 0.03 kb/s 0.00 kb/s 2.09 MB o
IPv6 in-pass 760.83 kb/s 22.58 kb/s 39.05 kb/s 1.70 GB i
IPv6 out-pass 35.06 kb/s 1.25 kb/s 5.90 kb/s 94.17 MB o
IPv6 in-block 90.89 b/s 6.58 b/s 3.63 b/s 494.21 kB i
IPv6 out-block 0.00 b/s 0.00 b/s 0.00 b/s 0.00 B o
Jan 27 13:14:12 2014
RRDTOOL / TOBI OETIKER

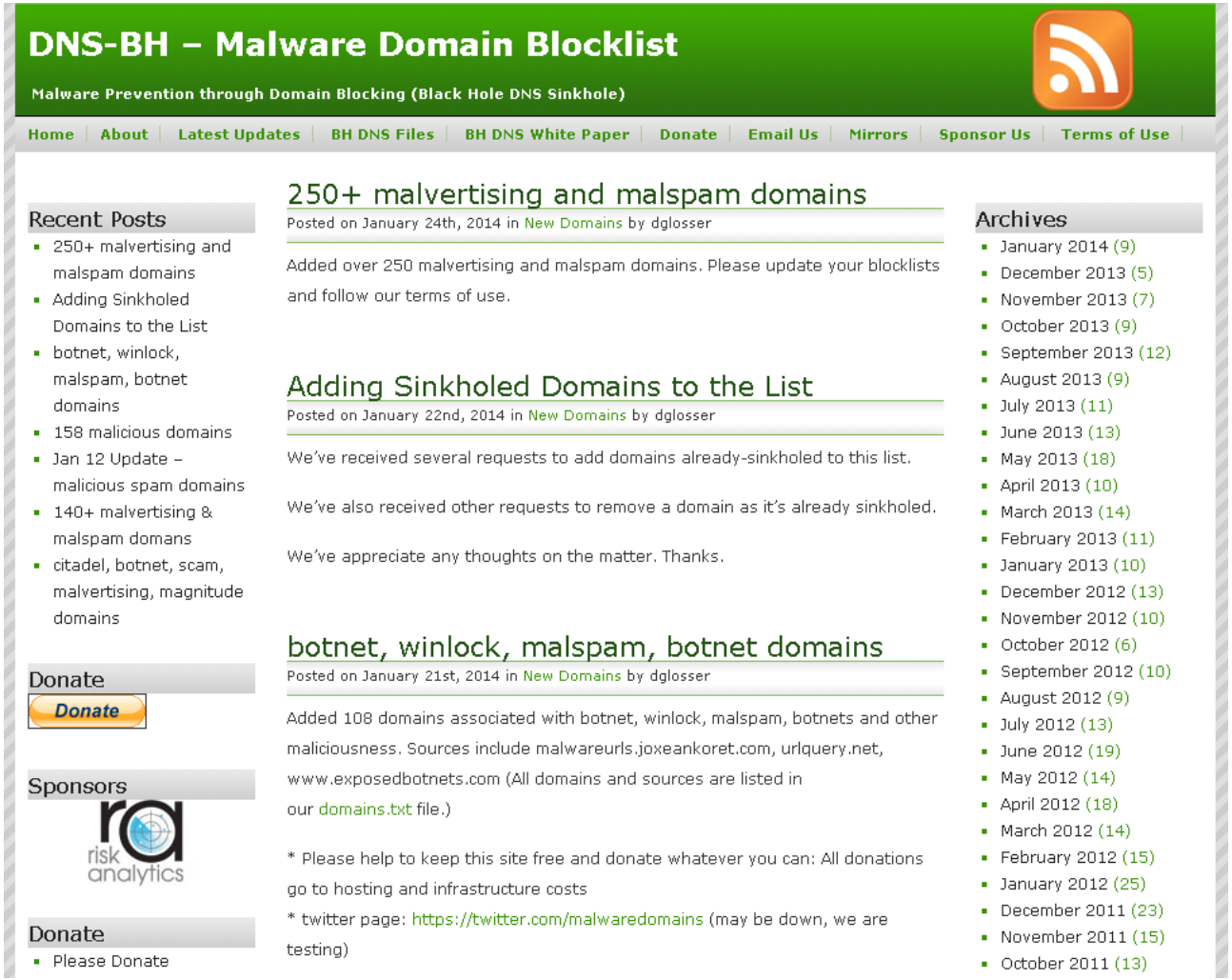
NetFlow / Firewall Logs

- Why is this server trying to connect to the wild Internet?
- Why is this laptop trying to connect to China?
- Why does this protocol suddenly appear?

DNS

- No DNS, no Internet!
- Malwares need DNS to communicate with C&C
- Alert on any traffic to untrusted DNS
- Investigate for suspicious domains
- Track suspicious requests (TXT)

DNS


DNS-BH – Malware Domain Blocklist
Malware Prevention through Domain Blocking (Black Hole DNS Sinkhole)
Home | About | Latest Updates | BH DNS Files | BH DNS White Paper | Donate | Email Us | Mirrors | Sponsor Us | Terms of Use
Recent Posts
250+ malvertising and malspam domains
Adding Sinkholed Domains to the List
botnet, winlock, malspam, botnet domains
158 malicious domains
Jan 12 Update – malicious spam domains
140+ malvertising & malspam domans
citadel, botnet, scam, malvertising, magnitude domains
Donate
Donate
Sponsors
risk analytics
Donate
Please Donate
250+ malvertising and malspam domains
Posted on January 24th, 2014 in New Domains by dglosser
Added over 250 malvertising and malspam domains. Please update your blocklists and follow our terms of use.
Adding Sinkholed Domains to the List
Posted on January 22nd, 2014 in New Domains by dglosser
We've received several requests to add domains already-sinkholed to this list.
We've also received other requests to remove a domain as it's already sinkholed.
We've appreciate any thoughts on the matter. Thanks.
botnet, winlock, malspam, botnet domains
Posted on January 21st, 2014 in New Domains by dglosser
Added 108 domains associated with botnet, winlock, malspam, botnets and other maliciousness. Sources include malwareurls.joxeankoret.com, urlquery.net, www.exposedbotnets.com (All domains and sources are listed in our domains.txt file.)
* Please help to keep this site free and donate whatever you can: All donations go to hosting and infrastructure costs
* twitter page: https://twitter.com/malwaredomains (may be down, we are testing)
Archives
January 2014 (9)
December 2013 (5)
November 2013 (7)
October 2013 (9)
September 2013 (12)
August 2013 (9)
July 2013 (11)
June 2013 (13)
May 2013 (18)
April 2013 (10)
March 2013 (14)
February 2013 (11)
January 2013 (10)
December 2012 (13)
November 2012 (10)
October 2012 (6)
September 2012 (10)
August 2012 (9)
July 2012 (13)
June 2012 (19)
May 2012 (14)
April 2012 (18)
March 2012 (14)
February 2012 (15)
January 2012 (25)
December 2011 (23)
November 2011 (15)
October 2011 (13)

virustotal.com

virustotal

SHA256: bf4c18e5d8e5e9f6fb221698e7f82d997abb01546d22df577fef15e2b710ae4f

File name: AM-ORDER-323131.exe

Detection ratio: 38 / 47

Analysis date: 2014-01-09 11:19:56 UTC (2 weeks, 4 days ago)

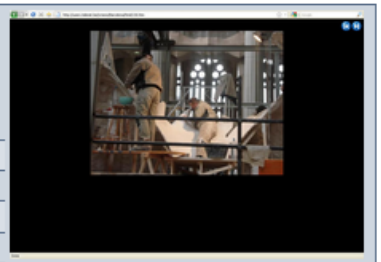
Analysis | File detail | Relationships | Additional information | Comments 4 | Votes

Antivirus	Result	Update
AVG	Zbot.ESE	20140109
Ad-Aware	Trojan.GenericKD.1479288	20140109
AhnLab-V3	Backdoor/Win32.Trojan	20140109
AntiVir	BDS/Androm.anmj	20140109
Avast	Win32:Crypt-QJT [Trj]	20140109
Baidu-International	Backdoor.Win32.Androm.aOI	20131213
BitDefender	Trojan.GenericKD.1479288	20140109
Bkav	W32.Clod2f9.Trojan.379f	20140109
CAT-QuickHeal	Trojan.Agent.su	20140109
Commtouch	W32/Trojan.FGWC-4799	20140109

urlquery.net

Overview

URL	http://users.telenet.be/jvnews/Barcelona/html/130.htm
IP	195.130.132.85
ASN	AS6848 Telenet N.V.
Location	Belgium
Report completed	2014-01-27 15:00:15 CET
Status	**Report complete.**
urlQuery Alerts	**Detected javascript associated with malicious code**



Settings

UserAgent	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13
Referer	
Adobe Reader	8.0
Java	1.6.0_26

Intrusion Detection Systems

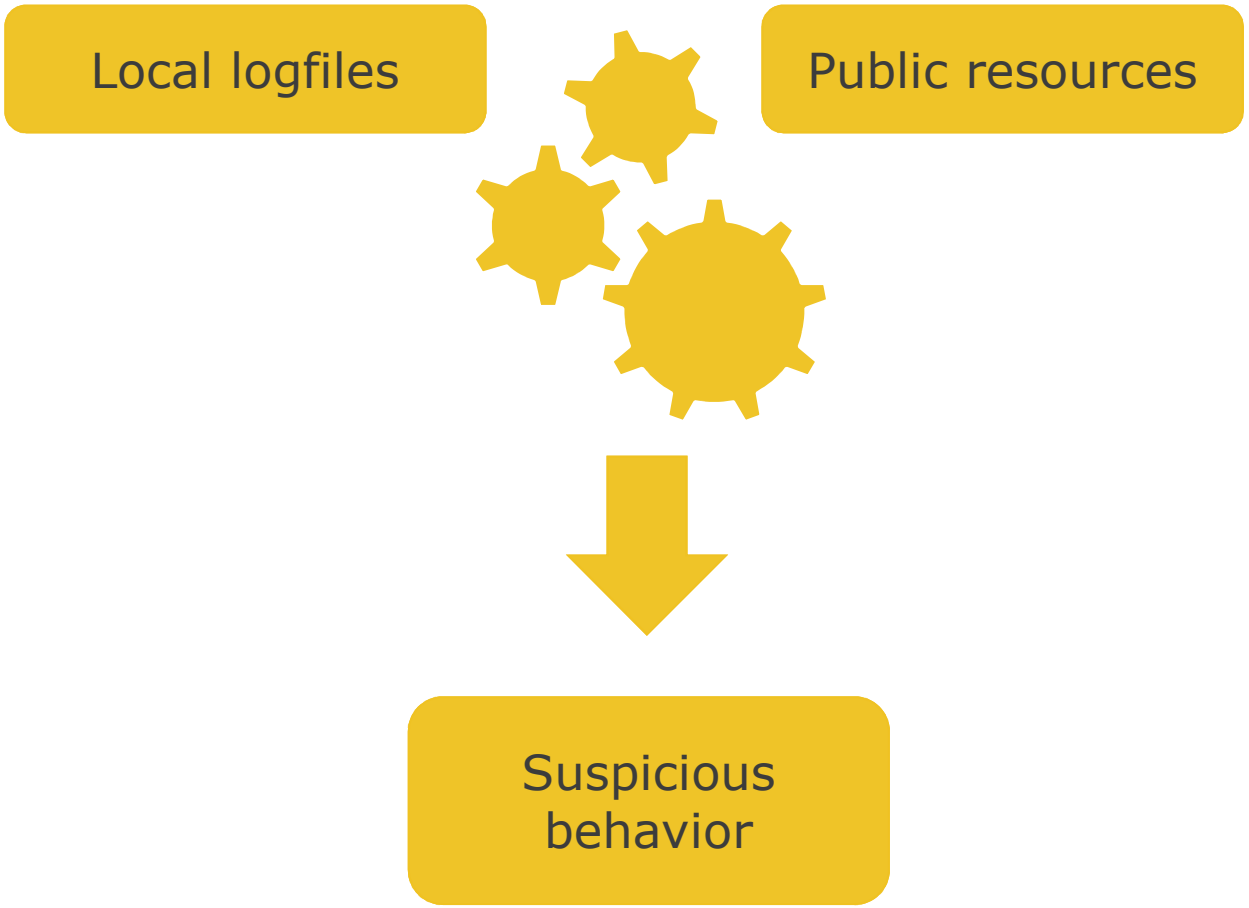
Suricata /w Emerging Threats Pro	No alerts detected
Snort /w Sourcefire VRT	No alerts detected

Recent reports on same IP/ASN/Domain

Last 6 reports on IP: 195.130.132.85

Date	Alerts / IDS	URL	IP
2014-01-25 20:46:50	0 / 1	http://users.telenet.be/parochie.kontich.kazerne	195.130.132.85
2014-01-13 09:20:21	0 / 0	http://users.telenet.be/marccordenier/	195.130.132.85
2013-12-23 13:40:05	1 / 2	http://users.telenet.be/netspace	195.130.132.85
2013-12-23 10:44:30	1 / 2	http://users.telenet.be/netspace	195.130.132.85
2013-12-11 20:01:04	0 / 2	http://users.telenet.be/cr41007/PrestoNotesSetup.exe	195.130.132.85
2013-12-11 15:38:25	1 / 0	http://users.pandora.be/flippersatellite	195.130.132.85

Intelligence

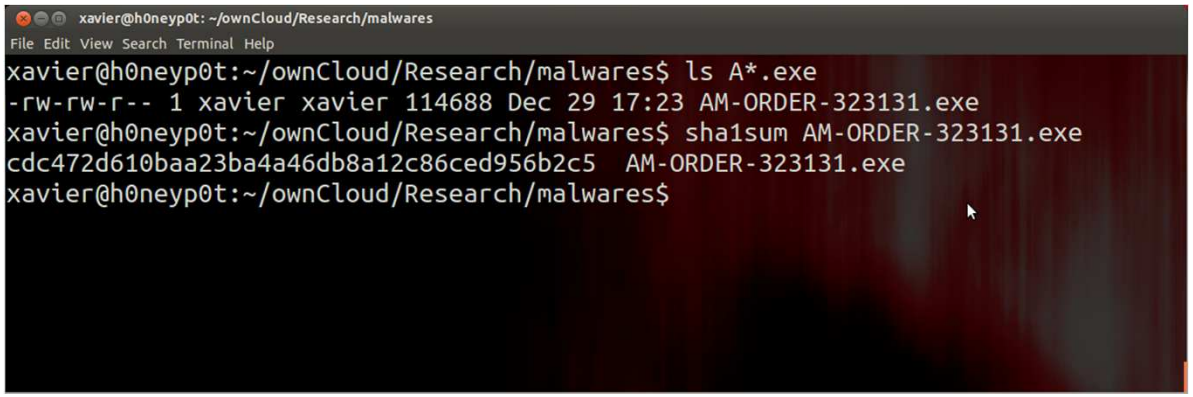


Action... Reaction!

Agenda

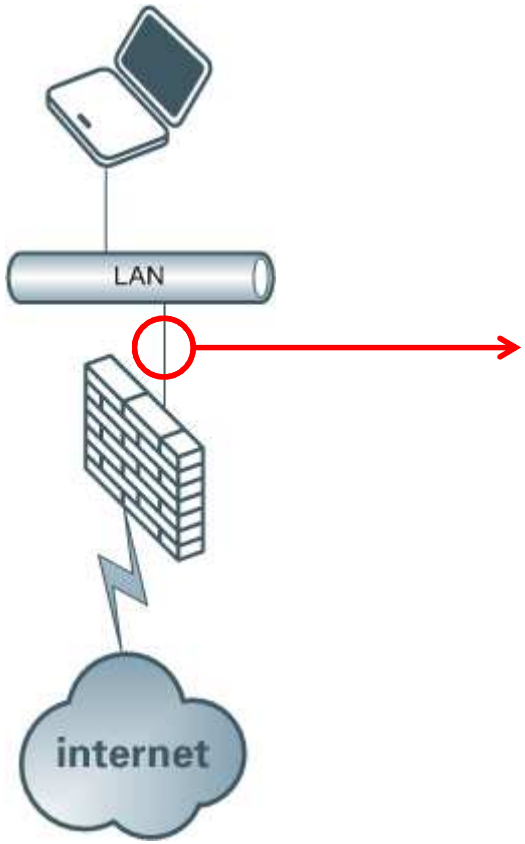
- Introduction
- How to fight?
- Quick wins
- **Real time analysis**
- Solutions
- Limitations
- Conclusions

Two Approaches



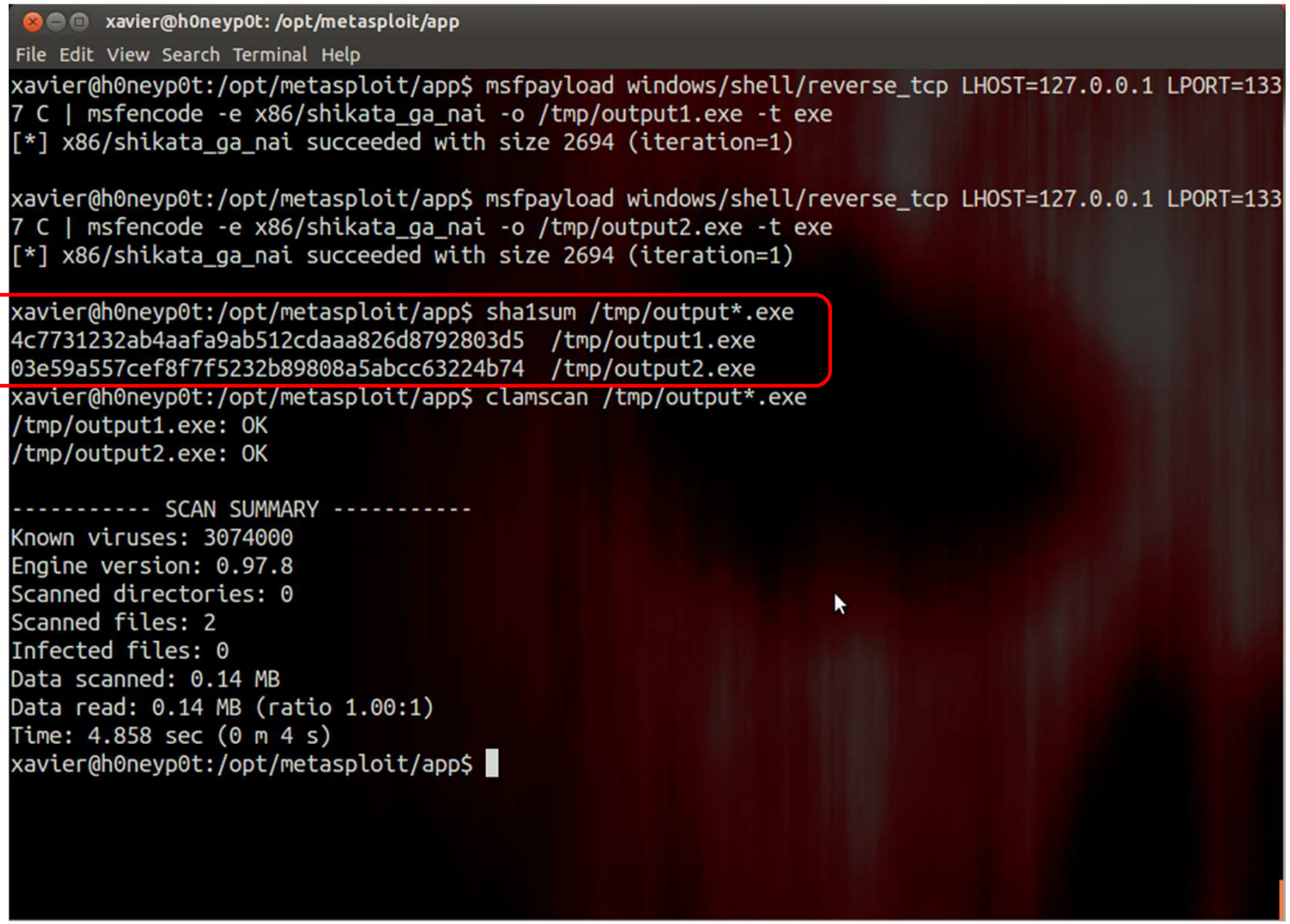
VS.

Hashing

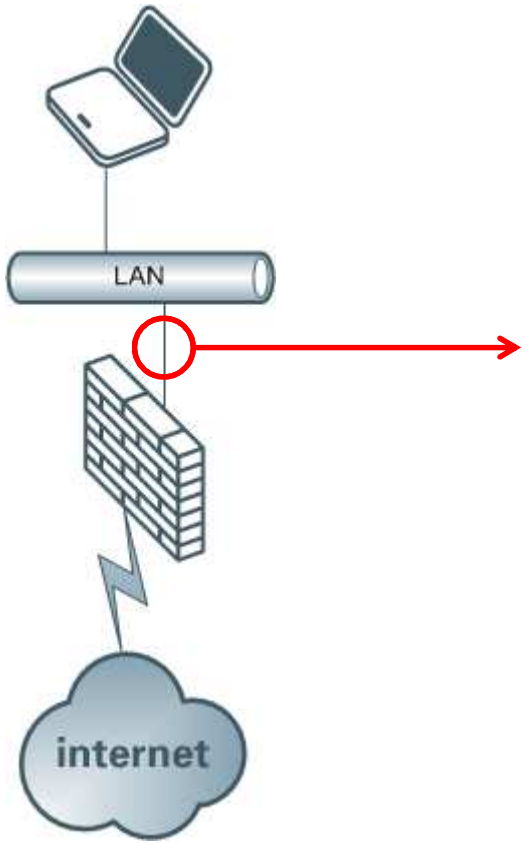


1. Files are extracted from network flows
2. Hash is computed
3. Hash is compared to a database (local or remote)
4. File is blocked (know hash) or allowed

Hashing


xavier@h0neyp0t: /opt/metasploit/app
File Edit View Search Terminal Help
xavier@h0neyp0t:/opt/metasploit/app$ msfpayload windows/shell/reverse_tcp LHOST=127.0.0.1 LPORT=133
7 C | msfencode -e x86/shikata_ga_nai -o /tmp/output1.exe -t exe
[*] x86/shikata_ga_nai succeeded with size 2694 (iteration=1)
xavier@h0neyp0t:/opt/metasploit/app$ msfpayload windows/shell/reverse_tcp LHOST=127.0.0.1 LPORT=133
7 C | msfencode -e x86/shikata_ga_nai -o /tmp/output2.exe -t exe
[*] x86/shikata_ga_nai succeeded with size 2694 (iteration=1)
xavier@h0neyp0t:/opt/metasploit/app$ sha1sum /tmp/output*.exe
4c7731232ab4aafa9ab512cdaaa826d8792803d5 /tmp/output1.exe
03e59a557cef8f7f5232b89808a5abcc63224b74 /tmp/output2.exe
xavier@h0neyp0t:/opt/metasploit/app$ clamscan /tmp/output*.exe
/tmp/output1.exe: OK
/tmp/output2.exe: OK
----------- SCAN SUMMARY -----------
Known viruses: 3074000
Engine version: 0.97.8
Scanned directories: 0
Scanned files: 2
Infected files: 0
Data scanned: 0.14 MB
Data read: 0.14 MB (ratio 1.00:1)
Time: 4.858 sec (0 m 4 s)
xavier@h0neyp0t:/opt/metasploit/app$

Sandbox (Live)



1. Files are extracted from network flows
2. Files are executed in a sandbox
3. Behavior is analyzed and score is computed
4. File is blocked (>score) or allowed

Sandbox (Live)

- Score is computed based on "actions" performed by the malware

Action	Score
Try to find a debugger	+1
Connect to a known IP	+2
Perform multiple sleep()	+1
Inject itself into a DLL	+3
TOTAL	+7

- If ($score > $threshold) { alert(); }

So what?

	Pro	Con
Hashing	• Speed • Privacy • Integrated into modern firewalls	• Less reliable • Database growing daily • 0-day or targeted malwares not detected
Live Analysis	• More reliable • Targeted malware detected	• Resources usage intensive • Requires dedicated hardware • Privacy issue?

Agenda

- Introduction
- How to fight?
- Quick wins
- Real time analysis
- **Solutions**
- Limitations
- Conclusions

Some products

- Palo Alto Networks “Wildfire”
- Check Point “Anti-bot” & “Threat Emulation”
- FireEye (core-business)
- Cuckoo (open source project)

WILDFIRE

FireEye™

Advantages

- PA & CP integrate smoothly with existing infrastructure
- Data is captured live
- Cloud or Appliance based
- Data sharing
- Web traffic, email protocols (SMTP, IMAP, POP), FTP, and SMB.

Mix Technologies!

- Inspect traffic with the product proposed by your firewall vendor
- Mix this with off-line tools to inspect network shares or suspicious computers
- On demand analysis

Agenda

- Introduction
- How to fight?
- Quick wins
- Real time analysis
- Solutions
- **Limitations**
- Conclusions

Cat & Mouse Game

Evasive Techniques

- Wait for user interactions
- Looks at the $ENV: HW devices, MAC addresses, disk size, processes, …
- Use non-standard protocols
- Use encryption

Let's tap!

- Access to malwares in motion?
- Where to capture the traffic?
- Malware could be already installed and stealthy

Sandboxes

- OS & software restricted to Windows
- Difficult to deploy your own images with commercial products
- Only droppers are analyzed, and after?

Agenda

- Introduction
- How to fight?
- Quick Wins
- Live Analysis
- Solutions
- Limitations
- **Conclusions**

Conclusions

- You will be hit by a malware! Be ready or … maybe already infected?
- You already have valuable data, use them to track suspicious activity
- Best practices might reduce risks
- Backdoors in software aren’t reported as suspicious
- Patch, patch and patch again…

Thank You!

Interested?
Contact your Account Manager for more information!