Session Plan

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
Part I Threat Landscape
What are cyber threats?

Who has ever become a victim of a cyber threat?
### Threat Landscape - Threats

<table>
<thead>
<tr>
<th>Top Threats 2017</th>
<th>Assessed Trends 2017</th>
<th>Top Threats 2018</th>
<th>Assessed Trends 2018</th>
<th>Change in ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Malware</td>
<td></td>
<td>1. Malware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Web Based Attacks</td>
<td></td>
<td>2. Web Based Attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Phishing</td>
<td></td>
<td>4. Phishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Spam</td>
<td></td>
<td>5. Denial of Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Denial of Service</td>
<td></td>
<td>6. Spam</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Ransomware</td>
<td></td>
<td>7. Botnets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Botnets</td>
<td></td>
<td>8. Data Breaches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Data Breaches</td>
<td></td>
<td>11. Information Leakage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Identity Theft</td>
<td></td>
<td>12. Identity Theft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Information Leakage</td>
<td></td>
<td>13. Cryptojacking</td>
<td>NEW</td>
<td></td>
</tr>
<tr>
<td>15. Cyber Espionage</td>
<td></td>
<td>15. Cyber Espionage</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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  
Threat Landscape – Threat Agents

- Cyber Criminals
- 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)

1. Phishing and Zero day attack
   A handful of users are targeted by two phishing attacks; one user opens Zero day payload (CVE-02011-0609)

2. Back door
   The user machine is accessed remotely by Poison Ivy tool

3. Lateral movement
   Attacker elevates access to important user, service and admin accounts, and specific systems

4. Data gathering
   Data is acquired from target servers and staged for exfiltration

5. Exfiltrate
   Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider

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 Denial of Service 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

Nowadays also known as stress tests
Threat Landscape – [D]DoS

- 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.

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

Image: © Trendmicro: https://documents.trendmicro.com/images/tex/articles/exploitkit-figure-1.jpg
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)

<table>
<thead>
<tr>
<th>Internet Explorer</th>
<th>CVE-2014-6332 3 to 11</th>
<th>CVE-2015-2419 10 to 11</th>
<th>CVE-2016-0189 9 to 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIG EK</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>GrandSoft EK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GF Sundown</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Magnitude EK</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flash Player</th>
<th>CVE-2015-7645 up to 19.0.0.207</th>
<th>CVE-2015-8651 up to 20.0.0.228</th>
<th>CVE-2018-4878 up to 28.0.0.137</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIG EK</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>GrandSoft EK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GF Sundown</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Magnitude EK</td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Case Study: Yahoo! Malvertisement
Threat Landscape – Malvertisement

- **Yahoo Mail**
  - ad with iframe 192.133.137.0/24
  - Magnitude EK 193.169.256.73/78
• 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.

Threat Landscape – Tor
PRIVACY IS NOT A CRIME
Threat Landscape – Deepweb and Darkweb

- Surface Web
  - Yahoo!
  - Google
  - CNN
  - Bing

- Deep Web
  - Academic databases
  - Medical records
  - Financial records
  - Legal documents
  - Some scientific reports
  - Some government reports
  - Subscription-only information
  - Some organization-specific repositories

- Dark Web
  - TOR
  - Political protest
  - Drug trafficking and other illegal activities

96% of content on the Web (estimated)

https://darkwebnews.com: image Creative Commons Attribution-Noncommerical-Share Alike 3.0 license
Threat Landscape – Deepweb and Darkweb

![Image of Silk Road Market](image-url)

- **Drug Categories**
  - Drugs 8,670
  - Cannabis 2,066
  - Dissociatives 155
  - Ecstasy 660
  - Opioids 591
  - Other 455
  - Precursors 50
  - Prescription 2,146
  - Psychedelics 981
  - Stimulants 1,102

- **Other Categories**
  - Apparel 284
  - Art 127
  - Biotic materials 1
  - Books 861
  - Collectibles 5
  - Computer equipment 32
  - Custom Orders 68
  - Digital goods 509
  - Drug paraphernalia 305
  - Electronics 77

- **Examples of Items for Sale**
  - 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 tab: £0.10
Part II Malware Techniques
Malware = Malicious Software

Four classes of malware: Potentially Unwanted Programs (PUP) and:

<table>
<thead>
<tr>
<th>Property</th>
<th>Virus</th>
<th>Trojan</th>
<th>Worm</th>
</tr>
</thead>
<tbody>
<tr>
<td>First named</td>
<td>1983</td>
<td>1200 BC ☹ 1972</td>
<td>1975</td>
</tr>
<tr>
<td>Distribution</td>
<td>replicates itself by attaching to a host</td>
<td>part of a legitimate program</td>
<td>copies itself cross media</td>
</tr>
<tr>
<td>Host</td>
<td>boot/partition sector, program, document</td>
<td>stand-alone</td>
<td>stand-alone</td>
</tr>
<tr>
<td>Spreading (typical)</td>
<td>User interaction</td>
<td>User interaction</td>
<td>Exploit</td>
</tr>
<tr>
<td>Market Share 2014*</td>
<td>2.7%</td>
<td>62.8%</td>
<td>2.7%</td>
</tr>
</tbody>
</table>
Malware Techniques - Terminology

- 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 a 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)
Malware Techniques - Steganography

**FF D8** = Start of the picture

**FF FE** = JPG Comment Indicator → configuration

**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)

Malware Techniques – Network technics

- **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;
Malware Techniques – Fast-flux

- 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

Dyre’s DGA for the date July 4, 2015 and the input number 16. This is only one of 333 possible domains generated 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
Malware Techniques – Network

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

![Diagram of Centralised botnet](image-url)
Malware Techniques – Network

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

Figure 2: Peer-to-peer botnet.
Malware Techniques – Host

- 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.
Malware Techniques – Host

- **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.
Malware Techniques – Code obfuscation

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

- **Decode**
  - CyberChef (https://github.com/gchq/CyberChef)

```php
error_reporting(0);
$qaplm=headers_sent();
if (!$qaplm){
    $referer=$_SERVER['HTTP_REFERER'];
    $uag=$_SERVER['HTTP_USER_AGENT'];
    if ($uag) {
        if (!stristr($uag,"MSIE 7.0")){
            if (stristr($referer,"yahoo") or stristr($referer,"bing") or stristr($referer,"rambler") or stristr($referer,"gogo") or stristr($referer,"live.com") or stristr($referer,"a9") or stristr($referer,"nigma") or stristr($referer,"webalta") or stristr($referer,"begun.ru") or stristr($referer,"stumbleupon.com") or stristr($referer,"bit.ly") or stristr($referer,"tinyurl.com") or preg_match("/yandex.ru/yandsearch\?\.*?sr=/\",$referer) or preg_match("/\"google\?\.*?url\?sa\="/\",$referer) or stristr($referer,"myspace.com") or stristr($referer,"facebook.com") or stristr($referer,"aol.com")) {
                header("Location: http://gigop.americanunfinished.com/");
            exit();
        }
    }
}
```

Image Source: https://secure.wphackedhelp.com/blog/eval-base64-decode-hack-wordpress/
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**

<table>
<thead>
<tr>
<th><strong>Synopsis</strong></th>
<th>The remote network time service could be used for network reconnaissance or abused in a <strong>distributed denial of service attack</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk factor</strong></td>
<td>Medium</td>
</tr>
<tr>
<td><strong>CVSS Base Score</strong></td>
<td>5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td>CVE-2013-5211, CWE-20, cpe://a:ntp:ntp:4.2.7</td>
</tr>
</tbody>
</table>
Hacking – Example 1: [DR]DoS

- **CPE: Common Platform Enumeration**
  - standard to describe and identify classes of applications, operating systems and hardware

- **CWE: Common Weakness Enumeration**
  - unified, measurable set of software weaknesses

- **CVE: Common Vulnerability and Exposure**
  - dictionary of common names for public known information security vulnerabilities

- **CVSS: Common Vulnerability Scoring System**
  - system to score/weight vulnerabilities between 0 and 10.0.

---

cpe://a:ntp:ntp:4.2.7

CWE-20: Improper Input Validation

CVE-2013-5211

CVSS 5.0 (Medium)
Hacking – Example 2: Improper Input Validation

- CWE-20: Improper Input Validation

Image Source: https://twitter.com/ericbaize/status/492777221225213952
CWE-89: SQL Injection

- How does it work?
  Database-powered applications often use **user-supplied** values to create a database queries:

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

- User-supplied value `$user`:

```php
$q = sql_query("SELECT * FROM users WHERE user='".$user.' 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:

Source: https://xss-doc.appspot.com/demo/2
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:

```html
URL https://xss-doc.appspot.com/demo/2?query=<u>test</u>
```

Sorry, no results were found for `<b><u>test</u></b>`. `<a href='?'>Try again</a>`.

```html
<script>top.postMessage(window.location.toString(), "*");</script>
```

Sorry, no results were found for `<u>test</u>`. Try again.
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:

```
Sorry, no results were found for <b><script>alert('hello')</script></b>. <a href='?'>Try again</a>.
```

Source: https://xss-doc.appspot.com/demo/2
### OWASP Top 10 - 2017

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>2017-Injection</td>
</tr>
<tr>
<td>A2</td>
<td>2017-Broken Authentication</td>
</tr>
<tr>
<td>A3</td>
<td>2017-Sensitive Data Exposure</td>
</tr>
<tr>
<td>A4</td>
<td>2017-XML External Entities (XXE)</td>
</tr>
<tr>
<td>A5</td>
<td>2017-Broken Access Control</td>
</tr>
<tr>
<td>A6</td>
<td>2017-Security Misconfiguration</td>
</tr>
<tr>
<td>A7</td>
<td>2017-Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A8</td>
<td>2017-Insecure Deserialization</td>
</tr>
<tr>
<td>A9</td>
<td>2017-Using Components with Known Vulnerabilities</td>
</tr>
<tr>
<td>A10</td>
<td>2017-Insufficient Logging &amp; Monitoring</td>
</tr>
</tbody>
</table>
Hacking – Hacking a system – step 1
Hacking – Hacking a system – step 2

Slides from: https://github.com/radicallyopensecurity/Digitally-Aware. License Creative Commons Attribution 4.0 International (CC BY 4.0)
Once started, the Hail Mary will launch a flood exploits at hosts in the current workspace. There is nothing stealthy about this action. If clumsily launching hundreds of exploits is what you would like to do, press Yes.
Hacking – Hacking a system – step 5

Slides from: https://github.com/radicallyopensecurity/Digitally-Aware. License Creative Commons Attribution 4.0 International (CC BY 4.0)
Hacking – Hacking a system – Total Control

Slides from: https://github.com/radicallyopensecurity/Digitally-Aware. License Creative Commons Attribution 4.0 International (CC BY 4.0)
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)

Image source: https://www.offensive-security.com/community-projects/google-hacking-database/
Part IV Defense and Mitigation
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

Image source: http://csirt.egi.eu/activities/ © EGI CSIRT
- 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

Image source: https://www.tenable.com/sc-dashboards/application-patch-rate
MISP is an 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.

Image source: https://www.misp-project.org/assets/images/banner.jpg
Defense and Mitigation – Virus Total

- 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

Image source: https://www.ghacks.net/2016/02/01/virustotal-scan-firmware-for-signs-of-manipulation/
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;

Source: https://www.cisecurity.org/controls/
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

Command
Propagation

Image source: https://mashable.com/2014/06/03/cyber-criminals-russia-ukraine-gameover-zeus/?europe=true#pkbm39g52Eqr
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 contacts
- …and many more – what else do you know / offer?
Thank you
Any Questions?

Authors: Slavo Greminger, Jeffen 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.