



certSIGN®  
BY UTI

## Fighting the cybercrime

from education, to trojans investigations and joint collaboration for botnet takedown

Teodor Cimpoesu, Technical Director, UTI-CERT

# UTI-CERT @ certSIGN

- Clear legal requirements and compliance
- Disaster recovery and business continuity
- “Trusted Introducer” member
- ISO 27001 & 9001 compliance
- Regular internal pen testing and security audit
- Structure enhanced to cover variety of customers
  - Oil and gas
  - Utilities providers
  - Banks
  - Telecom



- AI around cyber security services and solutions
- Flexibility for special projects customized according to client needs
- Customizable services
- Adaptable SLA
- Training, Knowledge transfer and technical support



# UTI-CERT

## SOC

### Consulting

Vulnerability  
Assessment

Security validation  
(Pen testing)

Security consulting

### Managed Services

Monitoring  
(SIEM)

Network  
Security

Communication  
Security

Data  
Security

Endpoint  
Security

### CSIRT

Alerting  
Services

Incident  
Handling

Vulnerability  
Handling

Forensics

Malware  
Analysis

Vulnerability  
Analysis

### Special Services

Cyber  
Investigation

Threat  
Intelligence

Advanced  
Monitoring

Special  
Projects

Research &  
Development

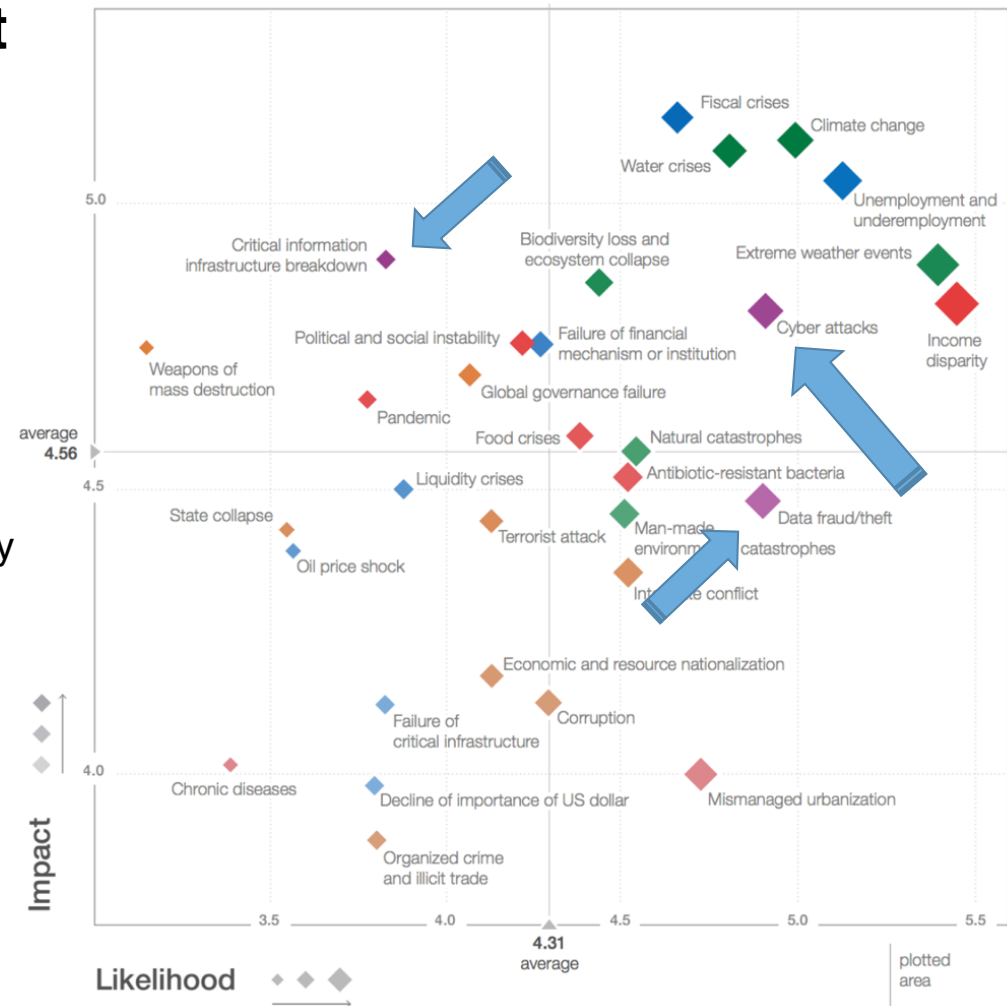
# **1. Cybercrime context**



# Cyber risks in global context

World Economic Forum study on global risks (2014) findings position Cyber attacks in high likelihood / high impact.

- Systemic risk is the risk of “breakdowns in an entire system, as opposed to breakdowns in individual parts and components”
- Systemic risks are characterized by:
  - modest tipping points combining indirectly to produce large failures
  - risk-sharing or contagion, as one loss triggers a chain of others
  - “hysteresis”, or systems being unable to recover equilibrium after a shock
- **Cyber risks** in key areas (e.g. financial) and attacks on critical infrastructure pose a **systemic risk**



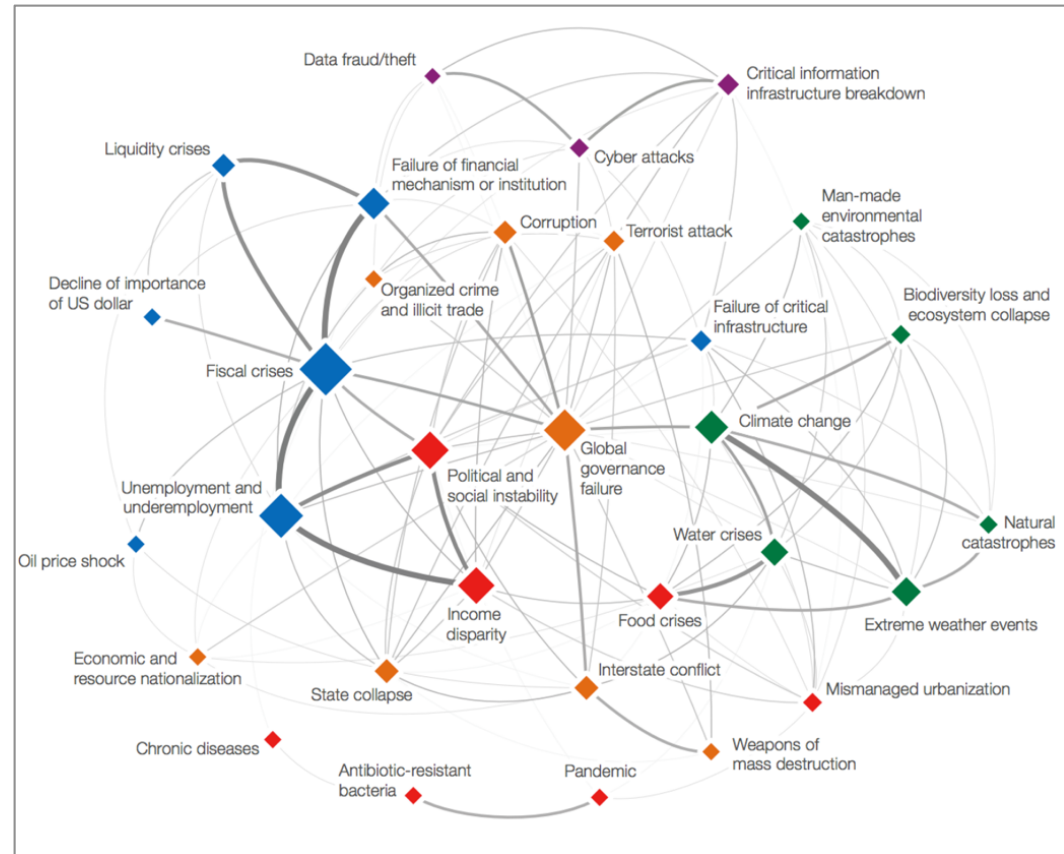
# Cyber risks in global context

On the The Global Risks Interconnection Map we can see the links and potential influences of the systemic risks.

The Technological Risks are strongly linked with geopolitical and economic risks.

Organized crime risk has a direct link to them.

Mitigating one area involves taking into consideration other indirect risk propagations as well.



Source: World Economic Forum, "Global Risks 2014" Ninth Edition

# Global Cybercrime

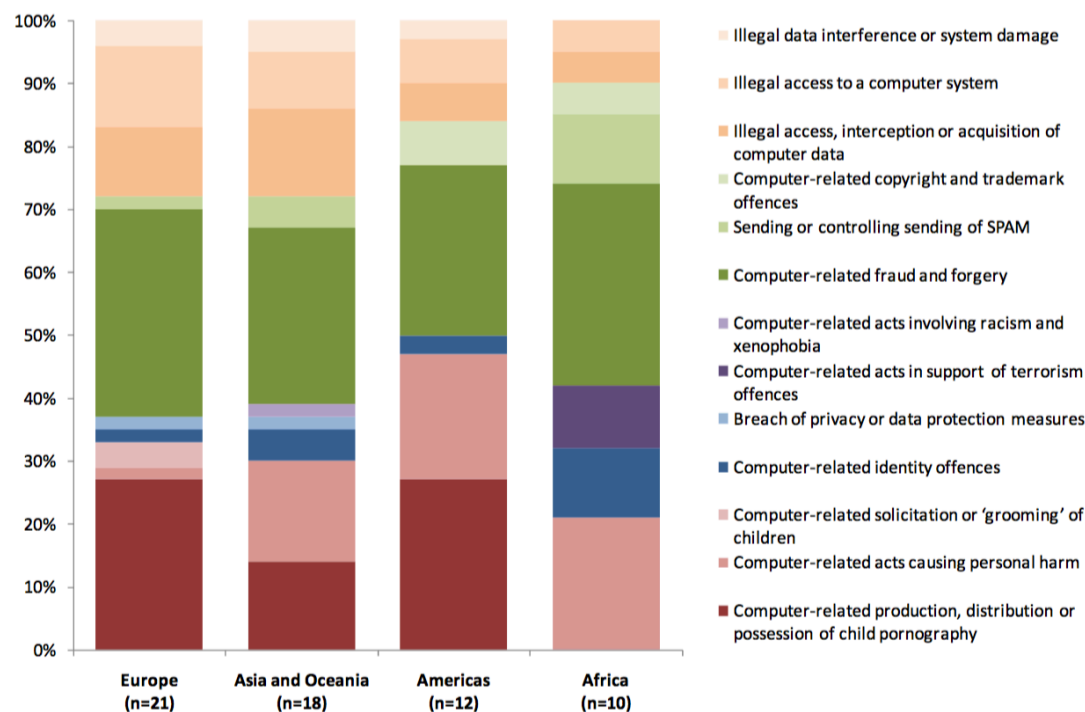
The Comprehensive study by United Nations Office on Drugs and Crime (2013) gives a perspective from GOV, COM, EDU view.

## Findings:

- Laws are fragmented, lack procedural powers and hinder intl cooperation.
- Law enforcement and criminal justice have limitations in their capacity to react and combat
- Preventions activities are lacking / require strengthening

Source: "Comprehensive Study on Cybercrime", UN ODC

Figure 2.1: Most common cybercrime acts encountered by national police



Source: Study cybercrime questionnaire. Q80. (n=61. r=140)

# Global Cybercrime

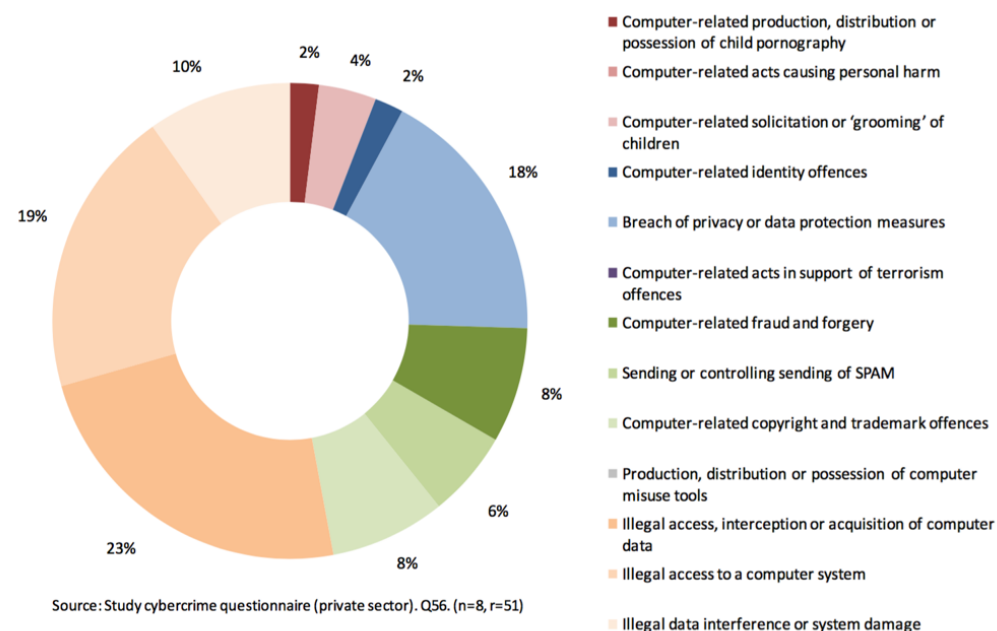
The Comprehensive study by United Nations Office on Drugs and Crime (2013) gives a perspective from GOV, COM, EDU view.

## Findings:

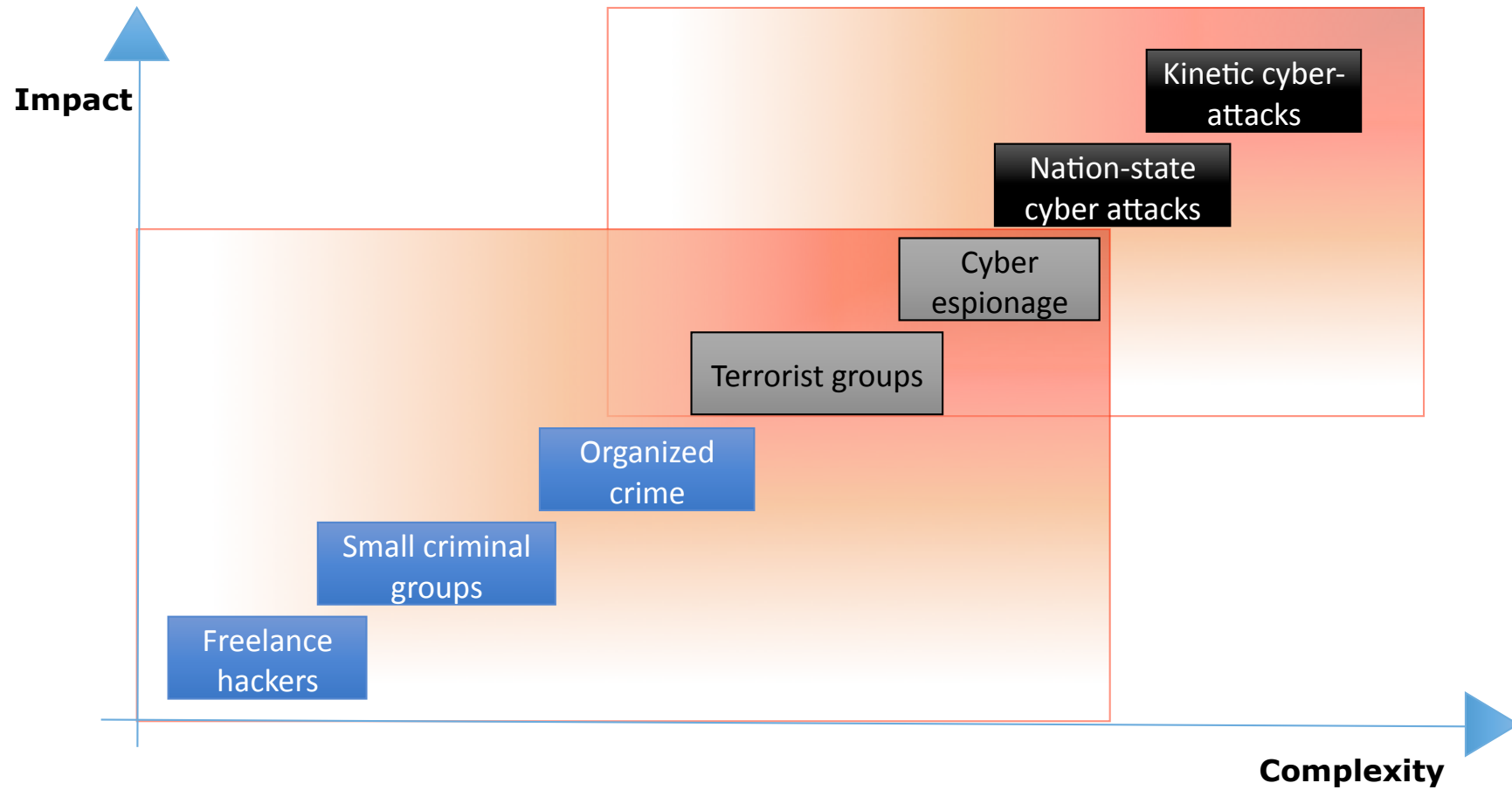
- Laws are fragmented, lack procedural powers and hinder intl cooperation.
- Law enforcement and criminal justice have limitations in their capacity to react and combat
- Preventions activities are lacking / require strengthening

Source: "Comprehensive Study on Cybercrime", UN ODC

Figure 2.3: Most significant cybercrime threats - views of private sector organizations

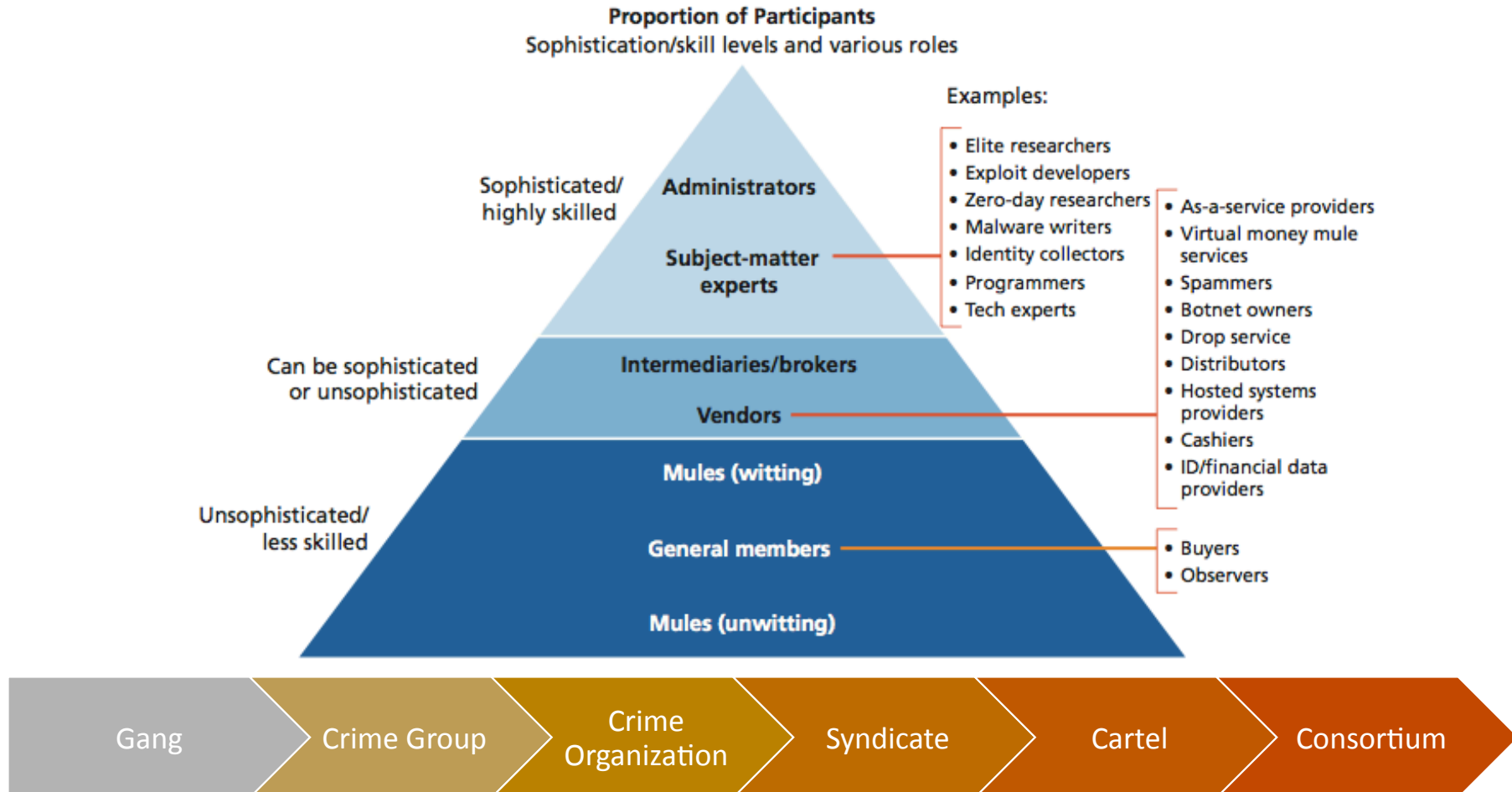


# Cyber threats dynamics





# Accelerators: Crimeware



Source: RAND Corporation, Markets for Cybercrime Tools and Stolen Data (2014), [www.rand.org](http://www.rand.org)

# Accelerators: business ecosystem

"The increasing **frequency**, **variety**, and **complexity** of attacks are the product of an emerging **cybercrime-as-a-service** provider market. This market allows malicious parties to execute attacks at considerably **lower cost**, with considerably **lower levels** of technical savvy."

- **Research-as-a-Service**
  - – Vulnerabilities, Exploits, IDs
- **Crimware-as-a-Service**
  - – Development, Malware Services
- **Infrastructure-as-a-Service**
  - – Botnets, Hosting, Exploitpacks
- **Hacking-as-a-service**
  - – DoS, Password Cracking, Financials

Source: "Cybercrime Exposed. Cybercrime-as-a-Service ", McAfee



# Accelerators: Cheap & easy

Recent prices from the black market			Price
			1BTC 213,200 EUR
N	SERVICES	BTC	EUR
50.000	Root shell	1,85	394,62
45.000	Wordpress admin passwords	1,50	319,80
50.000	SSH sniffer logs	1,20	255,84
1.000	Linux botnet	2,00	426,40
1.103.504	FTP/SSH passwords	3,00	639,60
N	SERVICES	BTC	EUR
1	Start your own maket	33,48	7.137,00
1	Virtual credit card + bank account	0,01	2,69
1	Unlimited REAL code signing	4,20	895,44
TYPE	KIT	BTC	EUR
spam	Wordpress Comment Spammer + Exploit	2,50	533,00
malware	Bitcoin Ransomware	0,21	44,77
malware	Tomcat Worm	7,40	1.578,67
malware	The real GovRAT	4,50	959,40
TYPE	EXPLOIT	BTC	EUR
1day	MS15-034 Microsoft IIS Remote Code Execution	308,53	65.778,11
1day	*NEW* ring0 LPE Exploit CVE-2015-0057	48,17	10.269,84
fud	Adobe Flash < 16.0.0.296 (CVE-2015-0313)	2,50	533,00
0day	Internet Explorer <= 11	35,00	7.462,00
0day	Android WebView 0day RCE	36,50	7.781,80
0day	Linux <= 3.13.0-48 Kernel Panic	2,00	426,40



Source: <http://darkmatters.norsecorp.com/2015/06/16/finding-hacking-services-and-more-in-the-deep-web/>

## Accelerators: Cheap & easy

Exploit Kit	Price	Year
Eleonore (v1.6.2)	\$2,500-\$3,000	2012
Phoenix (v2.3.12)	\$2,200 / domain	2012
Styx sploit pack rental	\$3,000 / month	2012
Exploit kits that employ botnets	up to \$10,000	2012
CritXPack	\$400/week	2012
Phoenix (v3.1.15)	\$1,000-\$1,500	2012
NucSoft	\$1,500	2012
Blackhole—hosting (+ crypter + payload + sourcecode)	\$200/week or \$500/month	2013
Whitehole	\$200–\$1,800 rent	2013
Blackhole—license	\$700/three months or \$1,500/year	2013
Cool (+ crypter + payload)	\$10,000/month	2013
Gpack	\$1,000–\$2,000	2013
Mmpack	\$1,000–\$2,000	2013
Icepack	\$1,000–\$2,000	2013
Eleonore	\$1,000–\$2,000	2013
Sweet Orange	\$450/week or \$1,800/month	2013
Whitehole	\$200–600/week or \$600–1,800/month, depending on traffic	2013

Source: RAND Corporation, “Markets for Cybercrime Tools and Stolen Data”

# Accelerators: Cheap & easy

## Credit Card Prices Based on Market Circumstance

Credit Card Price	Market Circumstance
\$20–\$45	Freshly acquired
\$10–\$12	Flooded
\$2–\$7	Clearance ("stale" data)

### Estimate of Prices (without PIN, with PIN, PIN and good balance)

#### Dumps

Dumps

	US			EU			CA, AU		Asia	
Visa Classic	\$15	\$80		\$40	\$150		\$25	\$150	\$50	\$150
Master Card Standard	\$90			\$140			\$150		\$140	
Visa Gold/Premier	\$25	\$100	\$200	\$45	\$160	\$250	\$30	\$160	\$55	\$150
Visa Platinum	\$30	\$110		\$50	\$170		\$35	\$170	\$60	\$170
Business/Corporate	\$40	\$130		\$60	\$170		\$45	\$175	\$70	\$170
Purchasing/Signature	\$50	\$120		\$70			\$55		\$80	
Infinite				\$130	\$190		\$60	\$200	\$190	
Master Card World	\$140									
AMEX	\$40			\$60			\$45		\$70	
AMEX Gold	\$70			\$90			\$75		\$100	
AMEX Platinum	\$50									

Source1: "Cybercrime Exposed. Cybercrime-as-a-Service ", McAfee

Source2: RAND Corporation, "Markets for Cybercrime Tools and Stolen Data"



# Accelerators: Cheap & easy

10-th version.

## Packages:

â€¢ Minimum: DDoS Bot, no free updates, no modules = \$450

â€¢ Standart: DDoS Bot, 1 month free updates, password grabber module = \$499

â€¢ Bronze: DDoS Bot, 3 months free updates, password grabber module, 1 free rebuild = \$570

â€¢ Silver: DDoS Bot, 6 months free updates, password grabber module, 3 free rebuilds = \$650

â€¢ Gold: DDoS Bot, lifetime free updates, password grabber + "hosts" editor modules, 5 free rebuilds, 8% discount on other products. = \$699

â€¢ Platinum: DDoS Bot, lifetime free updates, password grabber, unlimited free rebuilds, 20% discount on other products. = \$825

â€¢ Brilliant: DDoS Bot, lifetime free updates, unlimited free rebuilds, all modules for free, 25% discount on other products. = \$999

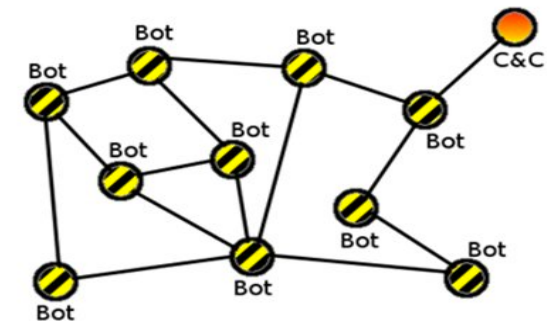
## Other:

â€¢ ReBuild (URLs changing) â€¢ \$35.

â€¢ Sources - ~3500-5000\$, discuss individually

â€¢ New features - discuss individually.

â€¢ Web-Panel reinstalling (1st time is free) - \$50



Source: "Cybercrime Exposed. Cybercrime-as-a-Service ", McAfee

## Accelerators: Defence gap

- In a Symantec study\*, **11 of 18** identified vulns were not known 0-days.
- Attacks with 0-days lasted b/w **19 days – 30 months**, with a MED of **8** and AVG of **10** month.
- After disclosure, the **variants** exploiting them explode **183-85k** times, and **attacks** increase **2-100k** times
- Exploits for **42%** of vulns are detected within **30 days** after disclosure
- **200+ days** MED, **243 days** AVG, the attackers **reside** within a victim network **before detection**
- **1 in 5** (~20%) of threat actors are **internal**
- **75%+** of all network intrusions are due to **compromised** user **credentials**, **84% w/ no admin rights**
- **60%** of cases attackers compromise the org within **minutes**. **Discovery** within **days or less** is below **25%**.
- **94%** of the breaches are **reported** by a **3<sup>rd</sup> party**

\* Source: Before We Knew It - An Empirical Study of Zero-Day Attacks In The Real World, Tudor Dumitras et al., Symantec Research Labs

Sources: Microsoft Advanced Threat Analytics, HP Security, Verizon DBIR2015, ObserveIT

## Accelerators: Geopolitics complication

- All world powers modern **warfare** doctrines include the cyber field - engagement playbook.
- Take Russia - from Myatezhevoyny (МЯТЕЖЕВОЙНЫ) to V. Gerasimov doctrine of **non-linear/hybrid** war.
- Inducing panic, doubt in the enemy's soul by means of **propaganda** / disinformation
- **Controlling territory** without conventional troops on the ground – cyberspace an important vector.
- Soviet military scholar G.Isserson – “War in general is **not declared**. It simply begins with already developed military forces.”



Source: Wikimedia.org

## **2. Legal context**

# EU response to cybercrime

## Policies and directives

- [The Cybersecurity Strategy of the EU \(2013\)](#)
- [Directive 2013/40/EU on attacks against information systems](#)
- [Directive 2011/92/EU on combating the sexual exploitation of children online and child abuse](#)
- [ePrivacy Directive 2009/136/EC](#)
- [Framework Decision on combating fraud and counterfeit - 2001/413/JHA](#)

## Institutions & Initiatives

- [2013 - European Cybercrime Centre \(EC3\) @ EUROPOL](#)
  - [2004 - European Network and Information Security Agency \(ENISA\)](#)
- <https://cybersecuritymonth.eu/>

## Cybersecurity Strategy Strategic Priorities

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyberdefence policy and capabilities
- Develop the industrial and technological resources for cybersec
- Establish a coherent international cyberspace policy for EU

## Directive 2013/40/EU

- Deadline for transposition in the Member States 4.9.2015
- Guidelines and best practices
- EU countries must:
  - have an operational national point of contact,
  - use the existing network of 24/7 contact points ,
  - respond to urgent requests for help within 8 hours to indicate whether and when a response may be provided,
  - collect statistical data on cybercrime.



# The terms - Directive 2013/40/EU

**Information system** - **device** or **group** of inter-connected or related devices, one or more of which, pursuant to a programme, **automatically processes computer data**, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;

**Computer data** - a **representation** of facts, information or concepts in a form suitable for processing in an information system, **including a programme** suitable for causing an information system to perform a function;

**Without right** – [...] including **access**, **interference**, or **interception**, which is not authorised by the owner or by another right holder of the system or of part of it

**Illegal access** - the **access without right**, to the **whole** or to any **part** of an information system, is punishable as a criminal offence

**Illegal system interference** - seriously **hindering** or **interrupting** the functioning of an information system by inputting computer data, by **transmitting, damaging, deleting, deteriorating, altering** or **suppressing** such data, or by rendering such data inaccessible, intentionally and without right

**Illegal data interference** - **deleting, damaging, deteriorating, altering** or **suppressing** computer data on an information system, or rendering such data inaccessible, intentionally and without right

**Illegal interception** – [...] by technical means, **non-public transmissions** of computer data to, from or within an information system

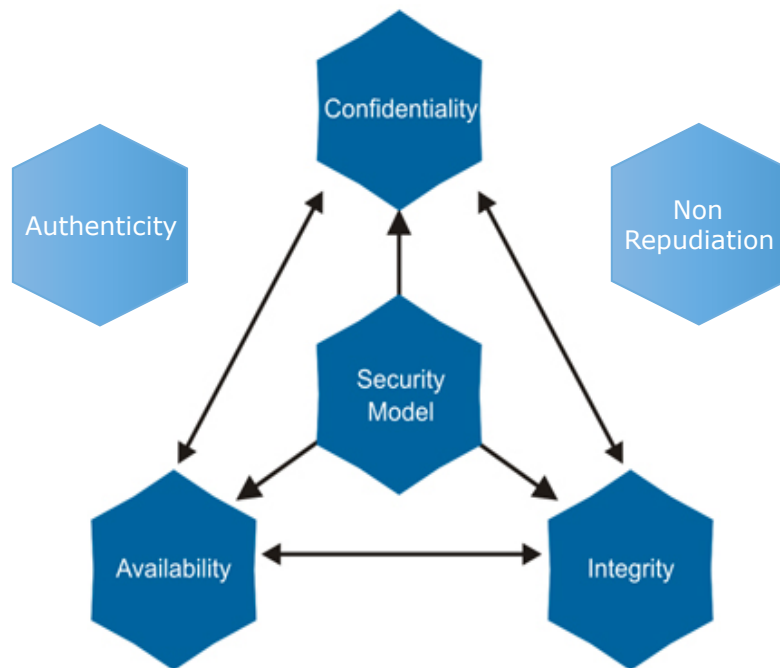
Topic	Observed good practice	Country or organisation where the practice was observed
All substantive criminal provisions (illegal access, illegal interception, tools for committing offenses)	The <b>publication of guidance</b> on the interpretation and application of the law, and particularly on the element of intent (i.e. the unlawfulness – without right). This can be done in the form of prosecution guidelines in countries that permit this, and/or in the form of jurisprudence overviews to show how courts apply the law in reality. Guidance should also explicitly cover conduct that is considered lawful, such as the activities of CERTs or security professionals.	UK, Sweden and <b>Portugal</b>
All substantive criminal provisions (illegal access, illegal interception, tools for committing offenses)	<b>Implementing legislation should be clear and explicit</b> , and include clear carve-outs of the applicability of the provision for the normal activities of CERTs, academic institutions, researchers, network operators and security service professionals, and any actions undertaken at the lawful request of businesses, governments and end users.	France (carve-outs not included in legislation, but explicitly discussed in Parliamentary discussions)
Botnets & identity theft	<b>Implementing legislation should avoid using technology specific terminology. It should focus on the exact harm that technologically enabled crimes cause.</b> E.g. rather than introduce the concept of botnets or DDoS attacks, UK legislation was amended to make it an offence to deliberately or recklessly impair the operation of any computer or program, or reliability of data, or to prevent or hinder access to data. Similarly, French and Italian identity theft initiatives focus on the intent to cause harm as a precondition for criminalisation, and emphasise the importance of respecting freedom of expression.	UK, France, Italy
Botnets & identity theft	CERTs can benefit from the <b>development of standardised processes or playbooks for taking appropriate action to respond to botnets or incidents of identity theft.</b> These should e.g. cover the questions that CERTs would need to ask, what information and recommendations they should provide, and what could proportionately and lawfully be done by service providers. This would also be useful to strengthen the	Romania, France

European Union Agency for Network and Information Security (ENISA) -

**“Good Practice Collection for CERTs on the Directive on attacks against information systems”**

### **3. Cyber terms**

# Information Security



# The Basics - Terms

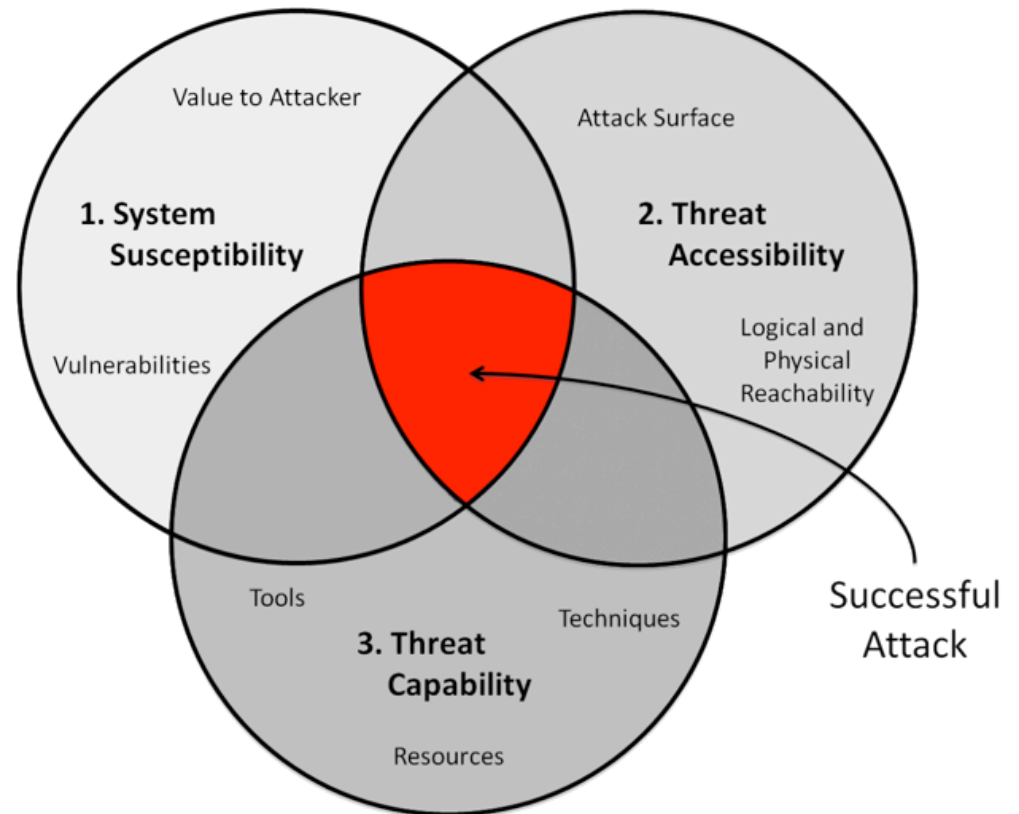
**Asset** – any information system or data that has value for the organization.

**Vulnerability** – A flaw or weakness in system security procedures, design, implementation, or internal controls that **could be exercised** (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy [NIST]

*Short: security flaws in a system that allow an attack to be successful.*

**Threat** – Any **circumstance** or **event** with the **potential** to adversely impact organizational operations (including mission, functions, image, or reputation), assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to **successfully exploit** a particular information system vulnerability.

*Short: there is someone who knows about, is able and willing to exploit a vulnerability*





# The Basics - Terms



**Exploit** – the defined way (specific steps/application) to use a vulnerability in practice, to breach a system. The **exploit range** can be **local** or **remote**.

**Zero-Day Vuln** – Vulnerability for which there is no patch (solution/countermeasure) from the vendor of the system or application.

**Zero-Day Exploit** – the actual means to use that vulnerability

**Attack** – The realization of a threat, through the means of exploits on existing vulnerabilities.

**Attack vector** - the method that the (exploit) code uses to breach or propagate. A **vulnerability** can have **several** attack vectors.

**Attack surface** – the sum of all attack vectors

**Impact** – financial and non-financial loss estimate = value of services, capabilities, data etc. after a threat materializes into an attack (if we take cyber attacks, not accidents).

**Controls** - Mechanisms used to restrain, regulate, or reduce **vulnerabilities**. Controls can be corrective, detective, preventive, or deterrent.

# The Terms – Malware & botnets

**Malware** – malicious software, that is any computer code with the potential to damage an information system or network

**Browser malware** – targets flaws in browser design principles, and exploits vulnerabilities in the components, plug-ins and OS layers.

**Virus** – program/code that infects a IS by attaching itself to another program, and propagating itself when that program is executed.

**Worm** – program/code that can make copies of itself and spread itself through connected systems and using up resources in affected computers or causing other damage

**Payload** - the specific malware **attributes** unrelated to insertion, infection, armoring, obfuscation, and self-defense; the actions taken after the successful infection of a system that is directly tied into the **purpose behind** the malware.

**Trojan** – program/code that does something that is not expected by the user (delete, modify, copy data).

**Trojan downloader** – A Trojan that downloads and installs malicious components on the host computer, or updates the commands/ configuration

**Trojan dropper** – a program that is capable of installing a Trojan or other malware on the target system, and prevent its detection (from the antivirus or other security systems).

**Remote Access Trojan (RAT)** – a trojan that communicates back to the attacker and can be controlled executing any commands.

**Zombie/bot** – a compromised computer that can be controller by the attacker (e.g. through a RAT)

**Botnet** – a network of infected computers (bots), that can vary in the sophistication of communication means and stealth capabilities. Examples includes IRC/HTTP/P2P botnets.

# The Basics



MAC Address

c8:2a:14:07:49:cd

IP Address

Private:10.0.1.10

IPv6: fe80::e2f8:47ff:fe27:f2b0 -> ICANN

URL

[https://www.portugal.gov.pt /](https://www.portugal.gov.pt/)

DNS

TLD / DNSSEC

Local Router

vs. switch. Ethernet/Wireless

BGP Router

Dynamic / SBGP

Local Router

vs. switch. Ethernet/Wireless

Web service

Port , Socket (80, 443)

Web Server

e.g. Apache / IIS

Web Application

e.g. PHP / ASP

# The Basics



MAC Address

c8:2a:14:07:49:cd

IP Address

Private:10.0.1.10

IPv6: fe80::e2f8:47ff:fe27:f2b0 -> ICANN

URL

DNS

Local Router

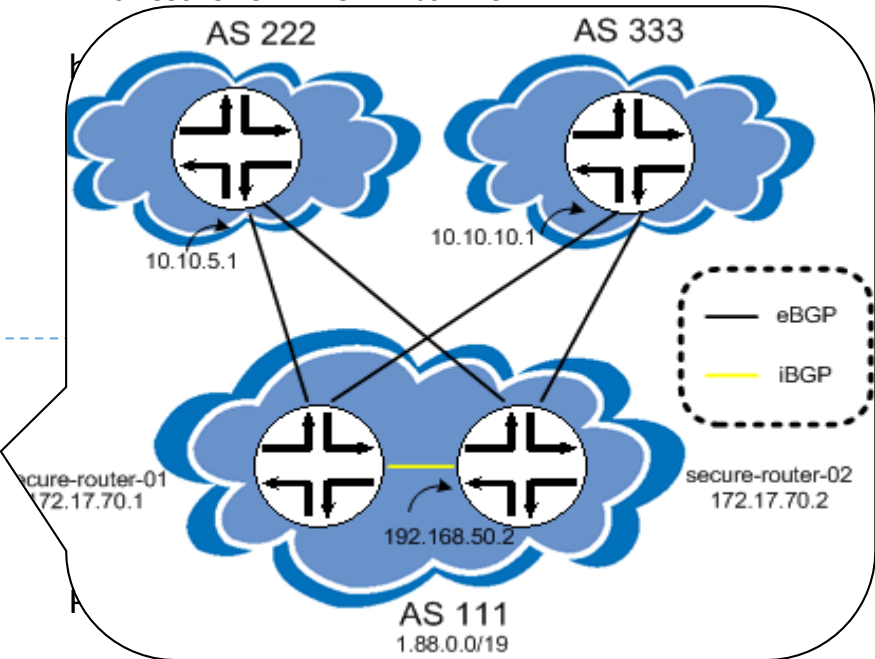
BGP Router

Local Router

Web service

Web Server

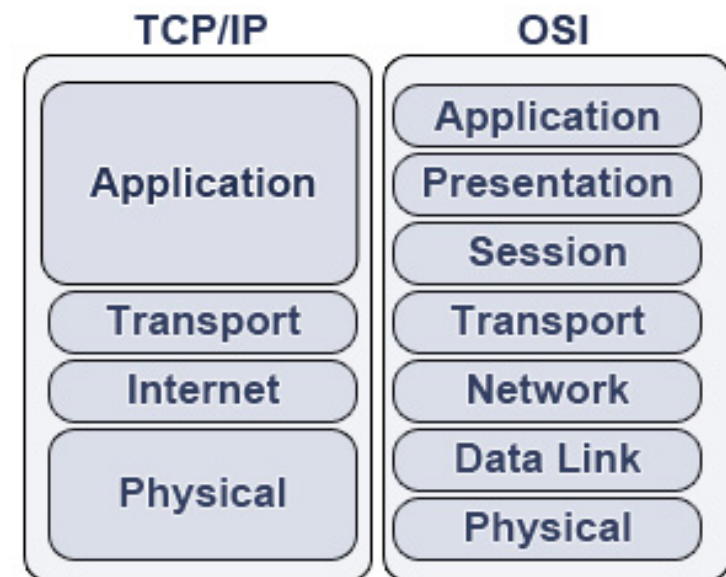
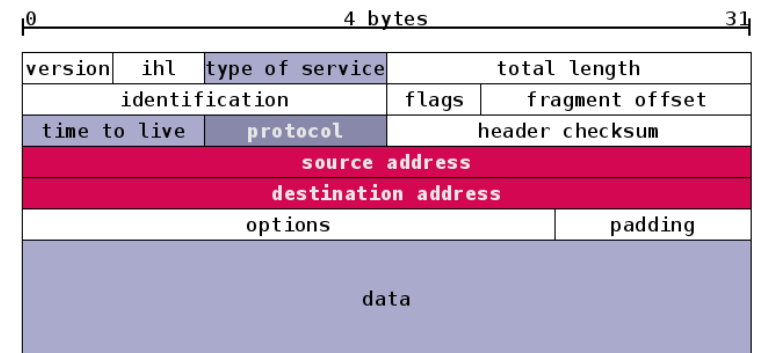
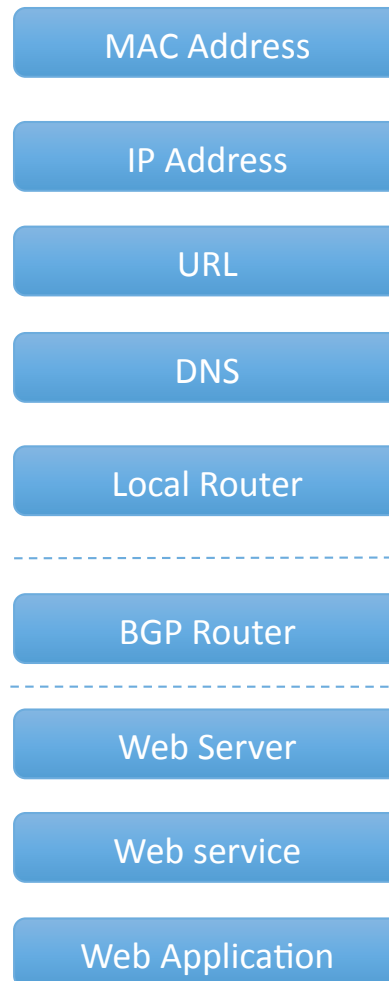
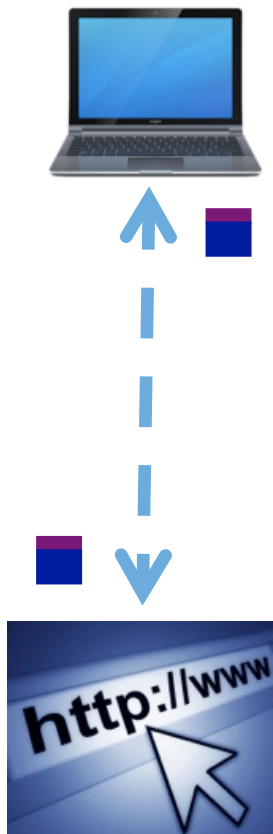
Web Application



e.g. Apache / IIS

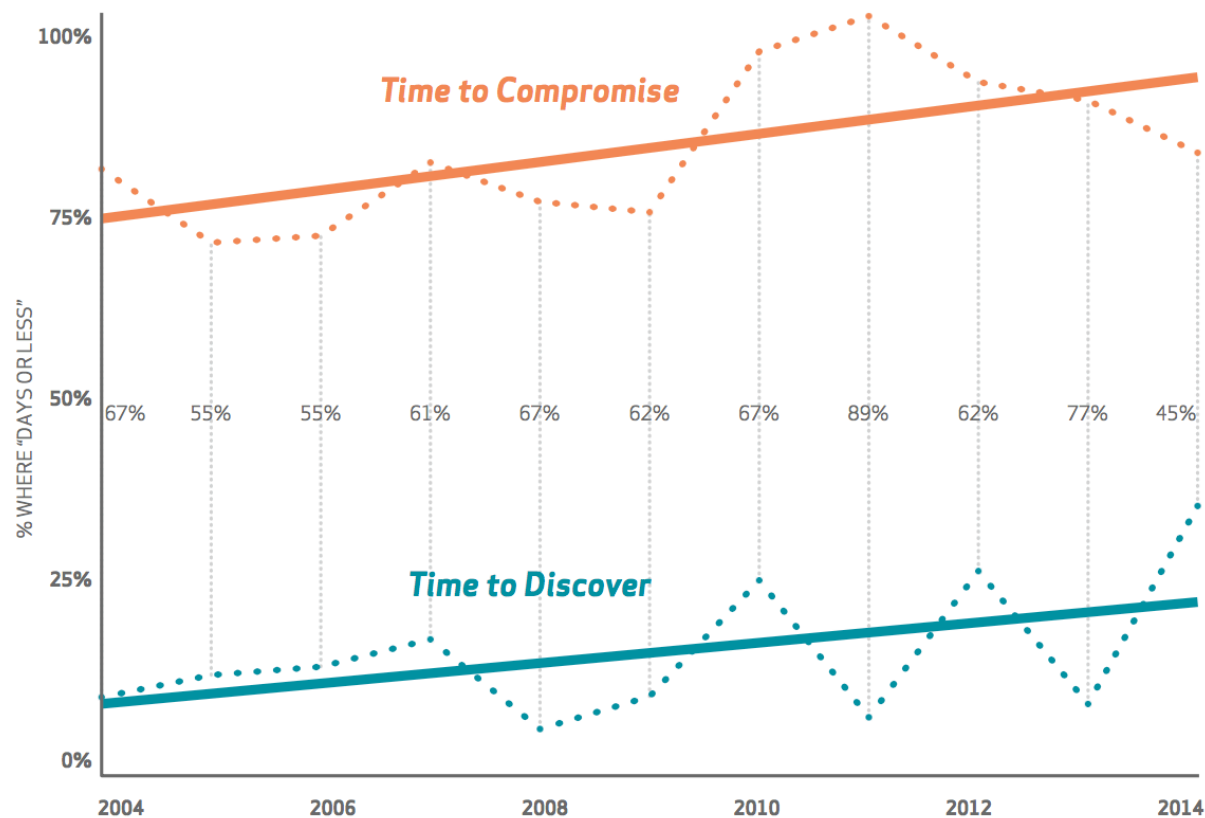
e.g. PHP / ASP

# The Basics



## **4. Challenges in defence and collaboration**

# Attacker vs. Defender - detection deficit



Source: Verizon DBIR2015

- Cyberspace favors **offense**
- Shift from **total security** to **assume compromise**

A: "We only have to be lucky once.  
You will have to be lucky always." (IRA, '84)

D: "There's no way that we are going to win the cybersecurity effort on defense. We have to go on offense."

(Steven Chabinsky, former head of FBI CyberIntelligence, CRO at CrowdStrike)



# Threat Modeling to Controls

STRIDE-LM	Threat	Property	Definition	Controls
<b>S</b>	Spoofing	Authentication	Impersonating someone or something	Authentication Stores, Strong Authentication mechanisms
<b>T</b>	Tampering	Integrity / Access Controls	Modifying data or code	Crypto Hash, Digital watermark/ isolation and access checks
<b>R</b>	Repudiation	Non-repudiation	Claiming to have not performed a specific action	Logging infrastructure, full-packet-capture
<b>I</b>	Information Disclosure	Confidentiality	Exposing information or data to unauthorized individuals or roles	Encryption or Isolation
<b>D</b>	Denial of Service	Availability	Deny or degrade service	Redundancy, failover, QoS, Bandwidth throttle
<b>E</b>	Elevation of Privilege	Authorization / Least Privilege	Gain capabilities without proper authorization	RBAC, DACL, MAC; Sudo, UAC, Privileged account protections
<b>LM</b>	Lateral Movement	Segmentation / Least Privilege	Expand influence post-compromise; often dependent on Elevation of Privilege	Credential Hardening; Segmentation and Boundary enforcement; Host-based firewalls

Source: "A Threat-Driven Approach to Cyber Security - Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization", Lockheed Martin Corp.

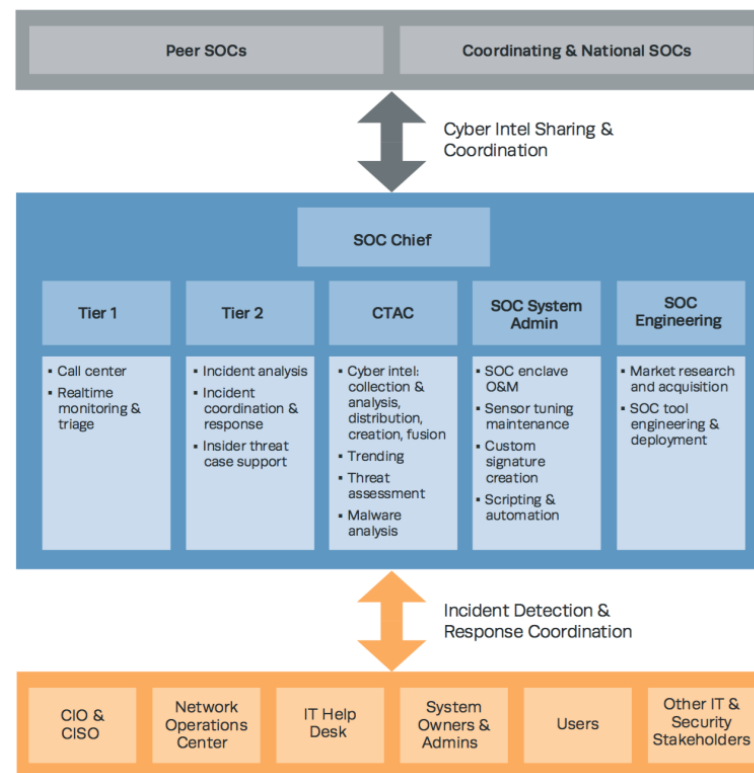
# Mature defence – e.g. banking

## ROLES (ENISA / SOC)

- **Duty officer / Tier 1 Analyst** – takes care of all incoming requests. Ensure that all incidents have owners.
- **Triage officer / Tier 1 Analyst** – deal with the reported incidents, decides whether it is an incident and is to be handled, and by whom
- **Incident handler / Tier 2 Incident Responder** – works on the incident: analyze data, create solutions, resolve the technical details and communicates about the progress to the manager and the constituents.
- **Incident handler / Tier 3 Subject Matter Expert** – advanced analyst that deals with complex cases that involve a cross-filed investigation.
- **Incident manager** – responsible for the coordination of all incident handling activities. Represents the team in communicating to the outside 3<sup>rd</sup> parties.

## STAFFING (ENISA)

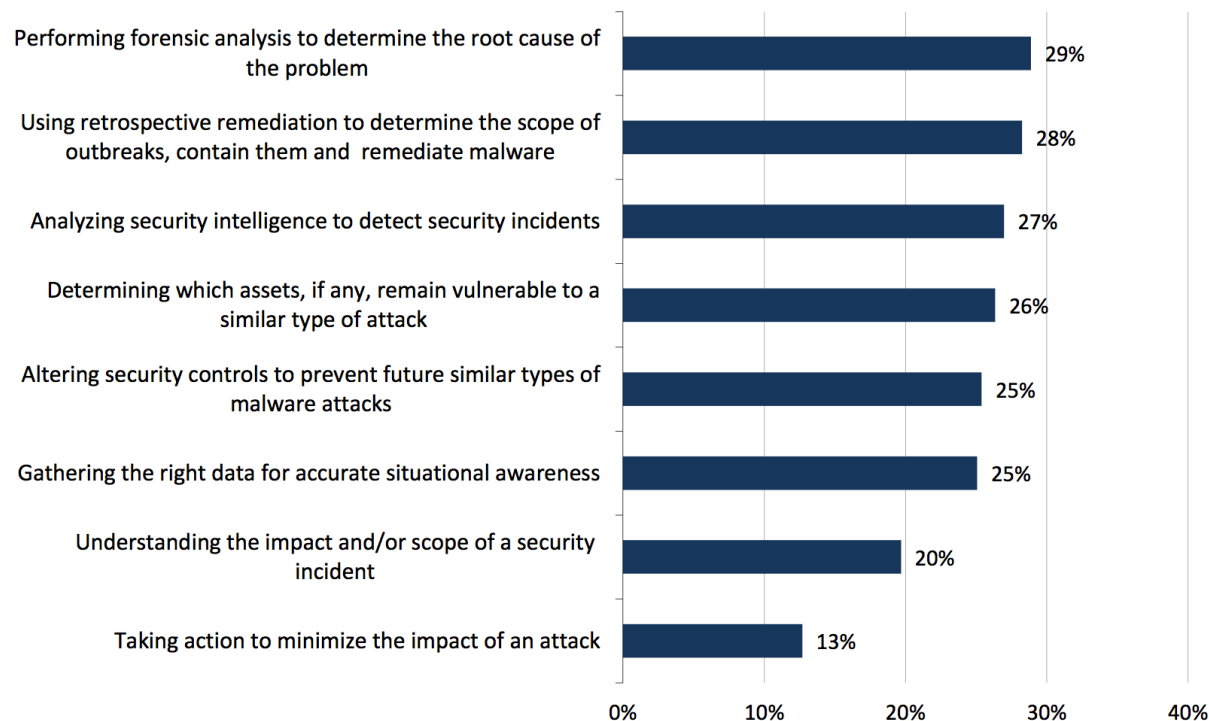
- to deliver two core services of the distribution of advisory bulletins as well as incident handling: a **minimum of 4 FTE**.
- For a full service CSIRT during office hours, and maintaining systems: a **minimum of 6 to 8 FTE**.
- For a fully staffed **24x7 shift** (2 shifts during out-of-office hours), **the minimum is about 12 FTE**.



Source: "Ten Strategies of a World-Class Cybersecurity Operations Center" (MITRE)

## Defence in real life – gap in IR/DF

Please consider this list of incident detection/response tasks. Which three are your organization's biggest areas of weakness (i.e., which are you worst at)? (Percent of respondents, N=315, three responses accepted)

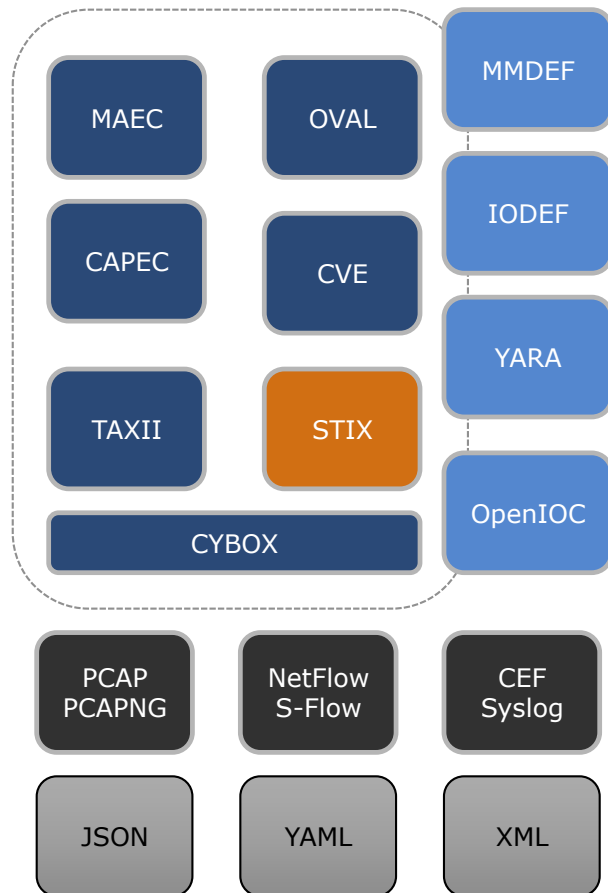


Source: Enterprise Strategy Group, 2015.

In reality, companies and organizations struggle with:

- Threat detection, investigation and incident response is **immature**
- Determining the **root cause** of incidents and then containing and remediating them is the tough nut
- Making use of **security intelligence**
- Evaluating assets **risk state**
- SIEM tools also require **advanced skills and knowledge**
- Many SIEM are **verbose** –give too many FPs
- Many attacks spread over larger period of time and **context** may be lost / lacking

# Incident Response (IR) - Threat Intel (TI) Frameworks



## Indicators

- [STIX](#) – Structured Threat Information eXpression (MITRE/OASIS)
- [TAXII](#) – Trusted Automated eXchange of Indicator Information (MITRE/OASIS)
- [CYBOX](#) – Cyber Observable eXpression (MITRE/OASIS)
- [OpenIOC](#) – Open Indicators of Compromise (FireEYE/Mandiant)
- [IODEF](#) – Incident Object Description Exchange Format (IETF – RFC5070).
- [YARA](#) – Yet Another Regex Analyzer – binary pattern scanning (OSS)
- [SNORT](#) – real-time analysis of network traffic (CISCO).

## Enumerations

- [MMDEF](#) – Malware Metadata Exchange Format (IEEE)
- [MAEC](#) – Malware Attribute Enumeration and Characterization (MITRE).
- [CAPEC](#) – Common Attack Pattern Enumeration and Classification (MITRE).
- [CVE](#) – Common Vulnerabilities and Exposures (MITRE)
- [CVSS](#) – Common Vulnerability Scoring System (NIST)
- [CPE](#) – Common Platform Enumeration (NIST)
- [OVAL](#) – Open Vulnerability and Assessment Language (MITRE)
- [OSVDB](#) – Open Sourced Vulnerability Database (OSF)

[MITRE](#) – Not-for-profit org that operates US federally funded research centers.

# Threat Intel in real life - IOCs

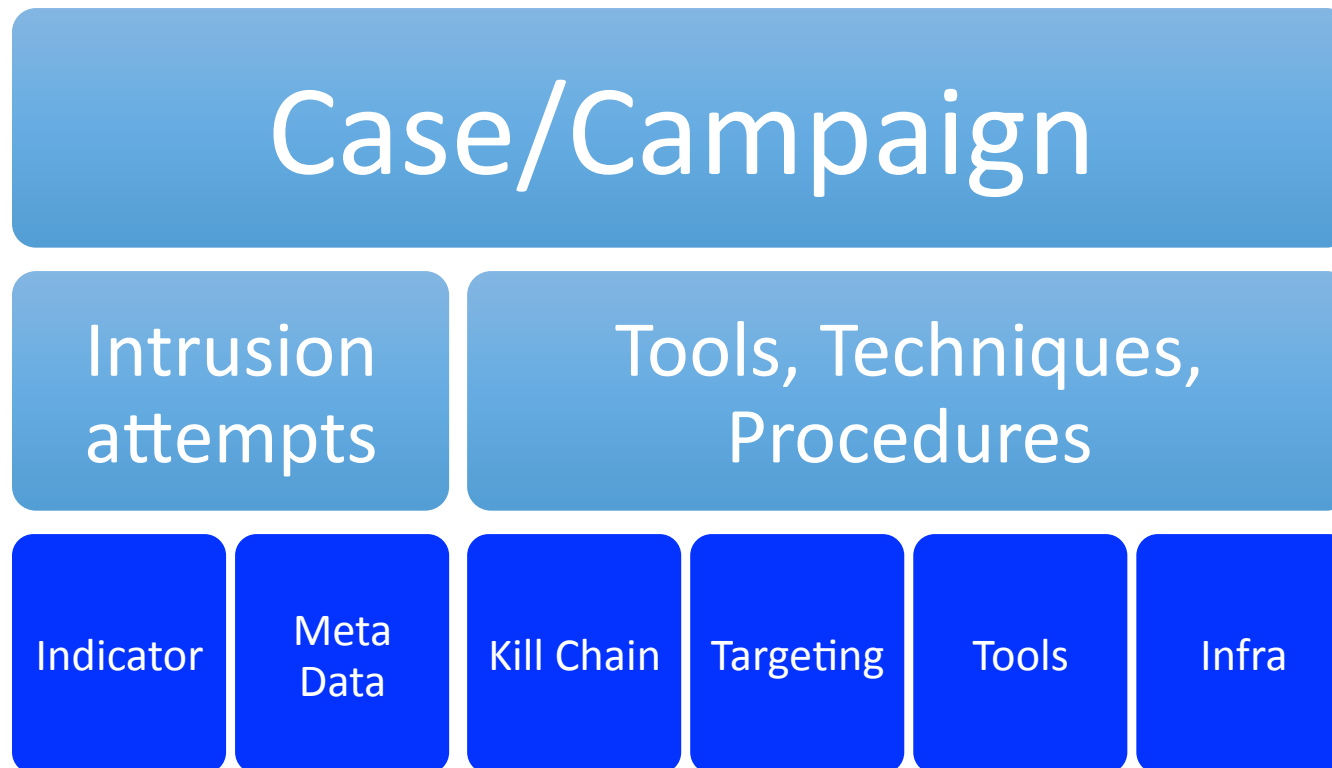
## Indicators of compromise (IoC)

- IP address / domain
- E-mail address, x-mailer
- URL
- User Agent
- File Hash
- Mutex
- Registry key
- Memory entity

## Why use them

- Actionable intelligence – act faster
- Kill chain – stop before goal
- Forces adversary to change behavior – divert.
- Sharing builds trust relationships.
- Core in Intelligence Driven Defense

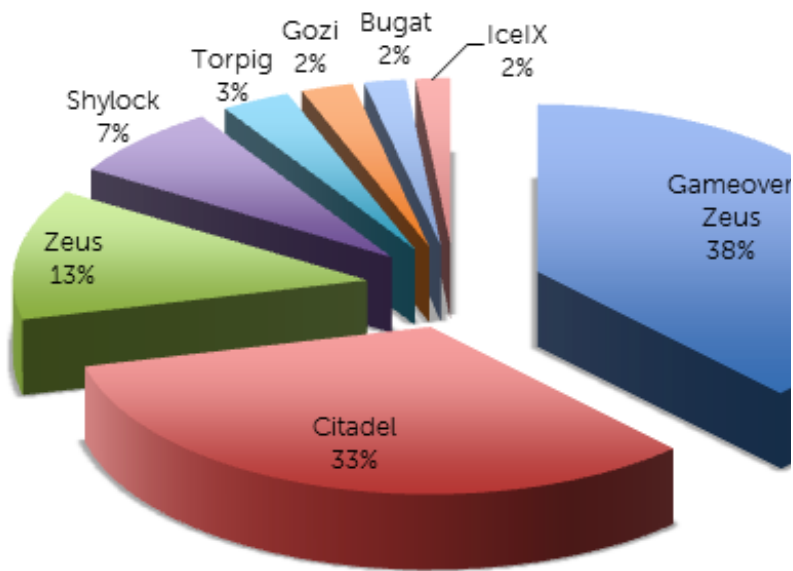
## Elements of Investigators' collaboration



## **5. Botnets & advanced attacks**



## Botnet business - stars



FEATURE	MITB	REDIRECT	BACK CONNECT	SCREENSHOTS	VIDEO CAPTURE	PROXY	CERTIFICATE STEALER
Zeus	Y	Y	Y	Y	Y	Y	Y
IceIX	Y	Y	Y	Y	Y	Y	Y
Citadel	Y	Y	Y	Y	Y	Y	Y
Gameover	Y	Y	Y	Y		Y	Y
Shylock	Y		Y		Y	Y	Y
Bugat	Y	Y	Y	Y		Y	Y
Gozi	Y		Y			Y	Y
Torpig	Y	Y	Y		Y	Y	Y

Table 2. Feature list of banking trojans.

# Fighting botnets

- **Bredolab (2010, NL) = CoinVault ransomware**
  - Jurisdictional powers? Dutch Police – National High Tech Crime Unit gave a go on back-hack, possible illegitimate use of art 125j
  - Helped by Kaspersky Lab – recovery possible.
- **GameOver Zeus (2014, US) ~ CryptoLocker, banking fraud**
  - Jurisdictional powers = 18 US Code §1345 /§2521 i.e. Injunctions against fraud/ Injunctions against illegal interception
  - Notification of the defendants via e-mail
  - Broad restraining order & preliminary injunction on the likelihood of damage
  - MLATs with the UK and Luxembourg, coordinated seizure of servers (CA, FR, DE, BX, NL, UA, UK)
  - **Temporary disruption** - security researchers exploited design flaws in the Gameover Zeus peer-to-peer (P2P) network, disrupting the criminal infrastructure by manipulating the peer list and redirecting traffic to nodes under their control.
- **Bugat/Cridex/Dridex (2015, US) ~ banking fraud**
  - Vector of infection – well crafted and obfuscated MS office documents as invoice via mail = spear phishing.
  - Large transactions: \$999k from City School District (PA,Us) to Kiev, \$2M from Penneco Oil to Krasnodar, +1M to Minsk.
  - Andrey Ghinkul aka Smilex arrested in Cyprus (Aug'15), charged in US, Pennsylvania on USC 18, §1030 (a)/(c) = fraud, and related activity in connection with computers
  - **Temporary disruption** - Palo Alto Networks reported Dridex was back operational by 2015-10-01
  - Collaboration with **international partners** and **private sector**.

Source: "How to dismantle a botnet the legal behind the scenes", Ku Leuven, BotConf EU

# Bugat/Dridex (2015)

- **Bugat/Dridex is a multifunctional malware package that has been in use since late 2009**
- **Used a keylogger** = **capture all typed text**, thus can access the victim's online bank account and execute unauthorized electronic funds transfers ("EFT"), such as Automated Clearing House ("ACH") payments or wire transfers, to accounts that they control.
- **Used a web inject / inject** = introduce (or inject) **malicious computer code into a victim's web browser** while the victim browses the Internet and "hijacks" the victim's Internet session. Different injects are used for different purposes.
- Some web injects are used to **display false online banking pages** into the victim's web browser to trick the victim into entering online banking information, which is then captured by the individual employing the web inject
- Eun as a **business** by a small number of conspirators primarily based in Russia and Moldova who have years of experience and well-developed trust relationships with one another.
- The members of the conspiracy have **specialized roles** within the Bugat/Dridex enterprise, including **expanding** the botnet by infecting new victims, **technical administration** of the botnet, and managing the network of **money mules** who launder stolen funds.
- Unlike most malware distributors, the Bugat/Dridex enterprise **maintains tight control** over the Bugat/Dridex malware code and does not appear to sell or distribute it to anyone outside the organization

Total losses associated with Bugat/Dridex exceed **\$10 million** in US, **\$25 million** WW.

Source: Special Agent Stevens Affidavit in Support of Temporary Restraining Order

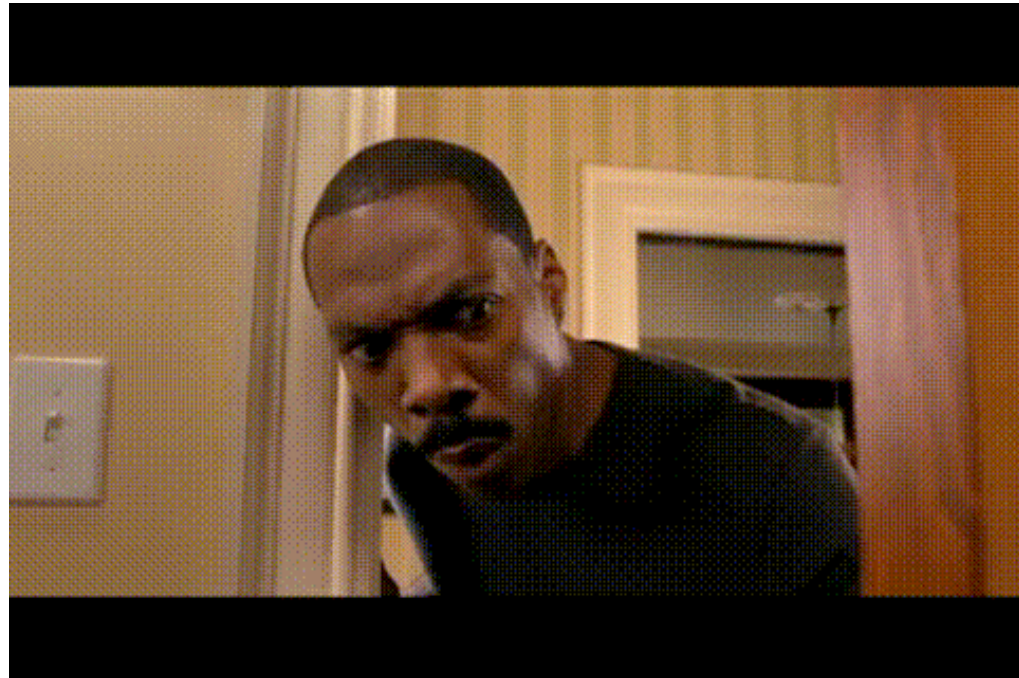
# Carbanak (2015)

- Losses up to **US\$1 billion** in ~2yrs from ~100 banks
- Joint collaboration of Interpol, Europol and Kaspersky Lab
- **Multinational** gang of cybercriminals from Russia, Ukraine and other parts of Europe, as well as from China.
- Gained entry into **employee's computer** through **spear phishing emails that appeared to be legitimate banking communications, with Microsoft Word 97 – 2003 (.doc) and Control Panel Applet (.CPL) files attached.**, infecting the victim with the Carbanak malware
- Exploited vulnerabilities in Microsoft Office 2003, 2007 and 2010 (CVE-2012-0158 and CVE-2013-3906) and Microsoft Word (CVE-2014- 1761).
- Cashing: A) Transfer to accounts under control B) **Penetrated the accounting systems** & inflated account balances before pocketing the funds.
  - For example: if an account has 1,000 dollars, the criminals change its value so it has 10,000 dollars and then transfer 9,000 to themselves. The account holder doesn't suspect a problem because the original 1,000 dollars are still there.
- Also seized control of banks' ATMs and ordered to dispense cash.

“This is likely the most sophisticated attack the world has seen to date in terms of the tactics and methods that cybercriminals have used to remain covert,” (Kaspersky Lab)

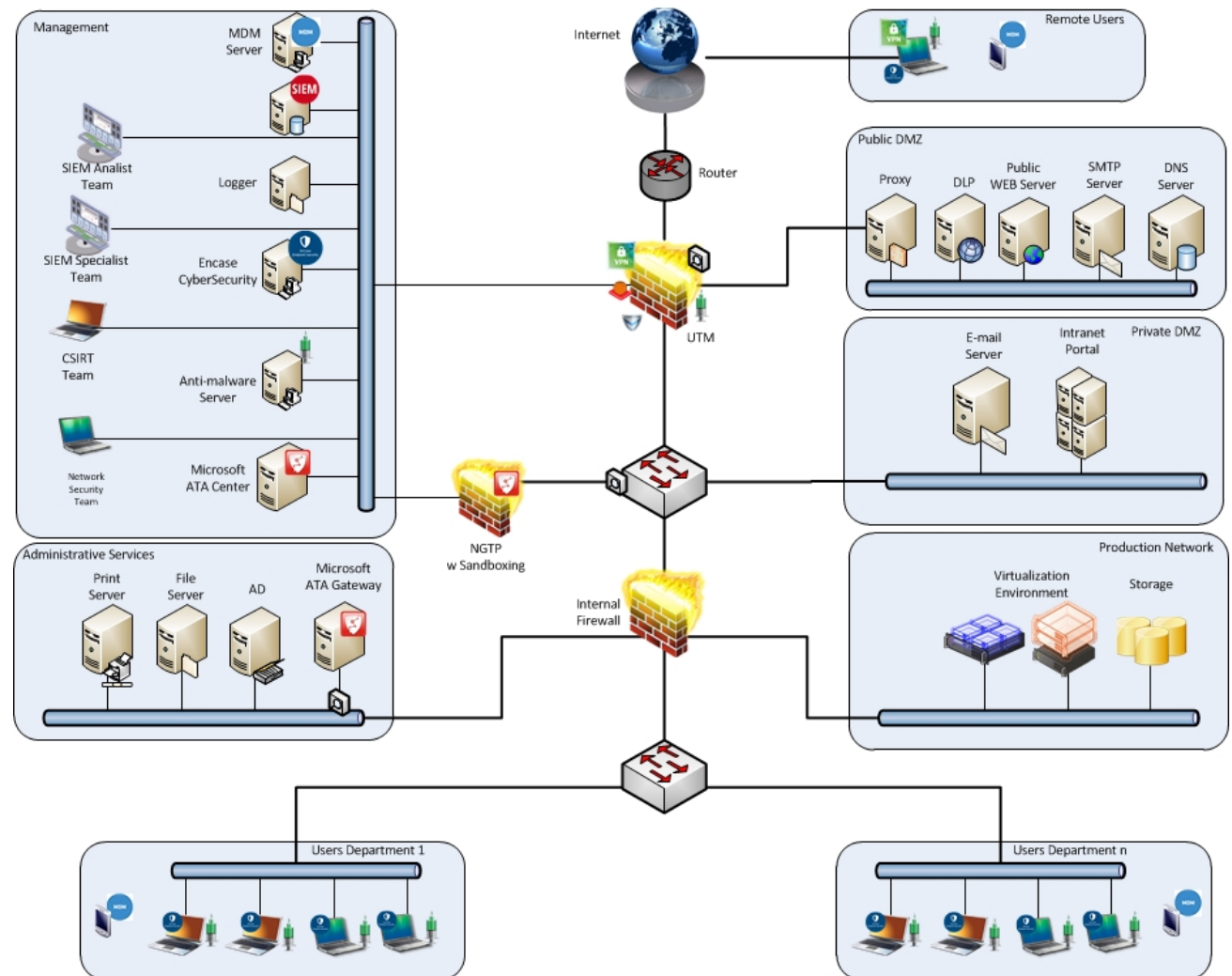
# Current Security State

When Pentesting....



# Modern Security Architecture

- ✓ **Intelligence driven defense**
- ✓ Threat vector analysis
- ✓ Data exfiltration analysis
- ✓ Detection dominant design
- ✓ **Zero trust model**
- ✓ Intrusion kill chain
- ✓ **Attack hunting**
- ✓ Visibility analysis
- ✓ Data visualization
- ✓ **Lateral movement analysis**
- ✓ Data ingress/egress mapping
- ✓ Internal segmentation
- ✓ Network security monitoring
- ✓ **Continuous monitoring**



# The Basics - Service Providers / Authorities

The screenshot shows the Censys web application interface. The browser address bar displays the URL: `https://censys.io/certificates?q=parsed.issuer.country%3A+PT+AND+parsed.subject.common_name...`. The search bar contains the query: `parsed.issuer.country: PT AND parsed.subject.common_name: gov\pt AND parsed.signature.valid: false`. The search results are displayed in a list format, showing details for three certificates. A red box highlights the summary statistics: **Page: 1/35 Results: 856 Time: 1660ms**.

**Search Results:**

- Certificate 1:**  
C=PT, ST=Lisboa, L=Lisboa, O=FinanÃ§as, CN=cloud.igf.gov.pt  
C=PT, O=SCEE, OU=ECEstado, CN=ec273a0650b881ecd0c14332  
Untrusted cloud.igf.gov.pt  
parsed.subject\_dn: \$as, CN=c1  
parsed.subject.country: PT
- Certificate 2:**  
C=PT, O=MULTICERT-CA, OU=Web Server, CN=testes.iap  
C=pt, O=MULTICERT-CA, CN=M  
89280e3a0120ba6dff684f8bd3e5bd8d4ccc9290e64213bfeaa0e4cc51d0bfd  
Untrusted testes.iap.gov.pt  
parsed.subject\_dn: Server, CN=testes.iap.gov.pt  
parsed.subject.country: PT
- Certificate 3:**  
C=PT, ST=Lisboa, L=Lisboa, O=Autoridade Tributaria e Aduaneira, CN=\*.at.gov.pt  
C=PT, O=SCEE, OU=ECEstado, CN=ECCE  
5b88593a8ca1a6ff9ca39bb2e7bf5b06867c1b7050d93acc85fa3dfd81b074c1  
Untrusted \*.at.gov.pt  
parsed.subject\_dn: Aduaneira, CN=\*.at.gov.pt  
parsed.subject.country: PT

Demo



# The Basics - Service Providers / Authorities

country:PT - Shodan Search

https://www.shodan.io/search?query=country%3APT

Lisbon	70,882
Porto	24,751
Braga	10,336
Maia	10,032
Vila Nova De Gaia	9,070

### TOP SERVICES

SIP	534,524
Modem Web Interface	67,432
HTTP	58,926
HTTPS	47,704
DNS	20,855

### TOP ORGANIZATIONS

PT Comunicacoes	628,520
Nos Comunicacoes S.A.	56,894
ZON Tv Cabo	38,109
Vodafone Portugal	36,550
NFSi Telecom, Lda.	28,785

### TOP OPERATING SYSTEMS

Linux 2.6.x	6,041
Linux 3.x	3,570
Windows 7 or 8	1,415
Windows XP	448
Linux 2.4.x	74

### TOP PRODUCTS

Apache httpd	34,822
OpenSSH	12,113
Exim smtpd	11,960
Microsoft IIS httpd	11,649
MySQL	6,329

**82.154.45.140**  
bl5-45-140.dsl.telepac.pt  
PT Comunicacoes  
Added on 2015-10-29 10:23:09 GMT  
Portugal, Sintra  
[Details](#)

SIP/2.0 500 Server Internal Error  
From: <sip:nm@nm>;tag=root  
To: <sip:nm2@nm2>;tag=1515bc8-529a2d8c-13c4-50029-7169eb-73015bb6-7169e  
Call-ID: 50000  
CSeq: 42 OPTIONS  
Via: SIP/2.0/UDP nm;received=xxx.xxx.xxx.xxx;rport=26810;branch=foo  
Supported: replaces,100rel  
Allow: INVITE, ACK, BYE, REFE...

**Vigor Login Page**  
85.246.110.55  
bl13-110-55.dsl.telepac.pt  
PT Comunicacoes  
Added on 2015-10-29 10:23:09 GMT  
Portugal, Sintra  
[Details](#)

**SSL Certificate**  
Issued By:  
|- Common Name: **Vigor Router**  
|- Organization: **DrayTek Corp.**  
Issued To:  
|- Common Name: **Vigor Router**  
|- Organization: **DrayTek Corp.**  
**Supported SSL Versions**  
SSLv3

HTTP/1.0 200 OK  
Pragma: no-cache  
Content-type: text/html  
Expires: 0  
Content-length: 8814  
Connection: close

**193.126.120.156**  
NOVIS Telecom, S.A.  
Added on 2015-10-29 10:22:43 GMT  
Portugal  
[Details](#)

HTTP/1.1 401 Unauthorized  
Connection: Keep-Alive  
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e361943980d2b85bfd85eedae9c1c559",qop="auth",algorithm=SHA-256  
Content-Length: 0

Lisbon	70,882
Porto	24,751
Braga	10,336
Maia	10,032
Vila Nova De Gaia	9,070

### TOP SERVICES

SIP	534,524
Modem Web Interface	67,432
HTTP	58,926
HTTPS	47,704
DNS	20,855

### TOP ORGANIZATIONS

PT Comunicacoes	628,520
Nos Comunicacoes S.A.	56,894
ZON Tv Cabo	38,109
Vodafone Portugal	36,550
NFSi Telecom, Lda.	28,785

### TOP OPERATING SYSTEMS

Linux 2.6.x	6,041
Linux 3.x	3,570
Windows 7 or 8	1,415
Windows XP	448
Linux 2.4.x	74

### TOP PRODUCTS

Apache httpd	34,822
OpenSSH	12,113
Exim smtpd	11,960
Microsoft IIS httpd	11,649
MySQL	6,329



**"Trust but Verify."**

- Ronald Wilson Reagan



Actually a Russian proverb,  
"Доверяй но проверяй",  
Suzanne Massie, a writer on  
Russia, taught Pr. Ronald Reagan

"The old mantra of "trust but verify" just isn't working.  
"Never trust and verify" is how we must apply security in  
this era of sophisticated breaches.

Quote: <https://networkinferno.net/implementing-a-zero-trust-security-architecture>

## **6. Recommendations & Future**

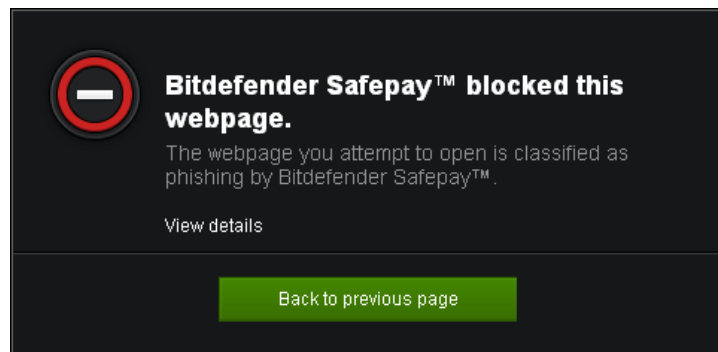
## **Basic Security – Safeguard online activity**

❖ **Install a mature AV solution** – AVG, Bitdefender, ESET, F-Secure, Sophos (all from EU), Kaspersky Lab, Symantec, TrendMicro.

❖ **Secure online banking and e-shopping**

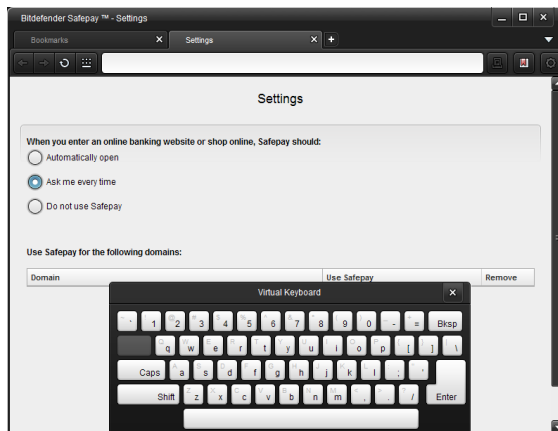
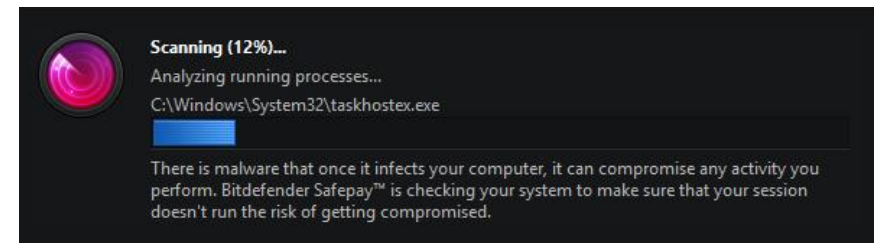
- ❖ Block tampering attempts
- ❖ Protect against keylogging

## Basic Security – e.g. Bitdefender SafePay



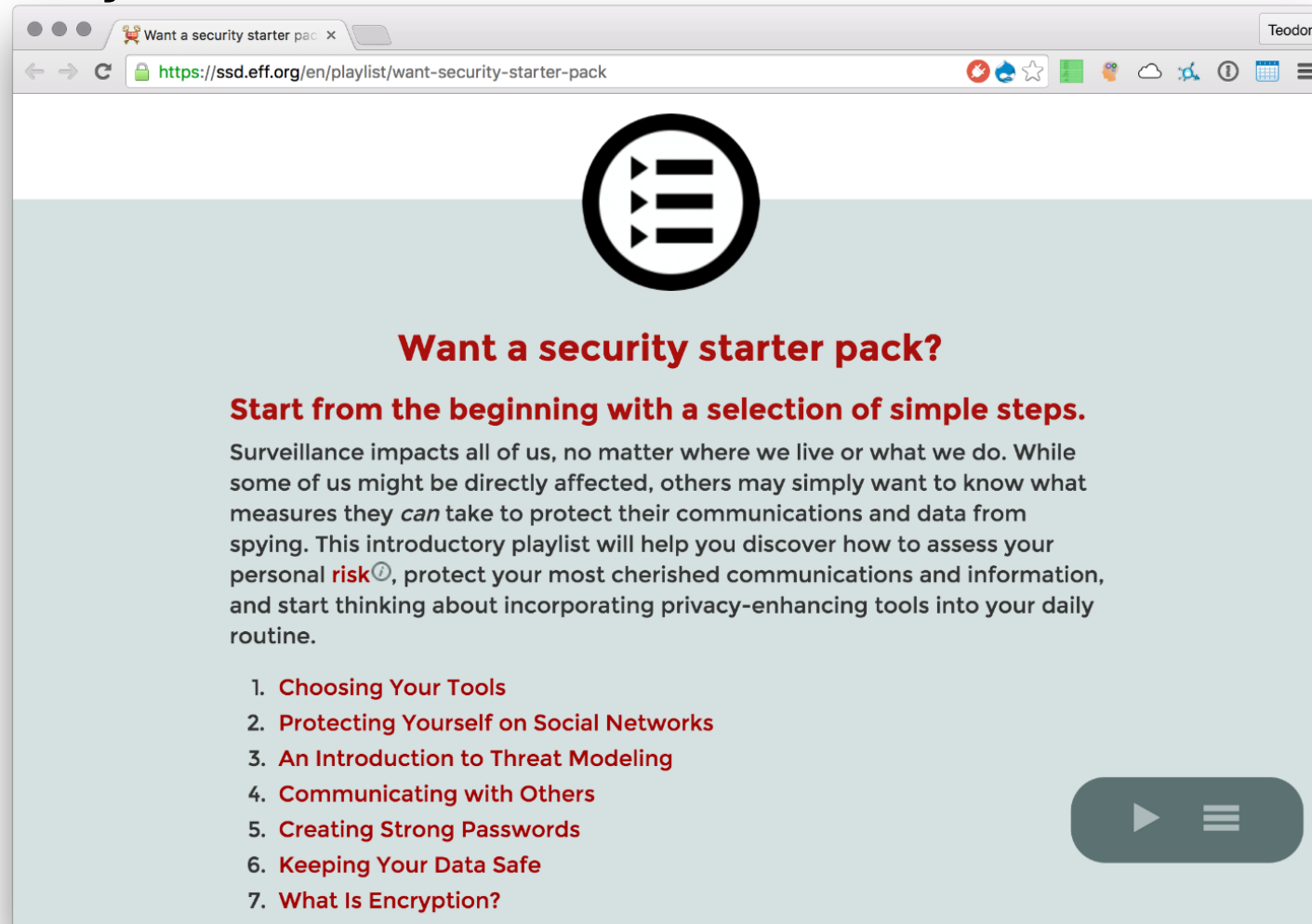
Stop fraud, phishing, and viruses in their tracks.  
Secures online banking and e-shopping.

Safepay ensures you there is no risk on your PC.  
Security assessment for your PC.



Features a secure hacker-proof browser.  
Blocks tampering attempts.

# Basic Security – Guides & Best Practices



The screenshot shows a web browser window with the address bar displaying <https://ssd.eff.org/en/playlist/want-security-starter-pack>. The page features a large circular icon with three horizontal bars and a play button. Below the icon, the text reads: "Want a security starter pack? Start from the beginning with a selection of simple steps." This is followed by a paragraph explaining the purpose of the playlist. At the bottom, there is a list of seven topics and a play button icon.

**Want a security starter pack?**

**Start from the beginning with a selection of simple steps.**

Surveillance impacts all of us, no matter where we live or what we do. While some of us might be directly affected, others may simply want to know what measures they *can* take to protect their communications and data from spying. This introductory playlist will help you discover how to assess your personal **risk**, protect your most cherished communications and information, and start thinking about incorporating privacy-enhancing tools into your daily routine.

1. **Choosing Your Tools**
2. **Protecting Yourself on Social Networks**
3. **An Introduction to Threat Modeling**
4. **Communicating with Others**
5. **Creating Strong Passwords**
6. **Keeping Your Data Safe**
7. **What Is Encryption?**

## **Education & Training**

- 1. Children** - Save the Children Org: Keeping Children Safe Online
- 2. Users** – basic “cyber hygiene” (refrain the click, updates, AV)
- 3. Employees** – AUP (acceptable use policy), SecPol (security policy), **awareness training**.
- 4. Consumers/Customers** – build trust in electronic commerce
- 5. Security implementors** – get self-updated with industry security practices.
- 6. Executives** – educate about business risk and impact
- 7. Law enforcement** – allocate proper resources



## Prepare for worse

1. **Crimeware ecosystem** is on the rise and current intl collaboration is not working/keeping pace (MLATs/rogatories -> 1-3 yrs cases)
2. **Digital crime** will have to deal with billions of information systems. Pressure is on the legal system.
3. **Civil code** is/will be challenged with **online** identities, properties and projectable crime on breach of private rights.
4. **Competencies** – there is a **scarcity of specialists** – use private sector collaboration.



Questions?  
Thoughts?

Teodor.Cimpoesu@certsign.ro  
+40722.754.319, @cteodor

UTI-CERT Team  
contacts: [CERT@uti.ro](mailto:CERT@uti.ro)