

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/309193488>

Criminal Use of Information Hiding (CUIng) Initiative

Presentation · October 2016

DOI: 10.13140/RG.2.2.25003.64808

CITATIONS

0

READS

49

1 author:



Jart Armin

CyberDefcon

5 PUBLICATIONS 0 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



All content following this page was uploaded by **Jart Armin** on 17 October 2016.

The user has requested enhancement of the downloaded file.

eCrime Symposium 2016
6th – 7th October, 2016 in Bratislava, Slovakia



Panel - Criminal Use of Information Hiding (CUIng) Initiative

Jart Armin – APWG EU, Moderator

Panelists

Edgardo Montes de Oca (Montimage, FR),

Piotr Kijewski (Shadowserver, PL),

Angelo Consoli (SUPSI - University of Applied Sciences and Arts of Southern Switzerland, CH),

Dr. Arturo Campos (CyberDefcon, SE)

STEGANOGRAPHY



to cybercriminals exploitation



Information hiding (IH): inspiration

- **Information hiding** is part of a wide spectrum of methods that are used to make secret data difficult to notice for the curious third party observers
- **Steganography** is one of the most well-known subfields of information hiding and aims to cloak secret data in a suitable carrier
- They have proved very handy and have been **utilized and mastered by humankind throughout the ages**
- Inspiration for such mechanisms is strongly related to phenomena observable in nature as they **have their roots in nature**




Follow the money?

Money laundering via Twitter ? –
The case of: *The Innocent five kittens posing in a garden*

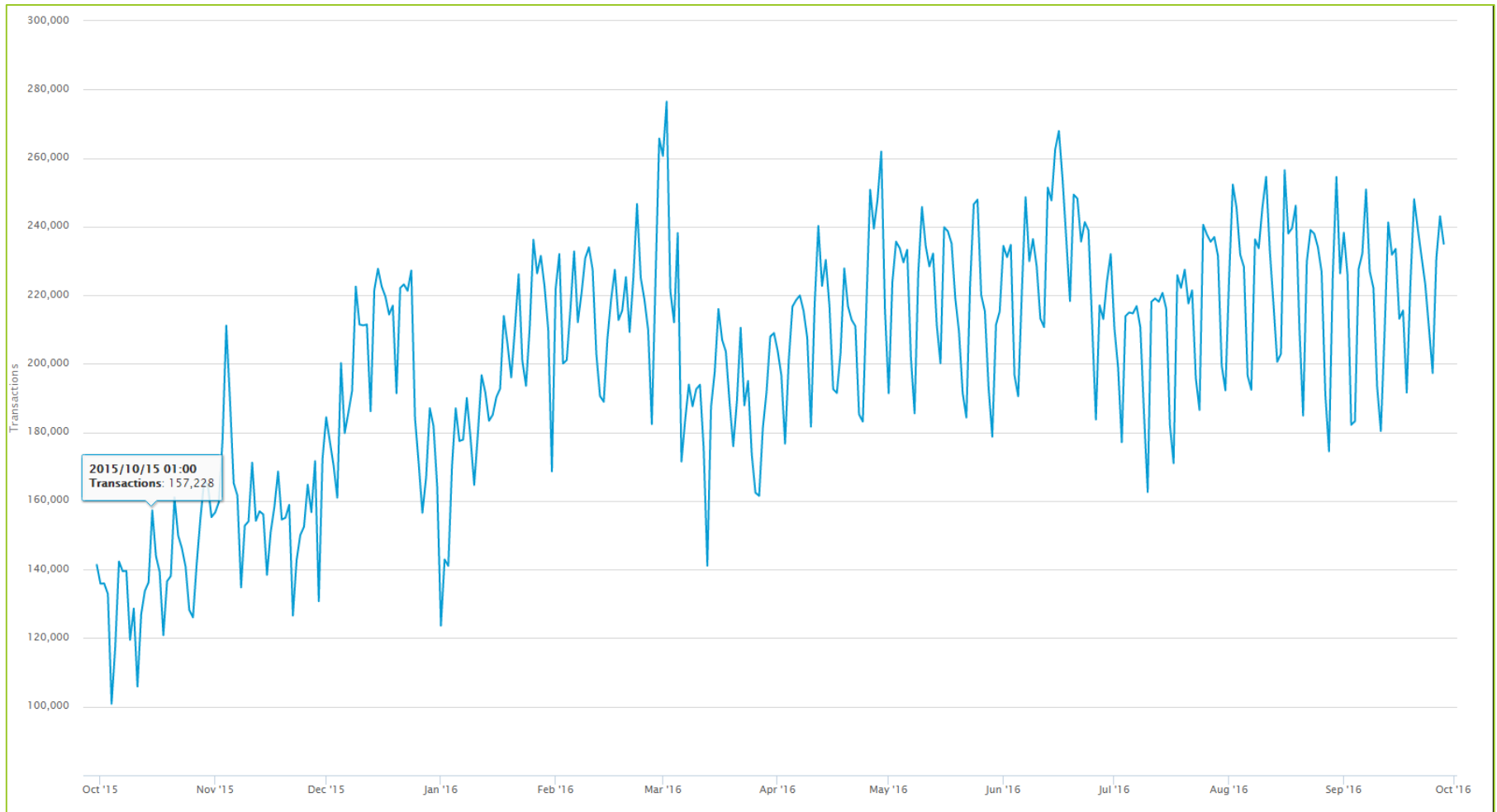


- First tweet 2015 contained a transaction worth \$12m USD via Twitter
- Second tweet in mid-November 2015 the transaction was worth more than \$100m USD.

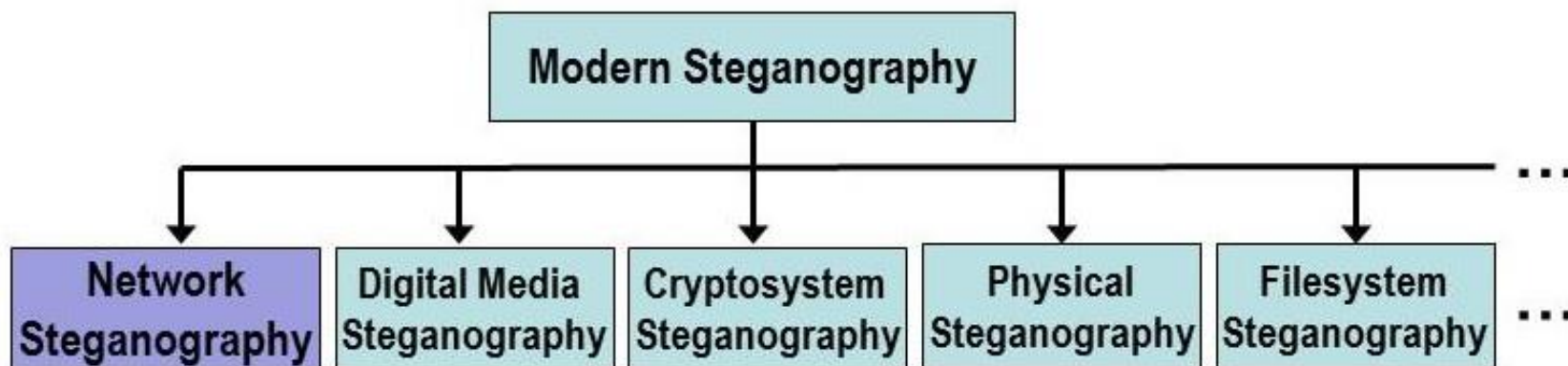


Summary		Transactions	
Address	1M8s2S5bgAzSSzVTeL7zruvMPLvzSkEAuv	No. Transactions	11 
Hash 160	dcdf2f9892bfa1cb086530354eab3ba078a2f090	Total Received	500,000.90367963 BTC 
Tools	Taint Analysis - Related Tags - Unspent Outputs	Final Balance	0 BTC 

Follow the money (2) – Bitcoin transactions via proxy (12 months)



Modern information hiding (IH)

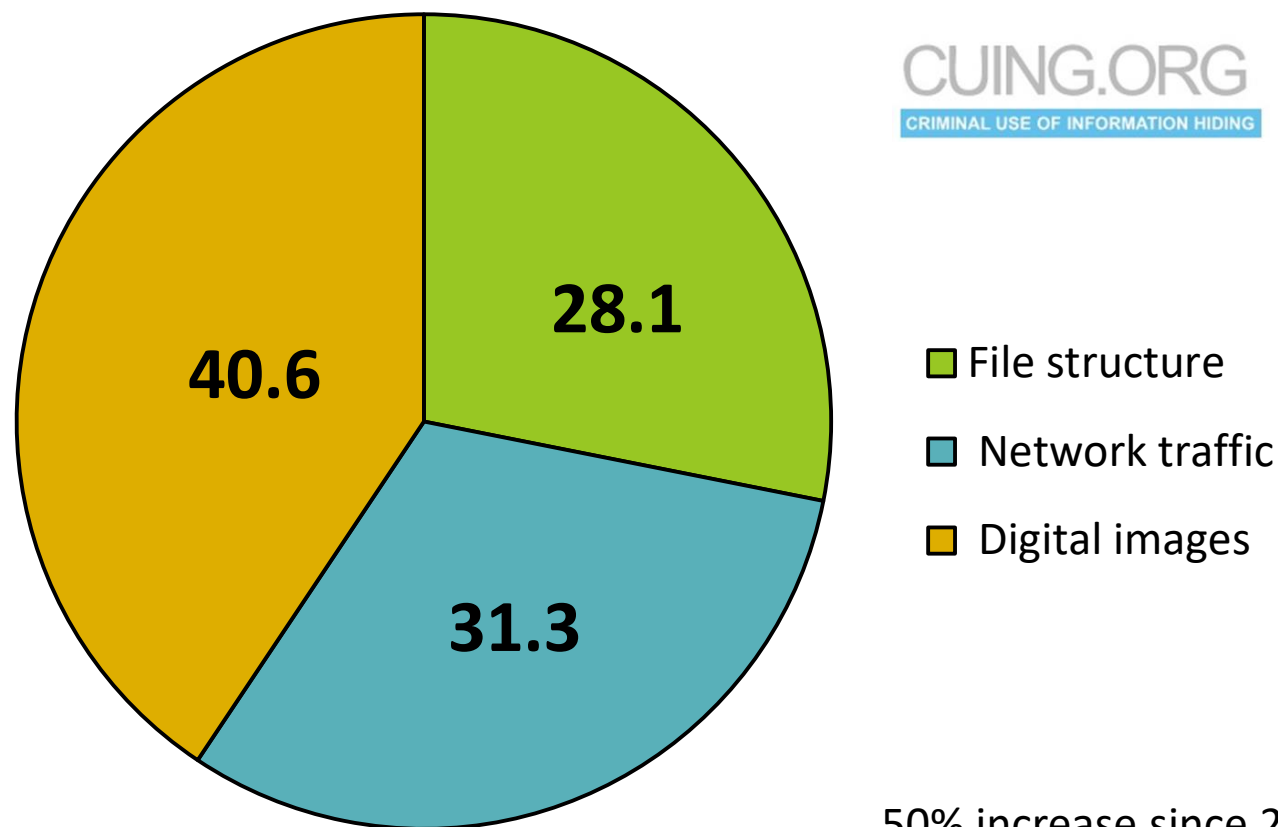


Many possible carriers exist – hard to monitor all of them!

Other types of information hiding are also possible:

- Traffic type obfuscation techniques
- Local covert channels
- Etc.

Distribution of information hiding-capable malware



50% increase since 2012 - Europol

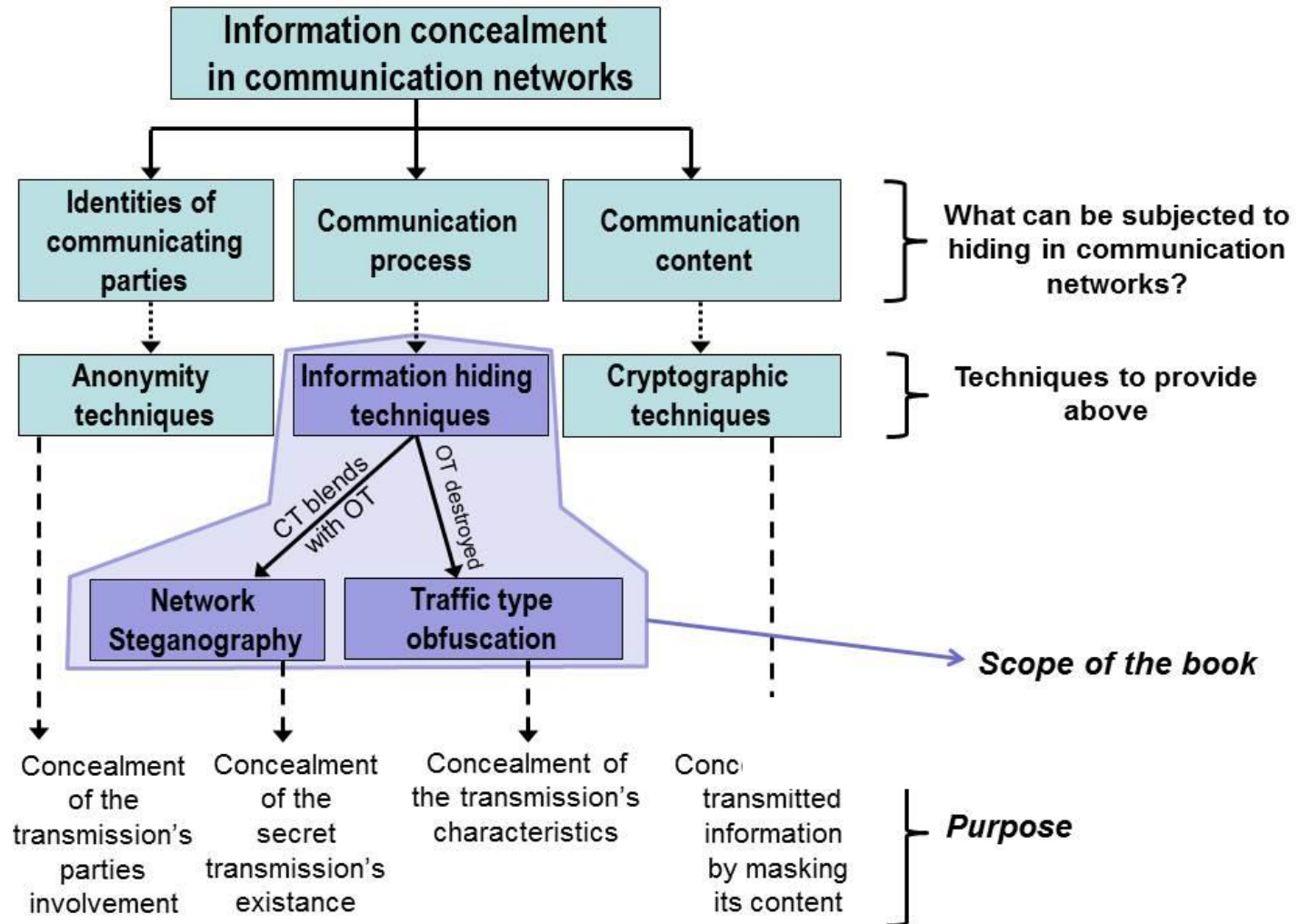
Group 1: malware that embeds secret data by **modifying a digital image file's structure**

Group 2: malware that embeds secret data by **using digital media steganography**

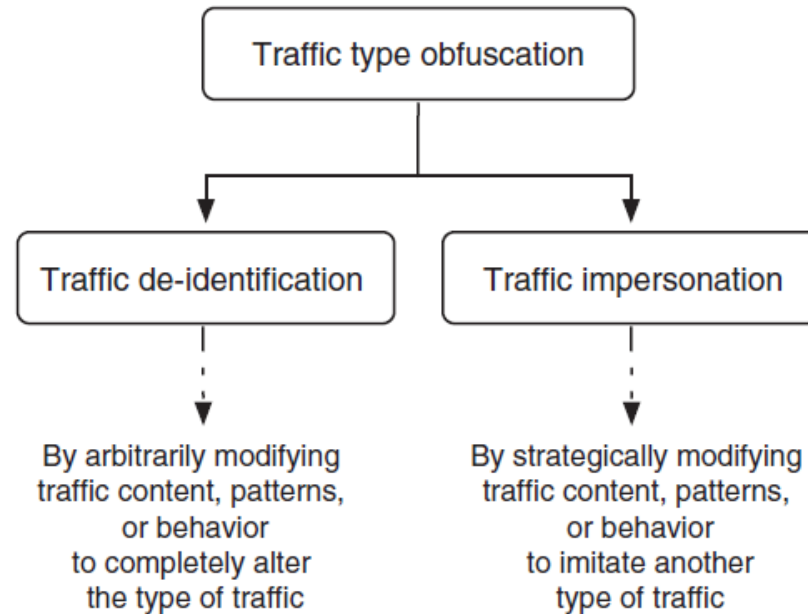
Group 3: malware that injects secret data **into network traffic**

Information concealment in networks

What can be subjected to hiding in communication networks?

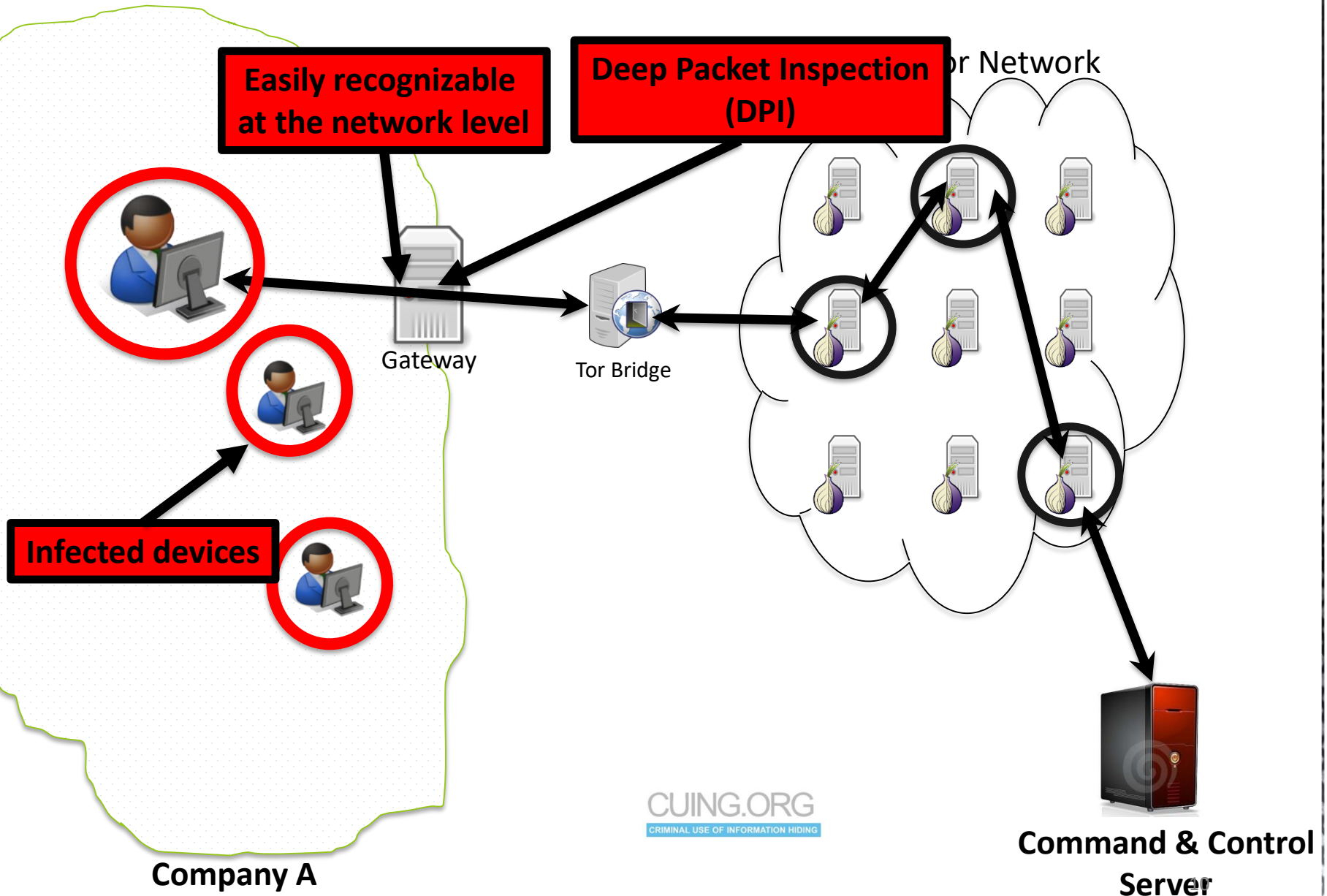


Traffic type obfuscation techniques

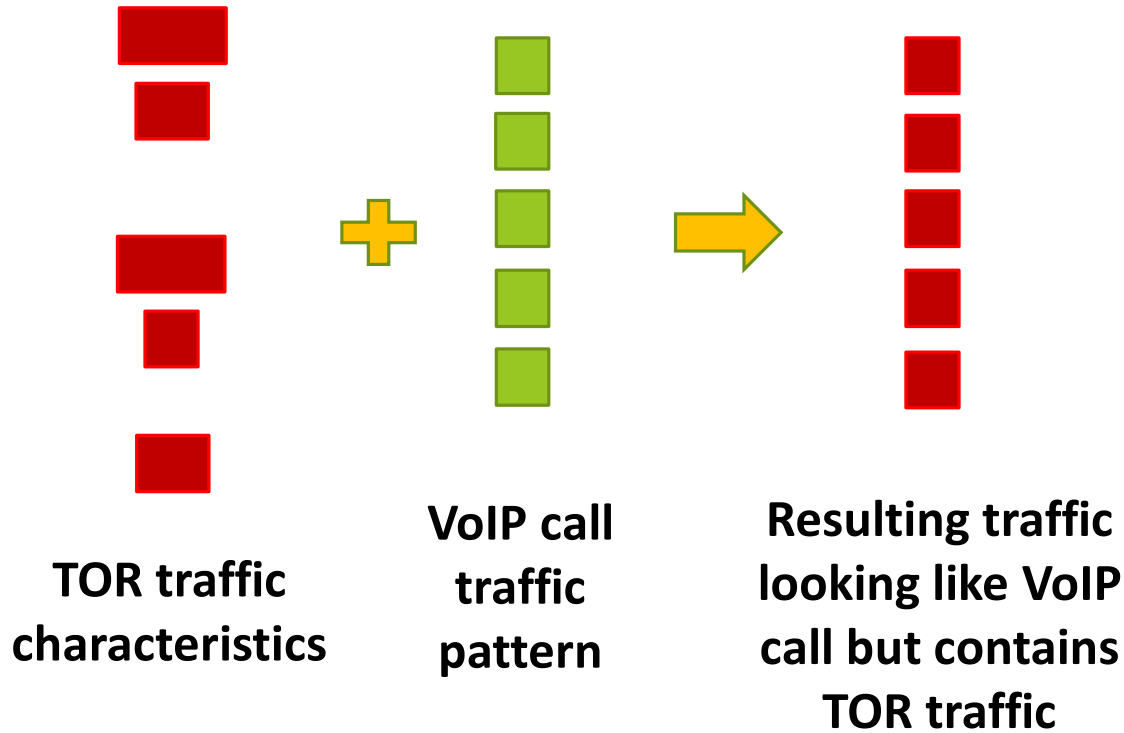


- **Traffic type obfuscation** hides the **nature of the network traffic flows** by obfuscating the underlying network protocol
- It modifies the **patterns and contents** of network traffic between two network entities so that a third entity **is not able to reliably identify the type of their communication** i.e. the network protocol

Characteristic malware traffic can be discovered

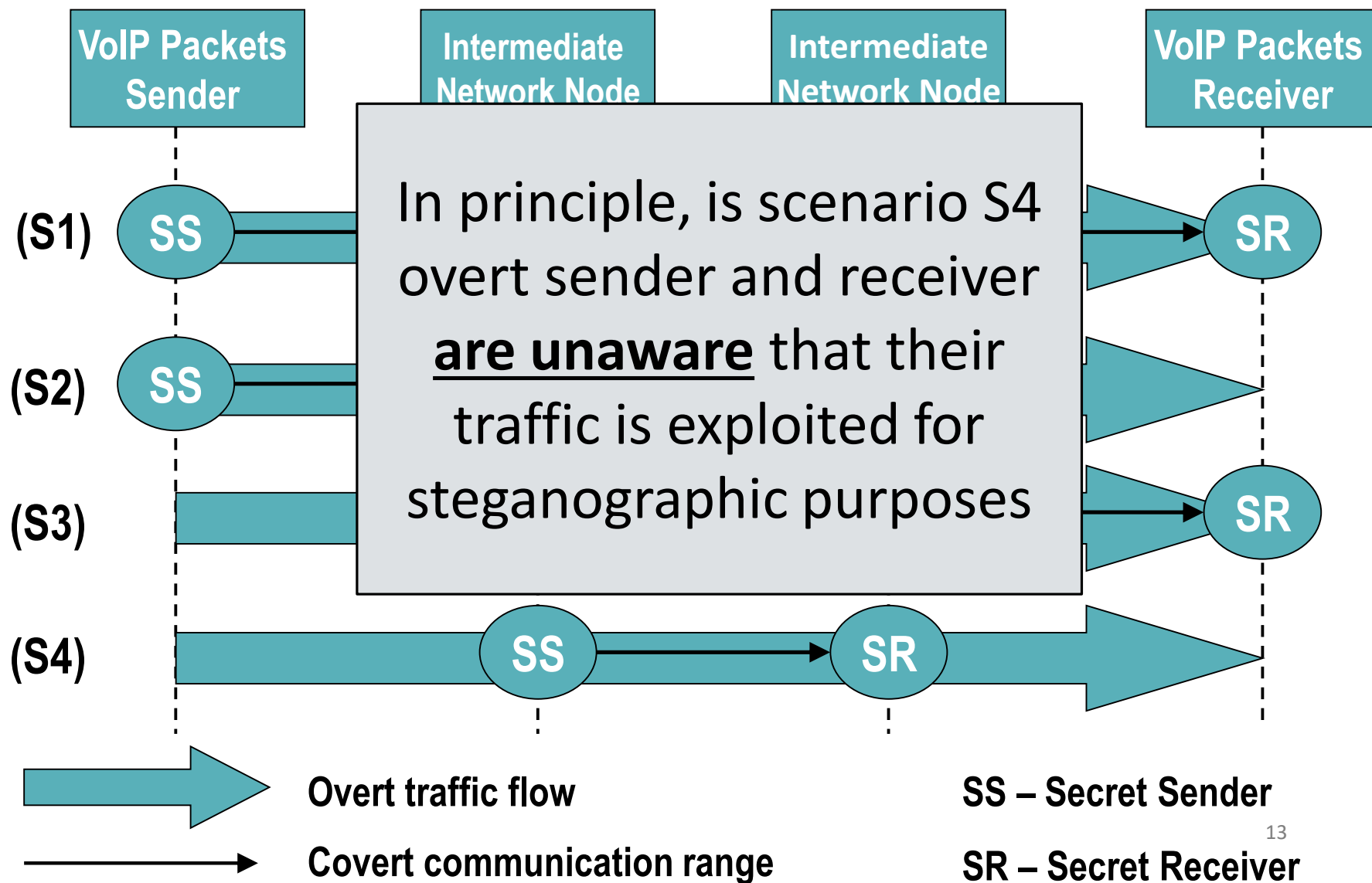


Traffic impersonation example



Network steganography

- **The newest trend in information hiding**
- Steganographic methods that utilizes as a hidden data carrier **network protocols** (PDUs and/or the way they are exchanged) **and/or the relationships between them**
- **Steganographic opportunities** in networks come from the **increasing complexity and redundancy of protocols/services**
- **To provide undetectability:**
 - Use of popular carriers
 - Use of anomalies that happen in the networks
 - Imitate behavior specific to certain types of traffic / protocols / services / users (mimicry)



Aim of network steganography

- Network steganography techniques **create covert (steganographic) channels** for hidden communication but such covert channels **do not exist in communication networks without steganography**
- The main aim of the network steganography **is to hide secret data in the normal transmissions** of users without significantly altering the carrier used
- The scope of network steganography is limited to all information hiding techniques that:
 - can be applied to the network traffic to hide the exchange of data by **creating covert communication channel(s)**
 - are **inseparably bound** to the transmission process (carrier)
 - do not significantly **alter** the carrier

Recent Example: SYNful Knock (data breaches)

- SYNful Knock is a type of persistent malware that allows an attacker to gain control of a device and compromise its integrity with a modified Cisco IOS Software image (via FireEye).
- SYNful Knock is a router implant different modules that are enabled via the HTTP protocol (not HTTPS) and controlled by crafted TCP packets sent to the device.
- Even the presence of the backdoor was difficult to detect as it uses non-standard packets as a form of pseudo-authentication.
- It was implanted via poorly configured routers (weak / default credentials).
- Attackers gain full control of the router and the traffic passing through it.
- A total of 199 unique IP Addresses have been identified worldwide as affected [via Shadowserver]
- No vulnerabilities appear to have been used in the spread of this implant.

Information hiding in the “DDOS scene”

ST Common architecture

- Front-end, public face (portal): bratistresser.com
Bullet proof front-end hosting: Cloudflare?
- Means to get paid: from paypal to bitcoins
- Set of servers able to spoof traffic: BlazingIO, Ecatel/Quasi/Novagara, Verdina...
- “Add-ons” infrastructure: Ampl. Scanners, Open Proxies, Compromised servers/stations, IoT gadgets

IoT botnets (1)

- 8th September 2016 VDOS take down
- Recorded > 600 Gbps at Akamai/Prolexic, 1 Tbps at OVH
- 24th-26th September 2016. Multiple attack vectors L3-4, L7 and GRE
- Malware was first spotted in May 2016. DdoS.87.
- GayFgt, Lizkebab, Torlus or BashLite, Bash0day, Bashdoor.
- > 1 Million devices infected → rather in the 300K for Mirai
- 30th September source released



IoT botnets (2)

- Mirai Botnet has a few large building blocks
 - Scanner/Brute forcer
 - Server side:
 - Reporter (collects passwords)
 - Loader (push malware into device)
 - Command and control (control of attacks)



IoT botnets (3)

- Hiding communication channels
- Communication with command and control is done by same port that the heavy scanning service 23,2323.
- Communication protocols are advertised as ASCII but turned out to be binary protocols

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/x3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/h3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/got-a-new-hi3518-ip-camera-modules/
root/k1v123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd8ab4f733ff047356198c781d27d
root/k1v1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd8ab4f733ff047356198c781d27d
root/jvzbz	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd8ab4f733ff047356198c781d27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/4111
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/11111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00E86FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/k1vkb	Toshiba Network Camera	http://faq.surveillixdvr.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AiROS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Sample Miria hijacked IOT logins

- BGP hijacks used to inject spam
- Increase of routing hijacks related to Stress Testing Services / DDOS
- Nullrouting victim → Nullrouting attackers servers

Hiding
interception(1)

- Backconnect AS203959 hijacks hidden servers from VDOSS where spoofed traffic was generated. Hijack is < 1h
- More route hijacks in the last six months (brief and prepending ASPATH to hide the hijacker)

Hiding interception (2)

- Three lessons learned
 - Command control protocols inside DDOS or Scanning Activity
 - Hijacking traffic in the name of other ASNs
 - Daisy chaining (free) CDNs solutions.

How the hide?

STEGANOGRAPHY



to cybercriminals exploitation



- **Criminal Use of Information Hiding (CUIng) Initiative** is set up in cooperation with the Europol European Cybercrime Centre (EC3) – launch in **June 2016** and here @ **Bratislava**
- By **working jointly and combining experiences from experts** from academia, industry, law enforcement agencies, institutions etc. it may be possible to tackle the information hiding problem while it is still not so widely-deployed
- We are open for **new members** from academia, industry, LEAs and institutions. If you are interested please contact us using:
info@cuing.org

Website: cuing.org

The main objectives of CUIng

- **Raise Awareness:** inform about the threat that information hiding techniques can pose. Increase sensitivity to cybercriminals' information hiding potential exploitation e.g. in companies
- **Track Progress:** monitor sophistication and complexity of information hiding techniques found in the wild used by cybercriminals, terrorists, spies, etc.
- **Threat Intelligence:** bring together security professionals from institutions, academics and industry to distribute information and share experience from different angles
- **Work Jointly:** cooperate and benefit from joint potentials to develop effective countermeasures and integrate it on a global scale (or at least EU level)
- **Educate & Train:** make law enforcement agencies, companies, institutions, individuals etc. ready and fully prepared to react to potential cybercriminals' information hiding exploitation

Requirements/prerequisites for success

- **Propagate information** about the initiative widely among potentially interested stakeholders (security professionals, academics, law enforcements, companies, institutions etc.) to get their attention and to create a “critical mass”
- **Create coordinated joint platform** that is easily accessible and intuitive which will serve as a hub to transfer/share experience, information and knowledge and to document the progress of steganography exploitation for malicious purposes
- **Acquire funding** – various stakeholders interested in developing effective countermeasures e.g. security products vendors or financial institutions can be interested in funding grants to support initiative activities. This initiative can form also a consortium to propose a project e.g. for H2020 programme (EU)
- **Meetings** – organization of events (e.g. conferences) at which networking, brainstorming and direct transfer of the experience, information and knowledge would be possible
- **Training** – organization of trainings related to information hiding. This can be also treated as a potential source of funding. If a “critical mass” is formed then it will be possible to develop trainings directed to different types of stakeholders (e.g. financial institutions, LEAs, agencies, companies, forensic investigators, etc.)

Our current activities

- We are using [Europol Platform for Experts EC3 - SPACE](#) as our working & contact space
- We have started collecting relevant reports, publications and documents on criminal use of information hiding techniques
- We **gather & share** the following information:
 - **General information on information hiding:** provides general overview on the subject
 - **Scientific publications:** relevant scientific publications (mostly surveys) which present current state-of-the-art in information hiding in academia
 - **Steg-capable malware:** analyses of real-life malware that is utilizing information hiding techniques for its purposes. Reports are mostly delivered by security professionals mostly from anti-malware companies) and share specific details on the malicious software and its techniques

eCrime Symposium 2016
6th – 7th October, 2016 in Bratislava, Slovakia



Panel - Criminal Use of Information Hiding (CUIng) Initiative

Cuing.org

info@cuing.org

STEGANOGRAPHY



to cybercriminals exploitation



Benefits	Better understanding of IH-based threats	Benefit of having improved countermeasures	Benefits of understanding how IH can be improved	Awareness/Training
Academia	Better opportunity to support industry, law-enforcement agencies and public	Providing Industry/LEAs/Public new countermeasures; improved view on detectability/preventability of selected hiding methods	Achieving advances in IH in academia before they are found in the wild and are applied by cybercriminals fosters the “fast” development of countermeasures and enables predictions on future threats and risks as well as on application scenarios of IH.	Improve the awareness of future professionals / researchers by means of ad-hoc courses for students and PhDs.
Industry	Consulting for business purpose; better possibility to evaluate threats and risks	Protection of sensitive business data (data leakage protection, DLP); protection against IH-based malware; development of new anti-malware and DLP solutions (new market)	Bring improved countermeasures to the market as fast as possible	Enhance the security pipeline within the enterprise or the development pipeline of products by means of well-trained experts.
Law-enforcement	Consulting and informing the public and the industry reg. threats/risks	Protection of confidential information; Consulting and informing the public and the industry reg. countermeasures; protection against IH-based malware/foreign secret service's data exfiltration	Being able to prepare for future IH-based threats	Make all the personnel involved in court/trials more aware of IH-based threats.
Public	Better understanding of threats and risks	Profit from better protected industry and enhanced LEA capabilities; improved security of public information infrastructure	Support for the free expression of opinions in censored parts of the Internet (e.g. as journalists or political opposition)	Make the public opinion aware of such mechanisms, which can definitely account for a more wise perception of the modern Internet.