Special Prosecutors Office for
High-Tech Crime of Serbia

International conference on Judicial Cooperation in Cybercrime Matters

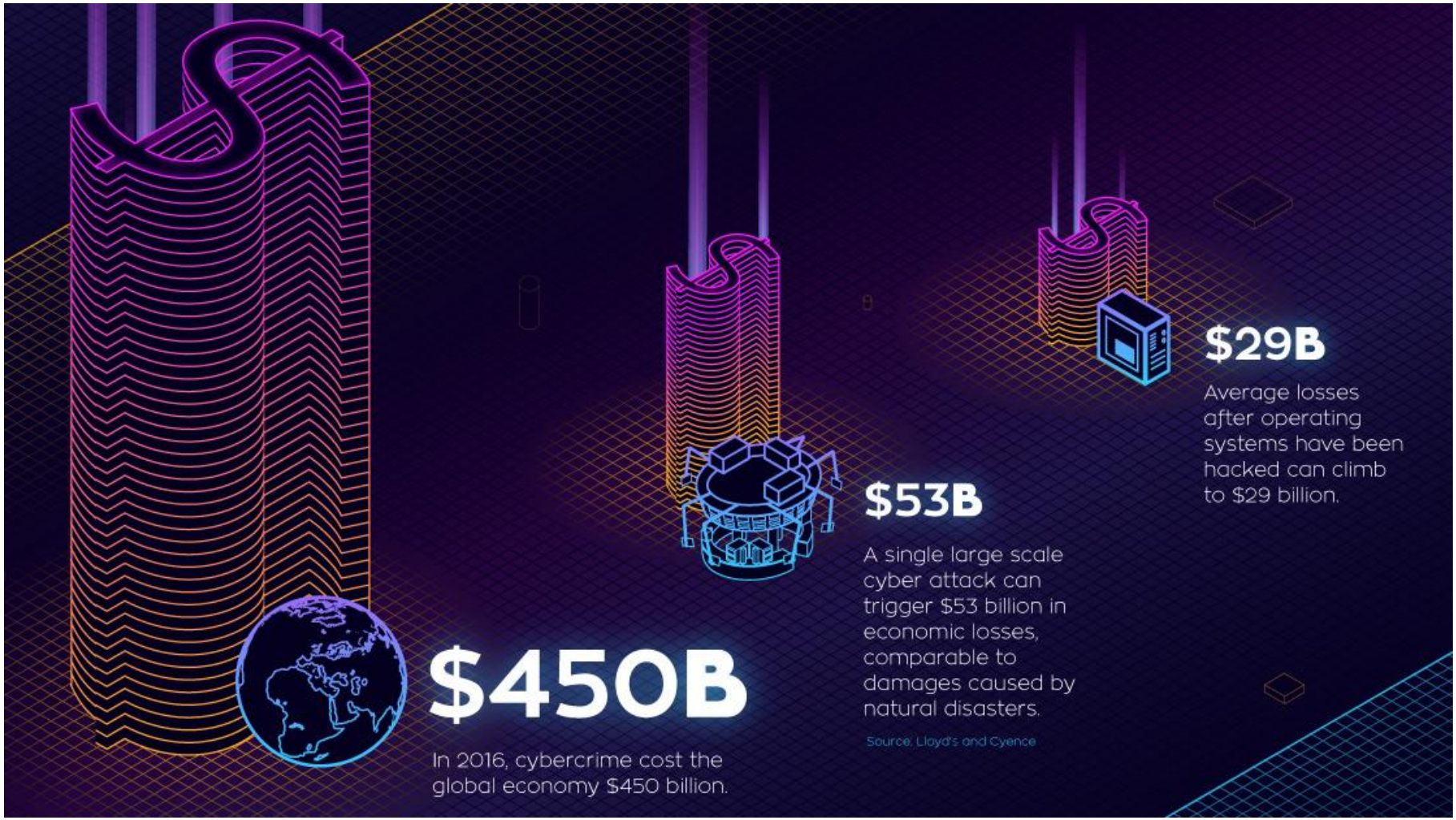
Cooperation with the Private Sector on cybercrime and electronic evidence and

Cases on cybercrime or electronic evidence

Experiences of the Special Prosecutors Office for High-Tech Crime of Serbia

7-8 March 2018, The Hague, Netherlands

Special Prosecutors Office for
High-Tech Crime of Serbia



Special Prosecutors Office for
High-Tech Crime of Serbia

November 2016

NHS hospitals

Hospital machines were frozen to demand ransom cash; at least four NHS (National Health Service) funds were attacked

November 2016

Yahoo

Data breach of 1 billion accounts

December 2015 & December 2016

Power grid in Ukraine

230,000 people were left without power for up to 6 hours; first time that a cyber-weapon was successfully used against a nation's power grid

November 2016

Tesco Bank

Around £2.5 million was stolen from around 9,000 customers in this hack, the largest on a UK bank

February 2016

Central bank of Bangladesh

USD 81 million were lost and a further USD 850 million in transactions were prevented from being processed

November 2016

Deutsche Telekom

900,000 (or about 4.5 percent of its 20 million fixed-line customers) suffered Internet outages over two days

February 2016

FBI and Homeland Security

Personal details of over 20,000 employees of the Federal Bureau of Investigation and 9,000 of the Department of Homeland Security were accessed

October 2016

Australian Red Cross

Personal data of 550,000 blood donators stolen

April 2016

Philippines' Commission on Elections (COMELEC)

Personal information of every single voter in the Philippines — approx. 55 million people — was compromised by Anonymous

October 2016

Domain name provider Dyn

A distributed denial of service attack resulted in the break-down of some of the biggest websites in the world including Twitter, The Guardian, Netflix, Reddit, Airbnb and CNN

April 2016

Democratic National Committee

Publication of 20,000 e-mails stolen from the Democratic National Committee

Special Prosecutors Office for
High-Tech Crime of Serbia

$6 TRILLION

EXPECTED CYBERCRIME DAMAGE BY 2021*

Comlinx | JUNIPER NETWORKS

Gartner Information Security Market Forecast 2017

Legal Framework - Serbia

- Criminal Procedure Code
- Electronic Communications Law
- Law on the liability of legal entities for criminal offences
- Law on Special Competencies for Efficient Protection of Intellectual Property Rights
- Regulation on conditions for providing Internet services and other data traffic and content of the approval
- Regulation on conditions for providing services of voice transmission on Internet and content of the approval
- **Law on Ratification of the Convention on Cybercrime**
- **Law on Ratification of Protocol to the Convention on Cybercrime**
- **Law on Ratification of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse**
- **Law on mutual legal assistance in criminal matters**
- **Law on Organization and Competence of Government Authorities in Combating High-Tech Crime**
- Criminal Code of the Republic of Serbia

Institutional Framework

- Ministry of Foreign and Internal Trade and Telecommunications
  (*Electronic Communications Law*)
- Republic Agency for Electronic Communications
  (*Electronic Communications Law*)
- Republic Broadcasting Agency
  (*Law on Broadcasting*)

- ***Law on Organization of Competence of Government Authorities in Combating High-Tech Crime***

  Special Prosecutor's Office for Combating Against High-Tech Crime

  Higher Court in Belgrade

  Ministry of Internal Affairs - Department for Fight Against High-Tech Crime

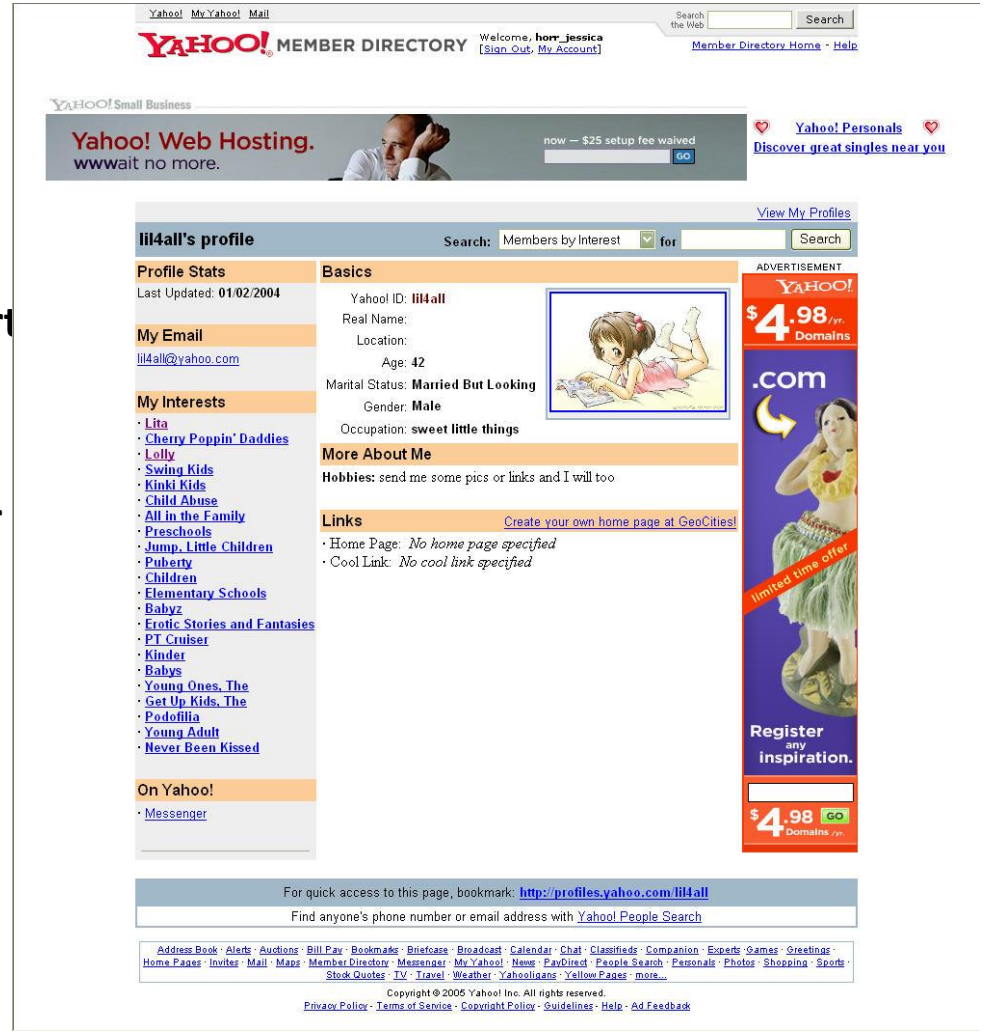
Legal framework and competencies

- **Criminal offences against security of computer data** defined by Criminal Code of the Republic of Serbia
- **Criminal offences against intellectual property** , property, commerce and industry and legal traffic which are committed by using , as object or tool of committing the offence, computers, computer networks, computer data, including their products in tangible or electronic form.
- and the number of items of copyrighted works is over 2000, or the amount of the actual damage is over 1.000.000,00 dinars (aprox. 10.000 EU or 14.000 USD).
- **Criminal acts against freedom and rights of man and citizen, gender freedoms, public order and peace, Constitutional system and security**, which can be considered by the way of commitment or used tools as cyber-crime.

	Known	Events	Unknown	
2006	19			19
2007	75	68	11	154
2008	110	60	14	184
2009	91	114	42	247
2010	116	443	13	572
2011	130	502	28	660
2012	114	609	65	788
2013	160	558	243	961
2014	294	770	352	1416
2015	198	1306	570	2074
2016	240	1237	580	2058
2017	213	1213	945	2371
TOTAL	**1760**	**6880**	**2863**	**11503**

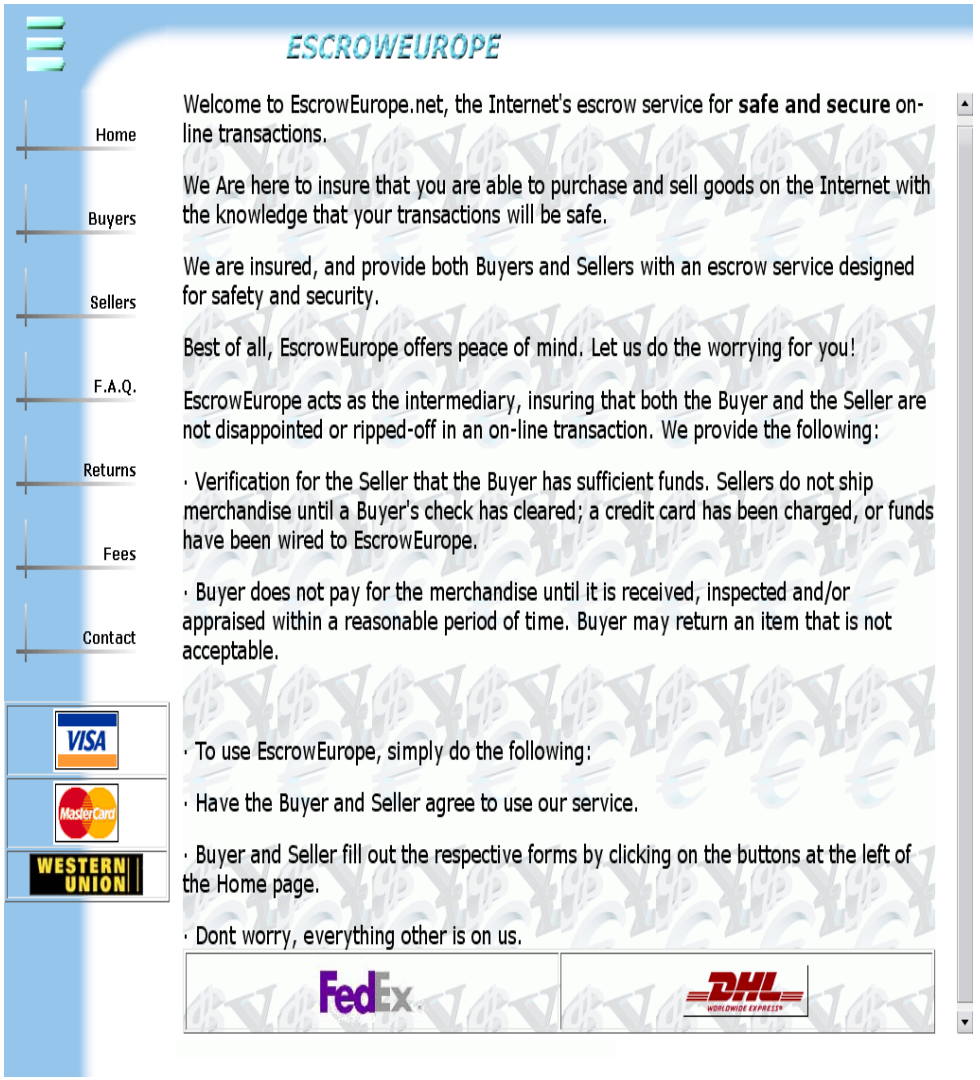
“Lone Wolf” Case

- **FBI – NCB Interpol Beograd: information about contact with possible perpetrator from Serbia.**
- **NCB Interpol Beograd – Prosecutor: report and delivery of data for competence an analysi**
- **After ISP evidence gathering, Court Order for search and seazure was obtained.**
- **Location search and seazure procedures.**
- **Special attention towards:**
- **- computer with accessories**
- **- data storages**



"StratoCaster" case.

- U.S. citizen – Belgrade – U.S. authorities and Interpol – Serbian Authorities.
- Internet fraud.
- Value of items: 100.000 USD.



Direct Query - Intranet - "Quick" Search

Page 1 of 1

UNITED STATES POSTAL SERVICE

Track/Confirm - Intranet Item Inquiry - International Outbound

Item: [illegible] Date/Time Mailed: 04/17/2003 14:43

Destination	City Code: BEG	City: BELGRADE	
	Country Code:	Country:	
	AMF Code: LAX	AMF: LOS ANGELES AMC	
Origin	ZIP Code: 93066-9554	City: SOMIS	State: CA

Dispatch#: 066	AMF Code: LAX	AMF: LOS ANGELES AMC
	Dispatch Date/Time: 04/18/2003 22:28	Bag#: 001
	Airline: JAT/YUGOSLAV AIRLINE	Flight: 263
	Transfer to: UNITED AIRLINES	Flight: 946

Class: Express Mail - PO to Addressee
Scheduled Delivery: 04/18/2003 23:59
Weight: lb: 38 oz: 9 Postage: $148.80

Special Services	Associated Labels	Amount
INSURED		$2.00

Delv Rqmt: Normal Po Box?: N

Under no circumstances should dispatch or flight information be released to anyone outside the United States Postal Service

Event	Date	Time	Location
INTERNATIONAL DISPATCH READY	04/18/2003	22:28	LOS ANGELES AMC, UNITED STATES
ENROUTE	04/17/2003	18:40	OXNARD CA 93030
ACCEPT OR PICKUP	04/17/2003	14:43	SOMIS CA 93066

Enter Request Type and Item Number:

Quick Search ◉ Extensive Search ○

Explanation of Quick and Extensive Searches

Item Number:

Submit

Inquire on multiple items.

Go to the Product Tracking System Home Page.

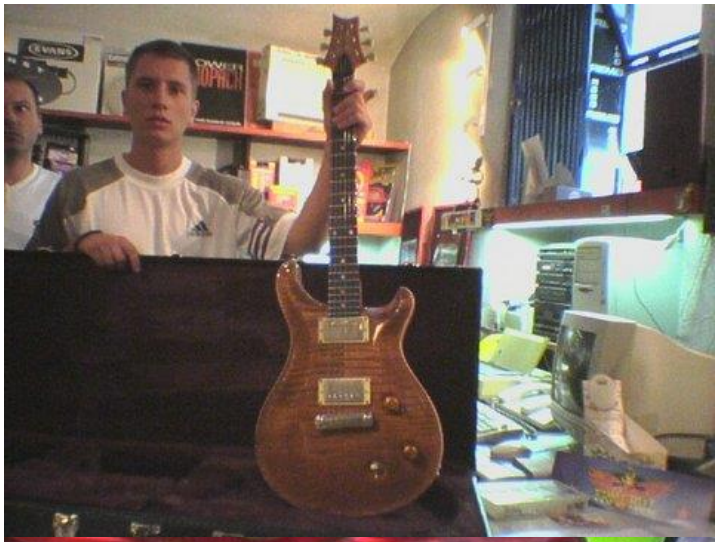
http://pts.usps.gov/netdata-cgi/db2www/cbd_242.d2w/OUTPUT 4/22/03

From: georgia
Category: Internet Scams
Date: 17 Jul 2003
Time: 16:59:10
Remote Name: 152.163.252.67

I also sold a vintage guitar over the internet using www.escroweurope.net. I was scammed out of a 1954 Gibson Les Paul original. Once the deal was completed I stopped receiving e-mails from the escrow site and have yet to receive a single penny. How do I report this and to whom do I need to talk with.

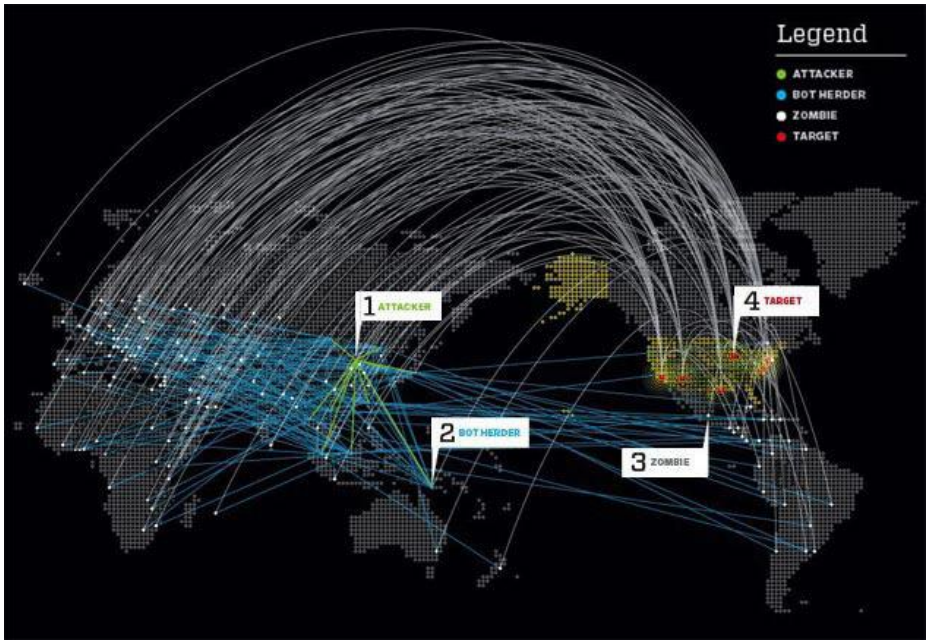
- From: roehrd@adelphia.net
  Category: Internet Scams
  Date: 14 Aug 2003
  Time: 12:55:51
  Remote Name: 68.71.14.74
- Georgia, I have been approached by Bojana Milosevic to buy your 54 goldtop. I stupidly sent $2550.00 to
- that fraud escroweuro
- pe.net. I have lost the money. I do have picturesd of your guitar in Bojana's hands if
- you would like them for evidence. I don't know who to contact that will do us any good. You have any ideas?

Special Prosecutors Office for
High-Tech Crime of Serbia



DDoS>RS backbone

- Aggrieved party – Public Postal Service of Serbia ISP
- Execution - Serbia
- Means of execution – sender, amplifier
- Exploit win service – 256 subdomen
- IRC

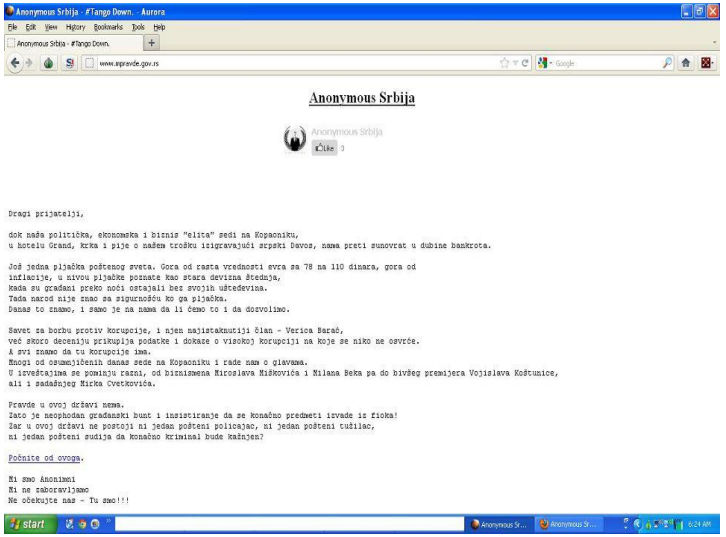


"StormFront Srbija"

- Perpetrators - Serbia
- Aggrieved parties – Serbia
- Tools of execution – Internet sight from USA
- International cooperation–freedom of speech

"Anonymous Serbia"

- Perpetrators: Serbia
- Criminar Acts of Computer Sabotage, Unlawful Access, Making of Computer Virus, Aiding to the execution of Computer Criminal Act.
- 5 groups of criminal acts, 28 separate executions over 1 year.
- Major ISP's compromised.
- 776.590 PHP shells seeded.



Bussines e-mail Compromise

- Targeting of specific victims or groups – Advanced Persistent Threath (**APT**)
- Abuse of “social engineering”
- Psychological manipulation for data disclosure and retrieval
- „**Black Energy**“ campaign
- Operation „**Windigo**“
- *Advanced Persistent Threat is most commonly used with “social engineering” techniques were by use of psychological manipulation victims are encouraged to take certain steps or disclose confidential data*

Advanced Persistent Threat (APT): The Uninvited Guest

How attackers remain in your network harvesting information and avoiding detection over time

1. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY

Once in, the attackers stay "low and slow" to avoid detection.

They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

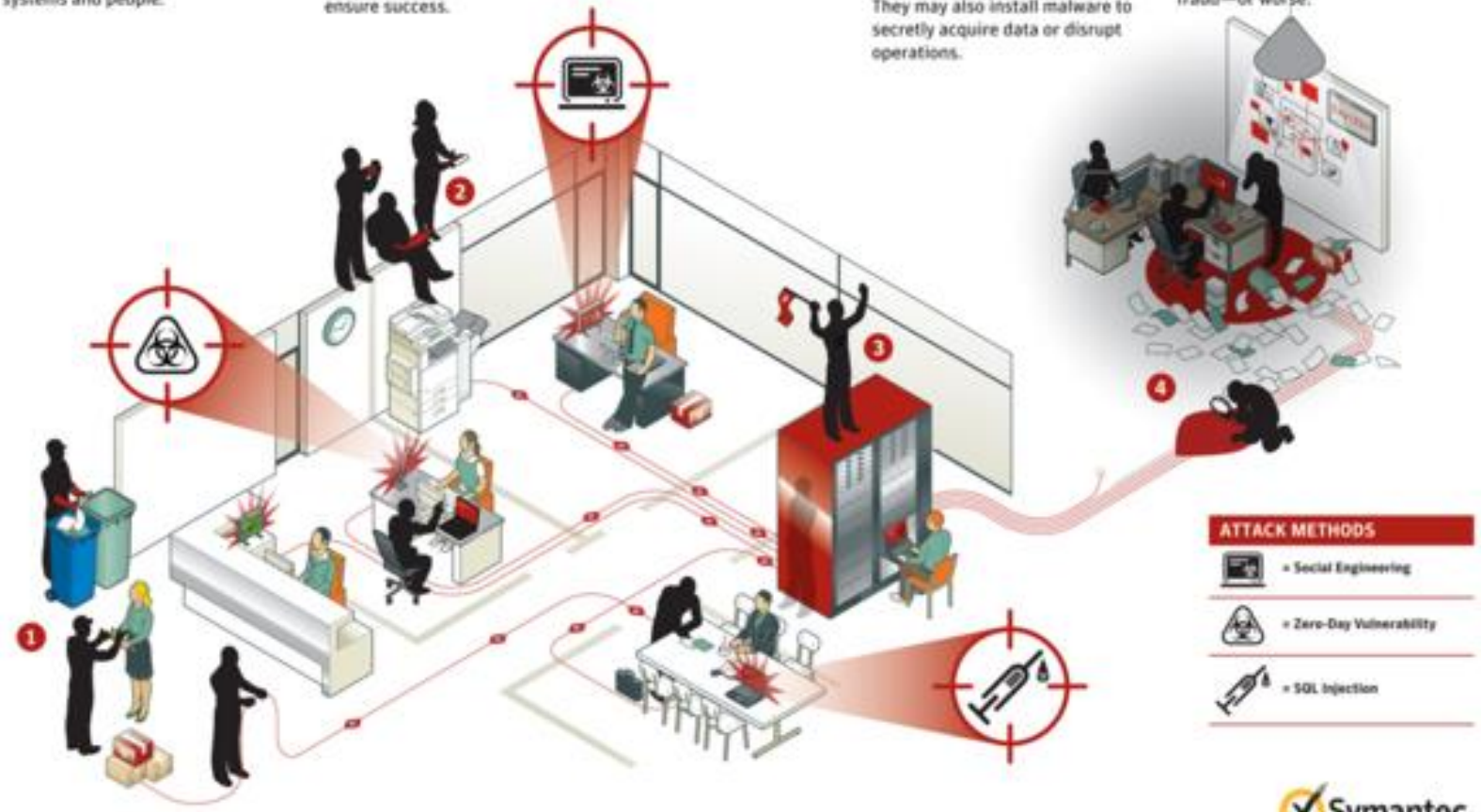
3. CAPTURE

Attackers access unprotected systems and capture information over an extended period.

They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION

Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.



Symantec.

Special Prosecutors Office for
High-Tech Crime of Serbia

WannaCry

Ransomware Attack

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

About bitcoin

How to buy bitcoins?

Contact Us

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Mobile transactions and currencies

- **Mobile transactions**
- **Mobile applications**
- **Mobile crypto-currencies**
- **600.000$ unlawfully acquired bitcoins and dogecoins with one hacker attack by „harvest“ method**

Detail Case Study

1. Unauthorised Access to the Computer, Computer Network or Electronic Data Processing;

2. Computer Sabotage;

3. Creating and Introducing of Computer Viruses;

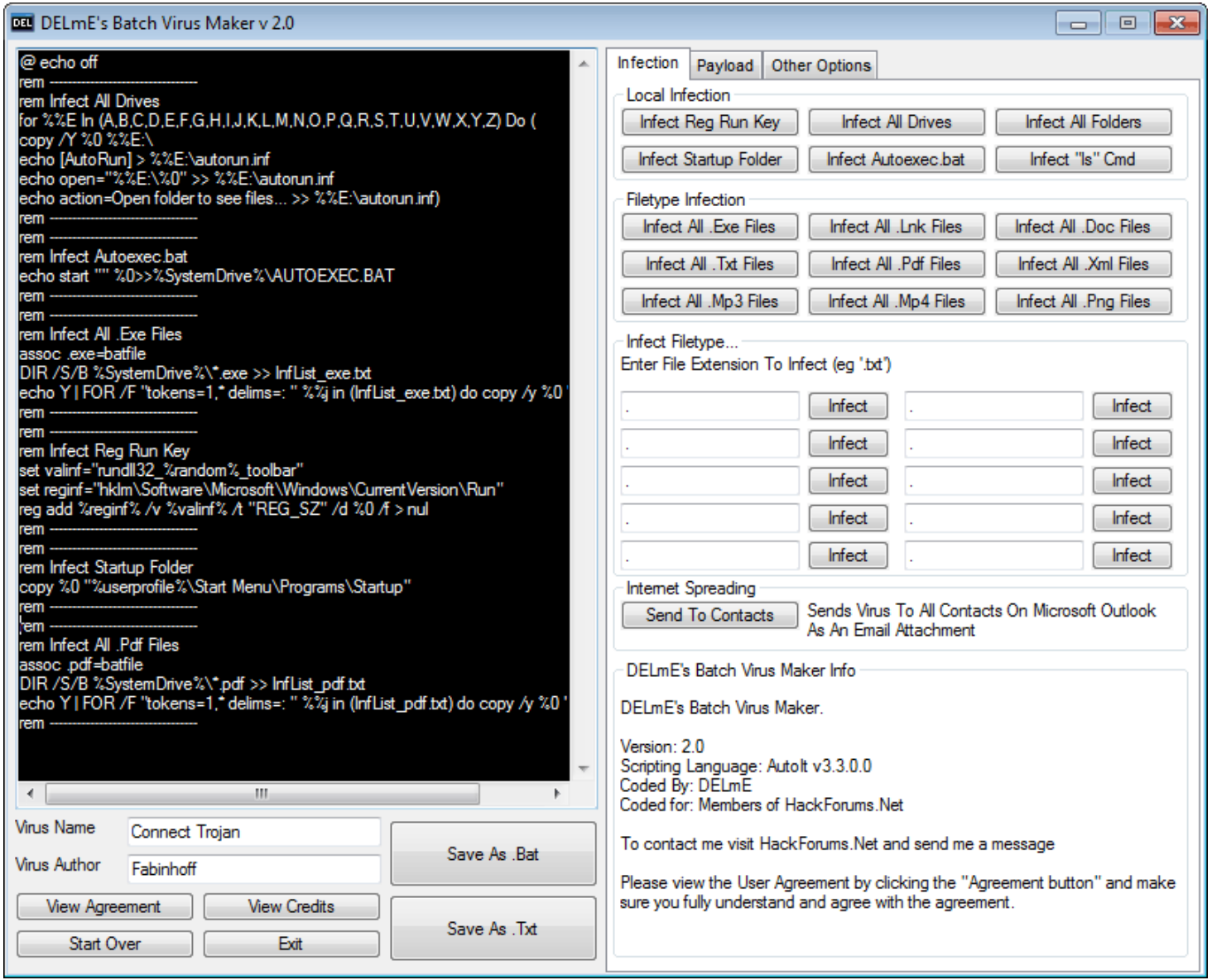
4. Manufacture, Procurement, and Provision to Others of Means of Committing Criminal Offences against Security of Computer Data;

Computer Viruses

- A **computer virus is a type of malicious software program** ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code.
- **Infected computer programs can include**, as well, data files, or the "boot" sector of the hard drive.
- **When this replication succeeds**, the affected areas are then said to be "infected" with a computer virus.
- **Without the consent** (or knowledge) of its user / administrator
- **With the aim of causing damage in this system**.

Special Prosecutors Office for
High-Tech Crime of Serbia

Computer Viruses



Investigation

- **Violating protective measures**, the defendant without authorization logged in to a computer network, accessed electronic data processing **previously using anonymous service providers** through open wireless access points **in order to change MAC addresses** (Media Access Control Address) of the Network Interface Cards of the computers that he had used, **using several Socks5 connection protocols** (Internet protocol that directs network packets between client and server via the proxy server and provides authentication so that only authorized users can access the server, which enables the IP (internet protocol) address to be concealed, i.e. that communication with another computer goes over a remote computer (server) for serving other computers that randomly assign IP addresses from any range of addresses, **keeping the true IP address unrevealed).**

Investigation

- **Without authorisation defendant accessed to a protected computer network**, a central server for control of web sites of an ISP on whose server a web site of a state authority was hosted.
- **Using his alias he entered, destroyed, erased and changed and thus made unusable computer data and programs**, **with the intent to disable and obstruct the process of electronic data processing which is of importance to the said state authority**.
- **The electronic record of the central control server**/ administrative user access data (user administrative name and password to unlock/provide access to editing of the website), **was deleted to disable further access by authorized persons** to data control and the website itself.
- **Defendant the changed the username and password entering so-called "standard values" for the name and password** which in this particular case were admin-admin, and after that he gave the data for use in such a way that he immediately distributed the said data through a variety of social and communication networks on the Internet to other persons, for continued unauthorized access and changes of the content.

Court Findings and Rulings

- **Second count charged the defendant with almost identical way of commission of the criminal offence**, and the only difference was that the defendant had accessed the central server for control of all websites of internet service providers, on whose servers there were websites of different state authorities, public services, companies and other subjects.
- **The defendant entered, destroyed, erased and changed and thus made unusable computer data by changing user access data**, and then in the electronic database of websites he changed the texts and photos and other electronic data or completely erased websites and information and instead of them he entered previously prepared his own presentations with various messages into publicly available electronic databases;
- **Thus accessing without authorisation and preventing or significantly interfering with the process of electronic processing and transmission of data on internet sites of several faculties and courts, and then accessed the websites of the various political parties, media agencies, ministries, the site for the parliamentary elections and others.**

Court Findings and Rulings

- **On the count five the defendant was found guilty for having made a computer virus with the intent to introduce it into others' computers and computer networks**.
- On his personal computer the defendant had made a computer virus and then published it on a number of hacker internet websites.
- **When a user would take it over and use it, it would return to the defendant in the form of the new PHP Shell** (which is used for administration and maintaining websites, for unpacking and moving large files) with the information where the virus is situated and exactly in which way an infected computer can be controlled.
- **On one of his e-mail addresses he had 600,000 Shells obtained in this way, and on the other 176,000 Shells**. One Shell served for access to one website, so the defendant had access to each infected computer used by another person who didn't even know that their computer was infected which enabled the perpetrator to access other websites on the servers via so-called "backdoor" approach.
- **He then entered those 776,000 PHP Shells in others' computers and computer networks on the websites that he had changed and by doing so caused damage by disabling access to and use of those websites in the way they were made, and thus at the same time caused material damage in an undetermined amount.**

Court Findings and Rulings

- **Final verdict was rendered against the defendant who was found guilty on five counts**:
- **on the first count** of the criminal offence of Unauthorised Access to Computer, Computer Network or Electronic Data Processing, of the criminal offence of Computer Sabotage, of the criminal offence Manufacture, Procurement, and Provision to Others of Means of Committing Criminal Offences against Security of Computer Data;
- **on second, third and fourth count** of Unauthorised Access to Computer, Computer Network or Electronic Data Processing, and of Computer Sabotage;
- **and on the fifth count** of prolonged Creating and Introducing of Computer Viruses, and prolonged criminal offence of Manufacture, Procurement, and Provision to Others of Means of Committing Criminal Offences against Security of Computer Data.

Serbian Criminal Code Acts used in this case study

Computer Sabotage

Article 299

Whoever enters, destroys, deletes, alters, damages, conceals or otherwise makes unusable computer datum or program or damages or destroys a computer or other equipment for electronic processing and transfer of data, with intent to prevent or considerably disrupt the procedure of electronic processing and transfer of data that are of importance for government authorities, enterprises or other entities,

- *shall be punished by imprisonment of six months to five years.*

Serbian Criminal Code Acts used in this case study

Creating and Introducing of Computer Viruses

Article 300

(1) Whoever makes a computer virus with intent to introduce it into another's computer or computer network,

- *shall be punished by fine or imprisonment up to six months.*

(2) Whoever introduces a computer virus into another's computer or computer network thereby causing damage,

- *shall be punished by fine or imprisonment up to two years.*

(3) Equipment and devices used for committing of the offence specified in paragraphs 1 and 2 of this Article shall be seized.

Serbian Criminal Code Acts used in this case study

Unauthorised Access to Computer, Computer Network or Electronic Data Processing

Article 302

(1) Whoever, by circumventing protection measures, accesses a computer or computer network without authorisation, or accesses electronic data processing without authorisation,

- *shall be punished by fine or imprisonment up to six months.*

(2) Whoever records or uses data obtained in manner provided under paragraph 1 of this Article,

- *shall be punished by fine or imprisonment up to two years.*

(3) If the offence specified in paragraph 1 of this Article results in hold-up or serious malfunction in electronic processing and transfer of data or of the network, or other grave consequences have resulted,

- *the offender shall be punished by imprisonment up to three years.*

Serbian Criminal Code Acts used in this case study

Manufacture, Procurement, and Provision to Others of Means of Committing Criminal Offences against Security of Computer Data

Article 304a

(1) Whoever possesses, manufactures, procures, sells, or gives to others for their use computers, computer systems, computer data or software intended for committing one of the criminal offences referred to in Articles 298 through 303 herein

- *shall be punished with imprisonment of six months to three years.*

(2) Items referred to in paragraph 1 hereof shall be seized.

Special Prosecutors Office for
High-Tech Crime of Serbia

Thank you

branko.stamenkovic@rjt.gov.rs