mvr.gov.mk
Министерство за внатрешни работи

CRIMINAL INVESTIGATION – SHIPMENT

Inspector: M-r Bojan Stefanovski

Sector for computer crime and digital forensic
Department for cybercrime investigations

Start of investigation:

- Initial information forwarded from the Customs Administration of the Republic of Macedonia, in which they informed us that they have registered fake shipments in their electronic system

Initial activities of the investigation:

- At the beginning the investigation was focused on computer terminals and electronic customs officers whose accounts appeared as registrants of suspicious shipments;
- These terminals were removed from their posts and taken to a laboratory for forensic analysis
- We did not have the right direction / guidance for the investigation until we received information from colleagues from Republic of Bulgaria

After mutual communication and coordination

- One person, Macedonian citizen, who we think is the relation between people in Bulgaria with the staff in border terminals of the Customs Administration of the Republic of Macedonia
- We also have one person employed in the Customs Administration of the Republic of Macedonia which we believe is directly involved in installation / attachment of the virus in the Electronic System
- We have forensic analysis of the computer terminals from the Customs Administration of the Republic of Macedonia, in which was installed malware
- The terminals are provided by two different border terminals and in different time periods

The results of forensic analysis are:

- Malicious software was found and installed in all terminals
- Based on the analysis, there are two varieties of this malware
- The difference is in the way the processes of this malware run in the windows background;
- Same USBs, (same brand= Kingston, vid =13fe & pid =4200) are found as initial point in which malware is transferred to the infected terminals

First type of malware:

- Found in the Usb for further injection on computer terminal.
- Contains files such as runme.bat, lasassa.exe, spoolsv.exe and svchost.exe
- After running runme.bat, malware infection is initiated and all the processes are rewritten and replaced with the new .exe files that are present on the usb drive.

Secound type of malware:

- Second type of the malicious software that is found on infected terminal computers runs all of the processes that are mention above but parallel with the originals windows processes.

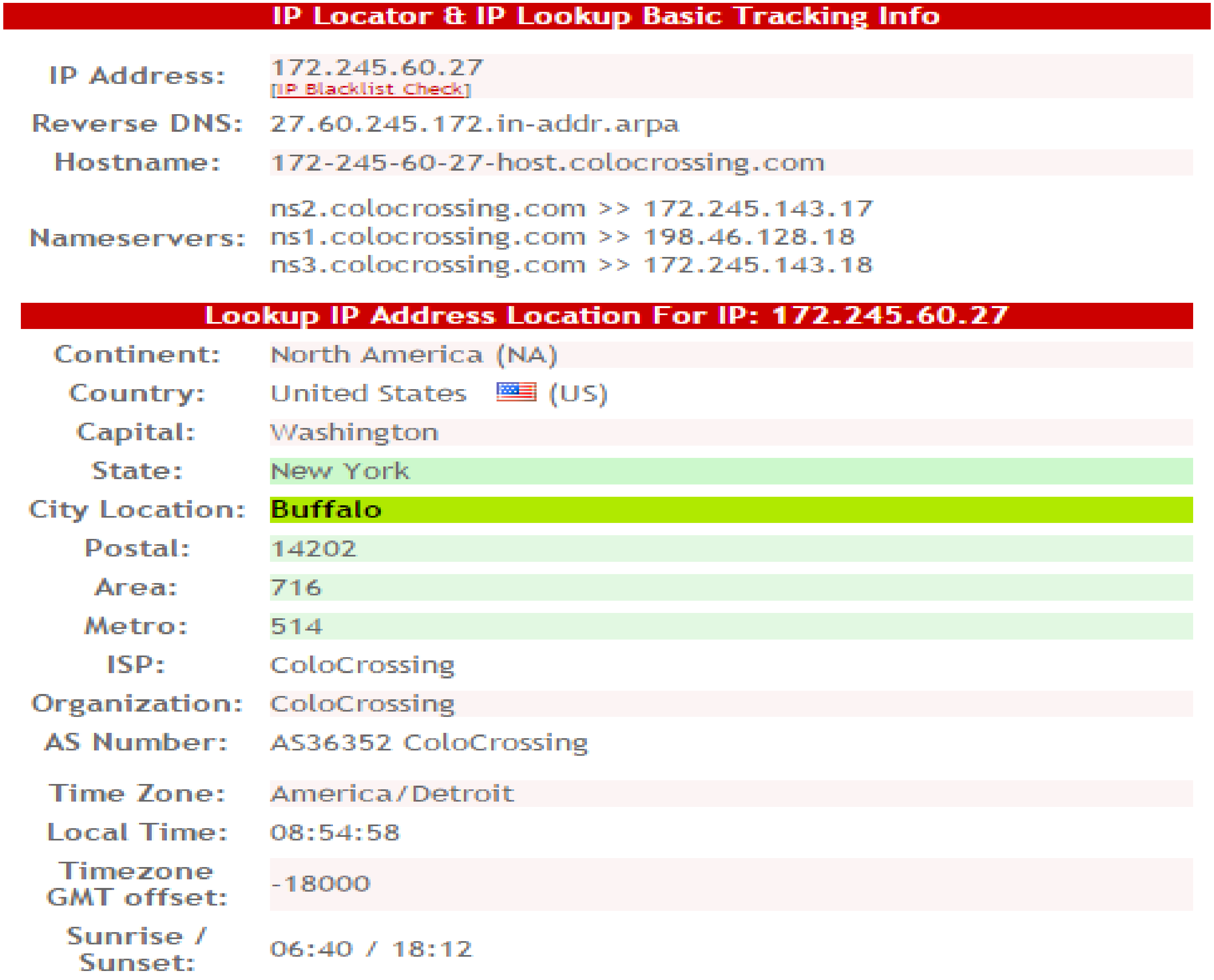
Different malware varieties:

- lsassa.exe
- runme.bat – start app
- spoolsv.exe
- svchost.exe

Second variety runs parallel in windows, in that way we can see in processes that two spoolsv.exe or svchost.exe processes are active.

CONCLUSION:

All malware better works under win 7 environment. From forensic analysis it can be concluded that it is the same malicious software that in both the variants communicate with IP address: 172.245.60.27 but there is a trouble with communication under Windows XP environment that is installed in the computer terminals from the Customs Administration of the Republic of Macedonia.



IP Locator & IP Lookup Basic Tracking Info

IP Address:	172.245.60.27 [IP Blacklist Check]
Reverse DNS:	27.60.245.172.in-addr.arpa
Hostname:	172-245-60-27-host.colocrossing.com
Nameservers:	ns2.colocrossing.com >> 172.245.143.17 ns1.colocrossing.com >> 198.46.128.18 ns3.colocrossing.com >> 172.245.143.18

Lookup IP Address Location For IP: 172.245.60.27

Continent:	North America (NA)
Country:	United States 🇺🇸 (US)
Capital:	Washington
State:	New York
City Location:	**Buffalo**
Postal:	14202
Area:	716
Metro:	514
ISP:	ColoCrossing
Organization:	ColoCrossing
AS Number:	AS36352 ColoCrossing
Time Zone:	America/Detroit
Local Time:	08:54:58
Timezone GMT offset:	-18000
Sunrise / Sunset:	06:40 / 18:12

Also some of the processes that this malware runs in background have active connection with **rubyw.exe** application

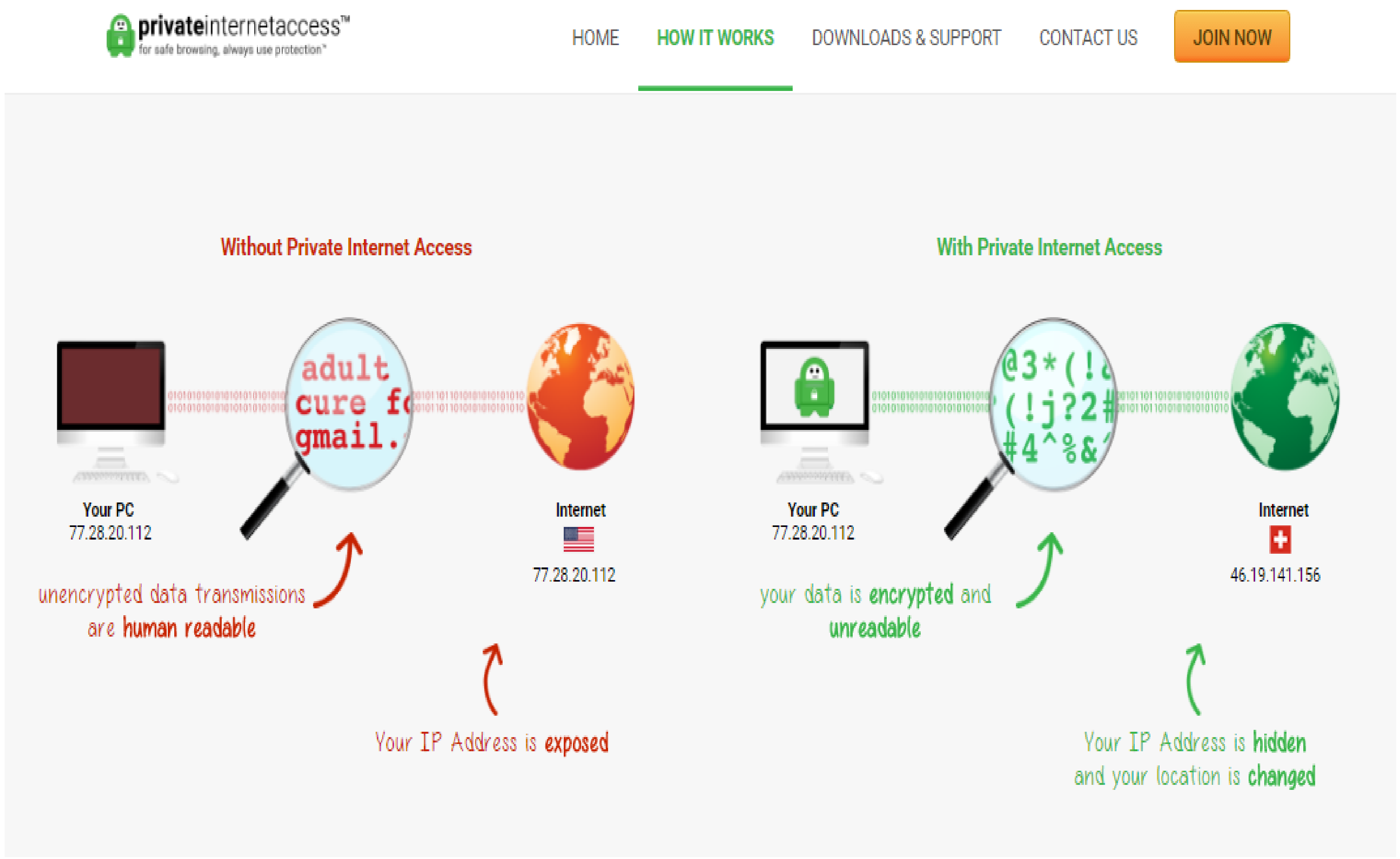
rubyw.exe

If you are using the popular VPN service Private Internet Access (PIA) and monitor outgoing network connections on your devices, you may have noticed that the program rubyw.exe attempts to connect to various Internet servers when you initiate the VPN connection to Private Internet Access.

This happens only if you are using the PIA software and not if you have configured connections to the service manually or in third-party network software.

Private Internet Access is a very popular VPN service thanks to anonymous payment options, unlimited bandwidth, impressive number of worldwide services, no traffic logging policy and advanced features such as a kill switch to drop the Internet connection when the connection to the VPN drops.

If you monitor the outgoing connections on the device you will notice that rubyw.exe connect to various remote Internet hosts under the process ID pia_`manager, which is the main process of the Private Internet Access application.



Without Private Internet Access

unencrypted data transmissions are human readable

Your IP Address is exposed

With Private Internet Access

your data is encrypted and unreadable

Your IP Address is hidden and your location is changed

Next steps:

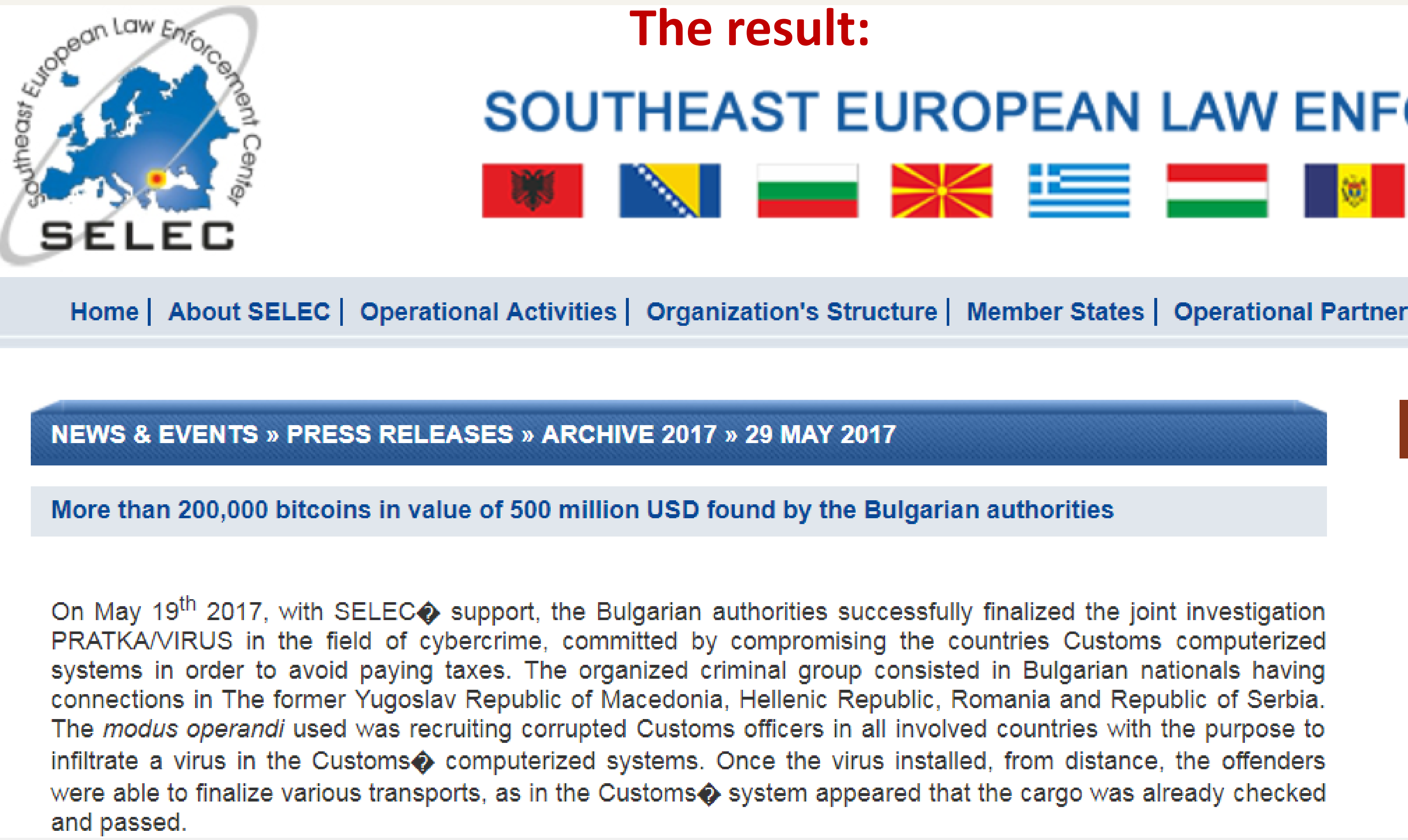
Based on the foregoing, with the aim of exchanging additional operational information and data related to possible identification of Macedonian citizens involved in the commission of the said criminal act and providing detailed information on the origin and manner in which the malicious software operates, Sector for International Police Cooperation (SELEC Center) organized a working meeting in Bucharest, Romania, on 08-10.03.2016, attended by the responsible officials from Sector for Cybercrime and Digital Forensic from Republic of Macedonia, and representatives from the Ministry of Interior of the Republic of Bulgaria, as well as representatives of the Customs Services and Computer Crime Units from Romania, Serbia and Greece .

Next steps:

- At the end of the working meeting, it was jointly concluded that it is necessary for officials from all participating countries to perform additional operational checks in order to determine the exact identity and number of persons involved, whose citizens are suspected of being part of the international organized criminal group.

- Also Public Prosecutors from Macedonia and Bulgaria exchanged information's and agreed on the dynamics of how the cooperation between the two countries would flow in the future in order to quickly and timely flow of information between the police services of the two countries

The result:



SOUTHEAST EUROPEAN LAW ENF

Home | About SELEC | Operational Activities | Organization's Structure | Member States | Operational Partner

NEWS & EVENTS » PRESS RELEASES » ARCHIVE 2017 » 29 MAY 2017

More than 200,000 bitcoins in value of 500 million USD found by the Bulgarian authorities

On May 19th 2017, with SELEC� support, the Bulgarian authorities successfully finalized the joint investigation PRATKA/VIRUS in the field of cybercrime, committed by compromising the countries Customs computerized systems in order to avoid paying taxes. The organized criminal group consisted in Bulgarian nationals having connections in The former Yugoslav Republic of Macedonia, Hellenic Republic, Romania and Republic of Serbia. The *modus operandi* used was recruiting corrupted Customs officers in all involved countries with the purpose to infiltrate a virus in the Customs� computerized systems. Once the virus installed, from distance, the offenders were able to finalize various transports, as in the Customs� system appeared that the cargo was already checked and passed.

The result:

The Bulgarian authorities have searched more than 100 addresses, suspects and vehicles. A large quantity of money was seized, as well as equipment, devices for communication, computers, tablets, bank documents, etc. 23 suspects were arrested, 5 of them acting as Bulgarian Customs officers. As result of this criminal activity the damages recorded by the Customs Agency, only for year 2015, is around 10 million Leva. It was determined that the members of the organized crime group invested the money obtained from these illegal activities in bitcoins, around 200,000 being discovered in the virtual space. As a reference, the value of one bitcoin is rating to 2354 USD. The offenders choose the bitcoin way of investing/saving the money, because it is rather difficult to be tracked and followed.

The judicial procedures against the offenders are currently ongoing, eight of them being already permanently detained.

THANK YOU
FOR YOUR ATTENTION !

Inspector: M-r Bojan Stefanovski

Sector for computer crime and digital forensic
Department for cybercrime investigations