

Sergeant Visar PACOLLI

CYBER CRIME INVESTIGATOR – KOSOVO POLICE

CYBERCRIME IN KOSOVO FIGHT AND PREVENTION



CYBERCRIME IN KOSOVO FIGHT AND PREVENTION

OLICELO

Kosovo Police

October, 2015



Internet World Stats December 2014

High Penetration of Internet

• Kosovo 84.4% users





Internet Service Providers

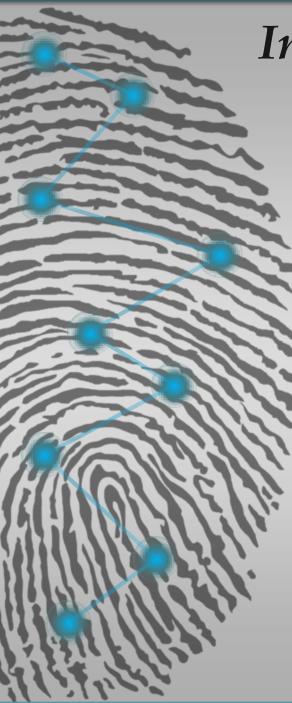
✤ IPKO

✤ PTK



CHARACTERIZES CHARACTERIZES CHARACTERIZES CHARACTERIZES CHARACTERIZES CHARACTERIZES CHARACTERIZES CHARACTERIZES CHARACTERIZES CONVECTION CON

© Can Stock Photo - csp11681816



Internet Penetration

- Internet users by age
 - **10-19 ----- 26.83 %**
 - 20-29 ----- 26.83 %
 - 30-39 ----- 19.15 %
 - 40-49 ----- 14.89 %
 - **50-59** ----- 8.16 %
 - 60-64 ----- 2.25 %
 - 65 or more 1.89 %

Legal Framework

Legal Framework

Legal Framework

Legal Framework

Legal Framework

Legal Framework

Law on Prevention and Fight against Cybercrime (2010 based on the Budapest Convention)

Law on Electronic Communication (2012)

Penal Code Penal Procedure Code

Police Law Standard Operating Procedures

National Cyber Security Strategy (in Process with the help of ENCYSEC Project - 2015)

Cybercrime Investigation Sector

 Cybercrime Investigation Sector is established in June 2011 and became operational in September 2011.

Structured within the Directorate for Organized Crime Investigation – Kosovo Police.

4 Units



Cases (1/6)

ATM Skimming of Credit Cards;

Fake news (through forged e-mail to the media);

960/01/00

Computer intrusion ;

DDoS attacks;

Phishing – Password stealing;

Online purchase with stolen credit

0101010101101010101 0110101 NAME ADRESS **01101001010**1010101010010011 OLIN 101 LOGIN N 011010010100101010101 JI. 01101010 NAME ADRES. 01101001010010101010010. 01101001010010101010010011010. 4040101101011010011010



Virus

Alert

rning! Threat deter malicious item has

Cases (2/6)

Online purchase with stolen credit cards;

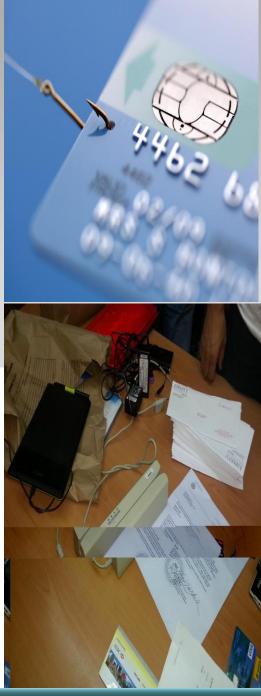
x https:/

POS purchase with stolen credit cards (credit cards cloning);

Drawing of cash money from ATM (forking system);

Fraud using fake e-mails (modification of bills and bank account) - Man in the middle; (emkei.cz - fake mailer)

1 Setet Lunguage 1 Uset Lunguage	ttps://emkei.cz			~	Date:	Mon. 19 Oct 2015 23:27:2	1 +0000 (UTC)	🗹 Current
Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML editor and advanced settings Image: Control of the mailer with attachments, encryption, HTML edito		Select Language				utf-8	•	
Free online fake mailer with attachments, encryption, HTML editor and advanced settings From Name: From Name: From E-mail: To: Subject: Subject: Attachment: Chose File No file chosen Attachment : Attachment : Attachment : Chose File No file chosen Attachment : Attachment : Chose File No file chosen Attachment : Attachment : Chose File No file chosen Attachment : Attachment : Chose File No file chosen Attachment : Attachment : Chose File No file chosen Attachment : Attachment : Attachment : Attachment : Chose File No file chosen Attachment : Attachment : Attachment : Confine delivey :	🖸 Flattr				Receiver's Public	No Ve	s 🗆 Do not encrypt at	tachments
From Name:	₿₿) Free onl	ine fake mailer with attachments, encryption, HTML editor and advanced settings					
Image: Serie From E-mail: image: Serie From E-mail: Image: Serie Subject: Image: Serie From E-mail: Subject: Subject: Subject: Subject: Matachandher file Image: Serie From E-mail: Image: Serie						ext/plain	🔍 text/html 💷 Edito	r
Image: Continue delivery: Image: Continue delivery: Image: Continue delivery: 234 Confirm delivery: Image: Continue delivery: Confirm delivery: Image: Confirm delivery: Image: Confirm delivery: Add Header: Image: Confirm delivery: Image: Confirm delivery: 2 Add Header: Image: Confirm delivery: 1 Confirm delivery: Image: Confirm delivery: 2 Add Header: Image: Confirm delivery:	■規■	From Name:			Text:			
Life: Subject: Image: Subject: </td <td>3600 R</td> <td>From E-mail:</td> <td></td> <td>📫 1.7k</td> <td></td> <td></td> <td></td> <td></td>	3600 R	From E-mail:		📫 1.7k				
Supject: Supject: 117k Attachment: Attachment: Advanced Settings 1 Advanced Settings 1 Ccc 234 Confirm delivery: G+1 Confirm delivery: G+1 Confirm delivery: 234 Confirm reading: 234 Confirm delivery: 24 Add Header:	前送表	To:		THE OWNER OF THE OWNER				
11x International releases 1x Attachandler file 1 Advanced Settings 1 Ccc 234 Image: Second Settings 235 Image: Second Settings 236 Image: Second Settings 237 Image: Second Settings 238 Image: Second Settings 239 Image: Second Settings <		Subject:		Concession of the local division of the loca				
Attach andher file 1 Advanced Settings 1 Some Reply-To: Errors-To: 234 Co: 234 Priority: Low Normal High Some Confirm delivery: 2 G+I Confirm delivery: 2 Add Header: In Sure Send	417	Attachment:	Choose File No file chosen	Share				
Sure Reply-To: 1 Cc; 1 Cc; 234 Bcc; Priority: Low 234 X-Mailer: -none - - G+1 Confirm delivery: Confirm reading: 2 Add Header; In Sure	and the second second							
I Cc 234 Y Tweet Bcc 234 Priority: Low Normal High 234 X-Mailer: -none - G+I Confirm delivery: 2 G+I Confirm reading: 2 Add Header: In Sure Send	🖪 Like		Advanced Settings	1				
1 Cc 234 9 Tweet Bcc 234 234 X-Mailer: -none - 234 X-Mailer: -none - Confirm delivery:	Share	Reply-To:		MT Turnet				
y Tweet Bcc 234 Priority: Low Normal High 234 X-Mailer:	1.0	Errors-To:		J Weet				
y Tweet BCC Priority: Low Normal High 234 X-M-lair: -none - G-1 Confirm delivery:	1	Cc:		224				
Priority: Low Normal High 234 X-Mailer: -none - G+I Confirm delivery: Confirm reading: 2 Add Header:	Tweet	Bcc:		234	Contribution			
234 X-Mailer: -none - Im not a robot G+I Confirm delivery: 2 Confirm reading: 2 Add Header: in State Send Clear		Priority:	Low Normal High	G+1	Captena:	_	7	
G+1 Confirm delivery: 2 Programmed 2 Programmed 2 Programmed 2 Clear	234	X-Mailer:	- none -			I'm not a robot	1.0	
2 Add Header: Send Clear		Confirm delivery:		2				
	G+1	Confirm reading:						
2 SMTP Server: Port:		Add Header:		in Share		Send	lear	
	4	SMTP Server:	Port:					





9	Apps		(ΛIC)					
1	Calendar CO	lses	(4/6)				Search Save	
	Contacts			nber	Duration	Date	 Address 	
ø	Blocked Site		044417722 044	417722	00 minute 00 seconde	2014/08/14 09:25:29	Address not available 🖗	
*	Remote Control	•	• 044417722 044	417722	00 minute 00 seconde	2014/08/14 09:22:13	Address not available 🕏	
	IM <	= *	044417722 044	417722	00 minute 13 secondes	2014/08/14 09:08:09	Address not available 🛿	
*	Note / Bugs	= ±	♥ 045945587 045	945587	00 minute 00 seconde	2014/08/06 22:05:14	Address not available 9	
	×	n 4	a a	1354684	00 minute 00 seconde	2014/07/19 12:34:30	Address not available 🕏	
			Cata Day In In	navdy Preverber				
	Data		Tracker Fast! install needed Satellite		Use Worldwide 1-1000 vehicles TraceSolutions Phone For The simple - sensors with Deaf Try It reliable - no			
	Blocked calls		Free @ Fast shipping From EU	Winning monitoring	TraceSolutions Today - Free contract! Fleet Test Calls Management	SAMSUNG		
	Localizations <						☎⊿∎11:35	
	Pictures					Applications manager		
	• Apps	10				Downloaded Running All		
1	Calendar				Search			
-	Contacts		Name Number	Duration	Date 🔻 Address	and the second	iperSU 19MB	
	8 Blocked Site		038545476 038545476	00 minute 00 seconde	2014/07/28 Address not available 9 16:11:23		ikBack	
	Remote Control	🗉 🛓 🚩	049187330 049187330		2014/07/26 Address not available 9		IOMB	
	● IM <	圇	Name Number		22:10:16		tal SMS Control	
	My account	-	Name Number	Duration	Date Address		ber	
	? Note / Bugs	Showing 1 to 2 of 2	SNMP Software- Download Management Jewels Facebook Software Campaucet Apps	Name Groups tracking res rotraccom Difecebook.com System Su	or wifi and gprs Diagnostic D sponse on data logger Solutions rveys? O equalmajat 🛥 dagaaloouk	DEvice memory G61148 axed T ±08 te		
			O helpsystems Point-of-sale D facebook.com Get alerted to for retail Get The Most		ofsms.com Aqualinkii is a Wireless. ata mahila islar friandivi Onlina			









THANK YOU FOR ATTENTION !

Sergeant Visar PACOLLI Supervisor - Computer Intrusion UNIT Cybercrime Investigation Sector KOSOVO POLICE E-mail: visar.pacolli@kosovopolice.com