

A hand in a blue and white striped shirt points at a computer monitor. The monitor displays several data visualizations: a bar chart on the left, a bar chart with a prominent peak in July on the right, and a line graph at the bottom right. A 3D pie chart is visible in the top right corner. A semi-transparent white box with a dark border is overlaid on the bottom left of the screen, containing text.

# OPSEC FOR SECURITY RESEARCHERS

**Vicente Díaz**

Principal Security Analyst

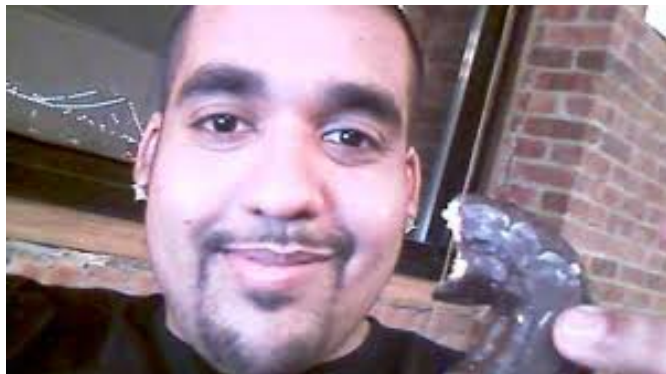
**KASPERSKY** lab

# WHAT IS THIS TALK ABOUT

“Operational security identifies critical information to determine if friendly actions can be observed by adversary intelligence systems”

- How does this apply to our industry?
- No counter-intel.
- Not only identify – apply best practices for good opsec.

# YOU ALL HAVE HEARD OF OPSEC FAILURES



We won't talk about them again.

**Golden rule:**

**Silence** as a defensive discipline  
aka STFU.

**Warning: discipline level 80  
needed**

# THE RULE IS PRETTY SIMPLE

But we fail miserably.

It's in human nature to **IMPRESS**.



**Golden rule2:**

OPSEC does not work  
retrospectively.

# I HAVE NO ENEMIES!

Let's put some context:

- \_ We work on cool stuff
- \_ We stumble upon “strange” things
- \_ The environment is sometimes poorly regulated
- \_ Hypocrisy vs red lines
- \_ Sense of invulnerability: we are the good guys, right?

Not here to define the ethics of the industry!

# BUT

Could our work be interesting for someone else?

Might it be perceived as dangerous for other's interests?

Are all our actions, as researchers, impeccable?

We might be the weakest link, in terms of OPSEC, when collaborating with LE.



# UNDER SCRUTINY

We might be in a group of interest

Objective: not become an **individual** of interest!

Silence, but not complete.

Avoid the escalation of surveillance: that means Game Over.



# ADVERSARIES

Broadly speaking:

- \_ Common cybercriminals
- \_ Non-common cybercriminals
- \_ Agencies
- \_ The future (or massive surveillance)

Otherwise – worse than  
not applying OPSEC at all.

**Important:** choose the OPSEC  
level you can adopt

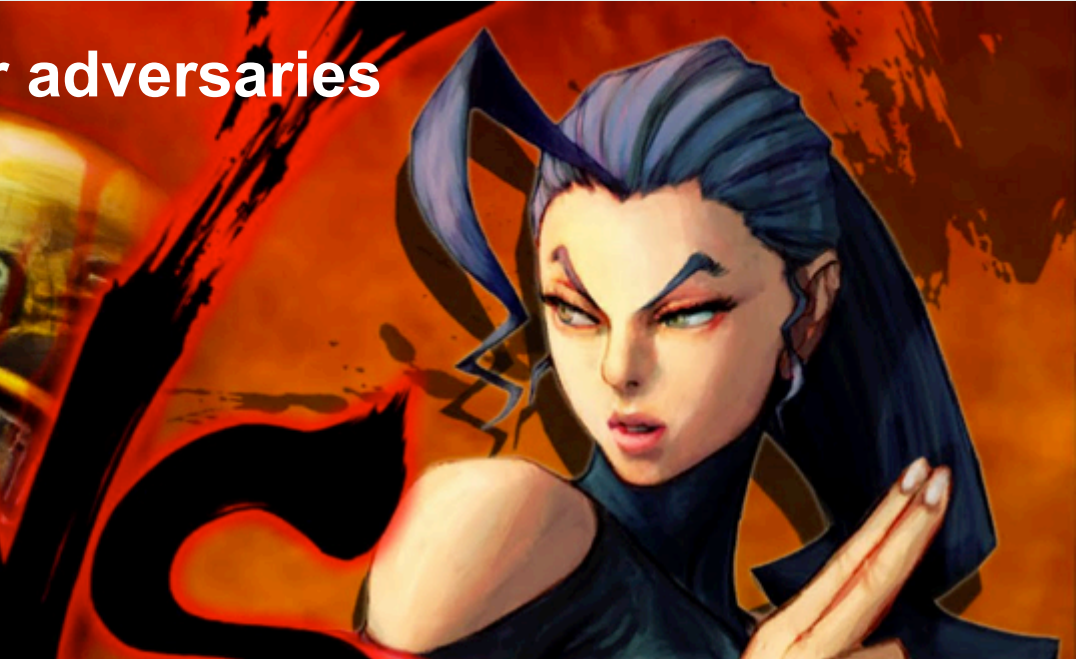


# Meet our adversaries



I Metsu Hadoken

Evil Ryu



I Illusion Spark

Rose

# COMMON CYBERCRIMINALS

From: Blac<hat Secured <[dont-try-to-know@yandex.ru](mailto:dont-try-to-know@yandex.ru)>

Date: 2010/1/21

Subject: you must know

To: [REDACTED]

In your blog you wrote about blackhats and some-ware for them. Nothing personally, but there is need to say that you must think and be careful before publishing yet another post-in-the-blog which contains inappropriate words such as : cr|meware/collaborates with cr|minal activities, etc. These unwelcome talks may cause a negative reaction of so-called BH. Be sure, they have enough money and possibilities to serious answer. It's just a freindly recommendation.

You are not c(l)p or judge (isn't it?). As civilized man you have to know the following: a presumption of innocence. Why are you doing this? Fame, money, trying to find a good job? For what reasons? Who cares? Don't become a yellow boulevard press ( with cheapest "shocking" news for a day) or sanctimonious sl/t saying : "...we can be friends quietly and even a beer someday" and "...actively collaborates with criminal activities, which isn't so funny" at the same time. Just be a real man and you will have all respects you need.

Many BH are very normal men who has families, hobbies, their own points of view and business goals at a time when economical situation in country isn't good...not so comfortable for legal professional job with world-level salary. Open your eyes - see the world from another side.

Let him do their work:)

However, thanks for reading this letter. I hope we can understand all the sides. Have a nice day!

P.S.: that's non-public thoughts, don't forget it.

# COMMON CYBERCRIMINALS

From: Blac<hat Secured <[dont-try-to-know@yandex.ru](mailto:dont-try-to-know@yandex.ru)>

Date: 2010/1/21

Subject: you must know

OW SEU FILHO DA PUTA VAI FICA DENUNCIANDO PISHING MESMO SEU MERDA NÃO TEM NADA PRA FAZER DA MERDA DA SUA VIDINHA NÃO SEU BOSTA A HORA QUE TE ACHAREM COM A BOCA CHEIA DE FORMIGA SEU FILHO DA PUTA NÃO VAI CHORA PRA DEUS NÃO VIU SEU MERDA TEM PORRA NENHUMA PRA FAZER DA MERDA DA VIDA A NÃO SER CAÇA PHISHING NA INTERNET PRA DENUNCIA SEU FILHO DE UMA PUTA TUA HORA VAI CHEGA SEU BOSTA A GENTE SE ENCONTRA NO INFERNO PODE ESPERA SEU MERDA.

Let him do their work:)

However, thanks for reading this letter. I hope we can understand all the sides. Have a nice day!

o.s: that's non-public thoughts, don't forget it.

# NON-COMMON CYBERCRIMINALS

Let's say, cybercrime is non their primary purpose.

Organized, dangerous,  
have resources.



Not directly the result of a direct investigation, stumble upon them.

So what if our OPSEC was not good?

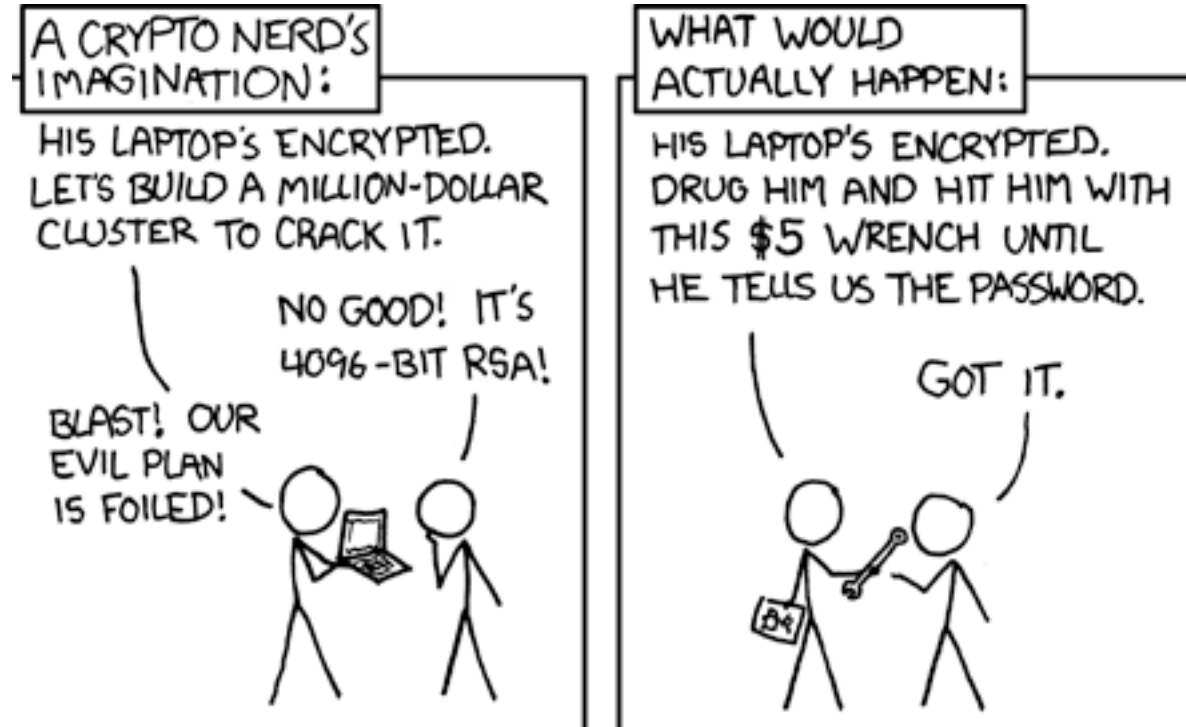


# AGENCIES

They have all the resources.

Non technical approach, that we tend to forget exists.

Usual approach:  
**Recruitment.**



# MASSIVE SURVEILLANCE – AGENCIES? NOT ONLY

Trail of data and metadata – insane levels.

What today looks secure, it might not be in the future.

Companies getting huge amounts of data too.

When leaks happen – fest.

# MASSIVE SURVEILLANCE – AGENCIES? NOT ONLY

T  
W  
C  
W

User: ssndob@ssa.gov. Balance: \$316. Searches quene (ALL/VIP): 0/0

News Regular Search **Super Search** **Manual (SSN,CR,BR)** Bulk **List** Fulls **Driver Licence** Archive Payments

Support (3) Settings Help Manual Admin Logout Admin Mode

Logged In Successfully

News

10 September	<b>Ticket system</b> Please dont send batches or payment info in ticket. Payments processed automaticly, SEND TICKET ONLY if you didnt get funds in 24h.
28 May	<b>Upgrades</b> Bitcoin payments is available now. New additional support jid is <a href="mailto:ssndob@jabber.dk">ssndob@jabber.dk</a>
28 March	<b>WE ARE BACK!</b> Service is private now. Registration is closed.



# MASSIVE SURVEILLANCE – AGENCIES? NOT ONLY

T  
W  
C  
W

User: ssndob@ssa.gov. Balance: \$316. Searches quene (ALL/VIP): 0/0

News Regular Search **Super Search** **Manual (SSN,CR,BR)** Bulk List Fulls Driver Licence Archive Payments

Support (3) Settings Help Manual Admin Logout Admin Mode

Logged In Successfully

News



**Ticket system**

Please dont send batches or payment info in ticket.  
Payments processed automaticly,  
SEND TICKET ONLY if you didnt get funds in 24h.

**Upgrades**

Bitcoin payments is available now. New additional support jid  
to ssndob@jabber.uk

**WE ARE BACK!**

Service is private now. Registration is closed.

**Important:**  
avoid being an anomaly!

---

## IMPLEMENTATION

Remember: be meticulous!

# IMPLEMENTATION PROCESS - APPROACH

Situational awareness

Understand your position

Threat actors (reduced)

Threat environment

Identify valuable data

Unintentional metadata

Analyze threats and vulnerabilities

Asses risks

Decide OPSEC measures to implement

# IMPLEMENTATION PROCESS - APPROACH

## Situational awareness

“There are a variety of different risk perspectives you can use to design a threat model: adversary-centric, asset-centric, or software-centric.

...

The reason that a small, agile startup can devise elegant OPSEC measures, is the same reason that compartmentalizing your OPSEC procedures in an operation-centric point-of-view is effective.”

ASSESS RISKS

Decide OPSEC measures to implement

# HOW TO IMPLEMENT IN A GROUP

As security, strongest as weakest link, somehow.

Externally:

who to trust, how to communicate with them

command chain, protocols for events → Opsec officer ?

Internally:

compartmentation

training and shaming

tag sensitiveness of information

**ProTip:** be careful with your language even internally.

# HOW TO

As secur

External

w

co

Internally

co

tra

ta



LEONARDO DiCAPRIO MATT DAMON JACK NICHOLSON AND MARK WAHLBERG

THE DEPARTED  
A MARTIN SCORSESE PICTURE

officer ?

with internally.

# IDENTITIES

Usual Opsec recommendation.

Necessary sometimes, but extremely difficult to do right.

An error means an advantage for the adversaries.

Advice: avoid if possible.

But if you cannot,

**Golden rule:** avoid  
cross-contamination



---

## TOOLS – QUICK REVIEW

# MINIMUM TOOLSET NEEDED



Encryption

Mail

IM

Phone

Internet

Minimum real world skillz

# ENCRYPTION

Inherent flaws – once broken all your past data is compromised.

This possibility increases with time.

Obviously the recommendation is to encrypt everything by default.

Anti-coercion credible partition is nice too.

# ENCRYPTION

Overall findings: “no evidence of backdoors or intentional flaws”

Obviously the recommendation is to encrypt everything by default.

Anti-coercion credible partition is nice too.

ENCRYPT

Overall  
or inten

Obviously  
default.  
Anti-coerc



The image shows a browser window titled 'TrueCrypt' with the address bar displaying 'truecrypt.sourceforge.net'. The page content includes a red warning message, a paragraph explaining the site's purpose, a paragraph about the end of development in 2014, and a section titled 'Migrating from TrueCrypt to BitLocker:'. Below this, there is a sub-section 'If you have the system drive encrypted by TrueCrypt:' followed by a numbered list starting with '1. Encrypt the drive by BitLocker first. Open the Explorer:'. At the bottom of the page, a partial Windows taskbar is visible with icons for the Start button, Internet Explorer, and Windows Explorer.

TrueCrypt

TrueCrypt

truecrypt.sourceforge.net

Google

**WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues**

This page exists only to help migrate existing data encrypted by TrueCrypt.

The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click [here](#) for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.

**Migrating from TrueCrypt to BitLocker:**

**If you have the system drive encrypted by TrueCrypt:**

1. Encrypt the drive by BitLocker first. Open the Explorer:

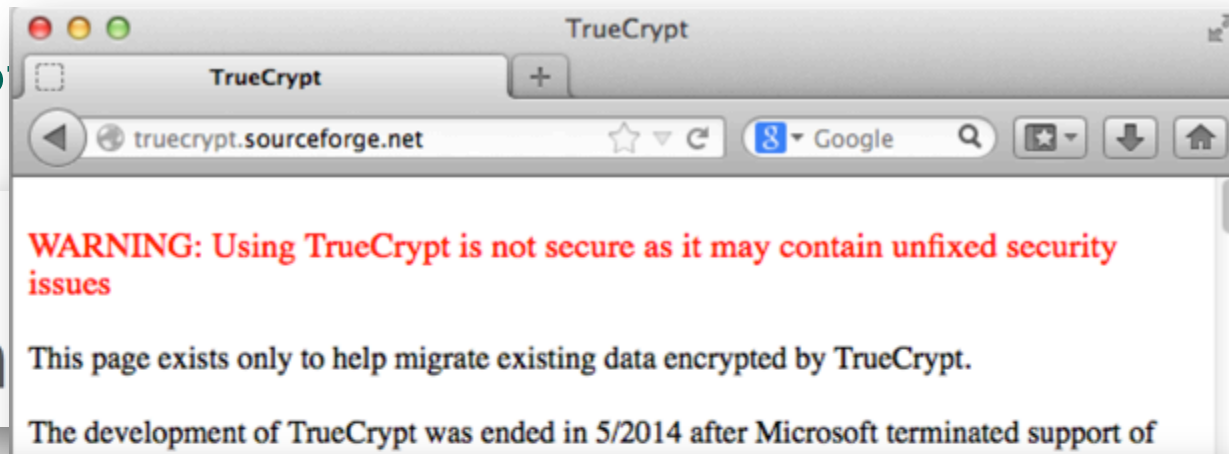


ckdoors

g by

ENCRYPT

Overall  
or inten



ckdoors

OACAP is continuing through with the Phase II (formal cryptanalysis) of the code

We have created a trusted repository of source and binaries for all platforms



## E-MAIL

Try to avoid it: metadata and the ID-ten-T problem.

Avoid external providers: ProtonMail, LavaMail, Gmail PGP.

If you use PGP, get a key bigger than 2048.

PROTONMAIL GETS THEIR PAYPAL  
ACCOUNT FROZEN WITHOUT  
EXPLANATION

IM with OTP is a much better option.



# IM

Adium and Pidgin: crypto seems to be ok. Some issues such as storing logs.

Cryptocat: young, minor issues like people joining your chat if they know the name.

Metadata, correlation and non-tech attacks still there!

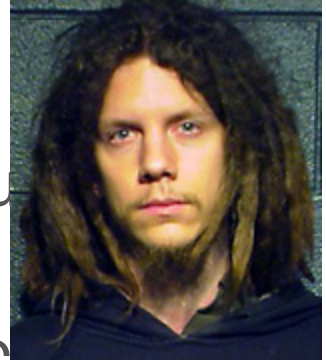
# IM

Adium and Pidgin: crypto seems to be ok. Some issues with  
as storing logs.

~~Cryptocat: young~~ minor issues like people joining you  
had been visited by the FBI in June 2011, and Sabu had been **arrested** and "turned." For months, he  
had been an FBI informant, watched 24 hours a day by an agent and using a government issued laptop  
that logged everything he did.

The FBI controllers behind Sabu must have found it grimly humorous to tease sup\_g with threats of  
arrest, but they were also using Sabu's chat for a more serious purpose—correlating the many names  
of sup\_g.

In the log above, note how Sabu suddenly addresses sup\_g by a new name, "anarchaos." It would turn  
out that sup\_g went by many names, including "anarchaos," "burn," "yohoho," "POW," "tylerknowsthis,"  
and "crediblethreat."



# TOR

Correlation everywhere.



Output nodes → For critical operations we are providing our logs for free!

Still, might be enough for avoiding most of the adversaries.

# TOR

## Tor security advisory: "relay early" traffic confirmation attack

---

Posted July 30th, 2014 by arma in [entry guards](#), [hidden services](#), [research](#), [security advisory](#)

This advisory was posted on the [tor-announce](#) mailing list.

### SUMMARY:

On July 4 2014 we found a group of relays that we assume were trying to deanonymize users. They appear to have been targeting people who operate or access Tor hidden services. The attack involved modifying Tor protocol headers to do traffic confirmation attacks.

The attacking relays joined the network on January 30 2014, and we removed them from the network on July 4. While we don't know when they started doing the attack, users who operated or accessed hidden services from early February through July 4 should assume they were affected.

# PHONE

Look, better not to use it – but it's a lost war.

Burner phones, change often, don't have anything important there.

Be coherent with what you have in your computer and in your phone.

# PHONE

## Operational Security: Spies v. Jihadis

Handbooks show that, as early as 2003,  
"Jihadi" security measures match those of Britain's spy agency GCHQ.

Look, better  
Burner phone  
there.  
Be coherent  
phone.

 GCHQ SECURITY GUIDE	RULES	 JIHADIST HANDBOOK
"The covert mobile phones... <b>MUST</b> not be switched on or used within a 50-mile radius of headquarters and within this radius <b>THE BATTERY MUST BE REMOVED FROM THE PHONE.</b> "	Remove Batteries 	"If the individual feels that his phone is being tapped, it is better to turn off his phone and remove the battery before he goes and meets someone."
"Calls between covert mobiles are permissible provided both are more than 50 miles from headquarters."	Maintain Closed Networks 	"Never call from the unofficial 'SIM' to a person whose mobile phone is registered with the company in an official way.... If the network is a closed network, it is ok they could call each other from the mobiles."
"Official phones are to be used only for official business in country and <b>MUST NOT</b> be used to make personal calls to the UK. If a call is unavoidable then only out of area numbers can be called, these are: - GSOC TRYST OOA - 0207 [REDACTED] - TAS TRYST OOA 0207 [REDACTED]"	Route Phone Calls 	"If someone wants to call his family from a suspected place, he could follow these steps to avoid the damage: Assume a person in Pakistan, he could call 'Turkey' on a certain number for this operation, and this number will connect the caller with his family in Jordan."
"The covert mobile phone <b>MUST NOT</b> be recharged at the officer's home address or at temporary residence e.g. a hotel room, if it is within the 50 mile radius. If a phone needs to be charged, then it is acceptable to do so either at the airport or at your destination."	Protect Your Location 	"The continuous communication from one place for long periods will lead to the fact that the owner of this chip lives in this location. Therefore be careful, never use the important SIM at your residence. Use it only at a different place other than your home."
"If you are carrying a covert mobile phone, you <b>MUST NOT</b> carry any personal communications device e.g. mobile phone, iPad, notebooks, PDAs, laptops etc."	Compartmentalize Devices 	"The arrest of 'Abu-Zubaydah' was only because of a mobile phone call (or calls)... Al-Wattan newspaper published an article 'Abu-Zubaydah's computer is the most important memory for the American'.... We have to learn from the story, that the computer is a dangerous memory."
"All contact with GCHQ should be via the <b>OUT OF AREA</b> numbers listed above."	Avoid Registered Landlines 	"If you are in a suspect country never call any individual on the ground phone line in that country because you will expose them."
"If you believe the phone to have been compromised, stop using it and report the incident to TAS staff as soon as possible i.e. on return to the UK."	Dispose of Compromised Equipment 	"If you...felt that someone knew your private number, then get rid of the SIM and the phone.... Remember getting rid of a \$300 phone is easier than sacrificing a brother who has important missions to carry out."
"It is recognised that officers who are departing from, or have recently arrive in the UK may wish to advise family or friends of disruption to their travel plans. In such cases the officer must use payphones that are available in the airport."	Use Pay Phones for Out-of-Network Calls 	"If there is communication outside the group, the right security procedure is to call from the street to the mobile phone and not from mobile to mobile."

important  
and in your

# REAL WORLD

Don't try to impress people – don't be impressed when approached by a stranger.

What if we are required by LE?

Have a travel laptop, travel phone, and lots of pennies in your pocket.





---

IN SUMMARY

# CONCLUSIONS

Opsec is hard – good news, no spy level is required.

Let's start educating ourselves and applying it by default.

Over tools – meticulousness.

Good Opsec is the one we can apply.

---

# QUESTIONS?



**Vicente Díaz**

Principal Security Analyst



[vicente.diaz@kaspersky.com](mailto:vicente.diaz@kaspersky.com)

[@trompi](https://twitter.com/trompi)