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

COMMON CYBERCRIMINALS

From: **Blac|<hat Secured** <dont-try-to-know@yandex.ru>
Date: 2010/1/21
Subject: you must know
To: [redacted]

In your blog you wrote about b|ackhats 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()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.

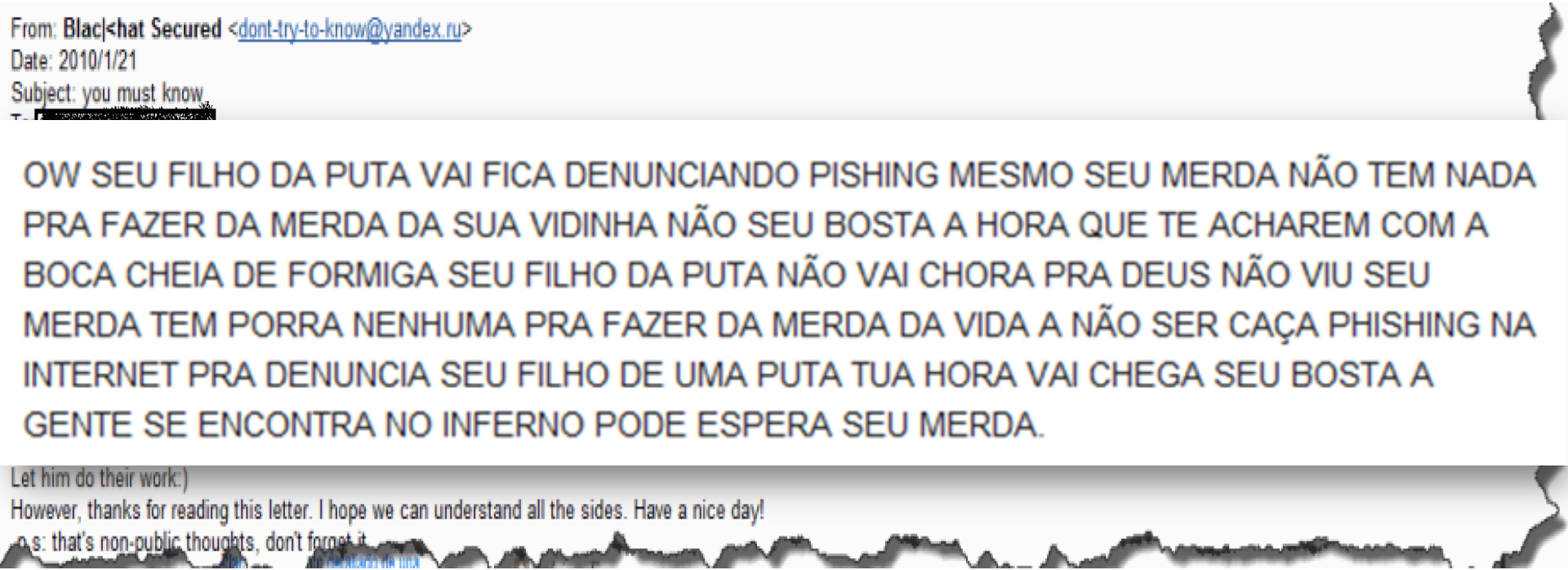
Let him do their work:)

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

KASPERSKY lab

COMMON CYBERCRIMINALS



From: Blac|<hat Secured <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!
p.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?

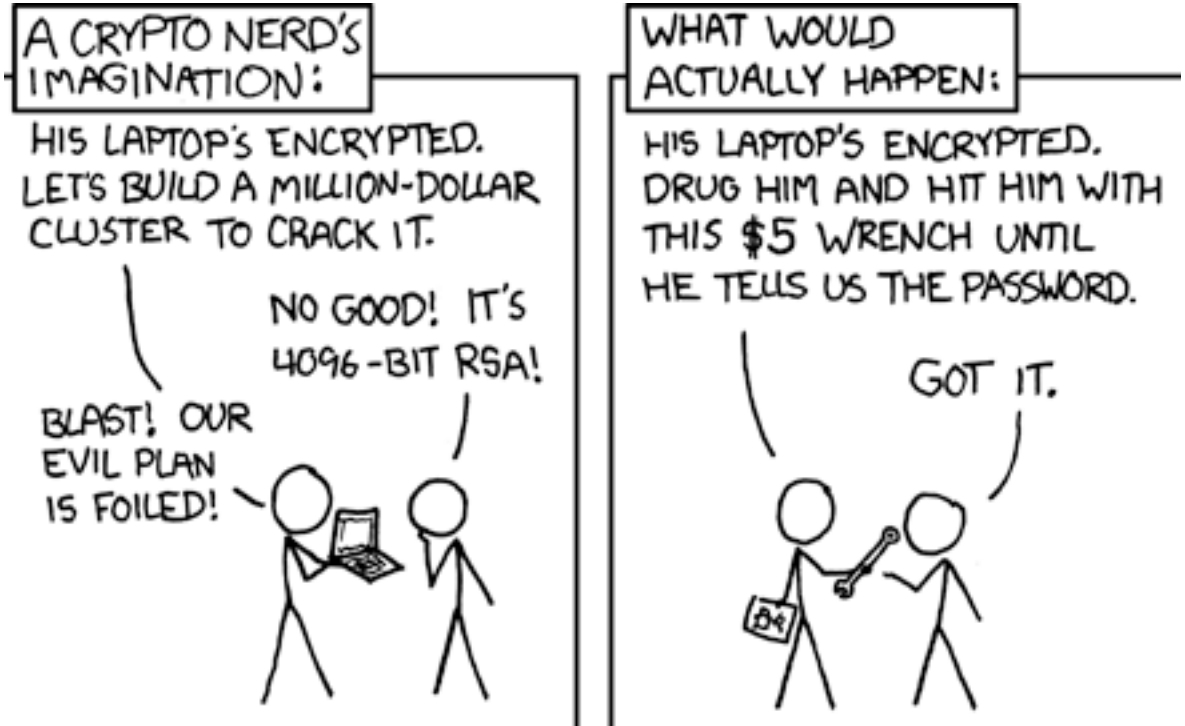
AGENCIES

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.

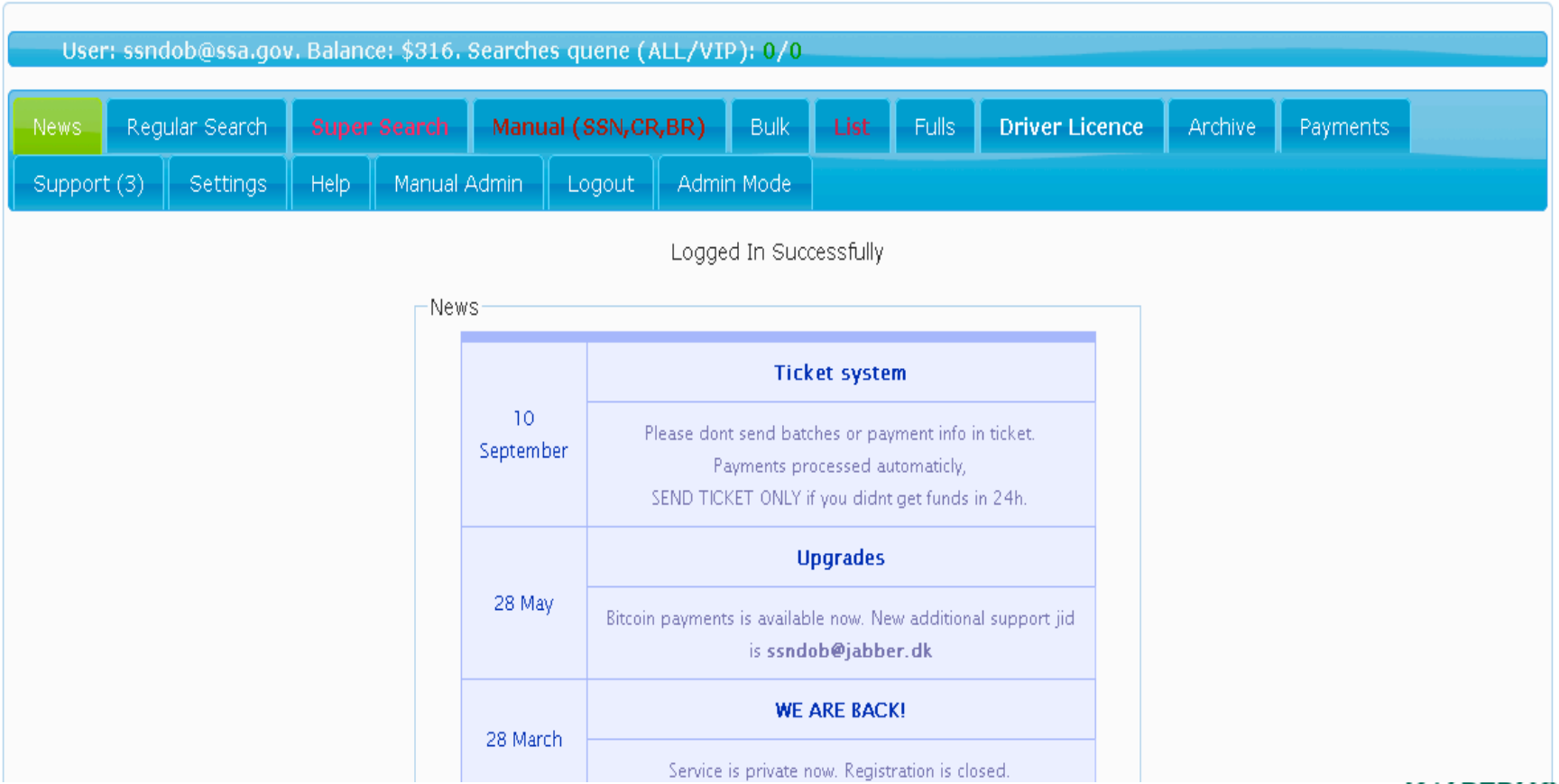
What today looks secure, it might not be in the future.

Companies getting huge amounts of data too.

When leaks happen – fest.

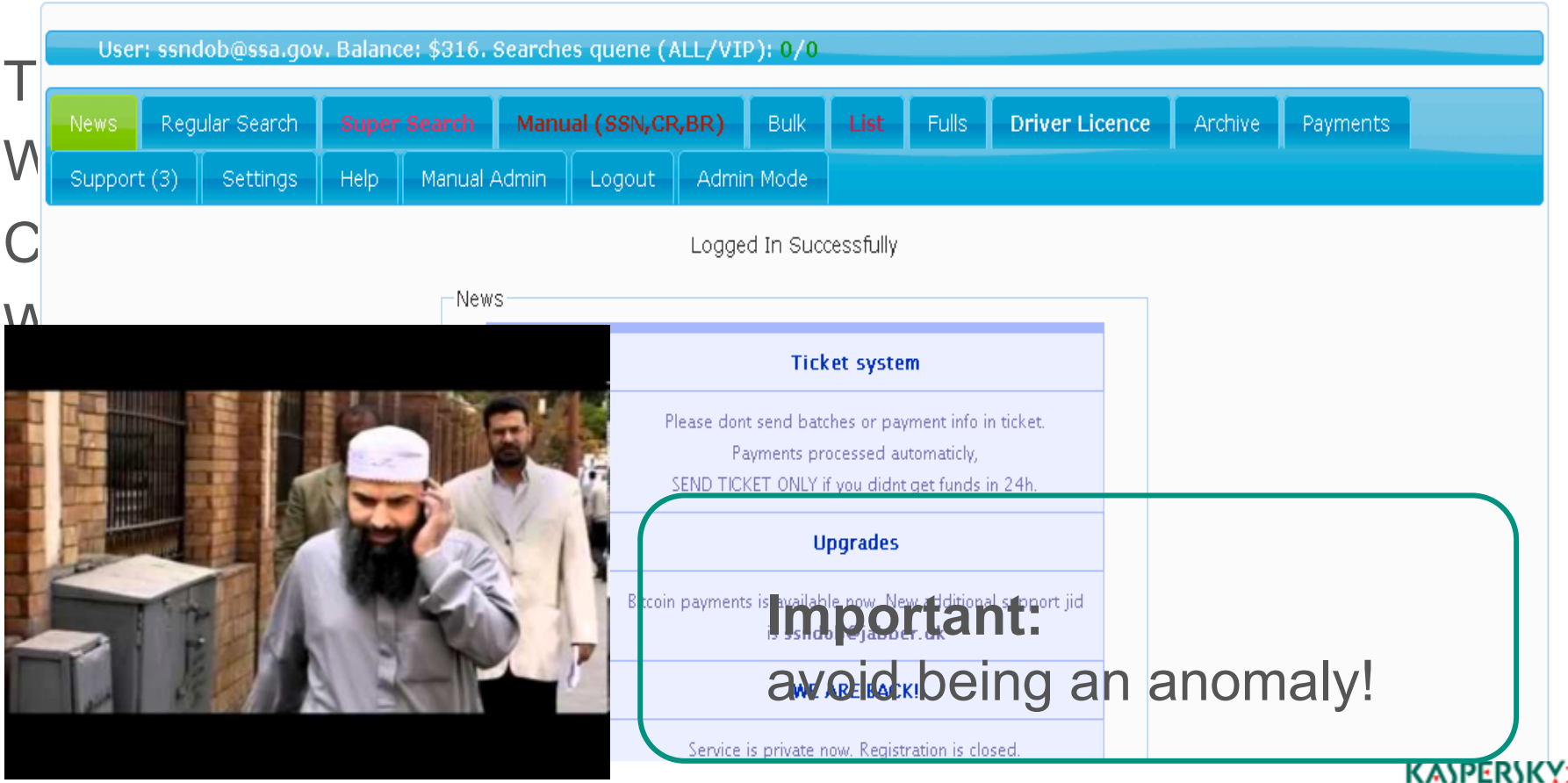
MASSIVE SURVEILLANCE – AGENCIES? NOT ONLY

T
W
C
W



MASSIVE SURVEILLANCE – AGENCIES? NOT ONLY

T
W
C
W



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

Externall

w

co

officer ?

Internally

co

tra

ta

ith

internally.

KASPERSKY lab

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

KASPERSKY lab

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.

ENCRYP

Overall

or inten

ckdoors

Obviously

g by default.

Anti-coerc

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:

KASPERSKY lab

ENCRYP

Overall
or inten

ckdoors

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

OCAP 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

KASPERSKY lab

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.

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 issu
as storing logs.

Cryptocat: young, minor issues like people joining yo

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

Look, better

Burner phon important there.

Be coherent and in your phone.

KASPERSKY lab

REAL WORLD

Don´t try to impress people – don´t be impressed when approached by an 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?

KASPERSKY lab

Vicente Díaz

Principal Security Analyst

vicente.diaz@kaspersky.com
@trompi