# OPSEC FOR SECURITY RESEARCHERS

*Dani Creus & Vicente Diaz*
Kaspersky Lab, Spain

Email {dani.creus, vicente.diaz}@kaspersky.com

## ABSTRACT

Being a security researcher nowadays is not an easy task, especially in times when we no longer deal only with technical aspects of security. The global picture of today's security landscape includes new actors such as governments, big companies, criminal gangs and intelligence services.

That puts researchers in a tricky situation.

It is not unheard of for researchers to be threatened by criminal gangs, or approached by intelligence services. On other occasions researchers have found themselves under surveillance or their devices have been compromised when on the road.

What precautions should we take in order to minimize risks? What can we do to avoid leaking information that could put us in an uncomfortable situation in the future?

Sometimes we are the public faces of research, while on other occasions we don't want to be in that position.

In some sense, we as security researchers have power and capabilities over some of the threats we analyse – for instance, we can shut down a cyber espionage operation. The main differences between us and law enforcement agencies are that attribution is not clear and we don't have any OPSEC training or capabilities to protect ourselves.

We believe that, as security researchers, it is very important to know OPSEC – our opponents certainly do!

## INTRODUCTION

The benefits of using electronic devices are obvious – however, sometimes we are not so conscious of the drawbacks. The digital footprint we leave with our digital activity may lead to our identification, and this could be especially worrisome in some sensitive environments.

Cyber espionage has a very low barrier to entry in comparison with the resources needed for traditional espionage. Additionally, our digital footprint is likely to last forever.

Both technically savvy and emerging countries are increasing their resources in this discipline, in some cases directly performing massive surveillance and selecting their targets when needed. There is no need for us to provide examples on this.

These resources are available not only to governments and law enforcement agencies. Many other actors have developed total or partial operative capabilities for following our digital traces now or in the future, with or without our knowledge.

Operational Security (OPSEC) is a term originally coined by the US Army as a process that identifies critical information and determines whether friendly actions can be observed by enemy intelligence systems, whether information obtained by adversaries could be interpreted to be useful to them, and then executes measures that eliminate or reduce adversary exploitation of friendly critical information. In a more general sense, OPSEC is the process of protecting little pieces of data that could be grouped together to show the bigger picture [1].

In this presentation, we analyse all aspects that a security analyst should take into account in order to minimize his digital footprint, what traces we leave, and which are the most dangerous in terms of the information we leak and how easily it can be used to track back to us.

We intentionally don't analyse counter-intelligence tactics that are used to try to manipulate our adversaries with the information we provide to them.

Finally, although this talk is focused in the digital aspects of operational security, rather than the 'real-world' ones, the real-world aspects cannot totally be ignored. Effective good practices in operational security should rely on both. We will provide some hints for the most basic situations related to the typical routines of security researchers.

## OPSEC 101

The golden rule in Operational Security is silence as a defensive discipline. If you don't really need to say something, then don't. If you do need to talk to someone, do it in a secure way where you don't compromise the content of your message and, if possible, don't generate metadata on the communication.

You need to learn how to blend into the masses, never be an anomaly in any sense [2], and keep your communications private between you and your interlocutor. Remember, the privacy of the message in your communication is as strong as the receptor is. So, again, silence is key. If you don't want anybody to know something, don't say it.

Security researchers such as The Grugq have shown in their presentations on the topic [3] how small pieces of information leaked in different environments have resulted in the identification of real people. One notable example is what happened with LulzSec and how their members were identified and arrested [4].

The main feature necessary for an effective OPSEC is not technical, but psychological: be meticulous, and paranoid to a certain healthy degree.

For given operations where electronic interaction is required, one very typical practice is the adoption of personas. That requires prior work on creating full background information and some resources to backup the stories. It is unusual not to find any *LinkedIn*/*Facebook*/*Twitter* profile or information in *Google* about someone. Using 'the persona' resource may be necessary under certain circumstances, but it's difficult enough to keep a single personality and do your daily work without leaving digital fingerprints, never mind using many of them and keeping them totally isolated and unrelated.

Contamination between personas is another typical (and fatal) error that increases in likelihood over time. So if you are forced to use personas, it's better to destroy them quickly after they have been used.

If we are to learn anything about how law enforcement has successfully identified suspects in operations, it is that electronic traces are eternal. In most cases, suspects started using OPSEC at some point in their lives, and previous data could be retrieved in order to identify them at a later point in time.

In other cases it was the sum of many small pieces of information that led to identification of the suspect. Sometimes these pieces allowed different personas and identities to be related. The lessons are: 1. avoid contamination between personas, and 2. remember that we leave many more traces than we think.

A single mistake can take down a complex OPSEC operation that has been successful for many years.

Another thing to consider is how to react when we are directly (digitally or not) confronted by people specially trained to manipulate their interlocutors. They will use many techniques such as compliments, pride or shame to provoke some kind of reaction. Under pressure we react differently. It is always a good idea, when having drinks with unfamiliar people, not to talk or brag about a piece of research you have done.

Don't trust anyone when talking about sensitive topics. In particular, don't trust anyone using any electronic means. This footprint will last forever, could be accessed by anyone, and whatever you say is stored somewhere. This could be used against you, even in a trial.

## WHAT TO DO

In this section, we provide some tips on how to deal with different scenarios:

Email:

- Always use cryptography for your communications.
- Keep in mind what kind of information you are giving and who is receiving it.
- Consider what kind of metadata you are generating, even if the content of the message is encrypted. From, To, Subject, Time, etc. are all in clear text.
- Consider the strength of your key and the encryption algorithm. The longer, the better.
- If your private key gets compromised, all the messages you have sent in the past will be compromised as well – so using email might not be a good idea at all in some cases.
- Be careful with third-party services, in some circumstances you should avoid them.

IM:

- You cannot trust any commercial service other than the ones using OTR.
- Again, keep in mind what you say and who is receiving this information. He may be logging the full thing.
- Never use *Skype* or any social network for discussing anything sensitive.

Telephone:

- Your telephone probably carries the same data as your computer – are you using the same security measures? Probably not because it's harder.
- Your telephone provides valuable information on your habits and location.
- When possible and applicable, use disposable phones.

HD encryption:

- Times are interesting now that *TrueCrypt* is no longer being developed. However, its use is still preferable to other solutions.
- Use an anti-coercion partition with real-looking data.

Browsing and research over computer networks:

- Never do anything 'dangerous' from your home or workplace. Use an air gap instead, with a 3G/4G connection using an anonymously acquired modem.
- VPNs encrypt your traffic but do not provide anonymity!
- Tor is not bad in most cases, but be aware of its weaknesses: Tor exit nodes, Tor middle nodes with high reputation controlled by the same organizations than can track back to you, correlation of Tor connections with your ISP connections to identify who you are.
- Do not accept cookies, do not allow the execution of JavaScript, do not log into any account, and do not use *Chrome*.

Physical world:

- When on the road, travel with the bare minimum possible. A travel phone and travel laptop is preferred.
- Do not carry more data than necessary for your work.
- The smaller the hardware attack surface in your laptop the better: be aware of hardware implants.
- Do not leave your hardware alone in your hotel room.
- Be aware of your environment, try to find suspicious patterns.
- To some extent, your close circle should be aware of basic social engineering techniques that can be used against them as well.

These tips, along with some others, will be explained in detail in the presentation, along with examples of threats, problems, solutions and open questions.

## CONCLUSIONS

OPSEC should quickly be adopted in a routine manner in the daily activities of security researchers. Given the kind of operations that are being discovered, and the actors involved, the lack of the proper knowledge and discipline in this area may result in terrible consequences for researchers doing their jobs.

We want introduce all of these difficulties and point out solutions for most of the scenarios. Some of them are hard to solve, and when we start looking into real alternatives for some of the problems we face we discover that, in many cases, there are none. In other cases, the solutions we use have many problems or are directly broken, as we are discovering in the light of some recent information.

But even if we don't have a perfect solution, we should make it as hard as possible for anyone to track us digitally. The first step is knowing how bad the problem is, and then selecting the best choices we have to stay safe and anonymous, and to protect our information. Finally, we should be aware of the drawbacks of the existing solutions.

These are the first steps towards adopting this discipline in our daily lives and automatically taking advantage of it. In our experience, we still make many mistakes, and yet in many cases we don't care about using the minimum precautions: we believe that, as experts, nothing bad can happen to us.

This is a mistake we need to eradicate as soon as possible, and we hope this presentation will be a step in the right direction.

## REFERENCES

[1] Operations security. Wikipedia. https://en.wikipedia.org/w/index.php?title=Operations_security&oldid=614191894.

[2] Omar, A. OPSEC Failure of Spies. Black Hat 2013. https://media.blackhat.com/us-13/US-13-Cole-OPSEC-Failures-of-Spies-Slides.pdf.

[3] Hacker OPSEC. http://grugq.github.io/.

[4] OPSEC for hackers: because jail is for wuftpd. http://www.slideshare.net/grugq/opsec-for-hackers.