Don’t act so surprised – You were always an obvious target

June 22, 2015 | Frode Hommedal

Expectations. We all have them – we all have them, and we all get a little upset when they are unfulfilled. Or sometimes more than just a little, to be honest. Unfulfilled expectations can trigger strong reactions of disappointment and resentment. Maybe you’re experiencing some right now. You thought you were going to read about espionage and here I’m serving you psycho-babble.

But let me put your mind at ease right now. This essay is about our adversaries' target development process, and about how I believe a base rate fallacy on our part makes us blind to important parts of it. **We tend to mix up "being prioritized targets" with "being obvious targets"**, and that’s the topic I want to comment on in this essay. But I want to do that by telling you a story, and our story begins in Russia – but maybe not in the way you expect.

This essay is about our adversaries' target development process, and about how I believe a base rate fallacy on our part makes us blind to important parts of it.

Deus ex machina

Not long ago Duqu 2.0 was all the rage in the security community. What is Duqu 2.0, you ask? Well, it's a very advanced espionage toolkit used to spy on the Russian company Kaspersky at its offices in Moscow. Not only Kaspersky of course, but Duqu's current claim to fame is the fact that it was used to attack Kaspersky – a cybersecurity company with customers all over the world, including countries in the Middle East, like Iran. Duqu 2.0 was suddenly and unexpectedly discovered as a developer at Kaspersky was compiling and testing a new detection algorithm for detecting advanced threats on his own computer. What a test run that turned out to be.

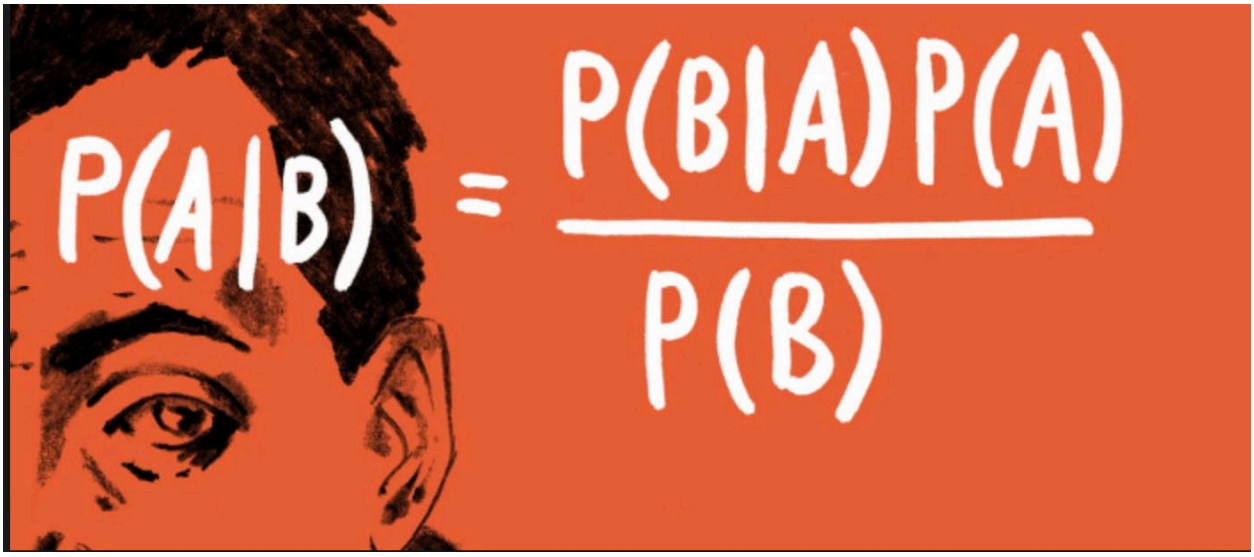
In the wake of the news there surfaced a lot of reactions, even rage, over the fact that a security company was targeted

The world got to know about this after Kaspersky went public with the incident, and in the wake of the news there surfaced a lot of reactions, even rage, over the fact that a security company was targeted by what is believed to be a national intelligence agency. Israel has been suggested as the culprit, but who knows. It would make sense if it was the Israelis, but it doesn't matter for our story.

What matters is that the attack has been called a "watershed event", as if this was some sort of collective cyber Rubicon crossing on the intelligence community's part. Others have acted all surprised by the fact that security companies have become targets of cyber espionage.

I believe security companies have always been obvious targets for espionage, and failing to recognize this I think is some sort of base rate fallacy.

A lot of people disagree of course, and I don't see it that way either. First of all Kaspersky isn't even the first security company to get hit. Look, for instance, on the RSA and Bit9 breaches. I believe security companies have always been obvious targets for espionage, and failing to recognize this I think is some sort of base rate fallacy.



I will not try to explain in-depth why I believe security companies are obvious targets for espionage in this essay. Others have done that already, and to be honest, it quickly becomes fairly obvious once you start thinking about it. Rather, I will try to explain why I think these reactions are based on a form of base rate fallacy, and I will do that because **I think the Kaspersky breach has revealed a giant blind spot for many companies and even security professionals: How we understand the targeting process of our adversaries.**

But first I must take you on a journey: My journey into cyber counterintelligence.

A long time ago in CSIRT far, far away…

I used to work for a national CERT. Years ago, after having heard the eerily sounding term "targeted attacks" for the first time, and then shortly thereafter being involved in the response and analysis of such attacks, I had a real awakening regarding the kind of work we were doing as defenders, as I guess many fellow information security professionals had.

Why was it such an awakening? Because detecting and responding to industrial espionage and intrusions into critical infrastructure and the core of the government had little to do with what we were doing when I first joined the information security

community and said national CERT. Then we were forwarding abuse reports to ISPs, sending out vulnerability alerts to our constituency and coordinating the take-down of phishing sites – with the occasional mass-infecting worm to worry about.

And let's be honest: It was relatively mundane routine work to increase the health of the Internet ecosystem. We were basically Internet janitors, and that was fine by us. We liked the Internet, and wanted to help keeping it clean.

We were basically Internet janitors, and that was fine by us. We liked the Internet, and wanted to help keeping it clean.

But our job descriptions slowly changed, and after a couple of years all we were doing was responding to espionage intrusions. Eventually it literally took all of our time, trumping all former priorities. But really understanding what that change meant took some effort. For me personally it took endless nights of struggling with cases, concepts and terms, trying to fit what I saw and experienced into mental models that made sense. But finally I realized that what we were fighting was espionage. I found no other label that fit what we were seeing and fighting.

It seems glaringly obvious now, right? But back then – I promise you – it didn't.

See, we were engineers. For the most part we were relatively young bachelors and masters of computer science. And this was long before espionage and cyber counterintelligence became marketing buzzwords. No one ever told us we were going to fight spies and intelligence agencies.

But the incidents we handled more and more often was cyber espionage, and the people we were sent to fight in daily hand to hand cyber combat were the operators of the cyber end of state sponsored intelligence collection.

No one ever told us we were going to fight spies and intelligence agencies.

We were no longer Internet janitors. To put it dramatically we were front line defenders under full assault.

This was not what we signed up for, but it was where we eventually found ourselves. And we had to learn the ropes by ourselves, because no one had prepared us for it, and to be honest, no one was there to help us figuring it out either.

And we learned the ropes. We didn't give up. We hung in there, and even got pretty good at our job. But then came another challenge: Trying to convince everybody around us of what was going on. Trying to explain to people that no, this wasn't just a computer virus, it was an espionage operation. It wasn't an IT problem, it was a risk management issue. And yes, they had been targeting us all for a long, long time without us even noticing or knowing about it.

But then came another challenge: Trying to convince everybody around us of what was going on.

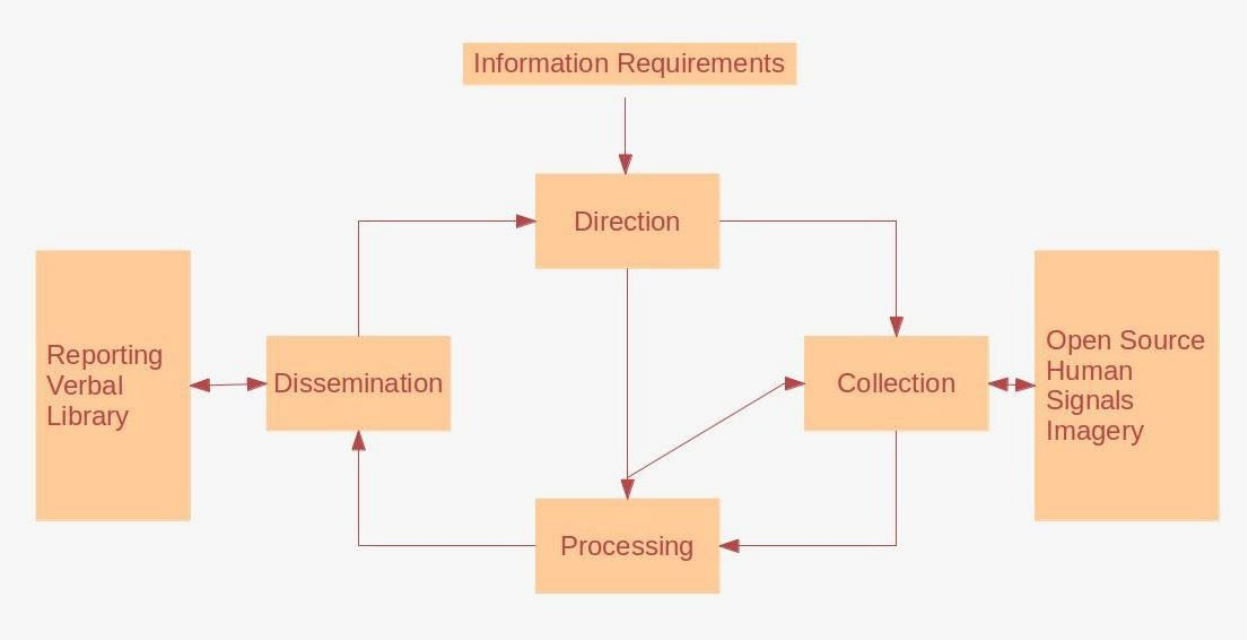
That proved to be the toughest challenge of all.

Understanding your adversary

It seems so long ago, and in Internet time it is. But it has only been around five years. The challenge of convincing people, both constituents, peers and managers, is still there though. And there are still a lot of defenders who can't draw some version of the intelligence cycle – the abstract process of our adversaries' collection and analysis capabilities – on a whiteboard and relate that to the adversary's operation they are currently looking at, and tie that back to a plausible goal of the operation.

How can you possibly have any real appreciation for the risk espionage exposes you to if you don't understand the mechanisms of intelligence collection, production and dissemination?

To me, this represents a problem – sort of a meta-problem. Because to quote Pink Floyd, how can you have any pudding if you don't eat your meat? That is, how can you possibly have any real appreciation for the risk espionage exposes you to if you don't understand the mechanisms of intelligence collection, production and dissemination?



If we as defenders don't understand this, how can we inform our decision makers? And if we don't, who will? I mean, no one else is looking at the intrusions. Decision makers all over the world are making bad risk management decisions because we don't inform and advise them properly.

Decision makers all over the world are making bad risk management decisions because we don't inform and advise them properly.

Actually, I need to re-iterate that: Decision makers all over the world are making bad risk management decisions when it comes to what they all collectively think of as “IT”, “cyber” and sometimes “cloud”.

Very, very bad risk management decisions.

But I believe it’s because they don’t know better. They are ill-informed. They are ill-advised. Or at least I hope that’s why. Sure, they also often seem to care a lot more for short term economic gain than longer term risks, but we also haven’t given them the decision support they need to make informed decisions.

Aside: If you suspect you are an ill-informed decision maker, engage your security people and start asking for updates on the threat landscape and the risks it exposes you to. I will write more on this topic in the future, but in the meantime you may benefit from reading this and this.

Update: A colleague of mine gave a remark the other day that was spot on. Sometimes managers aren't ill-informed. Sometimes they are are just being ignorant, and incompetent at making risk based decisions. The Sony case seems to give ample demonstration of such a situation.

Our slow, uphill struggle for improvement

We try to improve, though, as a community. And we are getting better. Lots of really bright people are constantly contributing to our curriculum. This lets us analyze and understand our adversaries' operations much better. The kill chain model, for instance, is a great analytical tool. So is the diamond model of intrusion analysis. The whole idea of intelligence driven defense has changed our community on so many levels.

The whole idea of intelligence driven defense has changed our community on so many levels.

But although immensely useful when analyzing intrusions, these methods are still rather low level analytical tools. If you can't map your findings to the enemy's overarching process, I believe you will find yourself unable to use them effectively to defend yourself, both on an operational and tactical level – and certainly on a strategic level. And these tools, by the way, are only used by the really mature defenders. Lots of defenders haven’t even heard of these methods.

If you can't map your findings to the enemy's overarching process, I believe you will find yourself unable to use them effectively to defend yourself.

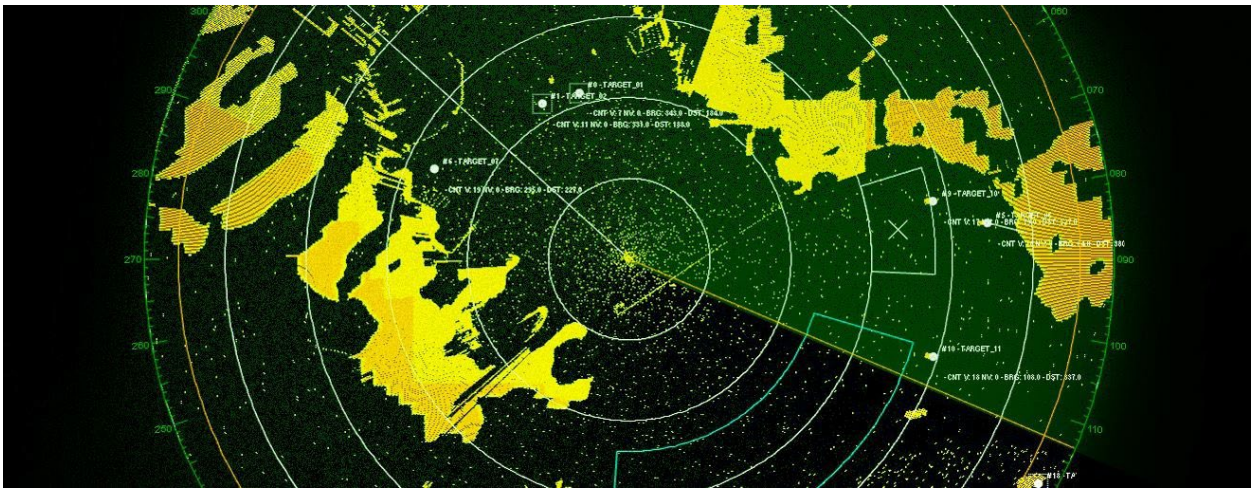
This, I believe, is a major reason why a lot of organizations still handle "computer viruses" as an IT problem, not a risk management issue. And so we fail at securing ourselves, our customers and our nations again and again.

Target development

A vital part our adversaries' preparation to infiltrate our networks and steal, manipulate or disrupt is target development. **This basically is the "targeted" part of "targeted attacks"**, and a very important part of the intelligence cycle or process or whatever you want to call it. Anyone can fire a web exploit during a watering hole attack or send a spear phishing email, but not everyone can identify and target exactly the right people and systems at the time they need it done.

Not everyone can identify and target exactly the right people and systems at the time they need it done.

Target development is difficult work, maybe even an art form. It is vital to the success of an espionage operation, and something that separates great intelligence capabilities from mediocre ones, dangerous adversaries from less dangerous ones.



In military terms it's the difference between bombing and burning a city to the ground and still possibly missing your intended target, instead of sending one cruise missile to hit exactly the right target to knock out exactly the right capability at exactly the right time to achieve one specific goal.

Or imagine you're engaged in contract negotiations, and you're not above committing a bit of cyber espionage. Knowing exactly who to hit, when to hit and how to both hit and

find the specific information you're after is what separates your success from a failure. All of that is either part of or adjacent to target development.

I personally know of one particular case where exactly such an intrusion occurred, and cost a company an estimated $100.000.000.

Yes. That much in one operation – because it hit exactly right at exactly the right time. Right for the adversary, anyway.

Tactical needs for information like this are one reason why we have intelligence agencies in the first place, and the reason why they are spending lots of resources on target development. The most skilled ones are straight up scary to watch in action. You just have to marvel at their ability to find your weak spots, and abusing them.

The most skilled ones are straight up scary to watch in action.

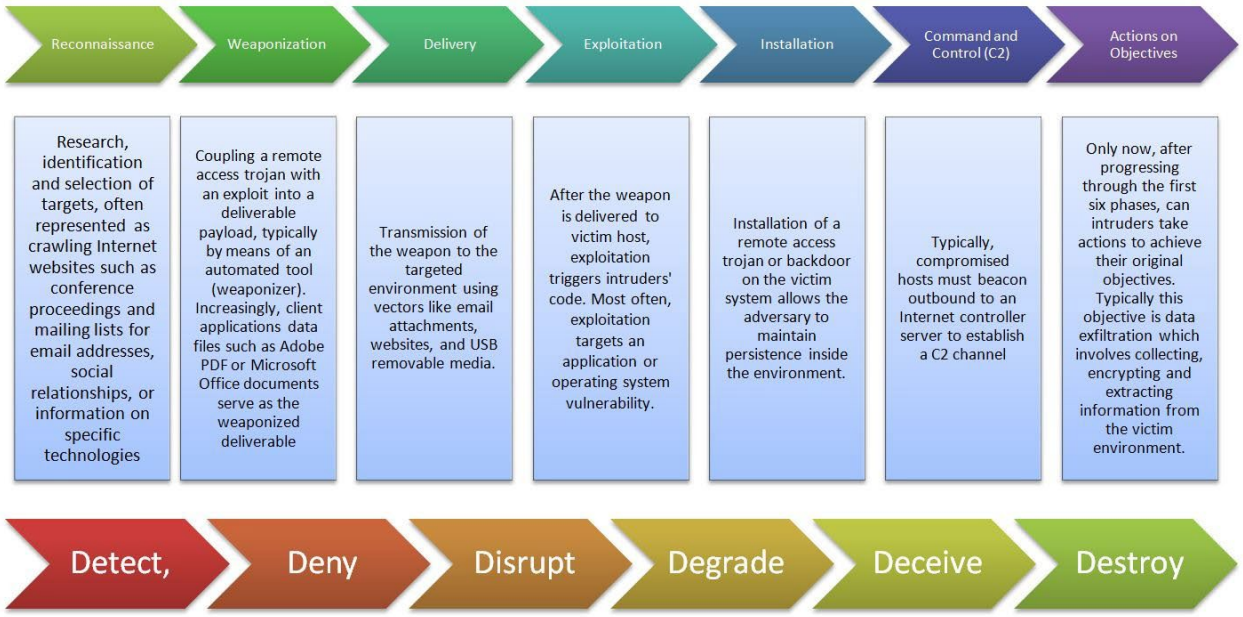
So how is this done in practice? A rare glimpse into the real world target development at a big intelligence agency is given by classified NSA material leaked by Mr. Snowden back in 2013. It's called "I hunt sys admins" and was published by The Intercept in 2014. It seems to be from an internal NSA blog, and the person who wrote it goes into quite some detail on how you could go about if you wanted to find and exploit system administrators to reach your goal of stealing information from an organization.

You should read it. It makes for a really fascinating and chilling read.

The gist of the blog post is simple enough though. Identify a system administrator by looking at traffic patterns from their computer in your SIGINT data, or even just via LinkedIn, and compromise them through their Facebook account or personal email account. Then use it to gain access to the systems of the company they work for to achieve your original goals. Voila.

As defenders, understanding how our adversaries work to gain access to our systems and information is crucial for our success, because it tells us where to look and who and what to protect.

In the kill chain model, target development is best covered by "reconnaissance". In the diamond model it's covered by the victim vertex. In F3AD it's covered by "find". But only briefly and implicitly.



You will have to spend a lot more time on the concept to grasp the implications, but when you do, buzz terms like "supply chain attacks" won't seem special at all.

It's just that during the target development process, that supply chain was found to be the weakest link, the least risky path or for some other reason chosen to be the preferred attack vector to reach a specific collection goal after careful target development.

Being an obvious target

So where am I going with all this? Well, as I stated in beginning:

You have <u>obvious</u> targets, and then you have <u>prioritized</u> targets.

From the defending side of things, you will have a hard time figuring out when you're going to get hit by an espionage operation. But you can figure out what kind of espionage operations you are an obvious target for, and to some extent how obvious, and which parts of your organization are most likely to get hit, should it happen.

You can probably get far by understanding the value of your assets to the archetypes of threat actors out there. This was one of the points I was touching upon in my previous essay, See it coming: The Four M's of Digital Espionage.

Now, if you discover incidents, you will get an indication on how much of a prioritized target you are. The more incidents brought onto you from the same threat actor, the

more of a prioritized target you probably are for that particular threat actor. And if you analyze incidents and are unable to place them into one of the larger categories of espionage operations you expect yourself to be an obvious target for, you must revisit your assumptions.

The more incidents brought onto you from the same threat actor, the more of a prioritized target you probably are.

Whether you are an obvious target or not depends heavily on what kind of information and access to information and systems you have or can provide. Whether you are a prioritized target depends much more on the current strategic, tactical and operational need of your adversary, whoever that might be. This is much more unpredictable.

The Belgacom case demonstrated that they were a prioritized target for what seems to have been the British signals intelligence agency, GCHQ. But for other telcos it clearly demonstrated that we were obvious targets for the great nation state threat actors.

We should of course act accordingly.

So maybe most of the time security companies and response teams aren't prioritized targets, but at no point were we not obvious targets. We are the sworn enemies of our adversaries. We live to find and fight them. An adversarial

relationship cannot get any more obvious than that. So it boils down to whether we're prioritized targets or not.

Kaspersky being hit by Duqu 2.0, along with the Bit9 and RSA breaches, are just known examples of security companies becoming prioritized targets of offensive cyber espionage operations.

So maybe most of the time security companies and response teams aren't prioritized targets, but at no point were we not obvious targets.

The problem arises when people confuse the evidence of how prioritized targets security companies seem to have been with how obvious targets such companies are. In my judgement they have always been obvious targets. We as a community have always been obvious targets. We should expect to be hit by cyber espionage. We should expect to see nation state intelligence collection capabilities being deployed against us.

Update: It seems like the NSA and GCHQ have been targeting AV companies for years, if you are to believe a recently released this article by The Intercept.

We should expect to be hit by cyber espionage. We should expect to see nation state intelligence collection capabilities being deployed against us.

As security companies are slowly catching up with the offensive capabilities of the big nation state threat actors, maybe we will see a shift in how prioritized targets they are. In the future information security professionals, CSIRTS and security companies may even become highly prioritized targets.

Now, that I *really* didn't sign up for.

I have no intent of backing down, though, and I hope you won't either. But what we collectively need to do as defenders is waking up and smelling the coffee, and start expecting the Spanish inquisition.

We are obvious targets. At some point they will probably come for us. Then we better be mentally and otherwise prepared for it.

P.S. Previous instalments in this series of essays include Dance like a Dragonfly, sting like a Bear and See it coming: The Four M's of Digital Espionage. And as always, if you found it useful I'd appreciate if you help me spread the message, and if you have comments, please leave them below. Thank you for reading.