See it coming: The Four M’s of Digital Espionage

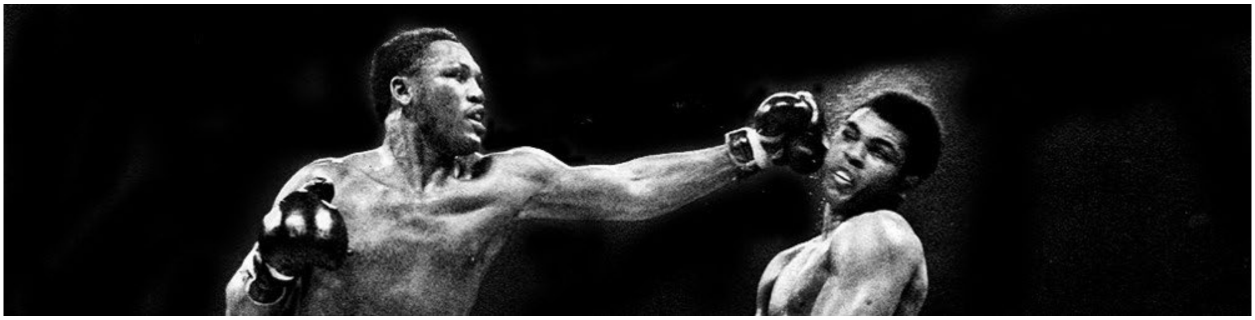
September 21st, 2014 | Frode Hommedal

We read about espionage in the papers almost weekly, but can you tell me how your company expects to be hit by cyber espionage? If not, you are in good – or perhaps bad – company. Threat perception is still a challenging area for most, and poor threat perception will render you vulnerable. It's time to change that. It's time to start understanding the attacker. Say hello to «the Four M’s of Espionage».

Or, let's postpone the introduction just a minute. Let me ask you another question first: Why is it important to be able to anticipate the espionage and intrusion attempts? Why should you worry yourself with trying to see it coming? To heed Sun Tzu's advice, and avoid being caught off guard.

Being caught off guard

It is slowly dawning on us that it is really hard to defend our networks, our systems and our digital assets in the rather unfriendly environment that we call cyberspace, the internet or just plain everyday digital life.



By now I guess we have all more or less accepted that intrusions can't be completely prevented, and that we must deal with the fact that our networks and systems will, at some point, be infiltrated, be broken into. There are no silver bullets. There are no magical security appliances.

Achieving a reasonable level of security is actually really hard when espionage is a real threat to you. And unfortunately, espionage is a real threat to many of us.

It never helped anyone being caught off guard.

But still, it never helped anyone being caught off guard. In a fight you will sustain a lot more injury if you can't anticipate the blows from your opponent. In the digital world, not seeing the attacks and infiltration attempts coming will pose major challenges to the efficacy of your security efforts. Not understanding – or maybe not even noticing – when and where you are under attack, will in itself make you more vulnerable.

The four M's

So what are the four M's of espionage? It is the motivation, the mission, the mindset and the methods of the attackers. Why will understanding them make you less vulnerable? Because understanding them will help you build situational awareness. Who are the enemy forces, and where, when and how will they attack? It will help you because it will afford you the opportunity to tailor your security efforts to the vulnerabilities and threats that are actually putting you in harm's way. And at the boardroom level, understanding the four M's will inform your risk management process, and enable you to spend time and money where it matters most.

When you have grown an understanding the four M's, you can start anticipating the digital blows from the attackers; the infiltration attempts towards you and your networks; the cyber espionage missions mounted against your company and nation.

Every security professional should have a strong understanding the four M's of espionage.

I believe every security professional should have a strong understanding of them in order to strengthen our collective, defensive posture against the attackers. Without knowledge, we fight blindly. When fighting blindly, we lose.

I will get back to the four M's in a bit, but before I do that, I want to discuss why I think this matters so much a bit more.

Why it matters

As a security professional I guess you often hear people tout how important it is that you, that we in the security community, understand the business and the business needs. You need to be «business savvy», they say. People love putting «business savvy security whatever» on their LinkedIn profiles. And it is of course true. Why? Because the security effort has to be tailored to the business needs. Or rather, tailored to the strategic goals of your company or organization. Otherwise the whole effort could be pointless.

If your security efforts aren't tailored to your particular threat landscape, your security efforts are much less effective.

Well, it's exactly the same with threat perception as with business savvy. If your security efforts aren't tailored to your particular threats, they are probably much less effective than they ought to be, maybe even bordering pointless. Just as they may be boardering pointless if they aren't tailored to the strategic goals.

This means that business needs sometimes trump security, and it means that security requirements sometimes trump business. Whatever contributes most to the overall strategic goals is given priority. Or so it should. But pulling this off requires knowledge and insight.

Whenever I hear the phrase «business is in business to do business, not to be secure», I normally assume that I'm talking to a person who doesn't understand risk. Because the business, or company, is *only allowed to stay* in business because it is able to balance the risks and come out on top more often than not. And these days that often requires a bit of security.

The company is only allowed to stay in business because it is able to balance the risks. These days that often requires a bit of security.

We are now getting close to the much announced discussion of the four M's, but before we dive into the details, I want to give you a brief summary of different kinds of threat actors that may end up mounting espionage missions against you, your company and your networks. That way you can hopefully imagine and visualize them with more ease when we discuss their motivation, their missions, their mindset and their methods.

The Threat Actors

Nation States

When it comes to mounting espionage missions, the most obvious kind of threat actor is of course the big, **nation state intelligence agencies**, like the US NSA, the UK GCHQ, the French DGSE, the Chinese 3PLA, the Russian FSB and the Israeli 8200.

These are all well known, and also known to be very active and with impressive capabilities and capacity. Their primary concerns are producing strategic intelligence for decision makers, supporting counter terrorism efforts and, in some countries, conducting industrial espionage for national industries. And they are known to target almost anyone and anything if it can help them advance their mission. They play by totally different rules than the rest of us.

Private companies can solicit help from intelligence services to conduct industrial espionage.

In several countries, like e.g. China, private companies can solicit help from intelligence services to conduct industrial espionage. France has been accused of this. Israel has been at it for a while. Even the NSA has supposedly been caught with their hands elbow deep in the cookie jar, and have plans to go deeper still.

Personally I believe we must expect this from a wide range of countries – if not all. Sadly, the evidence collected over time is just too overwhelming.

Contractors and enablers

Then you have a **big grey market of private corporations that governments contract** to run espionage campaigns and other types of intelligence activities. In the US, companies like Palantir Technologies, Berico Technologies, HBGary and Booz Allen Hamilton are examples of such contractors. Other countries probably have the same market for contractors.

What these contractors do with their offensive cyber capabilities when they aren't working for the government is something that is starting to worry me a bit.

Then you have another **big grey market of «enablers»**, companies that enables governments to spy. In this group you find suppliers of systems for so called «lawful interception», and companies that develop toolkits for offensive cyber operations. The most known one is perhaps the Gamma Group, which sells the FinFisher and FinSpy surveillance package, but you have several others.

Unfortunately there have been several examples of interceptions that weren't always all that lawful, and of customers of surveillance systems that weren't all that accountable. With little oversight and regulation, this is a market that I fear could spiral out of control, if it hasn't already.

And private companies can already rent **«hackers for hire»**. The Indian corporation Appin Security Group has been accused of selling their services to private companies, in addition to being a contractor to the Indian government.

The criminal underground

Then you have the black market, where anyone with money and the right – or wrong – connections can rent more or less structured «hacking outfits» from the digital underground. As the cyber underground economy grows, there are worrying signs that we are getting more and more specialized outfits that are building very advanced capabilities.

In a couple of years, some of these outfits may acquire capabilities that can match regular intelligence agencies within some domains. They may also acquire personnel from intelligence agencies and contractors, persuaded to a change in career by much higher salaries.

There are signs that this is already happening in e.g. China and Russia. And for both China and Russia there are also speculations that such groups are allowed to exist, as long as they don’t operate within their own country, don’t upset the regime and that they «lend a hand» to the government, when asked. This group of threat actors is probably one to watch in the coming years.

[Hacking] groups are allowed to exist, as long as they don't operate within their own country, don't upset the regime and that they «lend a hand» to the government, when asked.

Then, of course, there are the **criminal groups** that mount their own espionage missions to advance their criminal endeavors. Some groups have already specialized in breaking into data brokers to collect information on individuals, and large scale fraud is happening regularly after criminals have infiltrated private corporations and banks for weeks and months. There are also lots of examples of criminals hiring «hacking outfits» from the black market.

Chaotic actors

The last kind of threat actor I will mention is the lone **«hacker», or «hacktivists»**. These are people that may try to get into your network to steal information or break things just for the challenge or for a cause, political or other. These actors are sometimes – rightfully – called chaotic threat actors.

Bottom line

The bottom line is this: The threat actor landscape is diverse, and it's expanding. You could probably not keep track of it even if you tried. But the good news is that at some level, they all operate off the same playbook. This is where the four M's of espionage comes in, and now it's time we take a closer look at them. We will start with the one we have already briefly touched upon, the motivation.

The threat actor landscape is diverse expanding, but at some level they all operate off the same playbook.

The Motivation

Sometimes when you hear people talk about cyber security incidents, they talk about «computer viruses», like it was some decease their systems contracted. When it comes to espionage, this is of course far from reality.

These «viruses» are security incidents, and the results of deliberate actions from hostile entities.

What sometimes seems elusive to people is that these «viruses» are security incidents, and the results of **deliberate actions from hostile entities**. When it comes to espionage, the fundamental motivation, at an abstract level, is gaining an advantage in a competitive landscape.

No competition, no need for espionage. Espionage is an activity your engage in to gain a competitive edge over someone else.

Espionage is an activity your engage in to gain a competitive edge over someone else.

The following list contains examples of some very high level motivations for carrying out cyber espionage against you and your networks:

- Gaining a **long term strategic advantage** over you, or someone else through you, by accessing your information.
- Gaining a **strategic ability** by controlling or manipulating your systems.
- Gaining a **tactical victory** over you, or over someone else through you, by accessing your information or controlling or manipulating your systems.

An example of how to gain such a long term strategic advantage is to continuously steal all research and construction plans from a range of competing companies in your business, to enable you to stay technologically ahead of them. This is basically what the «APT1» actor, amongst others, has been accused of doing on behalf of the Chinese industry.

Another example is to gain an advantage in the stock market by continuously spying on a mergers and acquisitions company to get access to inside information. I don't have any examples of this, but it would surprise me a lot if this isn't going on.

Update: It was indeed going on. FireEye wrote about it already in June 2014, and again after I published this essay, FireEye released a report detailing a possible American group spying to beat the stock market in December 2014.

The ability to turn off the power grid and the telecommunications networks in different regions in a neighbouring country is an example of a strategic ability. This is the general direction where the speculations on Dragonfly are heading, as I commented on in my previous essay. A chilling thought, indeed.

Yet another example is the ability to turn a telco's infrastructure into a listening post for your spying on the telco's customers, e.g. any terrorist subjects or state and industry leaders that communicate via that telco. This is one of the things that GCHQ has been accused of doing in Belgium and in Germany, following the Snowden leaks.

If you did any of the above just once, for a time limited, specific purpose, I would call that a tactical operation, and a tactical victory, if successful. There are several examples of this happening to companies that have engaged in e.g. contract negotiations with Chinese companies.

The distinction between strategic and tactical may seem marginal, but tactics wins your battles by completing specific goals, while strategy wins you wars by gaining advantages.

Spying on you gives the threat actor – your adversary – some kind of advantage over you, or someone else through you.

The takeaway is that espionage is motivated by the fact that spying on you gives the threat actor – your adversary – some kind of advantage over you, or someone

else through you. And no matter who is the intended target, you and your company stand to lose control, trust and money.

You and your company stand to lose control, trust and money.

It is the cyber espionage missions mounted against you from your strategic adversaries that should worry you the most.

The Mission

A very important thing to understand when it comes to cyber espionage is that the people who are rummaging through your networks, servers and files didn't just stumble in from the streets on random. **They are highly trained professionals – cyber special forces so to speak – who have been purposely deployed within the perimeters of your network.**

They have orders to be there, and are right where they are expected to be. **They are on a mission, and you are the target. Your network is their area of deployment.** For a typical cyber espionage deployment, an important part of the mission will be to gain and sustain access to your networks over time.

They are on a mission, and you are the target. Your network is their area of deployment.

The following list is an example of how one such a mission into your networks could be described:

- **Identifying and developing you as a target**, doing reconnaissance and planning how to breach your defenses.
- Deploying within your networks by **gaining and sustaining access** to key elements within your ICT infrastructure through any suitable means.
- Carrying out the necessary actions to **achieve the goals** of the planned mission. What these goals are will depend on the motivation behind the mission, but the

deployed team probably has a set of information requirements, a **«shopping list»** of information, they are supposed to deliver on.
- Harvest login credentials and possibly deploy well hidden **«deep implants»** in your infrastructure as re-entry points for whenever the team is ordered to re-deploy within your networks.
- When the deployment is over, **clean up all tracks and leave** your networks, only leaving behind any «deep implants».

This is of course not a blueprint for every cyber espionage mission out there, but I do believe that a large portion of them would fit loosely within this description.

If you don’t look really hard, you probably will not spot them.

The takeaway is that there is a plan that is being executed, and it is being executed by professionals. These are professionals who know how to break into and hide within your typical corporate network environment.

```
Fri Aug 08 10:36:58 2008] [error] [client 87.106.191.136] File does not exist: /errors.php
Fri Aug 08 12:18:24 2008] [error] [client 85.214.97.225] File does not exist: /errors.php
[Fri Aug 08 12:35:52 2008] [error] [client 201.235.176.120] request failed: error reading the headers
[Fri Aug 08 15:02:35 2008] [error] [client 122.161.56.36] client denied by server configuration: /.htpasswd
[Fri Aug 08 15:04:58 2008] [error]

==> access.log <==
131.203.76.50 - - [08/Aug/2008:19:01:19 -0700] "GET /favicon.ico HTTP/1.1" 200 42627 "-" "Mozilla/5.0 (Windows; U; Window
74.6.8.121 - - [08/Aug/2008:19:01:21 -0700] "GET / HTTP/1.0" 200 14123 "-" "Mozilla/5.0 (compatible; Yahoo! Slurp; http:/.
131.203.76.50 - - [08/Aug/2008:19:01:22 -0700] "GET /favicon.ico HTTP/1.1" 200 42627 "-" "Mozilla/5.0 (Windows; U; Window
64.91.220.28 - - [08/Aug/2008:19:01:27 -0700] "GET /feed/atom/ HTTP/1.1" 302 569 "-" "Mozilla/5.0 (Windows; U; Windows NT
64.91.220.28 - - [08/Aug/2008:19:01:28 -0700] "GET /feed/atom/ HTTP/1.1" 302 569 "-" "Mozilla/5.0 (Windows; U; Windows NT
66.150.96.121 - - [08/Aug/2008:19:01:28 -0700] "GET /feed/ HTTP/1.1" 200 301 "-" "FeedBurner/1.0 (http://www.FeedBurner.c
64.91.220.28 - - [08/Aug/2008:19:01:28 -0700] "GET /feed/atom/ HTTP/1.1" 302 568 "-" "Mozilla/5.0 (Windows; U; Windows NT
64.91.220.28 - - [08/Aug/2008:19:01:29 -0700] "GET /feed/atom/ HTTP/1.1" 302 568 "-" "Mozilla/5.0 (Windows; U; Windows NT
64.91.220.28 - - [08/Aug/2008:19:01:29 -0700] "GET /feed/atom/ HTTP/1.1" 302 568 "-" "Mozilla/5.0 (Windows; U; Windows NT
74.6.8.121 - - [08/Aug/2008:19:01:38 -0700] "GET /htaccess/mod_rewrite-tips-and-tricks.rdf HTTP/1.0" 200 8500 "-" "Mozill
 - - [08/Aug/2008:19:01:41 -0700] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 460 "-" "Mozilla/5.0 (Window
```

If you don’t look really hard, you probably will not spot them, and if you don’t analyze really well, you probably will only uncover some of their presence. And if you manage to detect them and throw them out, they may re-enter at will if you don't also find and remove all «deep implants» and change any harvested login credentials.

They may re-enter at will if you don't also find and remove all «deep implants» and change any harvested login credentials.

The Mindset

You, your colleagues, your vendors, your partners and suppliers are probably used to think in terms of what technology was designed to do. You use and expect printers to print, and not much else. You use and expect the mail servers to relay emails, and not much else. Just like I do, and almost everyone else for that matter.

But your adversary's cyber special forces – or «hackers» if you like – don't look at your hardware infrastructure and software services and ask «what is this supposed to do». They ask **«how can we subvert this»** and **«what can we make this do»**, **«how can we break into it»** and **«how can we hide within it»**. More often than not they will show extreme resourcefulness when **turning your technological infrastructure against you**, without you even knowing.

They will show extreme resourcefulness when turning your technological infrastructure against you, without you even knowing.

And like any special forces, these teams avoid all unnecessary risk through proper training, planning and preparations, and through tradecraft and strong attention to operational security.

Some threat actors are more risk averse than others, but in general, **teams carrying out digital espionage or preparing for sabotage will be careful, will use deception, will cover their tracks and will monitor your actions to see if you are on to them**. And if they detect that you are on to them, they will immediately respond, one way or the other, most likely by trying to divert your attention while they cover their tracks and disappear.

Attackers have a different mindset than your workforce and even your defenders, and it needs to be understood if you want your security efforts to really matter.

The takeaway is that unless you start thinking like an attacker, or employ people who do, you probably would not know where to look for these intrusions, even if you decided to start looking. Attackers a have different mindset than your workforce and even your defenders, and it needs to be understood if you want your security efforts to really matter.

The Methods

It is highly likely that skilled cyber espionage attack teams are in very high demand by their employers. And like any other competent teams with a high demand for efficiency and results, the groups that carry out cyber espionage missions against you will probably work by established processes and used specific methods and tools to get the job done on time and on target – pun not intended.

Strengthen foothold
Expand access and obtain credentials
Advanced Persistent Threat
Build or acquire tools
Research target infrastructure/

The list of methods employed by the wide range of possible cyber adversaries is way too long for me to even contemplate compiling. The following list is only meant to give you a few examples:

- Researching your company and your employees on your company website and on LinkedIn, Facebook and Twitter.
- Researching your email correspondence from already compromised mail contacts.
- Entering your networks indirectly via phishing emails sent to you, compromised websites you visit or software you download and install.
- Entering your networks indirectly via compromised vendors and suppliers.
- Entering your networks directly by breaking into your exposed services like vulnerable scripts on webservers, unprotected FTP servers and SSH logins with weak passwords.
- Entering your networks with stolen credentials from legitimate users.
- Pivoting from compromised client computers to servers which can provide additional access to the network, like AD servers and other authentication services.
- Breaking into email servers and accessing file shares to compile and exfiltrate large dumps of information from your networks.
- Breaking into and hiding in places where security monitoring often is scarce or non-existent, like printers, routers and in the near future, the coffee machine.
- Deploying custom built tools – also called implants – on a selection of your computers and servers.

- Hiding the number of compromised clients and implants on your network by clustering them, and only let certain control nodes – like your compromised web-proxy – communicate directly with the internet.
- Controlling the implants within your infrastructure through an external infrastructure of proxies and control servers over HTTPS.
- Configuring the implants to never to access the internet to get new commands or exfiltrate stolen data unless the infiltrated computer is on a guest wi-fi network that doesn't belong to the targeted company.

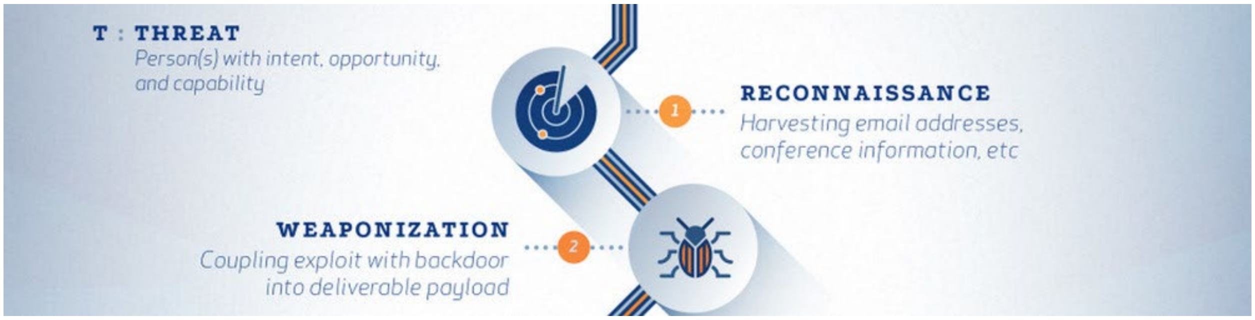
Understanding the motivation, the mission and even the mindset of your adversaries at an abstracted level may not be all that hard. But when it comes to the methods, or the tactics, techniques and procedures employed by actual cyber espionage teams, it starts getting messy and difficult really quick.

First of all it isn't easy to even define an abstract level when it comes to the methods. And when you try to sort it out at a more detailed level, you discover that you need deep technical insight, lots of knowledge of often well kept secrets on how these teams operate and a thorough understanding of the infrastructure you are defending. Without this you are well-meaning but ineffective.

The takeaway is basically this: To really fight back, you need skilled, experienced, passionate people who know your own infrastructure very well, who knows how the attackers think and work and who understand how they can be deterred, detected and thrown out. These people are rare, they are expensive and they are basically your only hope. They are senior SOC analysts.

The next step

If you were interested enough to read all this, you probably already know of SANS and their Critical Security Controls. But when trying to wrap your head around «the mission» and «the methods» you will eventually be lead in the direction of methods like «the Cyber Kill Chain» and models like «the Detection Maturity Level» and similar writing. Sooner or later you will have to read up on «the Intelligence Cycle» and «the Diamond Model of Attribution Analysis».


T : THREAT
Person(s) with intent, opportunity, and capability
1
RECONNAISSANCE
Harvesting email addresses, conference information, etc
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

And when you think you are about ready to handle it all, you will be adviced to read up on analysis methods for bias correction like «the Analysis of Competing Hypotheses» and books like «the Psychology of Intelligence Analysis», and you will realize that you are actually working in the field of counterintelligence, allthough noone around you ever told you that, or even understand it.

The takeaway is that a lot of smart people have contributed a lot of great knowledge that is relevant to the detection, analysis and reponse to cyber intrusions. And the sooner you start reading up on it and reaching out to the community, the faster you will be able to be effective in your efforts to secure your networks, your company and ultimately your nation.

Caveat

Throughout this article I have solely focused on cyber espionage missions. A very important thing to remember is that if you come across digital spies in your network, there's a fair chance that the threat actor is employing other means of intelligence collections on you. The digital spying is only one of several collection methods available to large intelligence agencies.

Also, it is important to understand that there is a big difference between collecting information from you and your networks, and handing over a useful intelligence report to whoever ordered it in the first place, being it a decision maker or an engineering department in a government or corporation. Understanding this is important, and this is where the mentioned «intelligence cycle» comes in.

The Takeaway

Dealing with cyber espionage is hard, but if you take the time to understand how your adversaries operate, you can enable yourself and your organization to take on the challenges posed by cyber espionage in a much more efficient and effective way.

You <u>*can*</u> *enable yourself and your organization to take on the challenges posed by cyber espionage in a much more efficient and effective way.*

Having a thorough understanding of your adversaries' motivation, mission, mindset and methods should help you anticipate where your adversaries may hit you, and why. It should help you see it coming. And it should help you scope, plan and execute your security monitoring, detection and incident response in a way that is adaptable to the way your adversaries operate.

There is enough evidence available to argue that this will have a **big positive impact** on the efficacy of your security efforts and the way you manage your overall risk.

Because of this it's time to get intimate with your threats. Sure, keep your friends close. But don't forget the advice given by Al Pachino's character Michael Corleone in the movie the Godfather: Keep your enemies closer.

P.S. Did you find this essay interesting? Please leave a comment if you did. I would also appreciate feedback, if you have questions or comments. I'm also available for comments on Twitter, using @FrodeHommedal. And if you know people who could benefit from or be interested in this essay, I would love if you helped me spread the message by sharing it with them. Thanks for reading.

P.P.S. This essay was written as a continuation of my previous one, Dance like a Dragonfly, sting like a Bear.