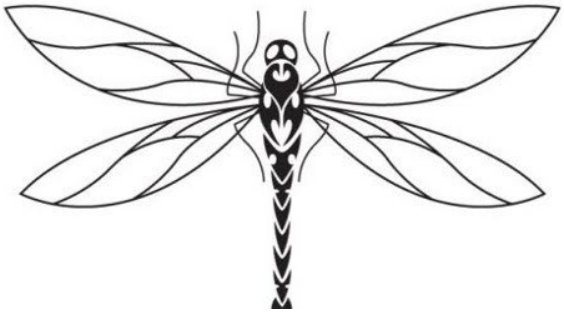
Dance like a Dragonfly, sting like a Bear.

September 2nd, 2014 | Frode Hommedal

On tuesday the 26th of August, the Norwegian national CERT, NorCERT issued a press release informing the public about a large notification effort. In cooperation with NVE and PTIL, NorCERT notified around 300 companies about a severe data breach attempt hitting parts of the Norwegian energy sector.

According to NorCERT, the effort was undertaken because at least 50 companies in the energy sector had already seen such attempts. Notification efforts on this scale are relatively seldom events, and alerting the public about it is rare, at least in Norway.



Based on this I find it tempting to infer that NorCERT assesses this particular data breach attempt particularly worrisome. If that is so, I share their judgment. Through the rest of this article I'll try to explain why that is.

The threat actor

NorCERT is quoted saying that the threat actor in question probably is Dragonfly. Dragonfly is the name given to this group by Symantec. According to Symantec, the Dragonfly threat actor has been active since at least 2011, and before turning their interest to the energy sector, they have been observed targeting defense and aviation.

The group has been given several names. It is called Energetic Bear by CrowdStrike, and by others it is sometimes referred to by the name of one of their hacking tools, Havex.

According to Symantec, the group has evolved over time and is now a capable one. According to F-Secure they may not be all that seasoned, because they aren't always managing their C2 infrastructure very well.

I don't see this as conflicting. As an incident responder I have seen lots of groups having difficulties managing the operational security of their C2 infrastructure well. But that hasn't rendered them any less capable or dangerous on the inside of the target organization.

The targets

One thing that sets Dragonfly apart is their target selection and the actions they carry out once they're on the inside of the target organization. It seems like they are actively going after critical infrastructure, and for the time being, especially the energy sector. And they're doing reconnaissance on SCADA systems.

Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to the energy supply in the affected countries.

SCADA systems in the energy sector can for instance be the systems controlling the power grid. Statnett, a company that controls vital parts of the Norwegian power grid, has confirmed that they have been targeted by what appears to be Dragonfly.

The motive

Dragonfly doesn't sound like your average information stealing espionage campaign, and so there is a growing concern that these infiltration attempts may actually be something more sinister. Some speculate that this may be the first stages of a nation state's preparations for future sabotage in critical infrastructure abroad.

There is evidence to support such speculations, and this would certainly be a chilling development:

The additional payload used to gather details about ICS/SCADA hardware connected to infected devices shows the attackers have direct interest in controlling such environments. This is a pattern that is not commonly observed today.

Attribution

It doesn't get any less chilling by the fact that some people are starting to point their fingers at Russia. Russia, which at this very moment is showing the world that it's not afraid of applying both cyber and traditional, military force abroad to secure national interests. To quote the Norwegian newspaper VG:

The combination of Russia's new military capabilities and Putin's will, has turned Europe on it's head. Russia is once again a significant military threat to Europe.

I am always skeptical to attribution, and this time is no different. I have no way of knowing if this attribution is accurate or not. Yet, I still think it serves a purpose to, for a moment, imagining Russia as the aggressor.

A mental exercise

Interpreting the actions of Dragonfly into the current and evolving geopolitical crisis in Ukraine, I think provides us with a realistic context for when we should fear strikes against our critical infrastructure from another nation state.

When we worry about what the consequences of operations like Dragonfly one day may be, I think we should imagine ourselves in a similar, but escalated version of the situation in Ukraine. We're on the verge of hot conflict, but we're not quite there.

In such a situation, an aggressor may knock out vital parts of a nation's critical infrastructure for one of at least two reasons. It could be as part of an invasion, disabling

infrastructure that is underpinning the defense, or it could serve as a serious warning or threat. «Look, we can turn off your power grid...»

Such a threat could even be sent to other nations than the one under threat of being invaded. It could serve as a warning to third parties. «Do not interfere...»

Stockpiling cyber weapons

The thing with offensive cyber capabilities is that they can't be stockpiled. You can't create and store «cyber weapons» that will enable you to take down random parts of another nation's critical infrastructure at will.

There are no «cyber cruise missiles».

Offensive cyber capabilities are more like a terror organization's offensive capabilities. It requires people in place. People that go undetected by the security police. People you can activate when the time is right. Sleeper cells.

To take out critical infrastructure, you will probably have to rely on «digital sleeper cells». On secret, unauthorized access gained and sustained over time.

To stop these sleeper cells from disabling your critical infrastructure one day, you must actively hunt for them, and disabling them.

We are in a dangerous place

It really is high time to wake up and smell the coffee. To quote Melissa Hathaway:

We have put every critical system on the backbone of the internet, but the internet wasn't ready for it.

It still isn't ready. Our systems aren't ready. We aren't ready. We aren't prepared.

For a couple of years now, we've seen how nation states have started to develop offensive capabilities to turn this lack of readiness and preparedness in critical infrastructure abroad into a strategic, offensive capability of their own. Right now, nation states are either preparing to, or are already actively placing «digital sleeper cells» in critical infrastructure abroad.

A really bad, but not unrealistic scenario for Dragonfly is that this is exactly what is going on. Right now, in the energy sector, in Norway and the rest of Europe and the US, a nation state may be in the process of placing «digital sleeper cells» for future sabotage on our critical infrastructure.

Until we, the defenders, start catching up in this game of offensive preparation, our critical infrastructure is in a dangerous place.

Final thoughs

Unauthorized access to our critical infrastructure, gained and sustained over time by a possible future aggressor should worry us. Worry us enough to take decisive actions. And so I encourage you, the reader, to join the debate and share your views and suggestions on how we can meet this challenge.

PS: In a future article I will go into more details on how I think we can better defend ourselves against infiltrations like these. But to forecast the likely and unsurprising conclusion: Skilled people doing data analysis and incident response.

References:

1. Norwegian National CERT, NorCERT.
2. Press release from NSM NorCERT, 26th of August.
3. «Tidenes hackerangrep», DN, 26h of August.
4. «Oljebransjen angripers av hackere», E24, 26th of August.
5. «Tidenes hackerangrep mot Norge», Offshore.no, 27th of August.
6. TV debate at «Aktuelt», NRK2, 27th of August.
7. «Hackergruppen Dragonfly mistenkt for å stå bak tidenes norske hackerangrep», Aftenposten, 27th of August.
8. «Tidligere cybersjef vil ha mer åpenhet om dataangrep», Aftenposten, 28th of August.
9. «Designet for sabotasje», DN, 28th of August.
10. A lot more info about Dragonfly at SCADAhacker.com.
11. «The Cyber Readiness Index 1.0», Melissa Hathaway.
12. «Bjørnen skraper på døra», Frithjof Jacobsen, VG.

Updates

2014-09-22: This article has later been published on my website.

2014-09-21: I have published a follow-up essay called See it coming: The four M's of espionage.