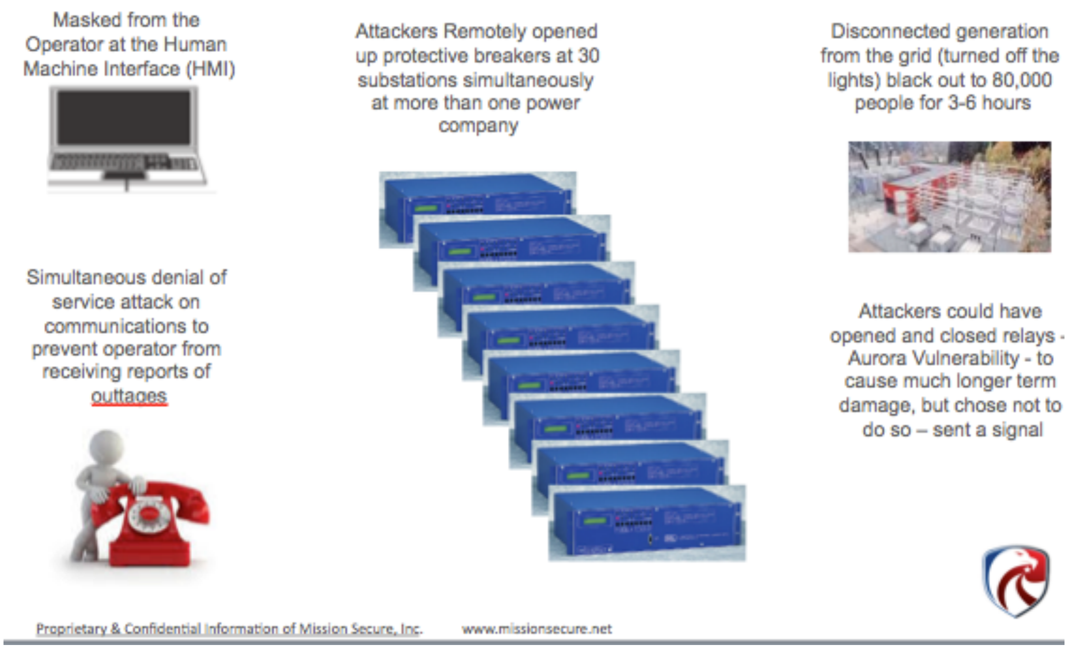
MSi has been tracking the ongoing cyber attack campaign against power companies, and now the energy supply chain, in the Ukraine. This is an issue of national importance. New developments are becoming public. Please read more.



Masked from the Operator at the Human Machine Interface (HMI)

Attackers Remotely opened up protective breakers at 30 substations simultaneously at more than one power company

Disconnected generation from the grid (turned off the lights) black out to 80,000 people for 3-6 hours

Simultaneous denial of service attack on communications to prevent operator from receiving reports of outtages

Attackers could have opened and closed relays - Aurora Vulnerability - to cause much longer term damage, but chose not to do so – sent a signal

Proprietary & Confidential Information of Mission Secure, Inc. www.missionsecure.net

Above is what we knew. It is ongoing and evolving.

This may not mean a lot to many of you, but this is an issue of national importance. A foreign actor has been leading an ongoing campaign against the Ukrainian power grid and more recently switching tactics to hit the energy supply chain (i.e. resource producing companies that supply material to make power and the trains that deliver them). TrendMicro first broke the news last night:
http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/

The first waves in December and early January of 2016 “turned off the lights” by disconnecting the power grid from generation by simultaneously opening the relays in the control network and turning off 30 substations (remotely, all at once, lights go out). The Ukraine utilities apparently did not even know this was a cyber attack and sent people out to the 30 substations to manually put the power back on. In the US, we are far more automated after decades of progression and returning to manual operation for any period of time (days) is not very feasible.

The adversary has been adjusting their attack tactics in near real-time as they see responses unfold. They recently began attacking and infiltrating the energy supply chain in phase 2 in an effort to take out the power, fuel and transportation sources (trains). This is not an attack on one plant or one company, it is an ongoing campaign against the supply chain of what keeps the power systems, and all that rely upon them, operating in a region of a major NATO country.

What is particularly scary is the attack mechanism appears to work like a worm, infecting one computer, then infecting the computers and servers connected to "patient zero", and so on. Think of your linked-in world and connections (i.e. infect you and all the people you know, all the people they know and pretty soon you have the equivalent of cyber ebola.) Then comes the payload, something called KillDisk. KillDisk goes in and wipes the hard drive clean. Say good bye to your operating system (Microsoft primarily, although flavors of Linux, iOS, Android, etc. all exist) and your applications go with it.

These applications are the control systems that command critical controllers running the power plant, substation, refinery, oil rig, Navy ship, and more. The computers at the command of all the controllers are wiped out, as are the automated back up servers. A similar attack happened to a large middle east oil company a few years ago destroying 30,000 computer hard drives that had to be replaced. This restoration process does not happen overnight. Multiply this across many plants, substations, now suppliers across industries and you see pretty quickly this is an issue of national importance. Lights go out, trains stop, no gas at the pumps, no food at the stores, no water to drink.

The really bad news is not much exists in the world today to prevent or stop this kind of attack. No single magic bullet, no pixie dust, no secret government lab about to issue the solution. DARPA has a proposal out for a four year effort to see if we can determine if our grid is under attack. Defending against this kind of attack involves a set of rigorous IT security solutions (defense in depth) to try and keep it out of the IT network, a similar suite of solutions to try and keep it away once inside the operational network and eventually you get to where

Mission Secure is focused as the last line of defense trying to detect and fight through these kinds of attacks at the control systems. Our current solution being released this month (MSi Secure Sentinel for ICS) would help, although still early and more remains to be done. If stuxnet was the first chapter, we are now in Chapter two of a new era in cyber warfare. This is just one of many sophisticated attacks to come.

We will continue to monitor this, expect DHS and other government organizations to provide guidance, media coverage to ensue once the importance and magnitude of this kind of ongoing campaign, its destructive force and how it would be really, really bad if a group like ISIS got a hold of this and turned it on the US. It is important to note BlackEnergy mentioned in the blog has been around since 2011 and this is the most recent iteration and improvement, BlackEnergy3+. BlackEnergy already compromised dozens of control systems in energy and critical infrastructure companies in the US, and hundreds globally, according to US government officials. The initial version of BlackEnergy has been used for reconnaissance - steal the blue prints on what to attack. This version is attacking and doing physical damage.

This is a fight coming to our great nation. It is important all of us in industry, government, military, politics and beyond to take note AND action! If you would like a briefing on this ongoing cyber campaign for senior management of your organization, or a more technical briefing, please contact us at info@missionsecure.net or 434.284.8071.