All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

How long does it take before people act responsibly? Hint: Forever!

I have been reading, with an increasing sense of the deja vu, about the power outages in the Ukraine. I am reminded of a quote I have had on the all.net home page for many years now:

"There is no limit to stupidity." - *Dario V. Forte*

And then came the announcements of the attacks on the Israeli power infrastructure.

What happened to the Ukrainian power grid?

In case you didn't see it in the news (i.e., you live in the United States and get your news from the various commercial news and radio shows), there have been sporadic power outages in the Ukraine since late in 2015. The cause has not apparently been definitively determined, but the asserted event sequence according to the industrial control sequence and related communities (i.e., rumor mills) is that it started when insiders got emails from malicious actors containing a Word document attachment with a macro that installed a Remote Access Trojan. This RAT was invoked when someone opened the email attachment on a computer attached to the control systems of the power systems of the Ukrainian power distribution infrastructure (i.e., the grid) and remote access was granted to the attacker. What happened next is still unclear. There were sporadic power outages.

How do I love this example? Let me count the ways... or at least start to ...

1. The (US) media failed to (adequately) report actual power outages apparently caused by malicious acts against a nation state even though they were talking about potential cyber attacks on US power and other infrastructure. Is rumor preferred over fact?
2. The cause has not apparently been determined (at least not the root cause – the proximate cause was that the power infrastructure systems stopped transmitting power to end users). For example, it may have been an insider ordering transmission systems to turn off. The public information remains unclear at this point.
3. The event sequence identified fails to link between the attack(s) gaining access to computer systems (cause) and the power outages (effect). They may be unrelated since these are common sorts of attacks that happen all the time and are widespread globally. Failure to link cause and effect makes attribution rather senseless.
4. The information sharing and analysis organizations, while helping to spread rumors of, from, and to relatively knowledgeable people, are not bringing any particular clarity to the situation. Hence they are acting as high quality rumor mills. Don't get me wrong. This is better than low quality rumor mills. It is more convincing that the people who know more about the issues don't know what's really going on yet.
5. The path to entry is asserted as email to computers attached to power infrastructure control systems. There is no rational reason that computers attached to systems that control power distribution systems should be able to accept or process email to users. These should be separated as has long been established, more details to follow.

6. The attackers apparently used Microsoft Office macros embedded as attachments to the emails to gain entry. Such macros were shown to spread viruses since the 1980s! That's more than 25 years ago!! Why are we still doing the same stupid things we did 25 years ago? Because ”There is no limit to stupidity”!
7. For the macros to run, they attachments must be “clicked upon” and various settings must be enabled in the email client. These settings have been known for as long as macro viruses have been known and apparently were not set safely for systems connected to the power infrastructure.
8. The macros apparently “bypassed” the mechanisms in the email client and/or Microsoft Office intended to detect and notify the user of them. This has been done since the 1980s as well, which leads to the question of when the providers of commercial software that opens email attachments and interprets their content will be capable of detecting the very things they themselves interpret. Why are we still dealing with this more than 25 years after the vulnerability was published. How long do such problems have to persist before people selling this software get punished for gross negligence or perhaps criminal negligence? Why are we still doing the same stupid things we did 25 years ago? Because ”There is no limit to stupidity”!
9. The installation of the remote access Trojan (a “hidden” program that keeps running and communicates to other computers allowing them to tell the program what to do with the access it has) should be detected in any system that is important enough to cause loss of life, directly or indirectly, through change control methods also from the 1980s. Why are we still dealing with this more than 25 years after the solution was published and commercial products enacting the solution were available? Why are we still doing the same stupid things we did 25 years ago? Because ”There is no limit to stupidity”!
10. Even if the RAT is installed, why is it allowed to communicate with arbitrary outside locations? While things like Web browsers and other authorized software may be allowed outbound connections, other ports and software not authorized for external communications generally should not be permitted to do such communication and this should be controlled by firewall settings which are generally available in every relevant platform. Now I know this is rarely done, but it is rarely done because ”There is no limit to stupidity”! The idea that we trust every program in the “inside” to do anything it wants inside or with the “outside” has long been known to be problematic, the solution is already in place, all you need do is configure it, and yet it is almost never done. And no, it doesn't cause programs doing legitimate activities to fail. It does cause programs doing illegitimate activity to be noticed immediately (and to fail), and if we add deception into the mix, it often gets even better for the defenders.
11. When the RAT is then used to download even more software … see item 9
12. So you get to run any program you want on the system my user uses to do email. In what world does this authorize you to then cause my power infrastructure to stop transmitting energy? There appears to be a complete disregard for architecture here. And we have known about computer and network architecture for a long time, there are gobs (more than enough to not be able to read them all) of published articles on security architecture, and apparently, these were ignored or...

13. We still don't have a causal link between the “attack vector” (or whatever they call it today) and what actually happened (which is still unclear from the reports).

I hope this is as clear as mud. None of the 13 things identified above should be the way things are, none of them have to be that way, and each represents something that should have been done better for at least the last 20 years.

What happened to the Israeli power grid? Apparently nothing

Despite news stories of the power systems of Israel being attacked later in January and some notional attempt in various communities (i.e., rumor mills) to link it to the Ukrainian incidents, it appears that the “power grid” attacks on Israel consisted of some phishing emails sent to the regulatory body, and not in any way connected to the control systems of power infrastructure. In other words, I did see some reporting of the attacks on the Israeli power grid, which never apparently happened.

What we should know about and share – and what we should not

Now don't get me wrong. I certainly believe that the Israeli power infrastructure is attacked on a regular and ongoing basis. This of course is not reported widely, nor are the ongoing attacks on power infrastructure in the US and elsewhere around the world. Indeed most attacks are not reported, nor likely should they be, at least not widely. It's like reporting every swerving car on the road. Plenty of cars swerve and of those few get in accidents. Should we report every swerve?

The “big data” folks will likely tell us that if we measure and report every swerve in real-time and do proper analytics, we can likely detect a wide range of conditions associated with cars, drivers, road conditions, and some other things, correlate them to things like credit card usage, location, history, etc. and predictively determine which of these cars is likely to get into an accident and when, leading to proactively pulling over the drivers that are getting sleepy, drunk, stoned, over caffeinated, smoking, in an argument, using their cell phone, texting, or whatever, each producing a reduction in accidents and saving of lives calculable by statistics. If we integrate this with the car electronics, we can force cars likely to produce bad outcomes to pull over and take a break before being allowed to continue. They will also calculate the likelihood of stopping the car producing negative side effects, like the death of the driver rushing to the emergency room caused by pulling them over, and the various other effects that will be likened to the flap of a butterfly wing causing nuclear war (without the data to prove any of it).

And they are probably right about all of this, assuming the data and analysis are done properly and in a timely fashion.

Summary:

The bright vision of the future in which we share data and rapidly detect and prevent bad things depends on the data we share being reliable and accurate and the analysis getting to the right answers in a timely fashion. But today, as a society, we cannot even get it together to configure an email system to stop things we knew how to stop 25 years ago. And even if we were able to do this, we still don't know what happened a month ago, but see mostly rumors. Before we can reasonably move toward this bright future, we need to limit stupidity and get to some real answers. But as Dario pointed out years ago, and as we see in our every day experience: "There is no limit to stupidity."

