Current State of Cybersecurity

Matthew Dowell

Abstract -- In a rush to catch up to larger, first-world countries, state-sponsored cyber warfare is on the rise globally. Stuxnet showed how you can physically attack another country within the anonymous confines of a well-funded office. As more controls are connected to the Internet, the danger level rises.

Keywords -- Industrial Control Systems (ICS), Stuxnet, Tailored Access Operations (TAO), Programmable Logic Controller (PLC), IronGate, Man-in-the-middle (MitM) attack, RS-232

I. Introduction

Our current state of cybersecurity is reaching a new level of sophistication. Stuxnet was an eye opener for the world in 2010. It was unlike any virus found in the world before, reaching a level of sophistication no researcher had seen before. Stuxnet included four zero day exploits (each zero-day exploit can fetch thousands of dollars on a underground market), and targeted a specific hardware profile in a specifically designed building. The researchers at Symantec had never seen anything like it.

"I was expecting some dumb DoS type of attack against any Siemens PLC," Langner later recalled. "So this was absolutely freaking. To see that somebody built such sophisticated piece of malware — using four zero-day vulnerabilities, using two stolen certificates — to attack one single installation? That's unbelievable."[1]

Stuxnet was written at least 7 years ago by a sophisticated group of experts. Current opinion is it was written by teams backed by Israel, Germany, the US, or a combination thereof. Stuxnet pointed the way for any government to anonymously conduct a strategic attack at a distant foreign installation.

The Internet of Things movement is paving the way for any hardware device to quickly and easily be connected to the internet. Like all technology-rushes, security concerns tend to be pushed aside with the first priority being a "first to market". A minnesota-based plumbing company just last week formed a new venture to put control of your household plumbing into the cloud. As Stuxnet shows, hackers have known for almost a decade, the benefits (and potential destruction) of maliciously controlling hardware.

There is a mindset between governments now, that when a hacker infiltrates your system, it is your fault. You left the door open, it's your fault. When does this mindset switch and become a declaration of war? When does an open (back)door get used to blow up a bomb, or cause death and destruction? When do governments stop primarily using hacking as information gathering and start focusing on mayhem? When innocent lives are lost (again) and there is enough evidence (or propaganda) to point to an enemy, all bets are off. Below I will list a current state of cyberwarfare dealings for just a few of the countries.

A. Russia

The Russian dispute with Ukraine was preceded by Russian hackers shutting off power in Ukraine to 700,000 people.[2] Perhaps it was a warning, or perhaps it softened a target prior to their physical invasion. Russian backed groups have been active for many years in more traditional "secret stealing" hacking type activities.

"Specific targets of the attacks detailed in the report include the former Georgian Information Center on NATO, the Ministry of Defense of Georgia, the ministries of foreign affairs in both Turkey and Uganda and government institutions and think tanks in the U.S., Europe and central Asia."[2]

This kind of hacking has been supported by governments since the 80's, as detailed in Cliff Stoll's book, *The Cookoo's Egg.* [3] As a graduate student, Stoll tracked a hacker using a backdoor in GNU Emacs to break into many university and government computers. The hacker was traced back to East Germany, prior to the felling of the Berlin Wall. The hacker was either killed by his "handlers" or committed suicide by self-immolation.

B. Iran

Iran, even with severe western sanctions has been targeting their foe's infrastructure. Recently they targeted a damn in upstate New York where they found vulnerabilities in the computer controlled damn infrastructure. Despite being roughly 20 feet high, and the underlying water being described as a "brook", this might be an early test for their fledgling government-sponsored hacking group.

C. Israel

Israel, for its size is a very technologically advanced society with a large technical base. The architecture behind Intel's modern low-power, multi-core chips was designed by an Israeli

firm in the 90's and purchased by Intel. Recently, an Israeli company helped the FBI crack the phone of the San Bernardino couple accused of terrorism.[5] Israeli companies are a valuable tool for the US Government if they want to skirt some US laws, or not come under the gaze of the American public or politicians and Israel has a lot of expertise in warfare and cyberwarfare as they have been in a constant state of conflict for the last 50 years. The Israeli government faces organized attacks from such groups as Anonymous[6] on a yearly basis, along with more sophisticated attacks from government organizations opposed to Israel.

D. China

The US and China have signed a pact to stop hacking into each others computers looking for trade secrets. It lasted for a couple days. The fact that the US has gone so far to sign a pact with China might suggest that Chinese hacking has reached a level of sophistication that warrants worry. Despite the integrated economies, the US and China square off regularly when it comes to cyber warfare. CrowdStrike, the security prevention company wrote on their blog last fall:

"Over the last three weeks, CrowdStrike Falcon platform has detected and prevented a number of intrusions into our customers' systems from actors we have affiliated with the Chinese government. Seven of the companies are firms in the Technology or Pharmaceuticals sectors, where the primary benefit of the intrusions seems clearly aligned to facilitate theft of intellectual property and trade secrets…"[7]

The chinese government has all the things needed to facilitate a powerful cyber army; willing participants, educated people, money, strong central government, and a large quantity of recruits. The Chinese economy is the second strongest in the world and growing fast. Many American tech products are produced (copied, and studied, and potentially modified) in Chinese factories.

E. United States

In the United States we might hear about Russian, Chinese, or Syrian hacking groups on the nightly news, or a in a our local paper. These groups produce fear in the American reader, so it is a product (or story) that is easy to sell for the media. We rarely hear about the US backed hacking groups but we know they exist. The Internet was created and is still (mostly) controlled by the US Government, most people around the world have an Google or Apple designed phone in their pocket and use American technology companies in their daily lives. The American government has a strong core and also produces a lot of patriotic, technologically advanced people. The American government also spends more money on defense than any other country in

the world by a large margin. With those clues, it was not a surprise when Edward Snowden released details about Tailored Access Operations (TAO) run by the NSA.[8] TAO has been collecting and analysing phone, email, and other communications on thousands and thousands of Americans and other targets since at least 2008.

"...multiple confidential sources have told him that TAO has "successfully penetrated Chinese computer and telecommunications systems for almost 15 years," in the process, "generating some of the best and most reliable intelligence information about what is going on inside the People's Republic of China."[9]

The level of sophistication and depth of US backed hacking should be evident. The Texas based TAO office supervisor (with a team of 14) estimates they have performed over 54,000 operations since 2013.

II. Summary

Cyberwarfare is cheap, easy, effective, and deniable. Who really knows if that hacker coming from a Syrian IP address is sponsored by the Syrian army? Who really knows if that person is hacking from Syria at all, potentially they are using a VPN service in Syria. The CIA triad has some conflicting principles for governments. They want (C)onfidentiality, but the also need (A)ccessability. That means making data available online to other parties, but how do you effectively protect it all? It's impossible. The NSA has the largest data-gathering and analysis operation in the world and this is done with massive computing power using state-of-the-art datacenters. There are lots of bugs and potential backdoors in their software, it's just our current state of affairs. Hopefully someone doesn't decide to use that information to start another world war.

III. Case Study

As a software engineer I consulted at a lead smelting company for a year. The company had two plants, on in Minnesota and a much larger facility in Florida. Both plants had several furnaces, a dozen 20 ton melting kettles, acid reduction facilities and all the people and machinery needed to run the operation. Every pump, valve, conveyor belt, fan, coolant-pipe, generator, and exhaust filter was connected to plant management software (via a RS-232 PLC)[12] in the supervisor's office. The supervisor could physically control the plant from the confines of his office, without having to get dressed into lead-safety, and heat-protection gear. His office computers were connected to the internet, just like any other office computer. With just a little knowledge of this plant's infrastructure, anyone could create a physical scenario that would endanger the lives of dozens of workers and potentially put the company out of business.

This company is also a strategic supplier of lead to the largest battery manufacturer in the world. If the small, Minnesota plant was put off-line for even a month, the economic impact would be in the hundreds of millions of dollars nationwide. This is only one, small, operation.

Researchers at FireEye, a Cybersecurity Company[10] found a virus uploaded to a message board that attacked Siemens PLC's in a way similar to Stuxnet. The malware replaces a DLL to perform a sophisticated Man-in-the-Middle attack:

"The malware replaces a Dynamic Link Library (DLL) with a malicious DLL, which then acts as a broker between a PLC and the legitimate monitoring software. This malicious DLL records five seconds of 'normal' traffic from a PLC to the user interface and replays it, while sending different data back to the PLC."[11]

The researchers have dubbed the virus Irongate. The second interesting feature Irongate has is it knows whether it is running in a sandbox, or VM environment. If so, it hides. This allows the virus to detect whether it is being studied in a non-production environment. This second feature was proof that researchers needed for malicious intent.

Currently Irongate only works in the simulation IDE provided by Siemens to program their PLC's, believing it was a Proof-of-Concept or a first iteration.

References

[1] Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*
https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/
[2] Jeff Stone, Russian Hacking Group Sandworm Targeted US Before Knocking Out Power In Ukraine
http://www.ibtimes.com/russian-hacking-group-sandworm-targeted-us-knocking-out-power-ukraine-2257194
[3]Cliff Stoll, *The Cookoo's Egg*
http://www.amazon.com/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1416507787?ie=UTF8&*Version*=1&*entries*=0

[4]Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*
http://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html
[5]Katie Bo Williams, *Israeli firm helped FBI hack iPhone*
http://thehill.com/policy/cybersecurity/274619-israeli-firm-behind-iphone-hack-report
[6] Wikipedia, https://en.wikipedia.org/wiki/OpIsrael
[7]Dmitri Alpervitch, *The Latest on Chinese-affiliated Intrusions into Commercial Companies*
http://www.crowdstrike.com/blog/the-latest-on-chinese-affiliated-intrusions-into-commercial-companies/
[8]Lance David Leclaire, *10 Ominous State-Sponsored Hacker Groups*
http://listverse.com/2015/01/08/10-ominous-state-sponsored-hacker-groups/
[9]Andrea Peterson, *The NSA has its own team of elite hackers*
https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/
[10]About Fireeye, https://www.fireeye.com/company/why-fireeye.html
[11]Josh Homan, Sean McBride, Rob Caldwell, IRONGATE ICS MALWARE: NOTHING TO SEE HERE...MASKING MALICIOUS ACTIVITY ON SCADA SYSTEMS

http://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html
[12]Wikipedia, https://en.wikipedia.org/wiki/RS-232