CyberPro

January 2010

Keeping Cyberspace Professionals Informed

BEWARE OF FALLING TURTLES

(PLUS OTHER THINGS THAT SHOULDN'T REALLY FRIGHTEN US)

BY JAYSON STREET

456 BC: Aeschylus, a Greek playwright, was killed when an eagle dropped a live tortoise on him, mistaking his bald head for a stone. The tortoise survived.

Dying by a falling turtle has been documented and therefore is a proven threat. However, it still remains unlikely for you to die that way. Cyber-War (what the cool kids are calling it) has in fact happened. This proven threat does not necessarily mean a country's smart grid is going down anytime soon.

I started doing research for a book I am writing that includes cyber-warfare. During that process, I was startled by a few things I observed:

1. People who know what is going on don't talk about it to either confirm or deny it. Conversely, people who don't really know what is going on have no problem speaking about it at great length with much authority.
2. In a realm where anonymous attacks are the norm and not the exception, people are really quick to lay blame on who is doing what.
3. Everyone is *involved*!

Observation One: I am not an expert on cyber-warfare. This is just something I started researching for supporting material in a book. Like a lot of people I had been reading about on this subject, I had not been to any of the countries commonly named as participants in cyber-warfare. I knew I would not get good answers without "boots on the ground" experience. I applied for my passport and took my first trip outside of the United States. I wanted to see what was really going on.

The best place to begin seemed like China. After all, the people who were doing the talking were dropping that name with great frequency. I attended Xcon, where I had dinner with GoodWell, the founder of the Green Army. He is commonly known as the godfather of the Chinese hacker movement, with activity going back to 1997. He has gone the way of his Western counterparts. He has left his past to apply the knowledge gained from underground hacking and illegal breaches for a more legitimate profession that pays better and comes with cool business cards. He now consults with billion-dollar clients.

I was amazed to sit there and listen to his concerns of how hacking has become more a tool of crime rather than exploration and political action. Here was one of the major figures of the Chinese hacking culture expounding on the problems with criminal hackers and worried about so many attackers

assailing Chinese networks. In fact, the typical Chinese home computer user is under constant attack from bots, Trojans and also a virus here and there (sound familiar?).

So my first trip abroad was a real eye opener. I learned to not be so quick to judge or take everything I hear about "Cyber-Warfare" as gospel. It was after I returned home that I started listening more to what "experts" were saying about cyber-war. I realized most have been using data from certain 2003 incidents (though, yes, there are many that predate Titan Rain). Their opinions were not based from data gained first-hand. Noted that while there are many people who have tremendous experience in this field, those who are in the employ of a government have access to data that paints a much broader and more complete picture of the current state of these types of attacks. In the world of digital munitions and online attacks, the vectors and the weapons change overnight. When that person leaves their job and is back in the public domain, their knowledge becomes dated and out of sync with what truly is going on, even though they are still better qualified most of the time to talk about this subject.

Since then, I have traveled to other countries and gained a more open perspective of what is going on in this realm. The most important thing I have learned still remains what I knew from the beginning: I am not an expert, but I can form opinions based on what I know first-hand. I am limited to information in the public domain, but that is not all there is to the story. Most of the sources offering opinions also have the same limitation.

Observation Two: I believe this to be the biggest problem facing those who are on the front lines – the battlefield is virtual. A physical attack is much easier to detect and trace back to the source. You can see the path the attackers take. You can see the bullets they fire. The person attacking you with a DDOS is harder to trace.

The recent attack on South Korean and U.S. Web sites showcases the perils of being quick to judge and even quicker to accuse. For example, within a week of the attacks, Congressman Peter Hoekstra of Michigan [1] insisted we needed "to send a strong message." Yet, to this day, there has been no positive proof of who was actually responsible.

With $50,000, anyone can hire a botnet to replicate these attacks. It is that easy because most criminals are not motivated by politics, but by money. This also poses another problem. When anyone can hire or create their own army of compromised computers, does it make the impact less because it was a guy in Paraguay who was curious and wanted to see if he really could take down the White House Web site? In a way it would be more comforting if such activity were limited to the high-tech branch of a rogue nation launching an opening salvo in a cyber-attack. That can be an easier target for a response. But the same damage is felt regardless of who dealt the blow.

As time goes on, expect to hear about more cyber attacks that are "thought" to be either this country or that country but with no publicly available proof of who was responsible. This is a problem that will not

[1] http://www.scmagazineus.com/cyber-retaliation-debate-is-north-korea-guilty-of-ddos/article/139968/

be going away. So how can you protect and, more importantly, trace the attacks when the bullets appear from everywhere, including from your own side?

This brings us to Observation Three: who is involved in cyber-war activity? The answer is *everyone*! I would say (just my opinion based on my research) that almost every industrialized nation is working on a military hacking division (or whatever a government wants to call it). The Chinese were probably the first with the Indonesian cyber-skirmish in 1998 [2]. 1998 was also a notable year for the ramping up of cyber-warfare capabilities in the United States. Attacks on Serbian air command were used to help facilitate U.S. airstrikes as well as targeting enemy bank accounts [3]. Also in the late 1990s, a computer specialist from Israel's Shin Bet was able to compromise the mainframe of the Pi Glilot fuel depot north of Tel Aviv [4].

So here we are, more than 10 years later, still wondering what "Cyber-Warfare" is, who is doing what and what we can do to defend ourselves. It is also a safe assumption that everyone is also getting much better at attacking.

We are not learning from the past and the old adage bears true that we will likely repeat it. The 1980s were the decade to fear the nukes. This decade we fear the digital arsenal. The good news is we did not die in atomic fire (though it was a proven threat). The bad news is we found something else to fear (and we always will).

We need to understand that the threat of a digital holocaust is a possibility. Also a nuclear war could break out, Swine flu become an epic pandemic, a meteor wipe out all life on the planet or a falling turtle could kill you. The threats are real. But should we panic? No, probably not.

About the Author

Jayson E. Street is an author of the book "Dissecting the hack: The F0rb1dd3n Network" http://f0rb1dd3n.com from Syngress. He is well-versed in the 10 domains of Information Systems security defined by the International Information Systems Security Certification Consortium ([ISC]2). He specializes in intrusion detection response, penetration testing and auditing. He also has a working knowledge of the implementation and administration of major firewalls, vulnerability scanners and intrusion detection systems. Street has created and conducted security awareness training for a major Internet bank and his consultation with the FBI and Secret Service on attempted network breaches resulted in the capture and successful prosecution of the criminals involved. He has also spoken in the United States, Belgium, China and at several other colleges and conferences around the world on a variety of Information Security subjects and is on the SANS GIAC Advisory Board as well as a mentor for SANS. On a humorous note, he was chosen as one of Time's persons of the year for 2006.

[2] http://www.disasterpreparednessblog.com/disaster-preparedness-blog/2009/10/22/chinas-cyber-warfare-capabilities-highlighted-in-report-to-c.html
[3] http://findarticles.com/p/articles/mi_qa5332/is_1_48/ai_n28827258/?tag=content;col1
[4] http://www.alertnet.org/thenews/newsdesk/LV83872.htm