Week 04 – Writing Assignment 01

William Slater

DET 630 – Cyberwarfare and Cyberdeterrence

Bellevue University

Discussion Questions and Answers Related to Studies in Cyberwarfare

Matthew Crosston, Ph.D. - Professor

September 23, 2012

1. Talk about the emergence of and belief system of the H.U.C.

H.U.C. is the Honker Union of China. Their website, which contains forums and information about the organization is located at http://www.huc.me/ (Honkers Union of China, 2012).

H.U.C. is a well-organized Chinese hacker organization that is based entirely in China. They are talented and apparently have extensive knowledge about hacking and computers and the Internet, as well how to conduct cyber attacks and cyber espionage.

They seem to have emerged shortly after the Chinese Embassy was bombed during U.S. airstrike operations in Belgrade in the former Yugoslavia. The group's primary motivations are reportedly patriotism and efforts to promote Chinese nationalism.

These are the types of operations that make H.U.C. so dangerous in cyberspace:

1. Hacking
2. DDOS
3. Malware distribution
4. Espionage

In addition, a friend who returned to the U.S. after teaching in China for several years told me this evening as we were discussing Chinese hackers and Chinese Hacker Organizations:

> "They are not really 'underground.' In China if you have the $$$ and the right connections, you can hire a hacker team to attack the competitor of your choice. Or you can pay a 'water army' do destroy someone's online reputation. Some of the bigger groups are multi-million dollar ops.

Some Brief Conclusions:

1) H.U.C. appears to be accomplished, well-organized, talented, capable, experienced, willing to announce and brag about their exploits, and determined to conduct further attack operations in the future (Honker's Union of China, 2012).

2) According to J. Schelesinger, the slowing economy in China has caused state sponsored hackers to increase their efforts to steal industrial and military secrets from U.S. organizations (Schlesinger, J., 2012).

3) H.U.C. makes the world of cyberspace a more dangerous place, particularly for those who are unprotected and/or unaware (Honker's Union of China, 2012).

References:

Honker's Union of China. (2012). Honker's Union of China website. Retrieved from http://www.huc.me/ on September 21, 2012.

Schlesinger, J. (2012). Chinese Espionage on the Rise in US, Experts Warn. An article published at CNBC.com on July 9, 2012. Retrieved from http://www.cnbc.com/id/48099539 on July 10, 2012.

CNBC. (2012) Cyber Espionage: The Chinese Threat. A collection of articles about the cyber threats posed by Chinese hackers. Retrieved from http://www.cnbc.com/id/47962207/ on July 10, 2012.

The Hacker's Underground. An article published at the Serpent's Embrace blog. Retrieved from http://serpentsembrace.wordpress.com/tag/honker-union-of-china/ on September 21, 2012.

SEM. (2011). The Hacker's Underground. Retrieved from http://serpentsembrace.wordpress.com/2011/05/17/the-hackers-underground/ on September 21, 2012.

Please elaborate and discuss in depth the principles of simple security.

As described in the brief web article, Three Simple Security Principles, these are the three simple security principles.

1. A secure network assumes the host is hostile

2. A secure host assumes the network is hostile

3. Secure applications assume the user is hostile

In the case of the first Principle No. 1, the network needs to have defenses that protect it from hosts that are possibly infected.

In the case of the first Principle No. 2, each host needs to have defenses that protect them from other hosts and from anything else attached to the network that could possibly be infected.

In the case of the first Principle No. 3, each host and the network and all applications need to have defenses that protect them from other hosts and from anything else attached to the network that could possibly be infected. This is also applying the concept of least privilege, in which every user is only allowed access to the required data and resources in a computer networked environment (Compare Business Products, 2010).

Ironically, when doing effective security control analysis and security risk analysis, most organizations take it a bit further than these three principles described above. In fact, they usually agree that an asset is secure if it is able to satisfy these criteria:

Is Confidentiality guaranteed?

Is Integrity guaranteed?

Is Availability guaranteed?

These are often referred to as the "CIA Triad." And if the answer to any of these questions is NO, then the asset is not considered secure and the control that is designed to secure that asset must be reevaluated.

However, one of the founding fathers of the computer security field, Mr. Donn Parker, also established three additional simple criteria that truly augment the CIA concept of security.

Is the asset under the owner's control?

Is the asset authentic?

Is the asset usable?

And if the answer to any of these additional three questions is NO, then the asset is not considered secure and the control that is designed to secure that asset must be reevaluated. These three additional concepts together with CIA form what is now commonly referred to as the "Parkerian Hexad", in honor of Mr. Parker (Hintzbergen, J., el al., 2010).

Finally, here is a short checklist for having some quick idea if an organization is practicing good information security principles:

How to Identify a Secure Environment

1. Do they have an established Security Program?

2. Are data and Information are classified according to their importance and sensitivity?

3. Do they have well-defined Security Policies?

4. Do they have clear Guidelines for Acceptable Use of Assets?

5. Do they have a companywide Security Awareness Education Program?

6. Are Risks Identified and Managed via a Risk Management Program?

7. Does an Incident Response Plan exist?

If the answer to each of these questions is YES, the organization is probably pretty serious about Information Security (Logicalis, 2011).

References:

Compare Business Products. (2010). Three Simple Security Principles. An article published at Compare Business Products on February 2, 2010. Retrieved from http://www.comparebusinessproducts.com/briefs/three-simple-security-principals on September 21, 2012.

Hintzbergen, J., el al. (2010). Foundations of Information Security Based on ISO27001 and ISO27002, second edition. Amersfoort, NL: Van Haren Publishing.

Logicalis. (2011). Seven Ways to Identify a Secure IT Environment. Published at IT Business Edge in 2011. Retreived from http://www.itbusinessedge.com/slideshows/show.aspx?c=92732&placement=body copy in May 5, 2011.

Please explain GhostNet.

GhostNet is an extremely sophisticated, malicious spyware program that deploys a Trojan remote access program called gh0st RAT (Remote Access Tool). The program usually spreads via e-mail attachments and continues to propagate using the address book found on each victim's computer. After a computer is infected with the gh0st RAT Trojan, it can be remotely controlled by the hackers that operate GhostNet. The gh0st RAT program can even turn on the computer's built-in camera and also eavesdrop and record sounds via the audio microphone. Other worrisome activities that gh0st RAT can engage in include:

- Download, upload, delete, and rename files
- Formatting drives
- Open CD-ROM tray
- Drop viruses and worms
- Log keystrokes, keystroke capture software
- Hack passwords, credit card numbers
- Hijack homepage
- View screen (to invade privacy and capture sensitive information such as passwords, bank accounts, financial data, etc.)

Besides e-mail attachments, gh0st RAT can also spread via P2P file sharing, downloads, and perhaps even via IRC chat windows.

The gh0st RAT Trojan can usually be detected because the performance of the system slows down. It operates as an .EXE file and removal of the gh0st RAT Trojan can require some technical skills because a user must open the Windows Registry Editor and look under this Registry Key:

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/RUN/

The EXE will be located there is the machine is infected and the related key wit the name of the EXE file should be deleted.

Any other possible references to the executable under

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion

Or

HKEY_LOCAL_MACHINE/SOFTWARE/

should also be deleted (KoushalBlog, 2009).

When in doubt, call an expert who is experienced with dealing with desktop malware infections.

References:

Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.

Koushal Blog. (2009). What is GhostNet and How It Works. Retrieved from http://koushalblog.blogspot.com/2009/03/what-is-ghostnet-and-how-it-works.html on September 21, 2012.

Analyze geopolitically a map of hot spots juxtaposed with potential cyber conflict. Explain any uniformity and discordance that one might expect to see between regular conflict and cyber conflict.

The area of the world that I chose was the Middle East with Israel and Iran, as well as the United States. It is obvious to me that as the possibility of a shooting war continues to become a real possibility, it will probably be preceded by cyberwarfare attacks.

In fact, this whole thing with the U.S., Israel, and Iran is probably about to get VERY UGLY - Take a look! Just yesterday, September 22, 2012, it was reported that Iranian conducted cyber attacks against U.S. Banks (Mayday, M. 2012).

As far back as 2011, it was starting to become known that the U.S. and Israel were working together to develop and unleash the Stuxnet cyberweapon attack against a large Iranian facility in which uranium was being processed (Zetter, K. 2011). Later, supposedly a follow on sophisticated cyberattack occurred and this cyberweapon had the code name of "Flame."

As far as uniformity, the cyberwarfare hostilities would be directed against high-value strategic targets inside each country, much the same as a bomber would strike these targets. But the discordance factors would include:

1) The cyberweapon strikes would be lightning fast and most likely unseen until they had accomplished their intended damage(s).

2) The other side would likely have problems with the attribution of the source location of the attack.

3) The two sides would be in bitter disagreement about the nature of the attacks and the effects of the attack, and this would likely erupt into a war of words and propaganda.

4) It is also likely that a shooting war may erupt soon after the cyberattacks, noting that the country which initiates it did so in an effort to wage what is known as a "Preemptory First Strike", which is a concept developed in 1970s military doctrine and nuclear strategy in which it was believed that the side that strikes first will have the greatest opportunity to inflict massive damage while still having the opportunity to use its weapons. The idea behind that doctrine was also known as "use it or lose it" because it was thought that if the country that struck first waited, its military capabilities could not survive well enough to launch a retaliatory strike (Freedman, L., 2003).

References:

Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.

Clarke, R. A. and Knake, R. K. (2010). Cyberwar: the Next Threat to National Security and What to Do About It. New York, NY: HaperCollins Publishers.

Czosseck, C. and Geers, K. (2009). The Virtual battlefield: Perspectives on Cyber Warfare. Washington, DC: IOS Press.

Edwards, M. and Stauffer, T. (2008). Control System Security Assessments. A technical paper presented at the 2008 Automation Summit – A Users Conference, in Chicago. Retrieved from the web at http://www.infracritical.com/papers/nstb-2481.pdf on December 20, 2011.

Freedman, L. (2003). The Evolution of Nuclear Strategy. New York, NY: Palgrave Macmillian.

Friedman, G. (2004). America's Secret War: Inside the Hidden Worldwide Struggle Between America and Its Enemies. New York, NY: Broadway Books.

Gjelten, T. (2010). Are 'Stuxnet' Worm Attacks Cyberwarfare? An article published at NPR.org on October 1, 2011. Retrieved from the web at http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet on December 20, 2011.

Gjelten, T. (2010). Stuxnet Computer Worm Has Vast Repercussions. An article published at NPR.org on October 1, 2011. Retrieved from the web at http://www.npr.org/templates/story/story.php?storyId=130260413 on December 20, 2011.

Gjelten, T. (2011). Security Expert: U.S. 'Leading Force' Behind Stuxnet. An article published at NPR.org on September 26, 2011. Retrieved from the web at http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force - behind-stuxnet on December 20, 2011.

Gjelten, T. (2011). Stuxnet Raises 'Blowback' Risk In Cyberwar. An article published at NPR.org on December 11, 2011. Retrieved from the web at http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar on December 20, 2011.

Grabo, C. M. (2004). Anticipating Surprise: Analysis for Strategic Warning. Lanham, MD: University Press of America, Inc.

Hyacinthe, B. P. (2009). Cyber Warriors at War: U.S. National Security Secrets & Fears Revealed. Bloomington, IN: Xlibris Corporation.

Kaplan, F. (1983), The Wizards of Armagedden: The Untold Story of a Small Group of Men Who Have Devised the Plans and Shaped the Policies on How to Use the Bomb. Stanford, CA: Stanford University Press.

Knapp, E D. (2011). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Waltham, MA: Syngress, MA.

Kramer, F. D. (ed.), et al. (2009). Cyberpower and National Security. Washington, DC: National Defense University.

Langer, R. (2010). Retrieved from the web at http://www.langner.com/en/blog/page/6/ on December 20, 2011.

Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: Rand Corporation.

Mayday, M. (2012). Iran Attacks US Banks in Cyber War: Attacks target three major banks, using Muslim outrage as cover. An article published on September 22, 2012 at Poltix.Topix.com. Retrieved from http://politix.topix.com/homepage/2214-iran-attacks-us-banks-in-cyber-war on September 22, 2012.

Payne, K. B. (2001). The Fallacies of Cold War Deterrence and a New Direction. Lexington, KY: The University of Kentucky Press.

Pry, P. V. (1999). War Scare: Russia and America on the Nuclear Brink. Westport, CT: Praeger Publications.

Reynolds, G. W. (2012). Ethics in Information Tehnology, 4th edition. Boston, MA: Course Technology.

Rosenbaum, R. (2011). How the End Begins: The Road to a Nuclear World War III. New York, NY: Simon and Schuster.

RT. (2012). Iran may launch pre-emptive strike on Israel, conflict could grow into WWIII - senior commander. An article published at RT.com on

September 23, 2012. Retrieved from http://rt.com/news/iran-strike-israel-world-war-803/ on September 24, 2012.

Sanger, D. E. (2012). Confront and Coneal: Obama's Secret Wars and Surprising Use of America Power. New York, NY: Crown Publishers.

Technolytics. (2011). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict. Purchased and downloaded from Amazon.com on April 16, 2011.

Wikipedia Commons. (2011). Stuxnet Diagram. Retrieved from the web at http://en.wikipedia.org/wiki/File:Step7_communicating_with_plc.svg on December 20, 2011.

Zetter, K. (2011). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. An article published on July 11, 2011 at Wired.com. Retrieved from the web at http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 on December 20, 2011.

5. In your weeks' 3 and 4 videos, you get diametrically opposite issues – hacking vs. establishing norms. Reflecting upon these two video together, explain what you consider to be some of the chief issues that make hacking a chronic problem to those looking to establish international norms of cyber behavior.

I enjoyed both of these videos, but I liked all speakers and the structure of the second video much better than the one with Professor Jonathan Zittrain. They were all brilliant and accomplished and well-researched and credentialed, but I felt that Professor Zittrain was trying too much to be ironic and funny at the same time.

After viewing both videos, these are some of the chief issues that I think are making hacking a chronic problem:

1) The hacking problem is not well understood either in this country or internationally.
2) The hackers know and understand their world better than others understand the world of cyberspace.
3) The hackers are MUCH more evil and determined and malicious than people realize. A great example is all the evil things that Anonymous attackers did to HBGary.
4) The hackers have a strange mindset and enjoy bragging about their exploits.
5) The hackers do what they do in a fearless manner, knowing that there is little or no chance that that will be caught.
6) The hackers are actually well-organized and can skillfully plan out and organize and execute precision attacks.
7) There are lot more well-organized hackers out there who well understand cyberspace and the good guys than there are good guys who understand the hackers.
8) The hackers revel in the stupidity and relative helplessness of their victims.

9) The hackers can and will strike from anywhere, at any time and in numbers and in ways that are not expected or can be accurately predicted.

10) I believe that the good guys should enlist skilled hackers into their cause to fight foreign hostiles, but I sincerely believe that the good guys don't have the skills or the diplomatic know how to do that.

11) The good guys believe that international agreements can be attained to define and agree on what cyberwarfare is and what cyberweapons are, and how to assess the effects of the damage of cyberweapons. They also seem to believe that 2012 would be the decisive year in which the groundwork for legislation and policy was laid to deal with cyberwarfare issues. The hackers do not even consider this a remote possibility, in my estimation.

References:

Georgetown University. (2012). International Engagement in Cyberspace part 1. A YouTube video. Retrieved from http://www.youtube.com/watch?v=R1lFNgTui00&feature=related on September 21, 2012.

Zittrain, J. (2012). Professor Zittrain Q&A Hacktivism: Anonymous, lulzsec, and Cybercrime in 2012 and Beyond. A YouTube video. Retrieved from http://www.youtube.com/watch?v=CZWjfxY8nmU&feature=related on September 21, 2012.