When the Media war hits home…
Thomas L. Freeman, Jr.
Version Number 1.2c
May 30, 2001

A media fueled "cyberwar" between United States and Chinese hackers did many things for the Information Security field. Not all of it good. I will discuss, in depth, the reasons surrounding this "conflict," the state of the "battlefield," and the outcome of all the hostilities. I will also take an in depth look at the steps taken after one of my sites were attacked. Finally I will answer the question; was this really a war or business as usual.

In the history of hacking there have been many incidents of politically motivated attacks on foreign websites. They are often used to spread the message of an individual's or group's cause. Sometimes they are used as a distraction for a malicious payload such as a backdoor or a worm. However, the most common attacks on websites are by "script kiddies" to draw attention to themselves, send out messages to other hackers and to remind Systems Administrators that they need to focus more on security. These rounds of attacks were just more of the same with one important difference. The media jumped on this one and caused more harm than good. Just like the Persian Gulf War of 1991, this was a media war.

On April 1, 2001 a collision between a Chinese Jet and a United States Spy plane left one Chinese Fighter Pilot dead and 24 United States personnel "guests" of the Chinese government as well as a crippled US Plane in the custody of the Chinese government. The plane was not just some ordinary plane. "The EP-3E is a sophisticated surveillance aircraft outfitted with state-of-the-art computers, cryptological equipment and sensors that are designed to monitor military communications deep within a country's borders. According to intelligence experts, even the slightest compromise of the plane's computers and equipment will likely help China further refine its information warfare capabilities."[1] Needless to say, this caused much concern in the United States Military, not only for the welfare of the crewmembers but also for the return of the plane. Also to take up the cause of this incident were the "script-kiddies" on both sides. According to one report dated May 1, 2001, "Since April 1, the date of the collision, hackers have vandalized about 360 Web sites in the U.S. and China."[2] However, was this merely a coincidence or was the start of another great rivalry between two countries. Let take a look at what was actually going on.

"Script-kiddies" on both sides of the pacific were breaking into each other's sites with a fever. Although the Chinese groups appear more organized and the message that they are splashing on American sites is clear and consistent, "most of the defacements have been attacks on Chinese Web sites, prompting security analysts to suggest that most of the hackers are probably U.S. teenagers."[3] Is this real warfare, or an excuse for notoriety from others in the hacking community. Thanks to sites like Attrition (www.attrition.org) who maintain mirror sites for all the confirmed hacks that they are made aware of, we can begin to get a clear picture of the battlefield.

If this were a true cyberwar, there would be clear state sponsorship. There is no clear indication of this. In fact, these "attacks" were nothing more than digital graffiti with the occasional worm being released. This will be discussed later. "[I]nformation warfare might be a reality within the military, but couldn't be further removed from this activity. Real computer warfare is beyond the ability of most of these so-called hacktivists."[4] What this round of political driven defacements amount to nothing more than name-calling. This activity is very common and seen everyday in the world of information security. Let turn our attention to the time frame of this conflict. What was the significance did the calendar play in the attacks.

Many media groups as well as the FBI's National Infrastructure Protection Center started calling attention to the defacements and stating that between May 1st and May 7th the Chinese hacking community would wage a campaign against websites in the United States. Why these dates, well they hold national significant as far as relations between the US and China. May 1st is May Day in China, which also happens to be the International Workers Day celebration. This promotes the success of the working class in society and in many communist governments, promotes the communist ideology over capitalism. May 4th is Youth Day. A date no doubt where all the little script kiddies in china get the day off school and get to spend even more time in front of there terminals. Finally May 7th was the two-year anniversary of the "accidental" bombing of the Chinese Embassy in Belgrade, Yugoslavia by American warplanes. As you may recall this caused a lot of tension between the two countries and is a significant date for any politically motivated anti-US movement.

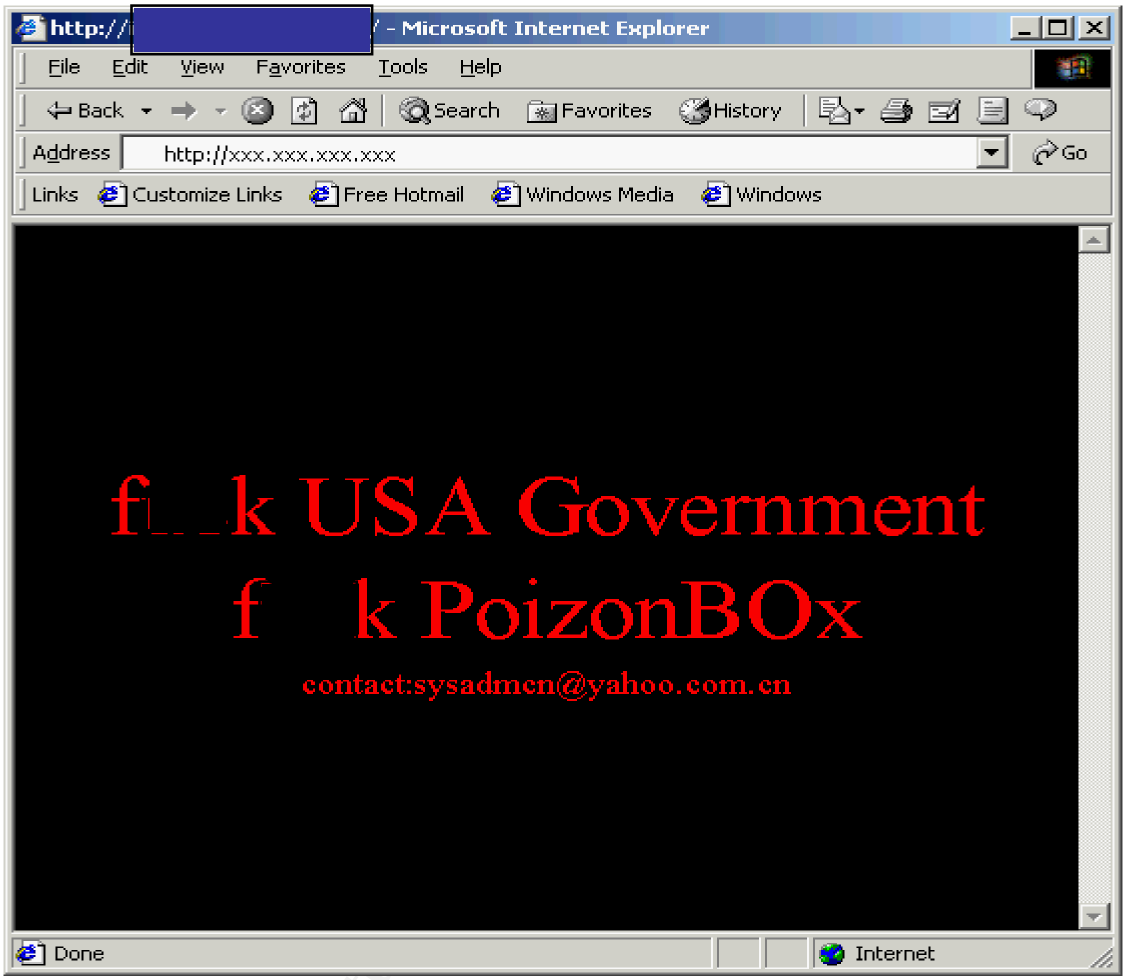
As previously mentioned, some of the Chinese hackers took this opportunity to release a new worm into the wild. The Li0n Worm written by the Li0n, leader of the Honker Union of China (HUC), infects computer systems and uses their mail client to email sensitive data back to a server in China. This worm primarily is targeting Linux computers and it is estimated that over a 12 to 14 day period, more than 5000 computers have been infected. In addition to send the sensitive information, the infected computers can also be used in Distributed Denial of Service attacks. Of all the activities of this war, this may have been the most damaging and the most overlooked by news agencies that continue to focus on the defacements.

While it is beyond the scope of this paper to examine all the attacks that took place during these days, we do have the ability to look at one attack and how it was handled from a security administrator's perspective.

On Monday, May 14th, 2001, at approximately 10:58 AM, our Accounting Manager sent an email to the Chief Executive Office (CEO) stating that he saw a "disturbing message when [his] browser" connected to our MS Exchange Server. The CEO in turn sent the message to our Chief Security Officer (CSO) who sent it to Computer Incident Response Team (CIRT) to investigate. Here is the detailed account of our response to this "attack" as well as the results of the investigation.

1. Verify the attack

The first thing we did was go to the URL in question to see for ourselves what the Account Manager saw and make a determination that the page was indeed altered. Upon connecting to the page we saw the attackers message and made the determination that an unauthorized change has occurred and that our security was breached. Below you will see a screen capture of the page in question:


http://[redacted]/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address Go
Links Customize Links Free Hotmail Windows Media Windows
Done
Internet

http://xxx.xxx.xxx.xxx

f[redacted]k USA Government

f[redacted]k PoizonBOx

contact:sysadmcn@yahoo.com.cn

Next we had to determine the extent of the breach. Was it merely the web page that got changed or did the attacker access more information on the box as well as install backdoors or viruses. Since the function of this machine was the Exchange server for the company it was important that we isolate the affected files and maintain the performance of day-to-day mail services. Looking at the web page files, we noticed that the creation date on the index.html, default.html, index.asp, and default.asp was May 9th, 2001 at 3:34 PM. Considering that these files were in place for sometime without anyone noticing concerned me a bit but also suggested to me that no other critical files were changed that would affect the primary purpose of this box. Since it was vital that mail services remain intact we had it implement our contingency options to stand up the backup exchange server and migrate the accounts off of them in order to perform a more thorough forensic analysis.

2. Mitigating the impact and restoring services

The first thing we did to mitigate the impact of this attack was to revisit the security barriers that we had in place and figure out if there was someway that this could have been avoided. In this environment we use public IP addresses that theoretically anyone can scan and access. Therefore the first and only line of defense we had in place was a Lucent Brick firewall. The firewall rule set allowed the following services through the firewall from any source address to the affected machine. They were SMTP, POP3, IMAP, and HTTP. The reasons that we have these services running and accessible through a firewall are clear. Keep in mind that this is a Microsoft Exchange Server, we need SMTP, POP3, and IMAP to pass mail through. We need HTTP to allow employees at home to access the mail remotely. The next step we took was to shut off the HTTP access through the firewall. This would cut off the remote access to the mail, but for now we felt that this would be an acceptable step.

The next step in the process was to prep the new exchange box. Since all of the programs were already installed. The first thing we did was install the ISS Real Secure Server Sensor on the machine. This would allow the Security Operations Center the ability to monitor the traffic on the box and verify that nobody was trying to get in. After this was completed, I generated new passwords for that machine. Theses passwords were a minimum of 8 characters long and all had upper and lowercase letters, numbers, and special characters. This way I would feel comfortable that it would take a while for somebody to brute force there way in. The next step was to migrate the mail accounts over to the backup exchange server. This would take a while and give me the opportunity to more closely examine the firewall logs from the Lucent Brick.

After logging into the Lucent Security Management Server (LSMS), I queried the session log to see who was going to the exchange server. The end result was a 150 MB file containing over 900,000 records. Going through these records would prove to be a daunting task.

3. Firewall Log Analysis

The first task in the analysis was to get the file off the LSMS machine and onto a workstation that could be used to parse through the information. In order to do this, I had to break the massive log file into 11 smaller files around 14 MB each. These smaller files were then zipped using a command line zip program. The files were then placed on diskettes and transferred via "sneaker net" to my workstation. These files were then transferred off the disks and in a folder for decompression. Once that was completed I reconstructed the file and imported it into a Microsoft Access database. This database will be used to sort and filter out extraneous information not helpful to the investigation.

After 2 days of parsing through the log file we were able to narrow our suspects down to one very suspicious IP address. This IP originated out of Brazil, a location well known for vulnerable computer systems.

Once we identified this suspect, I went back to the LSMS machine to run a Session Logged Report. From this we learned that not only was this suspect the person who was responsible for the defacement, but also all the activity that he did on that day. Not only did he go after our exchange server, he scanned every box on the affected system's subnet for HTTP (port 80). During his scans he found quite a few computers with port 80 open.

I looked at all of the other computers that our attacker tried to connect to and they all appear to look fine. In fact, the fact that he only was looking for computers with port 80 open confirms my statement that this was a mere defacement attack and not a attempt to steal information. The Closed Sessions Report even shows the exact moment of his upload and the duration of his visit. He was inside our exchange server for a mere 2 minutes and 2 seconds. Now that we know exactly what he did, we need to find out how he did it.

4. Putting it all together

After taking a closer look at the source address we decided to perform a scan of that system to see what kind of services he was running. After viewing the output of the scan it became apparent that this computer, although the source of the attack, was not home to the attacker. It is most likely that the machine was taken over by the true attacker. Below you will see the output of the scan:

Port	**Service**
7	Echo
9	Discard
13	Daytime
19	Character Generator
21	FTP
23	Telnet
37	Time
53	DNS
79	Finger
512	RPC
513	RLogin
514	cmd
515	Spooler
540	uucpd
1103	
4045	
6112	dtspcd
7100	X Font Service
36371	
36372	
36373	
36374	
36375	
37347	
37351	
37353	

This looks to me like a default Unix installation. From the FTP daemon it appears that this computer is running Sun Solaris 2.6. This computer fell victim to lazy system administration.

Therefore without the cooperation of the Brazilian ISP, the true identity of the attacker will likely never be known. However, looking at the message that was left on the web page I can almost guarantee that the source of this attack was somewhere in China or someone whom wanted to implicate China.

So why did he just break into one computer instead of going after all the boxes with port 80 open. The answer is fairly simple and at the same time an eye opener for us. Hackers will generally go for the "low hanging fruit" than spend the time and risk getting caught going after the harder targets. Frankly our Exchange Server was an easy target to break into. Once we discovered that that system was broken into, we ran L0pht Crack against it. To our astonishment, the administrator password broke within the first 7 seconds. The administrators of that box failed to do the simplest task in system security administration. Password Security! Not only was the password a word in the English dictionary, but a password of less than 8 characters, the minimum recommended password length for any type of secure environment.

5. Lessons Learned / Recommendations

Security in not only a department in the company but also an essential aspect to any System or Network Administrator. Without taking that into account we leave holes and weaknesses open for potential attack. In this case we failed to properly use secure passwords for our exchange servers. How many other boxes do we have with insecure passwords or vulnerable services running? Without the input from the Security Professionals we have on staff this could happen again.

While it is true that we fell victim to the latest Cyber War between the US and Foreign Hackers, we should use this wake up call to review every aspect of our security plan to see how effective it is and where we need to make adjustments.

I suggested that we go over the Firewall rule set and verify every rule that we have in there and see if there is a way to close any holes that might be present or have been overlooked for lack of updates. I also suggested that we set up a computer off the LSMS machine to FTP the daily firewall logs for analysis. This way we would be able to see potential malicious activity and not have a defaced web page out there for days without anyone knowing. I would also suggest a formal password policy for everyone in our company. This policy will ensure that an attack like this will be less likely to occur again. We have scheduled a complete rebuild of the compromised exchange server. Once that is complete that exchange server will take over the role as backup to the new Exchange Server, which is currently being used as the companies email server. Finally, since we still have the Web Outlook feature blocked. I would recommend that we implement Public Key Infrastructure (PKI) technology for authentication of remote users before we turn that feature back on. This could be accomplished by either generating our own key pairs and standing up our own Certificate Authority (CA) or obtaining signed certificates form companies such as VeriSign. This would ensure that not only would our email be encrypted but ensure that only authorized individuals would be granted access to the exchange server.

Sometime around the 8th of May, "the Honker Union of China issued a statement to the Chinese portal Chinabytes … declaring a truce and saying that they had reached their goal of hack[ing] 1,000 U.S. sites."[5] While it is hard to verify that they did in fact compromise that many systems, it would not be unheard of. Frankly the U.S. government does not maintain a mirror site and Attrition only will display the sites that they can verify. There are no estimates on the number of Chinese sites that were compromised. However, with the end of the war it is back to business as usual. Or is it?

Now that we have seen how the "cyberwar" affected me personally, I would like to address the question I posed in the opening paragraph. Was this really a war or just business as usual? Well thanks again to our friends at Attrition (www.attrition.org), they have put together a timeline which supports my summation that it was just business as usual with just a marginal increase by the younger or less experienced "Script Kiddies" who were looking for attention and recognition. Please see their article, "Cyberwar with China: Self-fulfilling Prophecy"[6]

It is clear by their analysis of sites hacked by two prominent hackers, Poisonb0x , and Pr0phet, that there were defacements on both sides of the lines before and after the plane crash. In fact, in Pr0phets case, he was merely looking to hack more Unix flavors, because he felt that MS Windows systems are too easy. China and other Asian countries mostly use some flavor of Unix. It was only after articles stating that there was a political agenda behind these actions that the defacements adopted political messages. This media war happened for two important reasons, the News agencies called for it, and the attention hungry script kiddies jumped on the train so they could give their "shout out's." For the sites that were not hit, system administrators may come away from this conflict with a false sense of security. For the sites that were hit, it provided us with a wake up to remind everyone that a security policy is a fluid an evolving beast that must be maintained and updated regularly. If we don't fix the holes, if we don't take care of the low hanging fruit, then that 13-year-old kid down the street will.

References

Knight, Will (2001) Experts question US vs China 'cyberwar' [WWW Document]
URL http://news.zdnet.co.uk/story/0,,s2086036,00.html

Verton, Dan (2001) U.S. – China cyberwar: Fact or fear-mongering? [WWW Document]
URL http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60116,00.html

Costello, Sam (2001) U.S.-China cyberwar a dud, though trouble still lingers [WWW Document]
URL http://www.itworld.com/Sec/2199/IDG010510china/pfindex.html

Martin, Brian (2001) Cyberwar with China: Self-fulfilling Prophecy [WWW Document]
URL http://www.attrition.org/security/commentary/cn-us-war.html

James, Michael S. (2001) Cyberbust? White House Hit, but Some Call Rumored U.S.-Chinese Hacker Battle Overhyped [WWW Document]
URL http://204.202.136.230/sections/scitech/DailyNews/cyberwar010504.html

Verton, Dan (2001) Spy plane incident raises concerns over access to secret U.S. technology [WWW Document]
URL http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59203,00.html

Dawn Group (2001) US-China 'cyberwar' heats up [WWW Document]
URL http://www.dawn.com/2001/05/01/int2.htm

The Times of India (2001) Indian, Pak hackers join US-China cyberwar [WWW Document]
URL http://www.timesofindia.com/today/03woru8.htm

[1] http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59203,00.html
[2] http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60116,00.html
[3] http://www.computerworld.com/cwi/story/0,1199,NAV47_STO60116,00.html
[4] http://news.zdnet.co.uk/story/0,,s2086036,00.html
[5] http://www.itworld.com/Sec/2199/IDG010510china/pfindex.html
[6] http://www.attrition.org/security/commentary/cn-us-war.html