Terrorist Threats to Cyber Security

Patrick Murray

East Carolina University

Abstract

This paper will focus on the current growing threat of terrorist organizations as it applies to network security threats. There are many ways that common traditional cyber-attacks could be applied by these organizations that would result in devastating results. These include simple mass DDOS attacks on government or corporate systems harming the economy of a nation. There could also be intrusions into systems to gain sensitive information about national security or weapons plans and other advanced technology from government contractors. Lastly they could attack the accounts of companies and individuals or use ransom ware to gain access to near unlimited sources of funding. The paper will then detail both the effects of each of these potential attacks in the context of a terrorist attack and also the means that can be used to prevent them.

I would like to separate, for the purposes of this paper, the term cyber terrorism from the other related types of attacks that could be included under this term. I would define cyber terrorism as the use of the internet and computer systems by terrorist organizations in order to carry out an attack on those that oppose them. Some people would include traditional hackers, hacktivists, and foreign governments under the umbrella term of cyber terrorists. I think that each of these types of attackers should be classified differently because the intent of the attack is different for each group. Traditional hackers usually gain access to systems for some type of personal gain by either obtaining information that is valuable or by executing tasks that they were hired to complete. Any damages or outages cause by traditional hackers are usually due to them being hired to do that specifically, a personal vendetta, or to cover their tracks after a breach. Hacktivists are much more likely to try to damage a system or cause an outage of the services provided but they do these things for political reasons. Hacktivists are not likely to cause harm to individuals and instead target mostly corporations in order to express their disagreement with certain policies. Lastly foreign governments may attack another nation with the purpose of bringing down infrastructure or to obtain national secrets but these attacks should be carefully planned and measured.

I think that actual cyber terrorists should be approached as terrorists are in the real world. There should be no expectation that the individuals executing the attacks have any motivation for personal gain and care only about causing terror to those that would oppose their organization. Any monetary gains caused by cyberterrorist attacks should be assumed to be used to fund further attacks by the organization. Also while some of the methods used by cyber terrorists and hacktivists are similar the cyberterrorist attacks are done much more maliciously. These attacks are also much more likely to target systems with attacks that could bring real harm to individuals. Lastly there should be no expectation that these cyber-attacks should follow any rules of war when classifying cyber terrorists.

Unlike foreign governments these groups should be expected to go to any length to accomplish their goals including targeting things like hospitals, emergency services, air traffic control, and other civilian systems.

There are several reasons that terrorists are moving more towards cyber-attacks especially when launching attacks on remote locations. One of the biggest factors is that it is much less expensive than traditional warfare. Once the computers and software is set up there are no additional costs for an unlimited number of attacks. There are no soldiers, no physical weapons, and, no ammunition. It is also much easier to hide using the Internet as one's physical location can be easily masked and the attacks can even be performed while traveling. There are also a near unlimited number of targets available and if one is too difficult to attack another can be selected in seconds. These targets include government networks, private companies, banks, and any other system connected to the internet.

One of the simplest and yet the most effective types of attacks that cyber terrorists can use is the distributed denial-of-service attack. The distributed denial-of-service attack has been used for many years by attackers to bring down systems. Traditionally these types of attacks are used to settle a personal grudge against the server owners, to prevent someone from winning a video game, or to facilitate or create a distraction for a more complex exploit type attack. More recently hacktivists have taken to using these attacks as their main form of protest against whatever they happen to be protesting at the time. The reason that distributed denial-of-service attacks seem to be used in attacks that would rate from petty bullying to cyber warfare is that they are probably the easiest cyber-attack to carry out. The only things that are required for this type of attacks are enough computers and software to coordinate all of the distributed computing power. This coordinated power is then used to flood the target system with traffic until in overloads the network and makes the system unavailable. There are

several variations of this type of attack and one variant can corrupt the firmware on devices so that they are permanently disabled until the hardware is replaced.

While in the past these denial-of-service attacks have mostly been seem as either petty attacks or political statements and have cost some companies a lot of money they are now being used to probe for weaknesses in national infrastructures. While there have been no major terrorist attacks using these methods yet it is feasible that they could be used to cripple an entire country given that there is enough resources behind the attack. Systems that could be targeted include businesses and banks, public utilities, transportation, hospitals, law enforcement, emergency services, and air traffic control. If any of these systems went down for a prolonged period of time it would likely cause the same amount of panic and disorientation as a traditional terrorist attack or more.

In addition to distributed denial-of-service attacks, cyber terrorists could also use more traditional hacking methods in order to gain access to the systems that they are targeting instead of just shutting them down. Taking the same list of targets from the distributed denial-of-service examples and applying them to this scenario can reveal many more motivations for terrorist groups to use these types of attacks. If government networks or the networks of government contractors were breached then classified information about personnel, projects, and facilities could be obtained and distributed by terrorists. This has already happened with a fifty-two page spreadsheet containing the addresses, email addresses, and retirement dates of former Army generals and that was just from a breached Twitter account. If cyber terrorists were able to get listings of cell phone numbers of potential assassination or kidnapping targets they could use software GPS tracking to locate these targets anytime. Also the damage caused by providing false information to law enforcement, emergency services, air traffic control and similar systems could be far greater than just preventing access to these services.

Intentional misdirection in these systems could also be used to facilitate a physical attack at the same time.

There are also concerns that the industrial control systems in place at many different types of facilities that run the country are vulnerable to attack due to the fact that their age and complexity make them hard to completely secure. Many of the vulnerabilities in these systems are well-known but have gone unfixed due to how complex the systems are. The problem is that many of these systems are now being connected to the Internet so that they can be remotely managed. This allows these facilities to be fairly easily breached from anywhere in the world. Some of the facilities that use these types of control systems include power plants, electrical grids, water treatment plants, and oil refineries. Once again the intentional misuse of these systems could cause much more damage than simply preventing access to them.

Lastly cyber terrorists can use techniques currently used by many hackers and cybercrime rings to exploit money from businesses and individuals. The easiest way to get money from anyone is to have them actually give it to you. This is the idea behind many types of malware that can infect computer systems. Two of the most common of these types of software are the fake anti-virus programs and the encryption type ransom ware. The fake anti-virus malware bombards the user with fake reports of viruses infecting their system and also prevents some of the functions of the operating system unless the user pays for the license or the software so that it can remove the infection. In most cases paying the cost will only lead to yet another mysterious infection that requires yet another purchase to remove. The encryption type ransom ware does not try to hide behind lies and plainly tells the user that their documents and pictures have been encrypted and the only way to decrypt them is to send payment to the account given. The fake anti-virus malware is fairly simply removed from the

system using traditional malware removal procedures and so is the ransom ware but removing the ransom ware leaves the files encrypted. There are a few initiatives to provide free decryption services for those affected by this malware but the best solution is to keep backups on media not connected to the computer. Assuming that only a small fraction of users on the internet were infected by these programs and that only a small fraction of the users infected paid the requested fees it would still bring a large amount of funding to the organizations behind them.

There is also the possibility that terrorist organizations will attack banks and bank accounts directly as well. This allows them to make larger sums of money more quickly than the malware infection scheme. The security of bank accounts against online attacks mostly rests on the account holder just like every other type of user account. This means that users with weak passwords, poor home network security, and a habit of falling for phishing attacks are most at risks of having their bank accounts hijacked. The banks themselves may also be targeted because, as was stated before, there are nearly unlimited target available via the Internet so finding a bank network vulnerable to attack only takes time. There are also programs available that are designed to completely wipe the data from systems and these programs could also be used once the attackers took money to cover their tracks and wreak havoc on the banking system.

There are ways to prevent and respond to these threats just as there are ways to prevent and respond to traditional cyber-attacks. Distributed denial-of-service attacks can be prevented by using a combination of network security devices and policies. A firewall that can block certain ports that may be used to flood traffic or certain IP address ranges of known attackers should be a first line of defense. The problem is that like most solutions to this problem it cannot block legitimate traffic without preventing access to the server. This would create the same effect as a successful attack though.

Routers and switches can be used so set more granular access control lists as well as limit the rate of traffic through certain ports. This can help by preventing a massive amount of traffic coming through within a small period of time. This may still limit the rate of legitimate traffic as well. The best solutions are an IPS type system that can inspect the traffic to identify denial-of-service signatures or a hosted solution that can filter traffic before it reaches the actual target network. The main problem with all of these solutions is that they can usually be defeated if enough power is behind the attack as they can only filter so much traffic before they have the either let all the overflow through or block all of it. It either situation the attack will succeed either by overloading the server or causing it to block traffic.

I think that preventing the more traditional types of attacks aimed at controlling system and stealing data should start with the organization analyzing what systems and data it has that may seem valuable to potential attackers. Many of the companies that have been attacked recently have been warned that they would be attacked and still did not manage to implement an effective defense. Cyber terrorist attacks should be handled in similar way that is similar to preventing cybercrime attacks. This includes network security, computer security, and security awareness training. The network security should be handled by firewalls, ACLs, and IPS systems that are properly configured to prevent and react to the types of attacks that might be expected. The computer security should consist of a strong authentication method and data encryption at a minimum. The security awareness training should explain all of the information security policies to employees and why they are necessary. This includes password policies, acceptable use policies, and personal device policies. In the case of the systems that are running the critical infrastructure facilities such as power plants, electrical grids, water treatment plants, and oil refineries these systems should not be connected to a network that is accessible from the internet if at all possible. There should also never be any personal devices on the same network as these critical systems and no personal external storage devices should ever be used on

them. A model for the security of these critical systems and really any system that needs to be secure can be based off of the recommendations given to NOAA after it was found to be vulnerable to cyber-attack.

There are already efforts by the FBI to take down the botnets that are responsible for running many of the malware extortion schemes that are being used currently but they are not able to shut them down fast enough especially if they are based in remote locations in foreign countries. The first thing to remember about these programs is that the money should never be paid. One measure that should be taken in order to prevent damage to systems by these malware programs is to always keep current backups of critical data preferably encrypted on external drives that can be stored separately from the computer. This will allow the computer to be wiped and rebuilt or at least the malware to be removed and the damage files to be recovered. These attacks rely a lot on the user being uninformed about what to do when they encounter these malware programs. It is unfortunately impossible to train every user on the internet on how to deal with these programs but a good security awareness training program can help to prevent this from happening in an organization. Unfortunately not every user pays attention to training and there will eventually be someone that installs the malware programs on their computer. This is where a combination of security software, backups, and training will hopefully prevent any negative effects.

As far as protecting bank accounts there should already be all of the security measures that include firewalls, IPS, anti-virus, backups, and others that have been listed in previous paragraphs. Because of the security already in place, the end-user is going to be the weak link in breaching an account. Users should always use reputable banks that employ proper information security measures to begin with. Users should also only log into their accounts through security encrypted connections that

are launched from the banks site and not from links or emails. All accounts should be signed out before closing the browser to make sure that the connection is closed. Strong random passwords should also be used if possible to prevent any brute force type attacks.

In conclusion I believe that the threat of cybercrime being used to further the agenda of terrorist organizations is on the rise and may one day be the top source of cybercrime in the world. There are some people that say the stance that critical systems are vulnerable to attack and that large scale catastrophic attacks could be executed over the Internet is over the top and that these things will never happen. I think that just because a large scale terrorist cyber-attack has not happened does not mean that it is not feasible and certainly it does not mean that security measures should not be put into place even just as a best practice. I hope that most governments, companies, and individuals have learned something from all of the recent breaches and distributed denial-of-service attacks that have been executed by traditional hackers and hacktivists. I hope that information security is being \pushed to the forefront of the cyber realm as I think that in the future computer networks will be the new frontlines in the war on terror.

References

Ellyatt, H. (2015, January 27). Beware: A national cyberterrorism attack may loom. Retrieved April 13, 2015, from http://www.cnbc.com/id/102367777

Krasavin Ph.D., S. (n.d.). What is Cyber-terrorism? Retrieved April 13, 2015, from http://www.crime-research.org/library/Cyber-terrorism.htm

Gregg, M. (n.d.). Five Ways Cyberterrorists Could Target the U.S. Retrieved April 13, 2015, from http://www.huffingtonpost.com/michael-gregg/five-ways-cyberterrorists_b_5874860.html

EU plans new team to tackle cyber-terrorism. (n.d.). Retrieved April 13, 2015, from http://www.bbc.com/news/technology-31851119

How terrorist hackers are ruffling the U.S. military. (n.d.). Retrieved April 13, 2015, from http://www.chicagotribune.com/news/opinion/commentary/chi-terrorist-hackers-threaten-military-comment-20150116-story.html

* Awan, I. (2014, January 1). DEBATING THE TERM CYBER-TERRORISM: ISSUES AND PROBLEMS. Retrieved April 13, 2015, from http://www.internetjournalofcriminology.com/awan_debating_the_term_cyber-terrorism_ijc_jan_2014.pdf

* The Cyber Terror Bogeyman. (2012, November 1). Retrieved April 13, 2015, from http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer