UTILIZING CYBER ESPIONAGE TO COMBAT TERRORISM

GARY ADKINS

INTELLIGENCE AND NATIONAL SECURITY STUDIES

APPROVED:

Larry A. Valero, Ph.D., Chair

Alexandra Luce, Ph.D.

Damien Van Puyvelde, Ph.D.

Benjamin C. Flores, Ph.D.
Dean of the Graduate School

UTILIZING CYBER ESPIONAGE TO COMBAT TERRORISM

by

GARY ADKINS

THESIS

Presented to the Faculty of the Graduate school of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE

INTELLIGENCE AND NATIONAL SECURITY STUDIES PROGRAM

THE UNIVERSITY OF TEXAS AT EL PASO

December 2013

Table of Contents

Table of Contents iv

List of Tables vi

List of Figures vii

1. Introduction 1

2. Research Question 3

3. Significance and Relevance 4

4. Literature Review 5
    4.1 Terrorists' Use of the Web 5
        4.1.1 Propaganda 6
        4.1.2 Recruitment 7
        4.1.3 Training 7
        4.1.4 Fundraising 8
        4.1.5 Communication 8
        4.1.6 Targeting 10
    4.2 Cyber Espionage in the Wild 10
        4.2.1 GhostNet 10
        4.2.2 Titan Rain 13
        4.2.3 Operation Aurora 14
        4.2.4 Red October 15

5. Research Design 16

6. Research Data 18
    6.1 Terrorist's Web Presence 18
    6.2 Longevity of Cyber Espionage Attacks 19
    6.3 Passive Vulnerability Scan 21
        6.3.1 Passing in Clear Text (High, Certain) 24
        6.3.2 Issuing an SSL Cookie Without a Secure Flag Set (Medium, Firm) 27
        6.3.3 Session Tokens in URL (Medium, Firm) 29
        6.3.4 Password Fields With Autocomplete Enabled (Low, Certain) 30
        6.3.5 HttpOnly Cookie Flag Not Set (Low, Firm) 31
        6.3.6 Cookies Scoped to Parent Domain (Information, Certain) 32
        6.3.7 Cross Domain Referrer Leakage (Information, Certain) 33
        6.3.8 Cross-Domain Scripts Included (Information, Certain) 34
        6.3.9 File Uploaded Functionality (Information, Certain) 35
        6.3.10 Email Addresses Disclosed (Information, Certain) 37

6.3.11 Private IP Address Disclosed (Information, Certain) 38
6.3.12 Cacheable HTTPS Response (Information, Certain) 39
6.3.13 Allowing Frame-able Responses, Potential Clickjacking Attack Vector (Information, Firm) 39
6.3.14 Directory Listings (Information, Firm) 40
6.3.15 Content Type Incorrectly Stated (Information, Firm) 40
6.3.16 HTML Does Not Specify Charset (Information, Tentative) 41
6.3.17 HTML Uses Unrecognized Charsets (Information, Tentative) 42
6.3.18 Vulnerability Scan Conclusion 42
6.4 Cost Analysis of Cyber Espionage Operation 42
6.4.1 The Team 43
6.4.2 Hardware Requirements 46
6.4.3 Software Requirements 48
6.4.4 Operational Costs 49

7. Analysis 51

8. Conclusion 55

Glossary of Technical Terms 57

Bibliography 62

Curriculum Vita 69

List of Tables

Table 6.1: Vulnerability Totals 22

Table 6.2: Operational Cost Breakdown 49

Table 7.1: Qualitative Analysis Rankings 51

List of Figures

Figure 6.1: Clear Text Password Code Snippet 24

Figure 6.2: Man-in-the-Middle Attack Example 26

Figure 6.3: SSL Cookie Without a Secure Flag Code Snippet 27

Figure 6.4: Session Tokens in URL Code Snippet 29

Figure 6.5: Password Fields with Autocomplete Enabled Code Snippet 30

Figure 6.6: HttpOnly Cookie Flag Not Set Code Snippet 31

Figure 6.7: Cookies Scoped to Parent Domain Code Snippet 32

Figure 6.8: File Upload Functionality Code Snippet 35

Figure 6.9: Private IP Address Disclosed Code Snippet 38

Figure 6.10: HTML Does Not Specify Charset Code Snippet 41

Figure 7.1: Vulnerability Distribution 52

1. Introduction

The world has effectively exited the Industrial Age and is firmly planted in the Information Age. Global communication at the speed of light has been a great asset to both businesses and private citizens. However, there is a dark side to the age we live in, where terrorist groups are able to communicate, plan, fund, recruit, and spread their message to the world. The relative anonymity the internet provides hinders law enforcement and security agencies in not only locating would-be terrorists but also in disrupting their operations. The internet is a loosely knit group of computers and routers and is spread globally with servers hosting files, forums, chat rooms, which makes it unlikely that many are only in one country's jurisdiction. Assuming the hosting country is friendly, action can take a long time; meanwhile, the website can easily be backed up and moved to another server in another country, beginning the process over again. Legal obstacles make it very hard to seize files or listen in on communications. What if a diverse group of hackers were allowed to do what hackers do best and infiltrate not only the servers themselves but use them to spider into the terrorist's computers and even cell phones? What information might be uncovered?

Take a moment and think of the trove of information that resides on your laptop and cell phone. A quick list might include banking information, tax forms, family pictures, self-portraits, and/or picture of your new car. Banking information might be in the form of cookies stored on your computer when you visit the website. Tax forms, while not advisable, do reside on many hard drives. Pictures might seem benign but they can be used to identify someone, and modern cameras and cell phones contain metadata in their files such as GPS location of any given picture taken. This sort of data was brought to the public's attention in

2010 when Adam Savage, from the show Myth Busters, took a picture of his Toyota Land Cruiser with his iPhone in front of his house and posted it on Twitter stating it was time to go to work.[1] The GPS tagging feature was enabled and not only gave away exactly where his house was but what kind of car he drove and when he leaves for work. In 2003 due to a bug in Photo Shop, TechTV's Cat Schwartz inadvertently exposed herself to the world when she posted a cropped photo of herself on her blog which contained EXIF data which held the nude photo.[2] Metadata is not only contained in picture files but also files such as Word documents which tend to save changes made to the file using the "auto save" feature. These examples are of normal people living normal lives but what kind of data might be residing in a terrorist's computer? This leads to another question: Is cyber espionage a viable tool to combat terrorism?

[1] Kate Murphy, "Web Photos That Reveal Secrets, Like Where You Live," New York Times, August 11, 2010, available at: http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?_r=0
[2] Sue Chastain, "TechTV's Cat Shwartz Exposed: Is Photoshop To Blame?," About.com Guide, July 26, 2003, available at: http://graphicssoft.about.com/b/2003/07/26/techtvs-cat-schwartz-exposed-is-photoshop-to-blame.htm

2. Research Question

To what extent is cyber espionage a viable tool to combat terrorist groups?

3. Significance and Relevance

Today, terrorism is an all too real threat to the western world and many other countries that may not be able to afford a large intelligence apparatus to fight terrorist activities. SIGINT is very costly, HUMINT does not always produce accurate information, and IMINT is almost useless when combating terrorist threats. If cyber espionage proves to be a useful tool to combat terrorism, then it could be a relatively low cost method of preventing terrorist threats.

4. Literature Review

There is no literature to review on the subject of utilizing cyber espionage as an effective tool to combat terrorism; the reason for this is unknown, but there may be a gap due to cyber espionage being a relatively new topic, researchers lack of knowledge/interest in cyber espionage and terrorism, or perhaps those knowledgeable in this area may not want to talk about it openly. Instead, the literature will be divided into two sections: Terrorist's use of the web, and cyber espionage. Combining these two sections will make the case of using cyber espionage to combat terrorism.

4.1 Terrorist's use of the Web

Terrorism has entered the phase called New Terrorism, which is mostly decentralized and non-state sponsored. Most of the major terrorist threats can be grouped in to the Religious Wave of terrorism, which started in the 1990's. It is based on religious ideals to justify terrorist activities.[3] Given the global and decentralized nature of terrorist groups they have begun leveraging technology such as the internet, cell phones, and software for various activities.[4] There are many websites dedicated to various terrorist groups.[5] The Institute for

[3] Richards, Julian, *The Art and Science of Intelligence Analysis* (New York, NY: Oxford University Press Inc., 2010), 57

[4] Gabriel Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," Haifa University, 2011, available at: http://95.211.138.23/wp-content/uploads/2012/08/2012-Terrorists-using-online-social-nerworking.pdf, 11

[5] Maura Conway, "Reality bytes: Cyberterrorism and terrorist 'use' of the Internet," First Monday 7:11 (Nov 2002): 4

Security Technology Studies has identified five ways terrorists use the web: propaganda, recruitment and training, fundraising, communication, and targeting.[6]

4.1.1 Propaganda

The internet has dramatically changed how terrorist groups can spread their propaganda to the world. Previously, terrorist groups would have to rely on news outlets reporting their message to the world after a terrorist act, in which the news outlet could report as much or as little of it as they wanted, interjecting their own views and skewing the message.[7] Now terrorist groups can easily post the message in its entirety on their own website and include any rebuttal to opposing views, which not only allows them to post their message in its entirety, but also allows for two-way dialog, thus increasing the effectiveness of the message.[8] Terrorist groups can easily portray themselves as victims seeking a peaceful resolution who were forced into acts of violence as a last resort.[9] Besides normal messages of propaganda, al-Qaeda offers a library services which holds over 3,000 books and monographs from "respected jihadi thinkers," which can be easily downloaded to cell phones.[10] Websites

[6] Hsinchun Chen, "Uncovering the Dark Web: A Case Study of Jihad on the Web," Journal of the American Society for Information Science and Technology 59:8 (June 2008): 1348
[7] Carsten Bockstette, "Jihadist Terrorist Use of Strategic Communication Management Techniques," European Center for Security Studies 20 (Dec 2008): 12-13
[8] Michele Zanini and Sean Edwards, "The Networking of Terror in the Information Age," John Arguilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), 41-42; Evan Kohlmann, "The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations," Testimony before the House Committee on Homeland Security, Dec 6, 2011, 7
[9] Freiburger, Tina and Jeffrey Crane, "A Systematic Examination of Terrorist Use of the Internet," International Journal of Cyber Criminology 2:1 (Jan 2008): 314
[10] Jarret Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," 30 Fletcher F. World Affairs 149 (2006): 153

also host videos of successful attacks against American targets in places like Iraq, creating jihadi heroes such as the "'Bagdad Sniper' and the 'Sniper of Fallujah'."[11]

4.1.2 Recruitment

Recruitment used to be accomplished through interpersonal relationships, but with the internet, the terrorist groups are no longer bound by geography and can not only reach but recruit individuals from anywhere in the world.[12] Websites can easily be customized to reach out and recruit specific audiences.[13] Second generation immigrants who are unfamiliar of their families' country of origin and do not quite fit in with others in their current country may turn to the internet in search of a community to belong to—people with similar problems—which is a susceptible target for terrorist recruiters.[14] Terrorist organizations even start planting the seeds of their ideology in the minds of children with video games, available for download on the internet, centered on defending the world against infidel invaders of various sorts and creating a "global Islamic caliphate."[15] Terrorist supporters, such as those of AQAP (al-Qaeda in the Arabian Peninsula), create "educational" cartoons to capture the minds of children and young people to follow in the steps of jihadi fighters.[16]

4.1.3 Training

Training new recruits no longer requires traveling to a foreign country to attend a terrorist boot camp. By leveraging technology, terrorist groups are able to train recruits much

[11] Ibid, 155
[12] Bockstette, "Jihadist Terrorist Use of Strategic Communication Management Techniques," 14
[13] Zanini, "The Networking of Terror in the Information Age," 43
[14] Freiburger,"A Systematic Examination of Terrorist Use of the Internet," 313
[15] Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," 156-157
[16] SITE, "Jihadist Announces Forthcoming AQAP Cartoon," available at: http://news.siteintelgroup.com/free-featured-articles/904-jihadist-announces-forthcoming-aqap-cartoon

like many distance learning classes offered by universities and professional training companies.[17] Many websites offer information and videos on physical training, bomb making, and kidnapping.[18] Examples are *The Terrorist Handbook*, which teaches bomb making techniques, or *The Mujahadeen Poisons Handbook*, which teaches how to create homemade poisons and poisonous gases.[19] Message boards and chat rooms also provide a way for would be-terrorists to receive instructions on bomb making by simply posting their question and receiving instructions from an expert.[20]

4.1.4 Fundraising

Terrorist groups raise funds in many different ways on the internet. They directly ask for funds to be donated for their jihad in some instances. This is the method favored by the Sunni extremist group Hizb al-Tahrir which has a plethora of websites with banking account information to send donations.[21] Other groups such as al-Qaeda and Hamas use charities and NGOs (Non-Governmental Organizations)(such as the Global Relief Foundation and the Holy Land Foundation for Relief and Development) to funnel money to them.[22] They will also

[17] Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," 153-154
[18] Freiburger,"A Systematic Examination of Terrorist Use of the Internet," 315; Kohlmann, "The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations," 8
[19] Gabriel Weimann, "www.terror.net How Modern Terrorism Uses the Internet," United States Institute of Peace, Special Report 116 (March 2004): 9
[20] Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," 2-3; Weimann, "www.terror.net How Modern Terrorism Uses the Internet," 9
[21] Ibid, 7; Chen, "Uncovering the Dark Web: A Case Study of Jihad on the Web," 1348; Dorothy Denning, "Terror's Web: How the Internet Is Transforming Terrorism," Yvonne Jewkes and Majid Yar, *Handbook on Internet Crime* (New York , NY: Willan Publishing, 2010), 19
[22] Weimann, "www.terror.net How Modern Terrorism Uses the Internet," 8; Michael Whine, "Cyberspace – A New Medium for Communication, Command, and Control by Extremists," Studies in Conflict & Terrorism 22 (1999): 238

attempt to sell goods through their websites to raise funds.[23] Other means include illegal activities such as credit card fraud and identity theft.[24]

4.1.5 Communication

Much like the rest of the world, terrorists use technology (such as the internet, email, and encryption software) to instantly and securely communicate around the globe.[25] Web forums, such as Al-Ansar's, an al-Qaeda group, are used as a "matchmaking service" to coordinate new militants for the front lines in Iraq.[26] Twitter and, to some extent, Facebook are used to plan and coordinate activities and ideas.[27] Paltalk, a voice and video chat room software that can be loaded on computers and cell phones, has been used for recruitment and planning.[28] Email and email groups, such as Yahoo! eGroups, are also extensively used.[29] Encryption software can be (and has been) employed by terrorists to secure many of these communications. For email, web boards, and social networking sites, terrorist have used PGP (Pretty Good Privacy) or their own variants such as al-Qaeda's Mujahideen Secrets to encrypt

[23] Qin, Jialun, and Yilu Zhou, "A multi-region empirical study on the internet presence of global extremist organizations," Information Systems Frontiers 13:1 (Mar 2011): 2
[24] Chen, "Uncovering the Dark Web: A Case Study of Jihad on the Web," 1348; Denning, "Terror's Web: How the Internet Is Transforming Terrorism," 19; Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," 117
[25] Denning, "Terror's Web: How the Internet Is Transforming Terrorism," 1
[26] Ibid, 14
[27] Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," 3-6; Kohlmann, "The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations," 5, 10
[28] Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," 156; Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," 3-4; Qin, "A multi-region empirical study on the internet presence of global extremist organizations," 1
[29] Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," 4; Kohlmann, "The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations," 7; Lachow, Irving and Courtney Richardson, "Terrorist Use of the Internet: The Real Story," Joint Force Quarterly 45:2 (2007): 100-102; Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," 150-152, 156; Denning, "Terror's Web: How the Internet Is Transforming Terrorism," 8, 20

messages.[30] To encrypt voice communications, PGPfone is described as being able to create "virtual STU-III devices."[31]

4.1.6 Targeting

The internet can also provide a wealth of information for planning attacks on targets.[32] Secretary of Defense Donald Rumsfeld described an al-Qaeda training manual as stating: "Using public sources openly and without illegal means, it is possible to gather at least 80 percent of all information required about the enemy."[33] The aftermath of the 2008 attacks in Mumbai showed that Lashkar-e-Taibas used GPS (Global Positioning System) and Google Maps to coordinate their beach landing, bypassing security forces and gaining access to India.[34] Information on public buildings or nuclear power plants can easily be found with a click of a button.[35] Web searches for news articles can easily show weak links in the TSA's (Transportation Security Administration) airport security net.[36]

4.2 Cyber Espionage in the Wild

There are probably many cases of cyber espionage that will never be known—after all, the whole point of espionage is to never be detected. Fortunately, there have been a few cases of cyber espionage that have not only been discovered but also reported, and, in some cases, analyzed. A few of the well-known cases are: GhostNet, Titan Rain, Operation Aurora, and

[30] Ibid, 21; Zanini, "The Networking of Terror in the Information Age," 37
[31] Lachow, "Terrorist Use of the Internet: The Real Story," 9
[32] Timothy Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," Parameters 33:1 (Spring 2003): 112
[33] Weimann, "www.terror.net How Modern Terrorism Uses the Internet," 7
[34] Bockstette, "Jihadist Terrorist Use of Strategic Communication Management Techniques," 15
[35] Weimann, "www.terror.net How Modern Terrorism Uses the Internet," 7
[36] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," 114

Red October. These examples are by no means an exhaustive list, but are some of the major cases that have been reported widely in the media.

4.2.1 GhostNet

Between June 2008 and March 2009, the Information Warfare Monitor conducted an extensive investigation into the GhostNet infections.[37] GhostNet targeted the Tibetan community and was most likely perpetrated by China (direct attribution of attacks in cyber space is extremely hard to obtain).[38] Given the location of the target, and the fact that 70% of the control servers had IP (Internet Protocol) addresses that were assigned to China, it is a safe bet that China was behind it.[39] Secondly, the operators responsible for GhostNet seemed to all be emanating out of Hainan Island in China.[40] Further evidence that points to China involves the investigation of a young woman, and member of Drewla (Tibetan outreach program) who was arrested on the Nepalese-Tibetan border when returning to her family in Tibet.[41] She was interrogated for two months by Chinese intelligence who produced complete transcripts of her internet chats over the years when she denied being politically active.[42]

GhostNet utilized the Ghost RAT (Remote Access Tool) Trojan, enabling the attackers to control the computer in real time, searching for and downloading files, logging

[37] Deibert, Ron, and Rafal Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor (March 2009): 14
[38] Ibid 52
[39] Ibid 22
[40] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," The US-China Economic and Security Review Commission (Oct 2009), available at: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA509000: 74
[41] Deibert "Tracking GhostNet: Investigating a Cyber Espionage Network," 28
[42] Ibid

keystrokes, and silently enabling attached devices such as microphones and web cameras.[43] The first known infection of GhostNet occurred on May 22, 2007.[44] The investigation found that GhostNet had infected 1,295 computers spread out over 103 countries; 30% of these infections were considered high value targets in many different countries' ministry of foreign affairs, news agencies, banks, unclassified computer systems in NATO headquarters, and in the OHHDL (Office of His Holiness the Dalia Lama).[45] The main attack vector of choice was social engineering by using a spoofed email (i.e. campaigns@freetibet.org) with a believable body and attached word document titled "Translation of the Freedom Movement ID Book for Tibetans in Exile.[46] Once opened, the file would infect the computer with the Ghost RAT Trojan.[47] In many of the cases, the attachment was a legitimate document stolen from previous infections.[48] The study showed that only 11 of the 34 antivirus tools at Virus Total (a website you can upload suspicious files to which uses multiple antivirus tools to scan the files for infection) were able to detect the malicious code embedded in the attachments, giving the attackers a high probability of not being noticed.[49] The attack seemed to be after strategic intelligence regarding the Tibetan movement gathering intelligence from both activists and in the OHHDL which held schedules for meetings with world leaders and time-sensitive communications.[50]

[43] Ibid 5
[44] Ibid 44
[45] Ibid 5
[46] Ibid 18
[47] Ibid
[48] Ibid
[49] Ibid
[50] Ibid 22

4.2.2 Titan Rain

Titan Rain was the name given to a series of cyber-attacks that concentrated on breaking into various US government and contractor computer networks.[51] It appears these attacks started as defacement attacks in early 2001 with the Code Red and Lion Worm.[52] These early attacks were very noisy, and easily detectable, posing more of an annoyance than a real threat.[53] Things got interesting in 2003 when Shawn Carpenter, a network security analyst at SNL (Sandia National Laboratory), investigated a series of intrusions at Lockheed Martin and noticed a few months later that very similar attacks started happening at SNL.[54] While working as a CI (Confidential Informant) for the FBI (Federal Bureau of Investigation), Carpenter was able to trace the attackers back to the Guangdong province in China before being told to stop his investigation.[55] The attackers were very hard to trace since they hid stolen data on the hard drive of the target before bouncing the data to various servers before bringing them back to mainland China.[56] These attacks continued through 2006, compromising systems of the U.S. Army Information Engineering Command, Defense Information Systems Agency, U.S. Army Space and Strategic Command, Army Aviation and Missile Command, Department of Energy, Homeland Security, State Department, and Naval War College.[57] In 2006, Major General William Lord acknowledged that China had downloaded between 10 and 20 terabytes of data from the DoD's (Department of Defense)

[51] Ibid 11
[52] Aaron Shelmire, "The Chinese Cyber Attacks formerly known as Titan Rain," Information Warfare 95 (2008): 2
[53] Ibid
[54] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," Time Magazine (Aug 29, 2005), available at: http://www.time.com/time/magazine/article/0,9171,1098961,00.html
[55] Ibid
[56] Shelmire, "The Chinese Cyber Attacks formerly known as Titan Rain," 3
[57] Ibid 3-4

NIPRNet (Non-classified Internet Protocol Router Network), which holds sensitive but non-classified data.[58]

4.2.3 Operation Aurora

Unfortunately, not much has been written in the academic circles about Operation Aurora. Most of the available sources are from media reports, but it is an important case nonetheless. Google first discovered the Operation Aurora malware in December 2009 and announced its discovery in January 2010.[59] Adobe announced a few days later that it had also discovered the malware.[60] Security researches from iDefense announced they had discovered that 33 additional companies were also hit.[61] The attack used a zero-day exploit in Adobe's Acrobat reader to infect their targets.[62] An investigation by HBGary discovered that the malware had been in development since 2006.[63] So far there have been no reports as to when the malware was first used. The malware used several levels of obfuscation, including encryption, up to three times, to hide itself from normal detection.[64] The main purpose of the attacks seemed to be to steal intellectual property from the various companies.[65] Google announced during their investigation that they found dozens of Chinese human rights

[58] Ibid 4
[59] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," Wired Magazine, January 14, 2010, available at: http://www.wired.com/threatlevel/2010/01/operation-aurora/
[60] Ibid
[61] Zetter, "Google Hackers Targeted Source Code of More Than 30 Companies,"
[62] Ibid
[63] HBGary White Paper, "Operation Aurora," HBGary Threat Report, February 10, 2010, available at: http://hbgary.com/attachments/WhitePaper%20HBGary%20Threat%20Report,%20Operation%20Aurora.pdf
[64] Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show,"
[65] Steve Ragan, "Was Operation Aurora really just a conventional attack?," The Tech Herald, January 27, 2010, available at: http://www.thetechherald.com/articles/Was-Operation-Aurora-really-just-a-conventional-attack/9124/

activists' accounts from users based in China, the US, and Europe were routinely breached; however, these may or may not be part of the Aurora attacks.[66]

4.2.4 Red October

In October of 2012, Kaspersky Lab's Global Research & Analysis Team discovered Red October, a sophisticated cyber espionage campaign originating out of Eastern Europe.[67] The earliest known attacks started in May 2007, but there are indications that they may have started earlier.[68] The main targets were various diplomatic, scientific research, and government agencies spanning over 42 countries and more than 300 unique systems.[69] The attack was deployed in two major stages consisting of the initial infection and then deploying additional modules to gather intelligence.[70] A unique aspect of the Red October attacks is that they did not just target normal computers but also smart phones and networking hardware, such as Cisco switches and routers.[71] Kaspersky Labs has not finished their investigation into Red October, so there is no information about specific data that was targeted.

[66] Graham Cluley, "Google, China, Censorship and Hacking," Naked Security, January 14, 2010, available at: http://nakedsecurity.sophos.com/2010/01/14/google-china-censorship-hacking/
[67] Kaspersky Labs, "'Red October' Diplomatic Cyber Attacks Investigation," Secure List, January 14, 2013, available at: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation
[68] Ibid
[69] Ibid
[70] Ibid
[71] Ibid

5. Research Design

A qualitative analysis of four areas will be conducted to determine the extent to which cyber espionage is a viable tool to combat terrorism. The four areas are: attack surface, length of cyber espionage campaigns, vulnerability of attack surface, and cost analysis of supporting a team for cyber espionage campaigns. The metric will consist of values from one to five with one being the least favorable and five the most favorable.

The first part of the research will be to evaluate if terrorists have a large enough attack surface to exploit. Similar to the business world, the larger their internet presence, the more likely it is they are able to be exploited. The attack surface will be evaluated using the following method: one will represent no attack surface; two a very small attack surface with most terrorist organizations not having websites; three will represent most terrorists organizations which have one website; four will represent most terrorist organizations have one website but some with multiple websites; five will represent most terrorist websites having multiple websites.

The second part will consist of analyzing how long known cyber espionage campaigns have been able to go undetected. The longer a campaign can go undetected, the more intelligence can be gathered. To evaluate the longevity of cyber espionage campaigns, one will represent a few days, two will represent a few weeks, three will represent at least six months, four will represent at least one year, and five will represent two years or greater.

The third part of this research will consist of checking, passively, for vulnerabilities in a small sample of terrorist websites. A passive scan has been chosen instead of an active scan

due to the legality of the scan methods. An active scan would reveal many more vulnerabilities but written permission is needed from the owner of the website. A passive scan works by analyzing the code the website sends to the browser. Since a passive scanner uses the website the same way a browser does it is legal to scan websites without permission. Unfortunately many of the vulnerabilities found during a passive scan cannot be verified without written permission of the website's owner. If a passive vulnerability scan can reveal even small vulnerabilities or a lack of use in IT best practices, then it will be a clear indicator of the likelihood an actual cyber attack will succeed. To evaluate vulnerabilities and IT best practice violations, one will represent no issues, two will represent most websites having at least one issue, three will represent all sites having one issue, four will represent some sites having more than one issue, five will represent all sites having multiple issues.

The fourth part will consist of a cost analysis of supporting a team for cyber espionage campaigns against terrorists. If costs are too high to support such a team, the viability of using cyber espionage to combat terrorism will suffer. To evaluate the cost of the operation, the first year of costs which include yearly costs, such as salary, and initial setup costs will be used. One will represent greater than ten million dollars, two will represent greater than five million dollars, three will represent greater than three million dollars, four will represent greater than one million dollars, and five will represent less than one million dollars.

6. Research Data

6.1 Terrorist's Web Presence

Terrorists use the web for a variety of tasks such as: propaganda, recruitment, training, fundraising, communication and targeting.[72] The main reason terrorists now use the web instead of close net social groups is because they are no longer confined to geographical boundaries.[73] Further, the web is a powerful tool to reach a wider, global, audience.[74] It has been found that "nearly all terrorist groups have a web presence."[75] As of January 2008, it was found that al-Qaeda had an estimated 5,600 websites and increases at a rate of approximately 900 per year.[76] Al-Qaeda and its affiliates use multiple websites in different languages and targeted to different audiences.[77] A research group consisting of 16 research assistants at a university in Israel regularly monitors 4,600 terrorist websites in the Dark Web for terrorist activities.[78] The Dark Web is a reference to websites that are not available through regular search engines. According to Southern Poverty Law Center, as of 2002, the US had 708 active extremist and hate groups; by 2003, 497 of these groups had websites.[79] The web landscape is constantly changing, and the number of terrorist web sites will rise and fall as authorities take measures to remove them; however, the terrorists simply load a backup of their website to another server. Each one of these websites can lead to potential terrorists

[72] Freiburger,"A Systematic Examination of Terrorist Use of the Internet," 311
[73] Ibid 312
[74] Ibid
[75] Zanini, "The Networking of Terror in the Information Age," 43
[76] Denning, "Terror's Web: How the Internet Is Transforming Terrorism," 4
[77] Weimann, "www.terror.net How Modern Terrorism Uses the Internet," 3
[78] Chen, "Uncovering the Dark Web: A Case Study of Jihad on the Web," 1357
[79] Jennifer Xu, Chen, Hsichun, Zhou, Yilu, and Qin, Jialun, "On the Topology of the Dark Web of Terrorist Groups," Intelligence and Security Informatics, 3975 (May 2006): 368

and sympathizers. For example, the French Interior Ministry announced that authorities had monitored a Neo-Nazi group's website and was able to identify 1,500 Neo-Nazi sympathizers spread across multiple countries, including America, Canada, Britain, Greece, and Poland.[80] Even if only a fraction of the number from the Neo-Nazi website example can be identified, then a cyber-espionage operation against these websites can prove fruitful for law enforcement and counter terrorism activities.

6.2 Longevity of Cyber Espionage Attacks

The length of time a cyber espionage attack can go unnoticed is extremely important to an effective cyber espionage campaign. If an attack can be discovered in a matter of days, the intelligence gathered will be very narrow in scope and would probably be confined to the primary target. For a cyber espionage campaign to be effective against terrorism, primary targets (mainly webservers) will need to be exploited for extended periods of time to allow for successful compromise of secondary and tertiary targets. This includes computers, laptops, smartphones, and tablets. Many cyber espionage campaigns will probably never be known; they are either never discovered or, if they were discovered, they were never made public. Even though this is a limiting factor, there have been a few well-noted cases—mainly GhostNet, Titan Rain, Operation Aurora, and Red October.

GhostNet, which was an attack allegedly carried out by China against the Tibetan community, was found to have made its first infection on May 22, 2007.[81] A study of the

[80] Whine, "Cyberspace – A New Medium for Communication, Command, and Control by Extremists," 242
[81] Deibert "Tracking GhostNet: Investigating a Cyber Espionage Network," 44

GhostNet infections was not done until June 2008 and was not concluded until March 2009.[82] This means that GhostNet was able to collect intelligence for approximately 22 months and went unnoticed for approximately 13 months. The Titan Rain cyber espionage campaign was first noticed in 2003 by Shawn Carpenter, a network security analyst at Sandia National Laboratory. No concrete data has been made public as to when the Titan Rain attacks began but they continued into 2006, giving it an operation time scale of at least 36 months. Operation Aurora was first discovered in December 2009 by Google Inc.[83] An investigation conducted by HBGary found that the attack started as early as 2006.[84] The Operation Aurora attacks were able to go unnoticed for approximately 36 months. The Red October cyber espionage attacks were discovered by Kaspersky Labs in October 2012.[85] Their investigation found that the first infection occurred in May 2007.[86] The Red October attacks had the longest operational time frame at approximately 65 months.

It is worth noting that these cyber espionage campaigns were against large companies and defense contractors which have a dedicated cyber security apparatus or were perpetrated in an automated fashion, as was the case in GhostNet. Large companies have security staff that routinely monitors network and system logs for anomalies which might be indicative of a cyber attack. The issue with automated attacks is they attack targets indiscriminately, which may include Honeypots. Honeypots are computers connected to the internet that mimic known vulnerabilities allowing an attack to attempt to infect the computer and capture the binaries in a sandbox (a digital container that allows code to be executed without fear of the

[82] Deibert "Tracking GhostNet: Investigating a Cyber Espionage Network," 14
[83] Zetter, "Google Hackers Targeted Source Code of More Than 30 Companies,"
[84] HBGary White Paper, "Operation Aurora,"
[85] Kaspersky Labs, "'Red October' Diplomatic Cyber Attacks Investigation,"
[86] Ibid

computer being compromised). This method is how security researchers for antivirus and IDS/IPS companies develop heuristics to match attacks. It is fairly safe to assume that a cyber espionage campaign performed in a stealthy manner against targets that do not have the vast security resources as large companies will have a longer operational window.

6.3 Passive Vulnerability Scan

Terrorists rely heavily on the internet; therefore, they present a rather large footprint. In reality, it is actually a bunch of little footprints which work in an attacker's favor. If the webpages were under the jurisdiction of one governing body, they would probably be harder to attack, since there would probably be some sort of security policy governing the content. Since this is not the case, some websites will inevitably be less secure than others. Some of the websites will follow IT best practices and others not. Even companies that have a large IT and security budget have a hard time maintaining security.

As an indicator of how secure terrorist websites (or propaganda websites with terrorist leanings) are, a simple passive scan can reveal a lot. The Burp Suite Professional scanner was used because it is considered one of the best tools by web application penetration specialists. Burp Suite Professional was used to passively scan 30 websites for probable vulnerabilities and to assess security and best practices. The Burp Suite Professional's passive scan is not truly a passive scan in the sense that it still touches the server requesting information, and then analyzes the websites itself by passing the responses to the HTTP GET request though a proxy server which analyzes the code. The term passive scan refers to the legality of the scan, which only accesses a website in a way that is authorized; it only gets

information the same way that a normal web browser would interact with the website. An active scan would include attacks such as SQL injection, but to do this legally under United States laws, an attacker would need written permission. While the passive scan is legal, the downside is it will return results that are very limited in scope, many of which cannot be confirmed without permission.

Burp Suite Professional uses a metric of high, medium, low, and information to assess the severity of an issue accompanied by a confidence level of certain, firm, and tentative. High, medium, and low are actual security concerns, while information refers to issues that are not a security concern but are contrary to accepted best practices that may lead to a compromise. The confidence level certain refers to issues that Burp Suite Professional can confirm exist. Firm and tentative confidence levels refer to issues that may exist but further investigation need to be performed to confirm they are not false positives. Below are the results of the scans performed:

Table 6.1: Vulnerability Totals

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	447	0	0	447
	Medium	0	25	0	25
	Low	459	15	0	474
	Information	9640	8003	3775	21418

These totals are the number of occurrences found with most websites containing multiple occurrences, inflating the number of issues depending on the size of the website.

The breakdown of the issues is as follows: (Grey boxes are code snippets from scan results showing the issue)[87]

- 9 sites passing passwords in clear text (High, Certain)
- 2 sites issuing an SSL cookie without a secure flag set (Medium, Firm)
- 3 sites with session tokens in URL (Medium, Firm)
- 6 sites had password fields with autocomplete enabled (Low, Certain)
- 18 sites without HttpOnly cookie flag set (Low, Firm)
- 3 sites with cookies scoped to parent domain (Information, Certain)
- 18 sites with cross domain referrer leakage (Information, Certain)
- 18 sites with Cross-domain scripts included (Information, Certain)
- 2 sites with file upload functionality (Information, Certain)
- 17 sites with email addresses disclosed (Information, Certain)
- 1 site with private IP address disclosed (Information, Certain)
- 2 sites with cacheable HTTPS response (Information, Certain)
- 28 sites with allowing frame-able responses, potential clickjacking attack vector (Information, Firm)
- 8 sites with directory listings (Information, Firm)
- 15 sites with content type incorrectly stated (Information, Firm)
- 14 sites where HTML does not specify charset (Information, Tentative)
- 9 sites where HTML uses unrecognized charsets (Information, Tentative)

[87] Burp Scan Results

6.3.1 Passing Passwords in Clear Text (High, Certain)

```
HTTP/1.1 200 OK
Date: Sat, 21 Sep 2013 15:54:45 GMT
Content-Type: text/html; charset=utf-8
Connection: close
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND
CNT"
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Expires: Sat, 21 Sep 2013 00:00:00 GMT
Last-Modified: Sat, 21 Sep 2013 15:54:44 GMT
Pragma: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 54792

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://*****"><html xmlns="http://*****" dir="rtl" lang="ar" xml:lang="ar"
...[SNIP]...
<div class="box-content"><form action="/login" method="post"><p>
...[SNIP]...
<p style="height:2em;valign:top;"><input type="password" id="password" name="password"
size="15" maxlength="25" class="inputbox autowidth" /></p>
...[SNIP]...
```

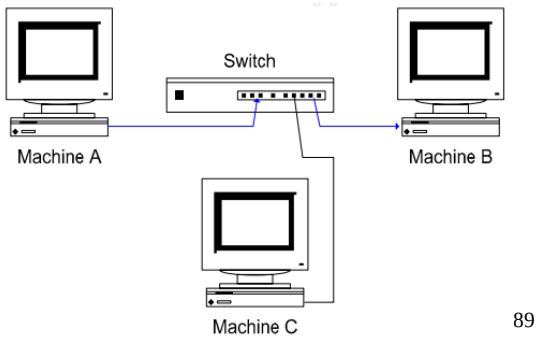
Figure 6.1: Clear Text Password Code Snippet

The submission of passwords in clear text (unencrypted) is a huge security concern because HTTP was never developed with security in mind. When one computer talks to another the packets are broadcasted to the entire network where other computers ignore packets without the proper MAC (Media Access Control) address. Essentially anyone with network packet monitoring tools such as WireShark (a popular packet analyzer software) can read, filter, and log passwords as they are submitted in real time. The usual remedy to this issue is having web traffic use HTTPS, on port 443, by encrypting the traffic using a SSL (Secure Socket Layer) certificate.

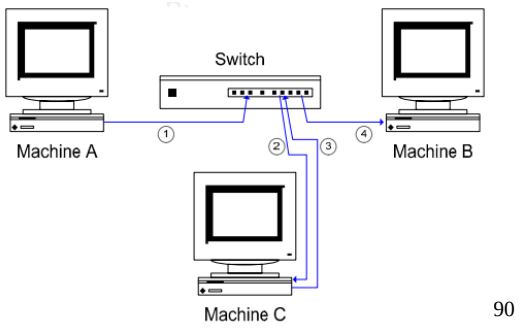
Most businesses buy SSL certificates, a form of public key cryptography, from a registered CA (Certificate Authority) that allows the web browser to automatically validate the certificate's authenticity. This ensures the visitor they have not been redirected to a site that is invalid. SSL certificates from a registered CA average about $70 per year, which is not a high cost. It is tied to the URL (Uniform Resource Locator), which is what most people enter into the web browser when they want to go to a website (for example www.google.com is a URL whereas Google's actual address is 74.125.227.195, which is the IP (Internet Protocol) address). The SSL certificate is tied to the URL and terrorist websites tend to be taken down forcing the website to be moved which could become costly. Another route, although less secure, is creating a self-signed SSL certificate for free, using software such as OpenSSL. Creating a self-signed SSL certificate is less secure because there is no CA to verify the legitimacy of the website, opening up the site to DNS (Domain Name System) redirect attacks; however, this will still encrypt the traffic, keeping passwords from being captured on a network.

Capturing passwords from unencrypted traffic is usually done on the webserver's internal network; they can also be captured on the client's network but this is inefficient since client machine has a one-to-one relationship with the webserver and webserver has a many-to-one relationship. The first step to capturing the passwords would be to gain access to the webserver's internal network. The easiest way is to rent a server at the same hosting company. If the hosting company uses a network hub to route internal traffic programs (such as WireShark) it can be set into promiscuous mode, capturing traffic not intended for their specific server, and a filter can be set to capture passwords. However, most webserver hosts

will usually be found in a switched environment which makes capturing packets more difficult, because switches will resolve where the packets need to go and only send them to the intended machine. Switched environments only offer limited protection from packet sniffing due to man-in-the-middle attacks, forcing network traffic from machine A to machine B to first travel through machine C—the attacker's machine. Man-in-the-middle attacks are accomplished by ARP (Address Resolution Protocol) spoofing, port stealing, DHCP (Dynamic Host Configuration Protocol), MAC flooding/duplicating, or ICMP (Internet Control Message Protocol) redirection. These techniques trick the switch into thinking that machine C is really machine B, and machine B into thinking machine C is really machine A. This causes all traffic to flow though the attacker's machine before it is sent to the intended target.[88]



89



90

Normal Traffic **Traffice in a man-in-the-middle attack**

Figure 6.2: Man-in-the-Middle Attack Example

[88] Tom King, "Packet Sniffing In a Switched Environment," SANS Institute InfoSec Reading Room, 2006, available at: https://www.sans.org/reading-room/whitepapers/networkdevs/packet-sniffing-switched-environment-244, 6
[89] Ibid 5
[90] Ibid 6

Sending passwords in an unecrypted environment illustrates a fundimental lack of understanding of basic cyber security, especially since there are free solutions to alievate this issue. Gathering passwords can have great intelligence value. The immediate value gained is access to the targeted system, but there is a chance for a secondary value since most people will reuse the same password for many different services (such as email). If the webserver that is targeted happens to be a message board of some kind they will usually have the user's email address stored, which (along with the password gained from the message board) may give access to the user's email account, allowing the attacker to gain more intelligence.

6.3.2 Issuing an SSL Cookie Without a Secure Flag Set (Medium, Firm)

```
        HTTP/1.0 200 OK
Date: Sat, 14 Sep 2013 17:31:34 GMT
Server: Apache/2.2.25 (Unix) mod_ssl/2.2.25 OpenSSL/1.0.1e PHP/5.3.27
X-Powered-By: PHP/5.3.27
Set-Cookie: PHPSESSID=8d838514facccccc016f8d6f001120ff; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 486
Connection: close
Content-Type: text/html;charset=Shift_JIS

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS" >
<title>Aleph...[...}.K.W...o.^.E....</title>
</head>
<body>
<center><h3>.....[...A.h...X.....[.....
...[SNIP]...
```

Figure 6.3: SSL Cookie Without a Secure Flag Code Snippet

As discussed above, SSL encrypts sensitive web traffic which is accomplished by issuing a session cookie. A session cookie is simply a small file of code sent from the

webserver to the client's computer that logs user preferences, previously selected material, webserver authentication, and, in the case of SSL, the encryption session key is embeded in it. In the code example above, the secure flag is not set; otherwise, it would have had ";secure" appended to it. This is important because while the cookie is being transmitted from the client to the web server after each navigation, the secure flag will ensure it is only transferred as long as the connection is an HTTPS connection, ensuring the cookie is encrypted. If the secure flag is not set, the cookie will be transmitted over HTTPS and unencrypted HTTP connections—as long as the connection remains in the same domain.

Many people believe that if the entire website utilizes HTTPS, the cookies will always be encrypted. Wwhile this is mostly true, an attacker can craft a link such as http://my.domain.com:443/somepage.html to cercumvent the encryption. Port 443 is the SSL channel, but because of the protocol, the browser sees "HTTP" and will send the cookie unencrypted to the server. The attacker can then use the same method of packet sniffing discussed earlier to capture the session cookie and use it in a session hijack attack. A session hijack attack allows an attacker to use a captured cookie to impersonate the victim on the webserver; gaining access to their account without having to know their username and password.[91] The downside to session hijacking is it is time sensitive, since the session token is only valid for a limited time (depending on the webserver's settings). However, it will still allow the attacker to gain access to information previously unavailable.

[91] OWASP Foundation, "Cookie Theft/Session Hijacking," OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Cookie_Theft/Session_Hijacking

Setting the SSL session cookie flag to secure is a simple part of IT best practices. Having the SSL session cookie not flagged for secure transmission illustrates a lack of knowledge of cyber security.

6.3.3 Session Tokens in URL (Medium, Firm)

```
HTTP/1.1 200 OK
Server: *****
Date: Sat, 14 Sep 2013 19:05:42 GMT
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
CF-RAY: adf59ab1c840105
Content-Length: 27361

<html>
<head>
<title>US could be going bankrupt - *****.com</title>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
<meta name="description" content="US could be goin
...[SNIP]...
<b>Source: <a
href="*****;jsessionid=XA0ZCUJPWL1Z5QFIQMFCFF4AVCBQYIV0?xml=*****">Tele
graph</a>
...[SNIP]...
```

Figure 6.4: Session Tokens in URL Code Snippet

In this example, the session token is transmitted in the URL, instead of in a cookie as in the previous example. URL submissions (such as clicking a link on a webpage) are logged in various places including 3rd party apps, webserver logs, client side logs, or even in a bookmark.[92] If an attacker is able to obtain the session tolken, they can impersonate the victim on the website, gaining access to previously denied material. If the webserver is not using an SSL connection, the session tolken can be stolen through packet sniffing. If the

[92] OWASP Foundation, "Session Fixation," OWASP Periodic Table of Vulnerabilities, 2011, available at: https://www.owasp.org/index.php/Session_fixation

webserver is using SSL, then the attacker can use the technique of sending a melious URL for the victim to click. IT best practice holds that the session tolken should be passed through a cookie with the secure flag set.

6.3.4 Password Fields with Autocomplete Enabled (Low, Certain)

```
HTTP/1.1 200 OK
Date: Sat, 21 Sep 2013 15:54:21 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND
CNT"
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Expires: Sat, 21 Sep 2013 00:00:00 GMT
Last-Modified: Sat, 21 Sep 2013 15:54:20 GMT
Pragma: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 45115

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html
xmlns="http://www.w3.org/1999/xhtml" dir="rtl" lang="ar" xml:lang="ar"
...[SNIP]...
<div class="box-content"><form action="/login" method="post"><p>
...[SNIP]...
<p style="height:2em;valign:top;"><input type="password" id="password" name="password"
size="15" maxlength="25" class="inputbox autowidth" /></p>
...[SNIP]...
```

Figure 6.5: Password Fields with Autocomplete Enabled Code Snippet

Most browsers have the ability to remember usernames and passwords for future use so the visitor does not have to re-enter it on subsequent visits. If an autocomplete=”off” tag is not included on with the password field, the browser will have a form box popup asking if the user would like the browser to remember the site. This is common on sites that want to offer convience at the cost of security. An example of the autocomplete tag switched to off can be

seen when trying to log into a financial institution's website; it should not allow the browser to remember the password due to the sensitive nature of the site. The reason sensative sites turn off autocomplete is because an attacker can retrieve stored passwords by accessing the client's machine, either locally or remotely. The storage of the websites passwords might not be of significance to the website, but if the user is a person of interest, retriving their passwords may yield access to other websites since people tend to reuse passwords.

6.3.5 HttpOnly Cookie Flag Not Set (Low, Firm)

```
HTTP/1.1 200 OK
Date: Sat, 14 Sep 2013 20:08:09 GMT
Server: Apache/2
X-Powered-By: PHP/5.3.19
Set-Cookie: PHPSESSID=oajacab9214tvcv858ak3agnb2; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding,User-Agent
Content-Length: 118932
Content-Type: text/html


<SCRIPT type=text/javascript>
<!--
var win= null;
function NewWindow(mypage,myname,w,h,scroll){
var winl = (screen.width-w)/2;
var wint = (screen.height-h)/2;
var settings ='height='+h+',';
settings
...[SNIP]...
```

Figure 6.6: HttpOnly Cookie Flag Not Set Code Snippet

Setting the HttpOnly flag protects the website's session cookie from being read by java scripts, essientially protecting it from potential XSS (Cross Site Scripting) attacks.[93] It is considered IT best practices to set the HttpOnly flag except in rare occasions when a java script needs to validate the session. The above code snippet shows the website uses java script, but that java script does not need to validate the session since that is being handled by the apache web server. If the attacker is able to use a XSS attack, they can retrieve the victim's session cookie, allowing them to impersonate the victim on the website. XSS attacks can potentially be used to infect a victims machine, allowing the attacker to gain remote access.

6.3.6 Cookies Scoped to Parent Domain (Information, Certain)

```
HTTP/1.1 200 OK
Date: Sat, 14 Sep 2013 19:09:54 GMT
Server: Microsoft-IIS/6.0
X-UA-Compatible: IE=EmulateIE7
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=dvwvqtbja1vwt2vsbq5zln55; domain=.*****; path=/;
HttpOnly
Set-Cookie: PortalTheme=Blue.ar; domain=*****; expires=Sun, 14-Sep-2014 19:09:54
GMT; path=/
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 96152

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">


<html xmlns="http://www.w3.org/1999/xhtml">
<head id="ctl00_Head1"><li
...[SNIP]...
```

Figure 6.7: Cookies Scoped to Parent Domain Code Snippet

[93] OWASP Foundation, "HttpOnly," OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/HttpOnly

Scoping a cookie to the parent domain is not strictly a vulnerability but it is against IT best practices, especially when the cookie contains a session token as the above code snipet does. When the cookie is scopped for the parent domain, a browser will send the cookie to any part of the domain, including subdomains. For most websites, this will not make a big differece because the parent domain controls and trusts all subdomains. The only time having cookie scoped to the parent domain will present a vulnerability is if the website does not control the parent domain. Many free and cheap webhosting providers will give the user a subdomain keeping them from having to pay DNS fees; for example, http://legit-page.webhost.com would be the use of a subdomain for legit-page. If the cookie is scoped to the parent domain (i.e. "webhost.com"), then any subdomain will receive the session cookie. An attacker would send a link to their page, http://attacker.webhost.com, to anyone who uses legit-page.webhost.com and receive the victim's session cookie, allowing them to impersonate the victim.

6.3.7 Cross domain referrer leakage (Information, Certain)

Cross domain referrer links are fairly common in today's website architecture. For instance, most news websites will have referrer links to Facebook, LinkedIn, and Twitter, enabling the reader to share or vote, thumbs up or down, for the article. Another example would be a referrer link to Google Analytics to measure website traffic. In fact, the Burp Suite scanner found referrer links to Facebook, LinkedIn, Twitter, Google Analytics, Pinterest, and various other third parties. The cross domain referrer links are not a vulnerability but can be a concern for security. The main issue with the cross domain referrer

links are that they can transmit information such as a URL session tolken to the third party.[94] An attacker could use a DNS redirect attack to intercept the traffic similar to the man-in-the-middle attacks discussed earlier. This could be accomplished by changing the DNS entry in the local DNS to point to the attacker's server before forwarding the traffic on to the proper recipient. Another way to gain access to the traffic is to work with companies such as Google, Twitter, or Facebook. Both senarios could, in theory, be used to inject milicious code into the victim's computer.

6.3.8 Cross-Domain Scripts Included (Information, Certain)

Including cross domain scripts is a potential security concern because the parent website sets the visitor's browser security and the script, which is executed in the browser. The script has the ability to do anything the parent web application has the rights to do. Generally, when a website uses cross-domain scripts, they trust the script's source; but if the administrator for the website does not understand the security implications, it can quickly become a vulnerability. It is also possible to use a man-in-the-middle attack to capture the script in transit, modify it, and pass it on to the victim using automation, thus making it transparent to the victim. This assumes the script is not transmitted over an SSL connection that has not been comprimised. At the very least it gives an attacker another vector for attack; if the parent website has hardened security, the website hosting the script might be more vulnerable.

[94] Sebastian Lekies, Tighzert, Walter, "Client-Side Cross-Domain Requests in the Web Browser: Techniques, Policies and Security Pitfalls," OWASP Foundation, 2011, available at: https://www.owasp.org/images/7/78/05A_Client-Side_Cross-Domain_Requests_-_Sebastian_Lekies%2BWalter_Tighzert.pdf, 4

6.3.9 File Upload Functionality (Information, Certain)

```
HTTP/1.1 200 OK
Date: Sat, 14 Sep 2013 17:23:28 GMT
Server: Apache/1.3.42 (Unix) PHP/5.2.14 mod_log_bytes/1.2 mod_bwlimited/1.4
mod_auth_passthrough/1.8 FrontPage/5.0.2.2635 mod_ssl/2.8.31 OpenSSL/0.9.8e-fips-rhel5
X-Powered-By: PHP/5.2.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html
Content-Length: 23135


<title>..... ..... .. ..... - .....</title>
<body onload="setInterval('blinkIt()',500)">

<script type="text/javascript">
function blinkIt() {
if (!document.all) return
...[SNIP]...
<td>
<input type="file" name="userfile" >

<input type="hidden" name="MAX_FILE_SIZE" value="6144">
...[SNIP]...
```

Figure 6.8: File Upload Functionality Code Snippet

File upload functionality can potentially given an attacker many modes of attack, including file path traversal, persistant XSS, placing client-side executable code on the domain, transmission of viruses, and DoS (Denial of Service).[95] These attacks largely depend on vulnerabilities and settings in the FTP (File Transfer Protocol) software the webserver is using. Many of these vulnerabilities are archived at websites (such as SecurityFocus). Gaining the FTP software name and version number is a trivial matter of doing a banner request with software such as nmap.

[95] Burp Scan Report

A file path traversal attack allows the attacker to start a file upload but craft the file name in such a way to gain access file and folders not typically accessable by a normal visitor, which is only limited on the permission level the webserver is running under in the OS (Operating System). For example, uploading a file called "../../../../etc/passwd%00.pdf" could potentially display the password file, containing usernames and passwords, assuming the webserver has read access to the passwd file.[96] The "../" part of the filename tells the OS to go to the previous directory, in our example four times. The next part, "etc/passwd," tells the OS to dump the contents of the passwd file, which will generally appear in error content on the webpage as the FTP software errors. The last part, "%00.pdf," is there in case the FTP software requires a certain file extension, and in this case a Null byte "%00" is sent, which causes most applications to drop anything after the Null byte as garbage.[97] If the FTP software does not allow "../" in the filename "%2e%2e%2f," or other variants can be used that may get around any filtering. This example not only gives the attacker the ability to crack users' passwords but also the ability to set themselves up as a root equivilant, or unrestricted, user if the webserver has write access to the password file. This can be accomplished by copying all the users and passwords and then crafting another passwd file including an extra user with its own encrypted passwords—or simply leaving the password blank.

Persistant XSS and placing of client-side executable code on the domain can occur if the FTP software does not parse out malicious code. XSS can occure if the FTP software allows the attacker to upload a malicious script, which can be executed as part of the normal

[96] OWASP Foundation, "Path Traversal," OWASP Periodic Table of Vulnerabilities, 2009, available at: https://www.owasp.org/index.php/Path_Traversal
[97] Ibid

web application by other visitors.[98] Similarly, client-side executable code can be uploaded and then a link can be sent to the victim, which would run with the same security settings allowed by the website. Viruses and also be uploaded, and, depending on how the web application handles the files, it can target the webserver itself or a link can be sent to a victim to infect their machine.

DoS are potentially the easiest to perform with file upload functionality. One way to accomplish the DoS attack is to upload a very large file overloading the alloted space the webserver has available. For example, if the webserver has 1Gb of space available and the attack attempts to upload a 2Gb file, visitors will not be able to upload more files. In addition, if the webserver uses the same partition as the filestore for executing code, it could potentially take the entire website down. This method is not particularly useful to intelligence gathering and it is worth noting that the above code snippit has a max file size value set to protect from this sort of attack. Another way to preform the DoS is to upload a file with a very large name, for example, 2,000 charaters long. Many FTP programs can not handle files with such a long namespace and will generally crash, thus not being available to visitors until the FTP service is restarted. This method can have benefits for intelligence because a buffer stack overflow attack can be used to gain remote access to the server.

6.3.10 Email Addresses Disclosed (Information, Certain)

Many websites disclose email addresses, such as someone@domain.com, and not constitute a vulnerability. However, email addresses can be useful to an attacker. Most email addresses will be for administrators of a website which can be used in a social engineering attack known as Phishing. In a Phishing, attack the attacker can craft documents, or the

[98] OWASP Foundation, "Cross-site Scripting (XSS)," OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

HTML in the email can be malicious, thus allowing access to the victim's computer (in this case, the website administrator). This potentially allows the attacker to gain access to the administrator's credentials for the website. The presence of email addresses that correspond to the same domain as the website also gives the attack that person's username on the website. If it is a developer's account it would be a good target for the attacker to break into, which is why most websites use anonymous email addresses such as helpdesk@domain.com.

6.3.11 Private IP Address Disclosed (Information, Certain)

```
HTTP/1.1 200 OK
Date: Sat, 21 Sep 2013 15:55:52 GMT
Content-Type: text/html; charset=utf-8
Connection: close
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND
CNT"
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Expires: Sat, 21 Sep 2013 00:00:00 GMT
Last-Modified: Sat, 21 Sep 2013 15:55:51 GMT
Pragma: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 65436

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html
xmlns="http://www.w3.org/1999/xhtml" dir="rtl" lang="ar" xml:lang="ar"
...[SNIP]...
<a href="http://*****/viewtopic?t=15757&amp;topic_name" target="_blank" title="..... ....
..... Media Convert Master 10.0.2.36">..... .... ..... Media Convert
Master 10.0.2.36 </a>
...[SNIP]...
```

Figure 6.9: Private IP Address Disclosed Code Snippet

Having a private (internal) IP address disclosed in a webpage, whether it is visible to the visitor or as part of the website's code, does not constitute a vulnerability, but is against IT best practices. There is no legitimate reason for an internal IP address to be disclosed in a website. By gaining the internal IP address for the server, it tells the attacker if the server sits

on a Class A (10.0.0.0-10.255.255.255), Class B (172.16.0.0-172.31.255.255), or Class C (192.168.0.0-192.168.255.255) network which will help gain time in the enumeration phase of an attack. The attacker will also know the internal IP address to the target machine if they are able to access the network through another route, instead of having to try to figure out which machine it is.

6.3.12 Cacheable HTTPS Response (Information, Certain)

Cacheable HTTPS responses are contrary to IT best practices simply because data retrieved via HTTPS are generally sensative in nature. Having HTTPS webpages with cashing enabled generally saves, caches, the website visited when using most browsers. This does not pose a risk to the webserver, but if an attacker is able to gain access, physical or remote, to a victim's machine, then website traffic that is generally encrypted can be retrieved. For example, most financial institutions turn off cacheable response when a visitor logs in and looks at their transaction history. With it turned on an attacker will be able to retrieve this information without having to log into the server.

6.3.13 Allowing Frame-able Responses, Potential Clickjacking Attack Vector (Information, Firm)

This issue is generally found on forums or websites that allow users to comment on the websites content. These functions should not allow frame-able responses because an attacker could potentially insert an iframe in the comment, making this frame with 100% opaque and on the top layer of the website. This frame could cover up other buttons or links on the website so when a visitor clicks what they believes is a legitimate link it can do what the attacker intended. An attacker, for example, could craft an iframe to exploit a victim's Adobe Flash plugin in the browser, changing the security settings and allowing the attacker to

use the victim's microphone and web camera.[99] With frame-able responses there is also the potential for a type of XSS exploit called XFS (Cross Frame Scripting).[100] This type of attack can be prevented by having the web application return the X-FRAME-OPTIONS value as DENY, which the websites that this issue was found in did not return.[101] Other techniques exist that attempt to do the same thing but can be circumvented by an attacker.[102]

6.3.14 Directory Listings (Information, Firm)

Directory listings are not a vulnerability but are generally frowned apon in IT best practices. When a directory listing is visable on a website it generally means the webserver has been misconfigured.[103] Having directory listing available could potentially divulge sensative information that would otherwise be obfuscated. Even if no sensitive information is divulged, a directory listing can quickly allow an attacker to identify interesting resources to start analyzing and attacking.[104]

6.3.15 Content Type Incorrectly Stated (Information, Firm)

Content type incorrectly stated is not a direct vulnerability but it can cause browsers to act in unexpected ways. This happens because browsers will detect an anomaly when attempting to open the file. It will then attempt to figure out it's MIME type and open it with the proper protocol which may not be the correct protocol. This is usually not of any

[99] OWASP Foundation, "Clickjacking," OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/Clickjacking
[100] OWASP Foundation, "Cross Frame Scripting," OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/Cross_Frame_Scripting
[101] Burp Suite Report
[102] Ibid
[103]OWASP Foundation, "Directory Indexing," OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Directory_Indexing
[104] Burp Suite Report

consequence unless the content is user uploaded, in which case, an attacker can use XSS or other client side attacks an victims.[105]

6.3.16 HTML Does Not Specify Charset (Information, Tentative)

```
HTTP/1.1 200 OK
Date: Sat, 21 Sep 2013 15:54:44 GMT
Content-Type: text/html
Connection: close
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 2168

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html>
<head>
<*****.net="verify-v1" content="8GPGB5/JV4ObT3OS31lsXi37oZSHrrdK/1
...[SNIP]...
```

Figure 6.10: HTML Does Not Specify Charset Code Snippet

Specifying the character set tells the browser how to interpret the website's content. Without a character set specified, the browser will attempt to determine what charset to use but can have unexpected results. If the website allows user responses, an attacker can insert non-standard characters such as UTF-7 to engage in a XSS attack which might normally be blocked by filters looking for responses in the standard UTF-8 format.[106] IT best practice is to specify the standard UTF-8 or other character set by including charset=UTF-8 in the content type header, although any content header can be used as long as the website's content filters are set to detect malicious code in that character set.

[105] Ibid
[106] Ibid

6.3.17 HTML Uses Unrecognized Charsets (Information, Tentative)

Unrecognizable character sets are generally the result of a typographical error in the coding or the use of a non-standard character set that is not a universal character set to most browsers.[107] When a browser receives an unrecognizable character set it will attempt to figure out the proper character set; this may lead to unexpected results, including not specifying a character set at all, such as in the previous issue.

6.3.18 Vulnerability Scan Conclusion

Each of the thirty sites in the passive scan had one or more issue. Many of the sites had major issues that could allow an attack to infiltrate the webserver itself, gather user credentials, or attack a visitor's computer directly. Most sites exhibited a variety of "informational" issues that range from not following IT best practices to potential attack vectors. While many of the issues are not confirmed (due to legal constraints) it is clear that the administrators of the scanned websites do not possess a fundamental understanding of cyber security, and many more vulnerabilities can probably be uncovered with an active scan.

6.4 Cost Analysis of Cyber Espionage Operation

Cyber espionage campaigns such as Red October, Operation Aurora, Titan Rain, and in particular GhostNet show us that cyber espionage is not just theoretical but practical. From the Burp Suite Professional passive vulnerability scan it appears that terrorist websites are poorly secured. There is one question that remains: Is it economically feasible to assemble a small team of experts, properly equipped, to gather intelligence on potential terrorist activities

[107] Ibid

to feed to various intelligence agencies? Good security professionals are not cheap, and entry level personnel would not be ideal for this kind of operation. Equipment will constitute the majority of the initial setup costs; servers, desktops, networking equipment, and popular devices, such as Apple and Android devices, will need to be purchased.

6.4.1 The Team

Team members would include a Penetration Specialist, Social Engineer, Reverse Engineering Specialist, Intrusion Detection Specialist, and a Language Specialist. A Penetration Specialist, known in the industry as a Penetration Tester, is responsible for the actual attacks. This includes initial scans of the target, enumerating services, finding potential vectors of attack, and the initial and continued exploitation of the target. They are also responsible for developing and testing exploits in an internal lab to ensure the attacks go unnoticed. The Penetration Specialist would need to be experienced and versatile since the initial target would be an affiliated terrorist website, but the webserver is only the staging ground to gain access to personal equipment a potential terrorist may have; this would include personal computers running Windows, Mac, and Linux OSes. Other targets would include devices such as smart phones, tablets, and netbooks. As of November 4th 2013, the median pay for a Penetration Specialist in the US is $92,000 per year.[108]

Social engineers deal with hacking the human brain. Social engineering attacks complement a Penetration Specialist's efforts. Social engineers not only conduct spear phishing campaigns, but specialize in getting sensitive information from people without their

[108] Indeed.com, "Penetration Tester Salary" 2013, available at: http://www.indeed.com/salary?q1=Penetration+Tester&l1=

knowledge. Spear phishing attacks are usually targeted email sent to individuals that get the victim to run malicious code on their computer or click a link taking them to a malicious website that can exploit their computer. Many social engineers are skilled at getting people to divulge sensitive information through seemingly innocuous conversation. Arguably, the most famous social engineer of our time is Kevin Mitnick. As of November 4th 2013, the median salary for a Social engineer is $89,000 per year.[109]

Reverse Engineering Specialists reverse engineer compiled programs to figure out how they work. They can be used to reverse engineer programs that servers, or computers, run to find zero day exploits. Zero day exploits are vulnerabilities in software that is not known to the software manufacturer or antivirus companies; this allows attacks to go undetected. Reverse engineering commercial software is only part of the Reverse Engineering Specialist's job; they would also need to reverse engineer other malware and viruses to allow the Penetration Specialist to incorporate them in their attacks. As of November 4th 2013, the median salary for a Reverse Engineering Specialist is $84,000 per year.[110]

The Intrusion Detection Specialist is one of the most important positions in a cyber espionage campaign. In the business industry, the Intrusion Detection Specialist monitors network traffic, with the aid of IDS/IPS (Intrusion Detection System/Intrusion Prevention System) software packages, for indications of a compromise. In this type of enterprise, they would be responsible for attempting to detect the Penetration Specialist's attempts to

[109]Indeed.com, "Social Engineer Salary" 2013, available at: http://www.indeed.com/salary?q1=social+engineer&l1=
[110] Indeed.com, "Reverse Engineer Salary" 2013, available at: http://www.indeed.com/salary?q1=reverse+engineer&l1=

compromise systems in the penetration testing lab to find various automated software, such as the SourceFire, Cisco IPS 4200, Juniper IPS, and TippingPoint. While the IDS/IPS software packages monitor network traffic for presence of exploits, it is also important to run attacks against various antivirus software. When an attack is detected, the Intrusion Detection Specialist will need to work with the Penetration Specialist to make the attack transparent to the software; stealth is the key to success in a cyber espionage campaign. The Intrusion Detection Specialist will need to continually monitor existing exploits being used for detection. If detection is possible, they will need to work with the Penetration Specialist to remove the detectable module and replace it with a module that is not detectable. As of November 4th 2013, the median salary for an Intrusion Detection Specialist is $75,000 per year.[111]

Finally, a Language Specialist will be needed because sooner or later the terrorist's native language will need to be used. The Language Specialist works with the Penetration and Social Engineering Specialists. The Penetration Specialist needs a Language Specialist to help identify worthwhile targets, such as areas of a website to use to infect potential terrorist's devices. The Social Engineering Specialist needs the Language Specialist to help craft spear phishing campaigns in foreign languages as well as to communicate with potential terrorists. Unfortunately, a wide variety of languages and dialects will probably need to be utilized making hiring a full time staff very costly. The most efficient use of resources will be to partner with other intelligence agencies, such as the DIA or CIA, on an ad-hoc basis to utilize their language specialists when needed.

[111] Indeed.com, "Intrusion Detection Salary" 2013, available at: http://www.indeed.com/salary?q1=Intrusion+detection+specialists+&l1=

6.4.2 Hardware Requirements

To support the team, a number of different equipment will need to be purchased. First the team will need desktops to complete work ranging from launching attacks to translating communications. Servers will need to be built for password file breaking; this ranges from brute force attacks to hosting rainbow tables, which are precompiled password hashes that speed up the process of password recovery. The bulk of the cost for the equipment will come from the penetration lab. The importance of the penetration lab is to test out attacks before putting them in practice to make sure they not only work but do not just crash the target's computer, thus tipping your hand.

Desktops will not need to be very powerful since they will be for regular office use; a simple midrange desktop will run approximately $500 each.[112] Brute forcing passwords and constructing rainbow tables will need serious computing power which a super computer would be ideal for, but are generally far too expensive. A cheaper alternative is to purchase a GPU high performance server. These servers range dramatically from several thousands of dollars to hundreds of thousands of dollars. A decent GPU server for passwords can be built for approximately $20,000 that will be able to crack eight or nine character passwords in a few days. Anything with longer passwords than nine characters and it would be worth acquiring time on supercomputers at the NSA or universities, especially for building vast rainbow tables. Rainbow tables require a lot of storage space, and separate rainbow tables would need to be computed for each type of password hashing method, such as NTLM, MD5, or SHA1. A 12 Terabyte NAS (Network Attached Storage) device should be able to

[112] Dell.com, "OptiPlex: Business class performance desktops," 2013, available at: http://www.dell.com/us/business/p/desktops-n-workstations?~ck=mn

accommodate most rainbow table needs and can be expanded if necessary. The Seagate BlackArmor NAS 440 12TB can be purchased for $1,800.[113]

The penetration testing lab will need to host multiple OSes with multiple configurations, such as security patch updates, to test vulnerabilities on. A VM (Virtual Machine) server will help keep costs down by using one set of hardware to host multiple OSes and their configurations. The Dell PowerEdge M620 midrange server is fairly standard for this type of setup and costs about $3,000.[114] Another VM server should be purchased to host IDS/IPS software, allowing for physical separation between the target machines and the IDS/IPS machines ensuring network traffic flows through physical switches, routers, and hubs to simulate real world setups. At least one switch, router, hub, and firewall should be purchased for the lab. Cisco products are the IT standard that most enterprise setups will have. A Cisco Catalyst 2960 48 port switch will cost about $2,900.[115] A Cisco RV016 router costs about $340.[116] A small Cisco Hub will be more than adequate for most penetration testing labs and costs about $34.[117] A Cisco ASA 5505 firewall will cost about $1,050.[118]

[113] Amazon.com, "Seagate BlackArmor NAS 440 4-Bay 12 TB (4 x 3 TB) Network Attached Storage STAU12000100," 2013, available at: http://www.amazon.com/Seagate-BlackArmor-Network-Attached-STAU12000100/dp/B0044UCGDQ

[114] Dell.com, "PowerEdge M620 Blade Server," 2013, available at: http://www.dell.com/us/business/p/poweredge-m620/fs

[115] Newegg.com, "CISCO Catalyst 2960 WS-C2960S-48TS-L 10/100/1000Mbps Ethernet Switch," 2013, available at: http://www.newegg.com/Product/Product.aspx?Item=N82E16833120540

[116] Newegg.com, "Cisco Small Business RV016 Multi-WAN VPN Router 2 x 10/100Mbps WAN Ports 13 x 10/100Mbps LAN Ports," 2013, available at: http://www.newegg.com/Product/Product.aspx?gclid=CL30xtnT0boCFWpk7AodEyMAXA&Item=N82E16833124154

[117] Newegg.com, "Cisco Small Business 100 Series SF100D-05-NA Unmanaged 10/100Mbps 5-Port Desktop Switch," 2013, available at: http://www.newegg.com/Product/Product.aspx?gclid=CJXUpJrU0boCFcnm7AoddSMAXA&Item=N82E16833150145

[118] Newegg.com, "Cisco ASA 5505 Network Security Appliance," 2013, available at: http://www.newegg.com/Product/Product.aspx?gclid=CM3jgurU0boCFU9o7AodAAgAHA&Item=N82E16833420109

Popular smartphones and tablets should also be purchased for the penetration testing lab. It is true that virtual machines can be set up to test attacks using SDKs (Software Developer Kits), but different hardware will interact with the OS differently when attempting to exploit them since manufacturers implement small changes to the OS. Manufacturers also install many applications by default which one study has concluded results in 60% of all vulnerabilities for smart phones.[119] It is safe to assume that on average these devices cost approximately $500 each, and to give the penetration testing lab a variety of popular devices 10 smart phones and 10 tables should be budgeted for. This will cost approximately $10,000.

6.4.3 Software Requirements

The VM servers will need an operational OS that hosts the VMs. A popular VM server is the VMware vSphere Enterprise which costs $2,875, which would need to be purchased for both VM servers. The OSes that run as virtual machines will need to be purchased as well; examples of these OSes would be Windows XP, Windows 7, Windows 8, Windows 2003 Server, Windows 2008 Server, Windows 2012 Server, Mac OSX, to name a few. OSes that have reached their official end of life should not be ignored because many personal computers as well as computers in the enterprise will often include these as well. A comfortable budget of $5,000 should be able to cover most popular OSes license needs.

IDS/IPS software/hardware (some IDS/IPS solutions are hardware based) will need to be purchased for popular enterprise solutions, such as SourceFire, Cisco IPS 4200, Juniper

[119] Lei Wu, et al, "The Impact of Vendor Customizations on Android Security," Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communication Security, 2013: 634

IPS, and TippingPoint. The SourceFire IPS costs about $9,000.[120] The Cisco IPS 4200 costs about $14,855.[121] The Juniper IPS solution costs about $4,500.[122] The TippingPoint IDS costs about $25,000.[123] The Intrusion Detection Specialist will also need to set up a virus scanning solution similar to Virus Total's, which uses 46 different virus scanners to scan for threats.[124] Virus Total could be used but it is not advised, since files being scanned will be used for future signatures and dispersed to virus scanner companies. Instead a subscription to the independent scanner companies should be used which would cost about $2,300 a year (assuming the average subscription cost is $50 for each yearly subscription).

6.4.4 Operational Costs

Table 6.2: Operational Cost Breakdown

Yearly Costs	
Penetration Specialist	$92,000
Social Engineer	$89,000
Reverse Engineering Specialist	$84,000
Intrusion Detection Specialist	$75,000
Virus Scanner Subscriptions	$2,300
Total	$342,300
Initial Setup Costs	
Desktops x5	$2,500
GPU Server	$20,000
12TB NAS	$1,800
Dell PowerEdge M620 x2	$6,000

[120] Michael Lipinski, "Sourcefire Next-Generation IPS v4.9," SC Magazine, 2011, available at: http://www.scmagazine.com/sourcefire-next-generation-ips-v49/review/3417/
[121] CDW.com, "Cisco IPS 4260 Sensor," 2013, available at: http://www.cdw.com/shop/products/Cisco-IPS-4260-Sensor/1090319.aspx
[122] NetworkScreen.com, "Juniper Networks SSG520M Appliance," 2013, available at: http://www.networkscreen.com/SSG520M.asp?gclid=CKaSht3i0boCFU8V7AodzCAAuQ
[123] SC Magazine, "TippingPoint UnityOne-1200 (Special report Intrusion prevention)," 2013, available at: http://www.scmagazine.com/tippingpoint-unityone-1200-special-report-intrusion-prevention/product/915/
[124] Virustotal.com, "Credits & Acknowledgements," 2013, available at: https://www.virustotal.com/en/about/credits/

Cisco Catalyst 2960	$2,900
Cisco RV016 Router	$340
Cisco Hub	$34
Cisco ASA 5505 Firewall	$1,050
Popular Devices	$10,000
VMware vSphere Enterprise x2	$5,750
OS Budget	$5,000
SourceFire IPS	$9,000
Cisco IPS 4200	$14,855
Juniper IPS	$4,500
TippingPoint IDS	$25,000
Total	$108,729
First Year of Operation	$451,029

The initial setup costs for the cyber espionage operation is approximately $108,729. The bulk of this cost is to setup the penetration testing lab. If the staff of the operation is only one individual per position, the yearly reoccurring costs will be approximately $342,300. If the operation proves a success, more staff may be added, until then, a small staff should be used to prove that a return on investment is achievable. The total for the first year of operation is approximately $451,029; this does not include office space rental or cost of language specialists. If the leaked intelligence "black budget" is to be believed, the US will spend $52.6 billion on intelligence in 2013.[125] Assuming this is correct, the initial cost for operation would constitute only .0009% of the intelligence budget, suggesting this would be an acceptable cost.

[125] Barton Gellman, Miller, Greg, "U.S. spy network's successes, failures and objectives detailed in 'black budget' summary," Washington Post (Aug 2013), available at: http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

7. Analysis

Table 7.1: Qualitative Analysis Rankings

	Qualitative Value				
	1	2	3	4	5
Attack Surface				X	
Longevity of Cyber Espionage Campaigns					X
Vulnerabilities					X
Cost					X
Average					4.8

The attack surface, or terrorist web presence, was evaluated as follows: one for no attack surface; two for a very small attack surface with most terrorist organizations not having websites; three representing most terrorists organizations having one website; four representing most terrorist organizations have one website but some with multiple websites; and five representing most terrorist websites having multiple websites. Research showed that almost all transnational terrorist organizations have at least one website, and many, such as Al-Qaeda, have multiple websites. The majority of smaller extremist groups located within the United States were shown to have at least one web site, but a sizeable amount did not have a website. These smaller extremist groups are not excluded from the analysis because they are based in the United States and can pose a possible terrorist threat. Due to the lack of websites for the smaller extremist groups, the value given to the attackable surface is four.

The longevity of cyber espionage campaigns was evaluated as follows: one representing a few days; two representing a few weeks; three will representing at least six months; four will representing at least one year; and five will representing two years or greater. There were not many widely publicized cyber espionage campaigns to draw

conclusions from. Of the four cyber espionage campaigns evaluated, Titan Rain, Operation Aurora, and Red October had the greatest operational time frames; Titan Rain and Red October operated at least three years while Red October operated for at least five years before discovery. GhostNet was the shortest-lived, being discovered shortly after one year, despite being discovered it operated for almost two years. Even though GhostNet fell just shy of the two year qualification, the value given to the longevity of cyber espionage campaigns is five since the other cyber espionage campaigns were in operation for three years or longer.

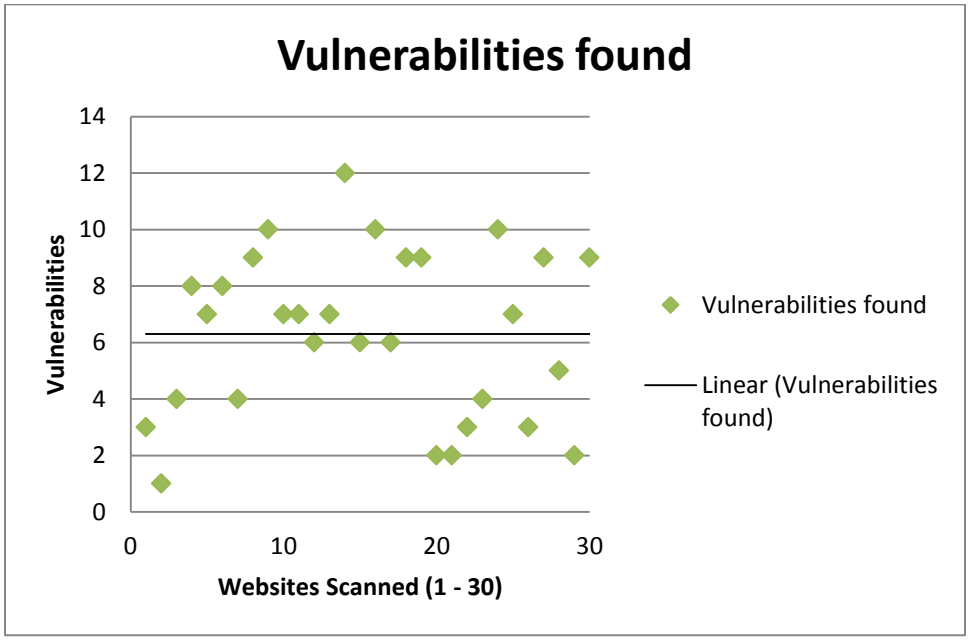


Figure 7.1: Vulnerability Distribution

To evaluate how vulnerable terrorist websites may be, a small sample of 30 terrorist and extremist group websites were passively scanned for vulnerabilities and other issues that may lead to a compromise. The qualitative evaluation for vulnerabilities was as follows: one representing no issues; two representing most websites having at least one issue; three representing all sites having one issue; four representing some sites having more than one issue; and five representing all sites having multiple issues. Of these 30 websites all (except

one) had more than one vulnerability. The average vulnerability per website was 6.3. The exception was a very small website with only a handful of pages, suggesting this instance was an outlier. The maximum number of vulnerabilities found was 12. The qualitative value given to the vulnerabilities was five.

A cost analysis was performed to calculate the cost of a generic setup for a cyber espionage team to evaluate the feasibility of implementing such a team. If operational costs are too high, then using cyber espionage to combat terrorism will not be feasible. To evaluate the cost of the operation, the first year of costs (which include yearly costs, such as salary, and initial setup costs) will be used. One will represent greater than ten million dollars; two will represent greater than five million dollars; three will represent greater than three million dollars; four will represent greater than one million dollars; and five will represent less than one million dollars. The yearly reoccurring costs that support the team's salary (a four person team without language specialists) and subscription service to virus scanner companies are calculated as $342,300. The initial setup cost, which includes operational equipment and a penetration lab, was calculated at $108,729. The total for the first year of operation is $451,029, which is substantially less than one million dollars, giving the qualitative value of five.

The findings suggest that cyber espionage is an extremely viable tool to combat terrorism. Terrorists have a very big attackable surface given their web presence, and their websites have been shown to have a number of possible vulnerabilities. Of the known cyber espionage campaigns, it has been shown that cyber espionage can be used to gather intelligence over extended periods of time. The cost of outfitting and running a cyber espionage campaign is very reasonable, especially compared to other intelligence budgets.

Future studies on this subject should address issues of analysis in longevity of cyber espionage campaigns and the vulnerability of terrorist websites. Cyber espionage is a relatively new topic providing an extremely small sample size. As time progresses, it is assumed that more cyber espionage campaigns will become known, expanding the sample size. Vulnerability of terrorist websites provides another avenue of expansion. Only 30 websites were passively scanned; this was due to the vulnerability assessment being only a fraction of the total analysis, but the 30 websites provided thousands of pages in the vulnerability assessment report. Another issue with the vulnerability scan is it was passive, meaning that many of the issues being found could not be confirmed. The passive scan was chosen due to legal restrictions but an active scan would not only help confirm vulnerabilities but would also provide many more vulnerabilities (such as SQL injection attacks) that could not be performed in a passive scan.

8. Conclusion

The world has changed dramatically in the last 20 years. 20 years ago, the Cold War had just ended and everyone thought it was safe to breathe once again. Terrorism was not on most American's minds; it was something that only happened in other countries. The entirety of the web could be backed up and stored on a modern hard drive. The web was a toy for geeks, scientists, and businesses were barely beginning to take notice. Now, in 2013, everyone uses the web in their daily lives, terrorism is on the forefront of debate, and most Americans carry the same computing power available in 1993 in their pocket.

Like most businesses, terrorists have adopted technology to collaborate, train, fund, and reach wider audiences than ever before. Law enforcement agencies are poorly equipped to deal with terrorists using the web, since websites are hosted in one country today and possibly another tomorrow. Intelligence agencies can listen to as many phone calls as they want and never get the full picture, since almost everything happens online. Collecting the world's web traffic is an inefficient and futile task. The majority of web traffic has no intelligence value pertaining to terrorism, and attempting to collate and filter this data is a monumental task that, even if successful, will not produce much usable intelligence and will be a huge drain on taxpayer dollars. Targeted attacks in the form of cyber espionage will not only be more cost effective but will probably produce much more actionable intelligence.

By using cyber espionage, intelligence can be gathered stealthily from primary sources by compromising websites that terrorists use to collaborate and train. Using the websites as a staging point, the personal devices of the terrorists can be compromised enabling an in-depth social networking analysis to be conducted. Being able to track a terrorist by GPS 24/7 on

their smartphone could provide tremendous intelligence. Using their phone as a bugging device by turning on the microphone could provide even more intelligence. Encrypted communications can be intercepted before encryption ever takes place. The use of cyber espionage can open up many possibilities.

As in any intelligence operation, there is potential for abuse. Cyber espionage in particular is incredibly invasive, given how technology is so intertwined in everyday life. Proper oversight on targeting and collection is critical. A governing body, such as the FISA court, should be assembled with people who not only understand the legal and ethical ramifications but also understand technology in a way that they truly comprehend what is being asked of them. Cyber espionage can be a powerful in the war on terror, but without proper safeguards in place, an Orwellian society becomes a very real possibility.

Glossary of Technical Terms

Active Web Vulnerability Scan – A vulnerability scan performed on a website that is invasive, attempting to circumvent security measures.

Antivirus – Commercial software that searches for, identifies, and removes computer viruses by matching known heuristic patters.

ARP – Address Resolution Protocol, part of the computer network layer used to resolve network IP address to corresponding MAC addresses.

Browser – Software that interprets webpages to viewed. Examples are Internet Explorer, Google Chrome, and Mozilla Firefox

Buffer Stack Overflow Attack – An attack that overflows a software's allotted memory buffer in RAM allowing an attacker to gain access to other parts of an OS's memory location. This attack is often used to inject a payload that will give an attacker remote access to the computer.

Burp Suite Professional – A popular software suite that is used for evaluating web application and website security.

CA – Certificate Authority, an entity that issues SSL certificates that browsers can then query to insure a valid certificate is being used.

Character Set – A predetermined set of characters that computers use such as ASCII, UTF-7, and UTF-8 to display fonts.

Client – A computer that is initiating a connection to another computer, usually a webserver.

Cookie – A small piece of data that is stored in a user's browser that tracks movement and stores user preferences.

DHCP – Dynamic Host Configuration Protocol, is used to automatically issue an unused IP address to a computer connecting to a network.

DNS – Domain Name System, is a hierarchical distributed naming system used to resolve domain names, such as google.com, to their corresponding IP address, such as 74.125.227.174.

Domain – Domain Name, is the name given to a specific website for ease of access. An example is google.com is the Domain of www.google.com.

DoS – Denial of Service attack, an attack that is made in an attempt to deny the use of a web service to its intended users.

EXIF data – Exchangeable Image File Format, a standard that uses Metadata imbedded in image files to simplify the use of the image across multiple software and OS platforms.

Firewall – A piece of software or hardware that analyzes incoming and outgoing network packets to allow or deny transmission to its indented recipient based on a set of rules.

FTP – File Transfer Protocol, a standard network protocol for the transmission of uploading or downloading files from one computer to another.

Honeypots – Computers that are employed by security research and connected to the internet that mimics vulnerabilities. When the Honeypot is attacked it captures any binaries that are transferred, runs them in a sandbox, and logs the malware's activities.

HTTP – Hypertext Transfer Protocol, is the tag based programming language that is the basis for the world wide web.

HTTPS – Hypertext Transfer Protocol Secure, is the standard protocol for secure transmission of HTTP, usually achieved by SSL encryption.

ICMP – Internet Control Message Protocol, is used by various networking devices such as routers to send messages to other devices.

IDS – Intrusion Detection System – Is a system of software or hardware that monitors network traffic in an attempt to discover malicious traffic.

IPS – Intrusion Prevention System – Is much like an IDS but goes a step further and not only detects malicious traffic but also attempts to actively prevent the transmission of the malicious traffic.

Iframe – is an inline frame that allows a document to be placed inside an existing frame on a HTML document.

IP address – Internet Protocol address, a numerical address that is assigned to a device that is connected to a computer network.

MAC address – Media Access Control address, is a unique identifier assigned by a manufactured to all network interface hardware.

Metadata – Is data about data, it is often attached to computer files to be accessed by software for various reasons.

MIME – Multipurpose Internet Mail Extensions, was originally created to extend the functionality of emails to handle non-standard character sets and non-text attachments, it has sense been extended to HTML use as well.

Network Hub – Is a device that is used to connect multiple Ethernet connections to work as one network segment.

Network Router – Is a device that forwards traffic between networks and is the underpinning infrastructure of the internet.

Network Switch – Is a device that receives network traffic and only forwards the traffic on to the intended recipient.

OS – Operating System, is a software package that communicates directly with computer hardware acting as a bridge between most software and the hardware.

Passive Web Vulnerability Scan – A vulnerability scan that only intercepts a website's code that is accessible through normal browsing; it then checks the code for potential vulnerabilities.

Phishing – Is an attempt to obtain sensitive information, through email, from a target by masquerading as a trusted source.

RAT – Remote Access Tool, a piece of software that allows access and control of a computer over a network by another computer.

Spear Phishing – Is a phishing campaign that is specifically tailored to the recipient in order to grain trust.

Spoofing – Is the act of falsifying data to masquerade as another, usually trusted, source.

SQL – Structured Query Language, is a type of programming language used in relational databases.

SQL Injection – Is a type of attack that gains access to a database in an unintended manner due to poor security.

SSL – Secure Socket Layer, is protocol used to encrypt network traffic by use of public/private key encryption.

Subdomain – Is the domain to a separate webpage that is still under the umbrella of the parent domain, an example is www is the subdomain in www.google.com.

URL – Uniform Resource Locator, is also known as a web address, an example is http://www.google.com.

Webserver – Is a server that hosts one or multiple websites.

XFS – Cross Frame Scripting, is a form of XSS that uses expanded frames to trick victims into clicking a malicious link by overlaying the frame on top of legitimate buttons.

XSS – Cross Site Scripting, is an attack of injecting a script from a different website into a targeted website's script.

Zero Day Exploit – is a vulnerability in a software that is previously unknown to the software company or virus scanner companies.

Bibliography

Amazon.com, "Seagate BlackArmor NAS 440 4-Bay 12 TB (4 x 3 TB) Network Attached Storage STAU12000100," 2013, available at: http://www.amazon.com/Seagate-BlackArmor-Network-Attached-STAU12000100/dp/B0044UCGDQ

Bockstette, Carsten, "Jihadist Terrorist Use of Strategic Communication Management Techniques," European Center for Security Studies 20 (Dec 2008)

Brachman, Jarret, "High-Tech Terror: Al-Qaeda's Use of New Technology," 30 Fletcher F. World Affairs 149 (2006)

CDW.com, "Cisco IPS 4260 Sensor," 2013, available at: http://www.cdw.com/shop/products/Cisco-IPS-4260-Sensor/1090319.aspx

Chastain, Sue, "TechTV's Cat Shwartz Exposed: Is Photoshop To Blame?," About.com Guide, July 26, 2003, available at: http://graphicssoft.about.com/b/2003/07/26/techtvs-cat-schwartz-exposed-is-photoshop-to-blame.htm

Chen, Hsinchun, "Uncovering the Dark Web: A Case Study of Jihad on the Web," Journal of the American Society for Information Science and Technology 59:8 (June 2008)

Cluley, Graham, "Google, China, Censorship and Hacking," Naked Security, January 14, 2010, available at: http://nakedsecurity.sophos.com/2010/01/14/google-china-censorship-hacking/

Conway, Maura, "Reality bytes: Cyberterrorism and terrorist 'use' of the Internet," First Monday 7:11 (Nov 2002)

Deibert, Ron, and Rafal Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor (March 2009)

Dell.com, “OptiPlex: Business class performance desktops,” 2013, available at: http://www.dell.com/us/business/p/desktops-n-workstations?~ck=mn

Dell.com, “PowerEdge M620 Blade Server,” 2013, available at: http://www.dell.com/us/business/p/poweredge-m620/fs

Denning, Dorothy, “Terror’s Web: How the Internet Is Transforming Terrorism,” Yvonne Jewkes and Majid Yar, Handbook on Internet Crime (New York , NY: Willan Publishing, 2010)

Freiburger, Tina and Jeffrey Crane, “A Systematic Examination of Terrorist Use of the Internet,” International Journal of Cyber Criminology 2:1 (Jan 2008)

Gellman, Barton, Miller, Greg, “U.S. spy network’s successes, failures and objectives detailed in ‘black budget’ summary,” Washington Post (Aug 2013), available at: http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

HBGary White Paper, “Operation Aurora,” HBGary Threat Report, February 10, 2010, available at: http://hbgary.com/attachments/WhitePaper%20HBGary%20Threat%20Report,%20Operation%20Aurora.pdf

Indeed.com, “Intrusion Detection Salary” 2013, available at: http://www.indeed.com/salary?q1=Intrusion+detection+specialists+&l1=

Indeed.com, “Penetration Tester Salary” 2013, available at: http://www.indeed.com/salary?q1=Penetration+Tester&l1=

Indeed.com, “Reverse Engineer Salary” 2013, available at: http://www.indeed.com/salary?q1=reverse+engineer&l1=

Indeed.com, “Social Engineer Salary” 2013, available at: http://www.indeed.com/salary?q1=social+engineer&l1=

Kaspersky Labs, “’Red October’ Diplomatic Cyber Attacks Investigation,” Secure List, January 14, 2013, available at: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation

King, Tom, “Packet Sniffing In a Switched Environment,” SANS Institute InfoSec Reading Room, 2006, available at: https://www.sans.org/reading-room/whitepapers/networkdevs/packet-sniffing-switched-environment-244

Kohlmann, Evan, “The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations,” Testimony before the House Committee on Homeland Security, Dec 6, 2011

Krekel, Bryan, “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” The US-China Economic and Security Review Commission (Oct 2009), available at: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA509000

Lachow, Irving and Courtney Richardson, “Terrorist Use of the Internet: The Real Story,” Joint Force Quarterly 45:2 (2007)

Lekies, Sebastian, Tighzert, Walter, "Client-Side Cross-Domain Requests in the Web Browser: Techniques, Policies and Security Pitfalls," OWASP Foundation, 2011, available at: https://www.owasp.org/images/7/78/05A_Client-Side_Cross-Domain_Requests_-_Sebastian_Lekies%2BWalter_Tighzert.pdf

Lipinski, Michael, "Sourcefire Next-Generation IPS v4.9," SC Magazine, 2011, available at: http://www.scmagazine.com/sourcefire-next-generation-ips-v49/review/3417/

Murphy, Kate, "Web Photos That Reveal Secrets, Like Where You Live," New York Times, August 11, 2010, available at: http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?_r=0

NetworkScreen.com, "Juniper Networks SSG520M Appliance," 2013, available at: http://www.networkscreen.com/SSG520M.asp?gclid=CKaSht3i0boCFU8V7AodzCAAuQ

Newegg.com, "Cisco ASA 5505 Network Security Appliance," 2013, available at: http://www.newegg.com/Product/Product.aspx?gclid=CM3jgurU0boCFU9o7AodAAgAHA&Item=N82E16833420109

Newegg.com, "CISCO Catalyst 2960 WS-C2960S-48TS-L 10/100/1000Mbps Ethernet Switch," 2013, available at: http://www.newegg.com/Product/Product.aspx?Item=N82E16833120540

Newegg.com, "Cisco Small Business 100 Series SF100D-05-NA Unmanaged 10/100Mbps 5-Port Desktop Switch," 2013, available at: http://www.newegg.com/Product/Product.aspx?gclid=CJXUpJrU0boCFcnm7AoddSMAXA&Item=N82E16833150145

Newegg.com, “Cisco Small Business RV016 Multi-WAN VPN Router 2 x 10/100Mbps WAN Ports 13 x 10/100Mbps LAN Ports,” 2013, available at: http://www.newegg.com/Product/Product.aspx?gclid=CL30xtnT0boCFWpk7AodEyMAXA&Item=N82E16833124154

OWASP Foundation, “Clickjacking,” OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/Clickjacking

OWASP Foundation, “Cookie Theft/Session Hijacking,” OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Cookie_Theft/Session_Hijacking

OWASP Foundation, “Cross Frame Scripting,” OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/Cross_Frame_Scripting

OWASP Foundation, “Cross-site Scripting (XSS),” OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

OWASP Foundation, “Directory Indexing,” OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Directory_Indexing

OWASP Foundation, “HttpOnly,” OWASP Periodic Table of Vulnerabilities, 2013, available at: https://www.owasp.org/index.php/HttpOnly

OWASP Foundation, “Path Traversal,” OWASP Periodic Table of Vulnerabilities, 2009, available at: https://www.owasp.org/index.php/Path_Traversal

OWASP Foundation, “Session Fixation,” OWASP Periodic Table of Vulnerabilities, 2011, available at: https://www.owasp.org/index.php/Session_fixation

Qin, Jialun, and Yilu Zhou, “A multi-region empirical study on the internet presence of global extremist organizations,” Information Systems Frontiers 13:1 (Mar 2011)

Ragan, Steve, “Was Operation Aurora really just a conventional attack?,” The Tech Herald, January 27, 2010, available at: http://www.thetechherald.com/articles/Was-Operation-Aurora-really-just-a-conventional-attack/9124/

Richards, Julian, The Art and Science of Intelligence Analysis (New York, NY: Oxford University Press Inc., 2010)

SC Magazine, “TippingPoint UnityOne-1200 (Special report Intrusion prevention),” 2013, available at: http://www.scmagazine.com/tippingpoint-unityone-1200-special-report-intrusion-prevention/product/915/

Shelmire, Aaron, “The Chinese Cyber Attacks formerly known as Titan Rain,” Information Warfare 95 (2008)

SITE, “Jihadist Announces Forthcoming AQAP Cartoon,” available at: http://news.siteintelgroup.com/free-featured-articles/904-jihadist-announces-forthcoming-aqap-cartoon

Thomas, Timothy, “Al Qaeda and the Internet: The Danger of ‘Cyberplanning’,” Parameters 33:1 (Spring 2003)

Thornburgh, Nathan, “The Invasion of the Chinese Cyberspies,” Time Magazine (Aug 29, 2005), available at: http://www.time.com/time/magazine/article/0,9171,1098961,00.html

Virustotal.com, “Credits & Acknowledgements,” 2013, available at: https://www.virustotal.com/en/about/credits/

Weimann, Gabriel, “Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking,” Haifa University, 2011, available at: http://95.211.138.23/wp-content/uploads/2012/08/2012-Terrorists-using-online-social-nerworking.pdf

Weimann, Gabriel, “www.terror.net How Modern Terrorism Uses the Internet,” United States Institute of Peace, Special Report 116 (March 2004)

Whine, Michael, “Cyberspace – A New Medium for Communication, Command, and Control by Extremists,” Studies in Conflict & Terrorism 22 (1999)

Wu, Lei, et al, “The Impact of Vendor Customizations on Android Security,” Proceedings of the 2013 ACM SIGSAC Congerence on Computer & Communication Security, 2013

Xu, Jennifer, Chen, Hsichun, Zhou, Yilu, and Qin, Jialun, “On the Topology of the Dark Web of Terrorist Groups,” Intelligence and Security Informatics, 3975 (May 2006)

Zanini, Michele and Sean Edwards, “The Networking of Terror in the Information Age,” John Arguilla and David Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy (Santa Monica, CA: RAND, 2001)

Zetter, Kim, “Google Hack Attack Was Ultra Sophisticated, New Details Show,” Wired Magazine, January 14, 2010, available at: http://www.wired.com/threatlevel/2010/01/operation-aurora/

Zetter, Kim, “Google Hackers Targeted Source Code of More Than 30 Companies,” Wired Magazine, January 13, 2010, available at: http://www.wired.com/threatlevel/2010/01/google-hack-attack/

Curriculum Vita

Gary Adkins was born in Worms, German. The only son of Robert Adkins and Kathleen Adkins, he graduated from J.M. Hanks High School, El Paso, Texas, in the spring of 1999. He worked as a Drafting Technician for the Niland Company during high school, continuing remotely while attending Texas A&M University as an Electrical Engineering student until 2003. From 2003 to 2007 he attended the University of Texas at El Paso graduating with a BBA in Computer Information Systems. Since 2008 Gary has been working in the IT field at El Paso Area Teachers Federal Credit Union. In the spring of 2011 he enrolled in the Intelligence and National Security Studies Master's program at the University of Texas at El Paso. In May 2013 he was a guest speaker at the Ninth Annual International Association for Intelligence Education Conference hosted in El Paso, Texas. He published *Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism* in 2013 in the *Journal of Strategic Security*.