JOINT REGIONAL INTELLIGENCE CENTER

BULLETIN **5 July 2011**

(U//FOUO) Awareness, Detection, and Mitigation of Cyber Threats and Attacks

(U//FOUO) US citizens and assets – including the White House, the Central Intelligence Agency, InfraGard[i], the state of Arizona, and major defense contracting companies – experienced high-profile cyber threats and attacks in the first half of 2011. Most of the tactics and techniques used were not new, however the increase in attacks during the past few months exemplifies the growth of cyber incursions and reinforces the need to be aware of risks and mitigation techniques associated with cyber threats. Appendices A, B and C contain detailed lists of threats, potential indicators of attacks, and possible remedies; some areas may contain overlap.

(U) Different Actors, Different Motives, Different Threats

(U) The flag representing *Anonymous*, a self-proclaimed hacktivist[ii] group responsible for attacking sites such as Sony, PayPal, and Amazon.

(U) Recent reporting has largely centered on attacks by "hacktivist" groups – loose collectives that conduct cyberactions to raise awareness regarding particular grievances or causes.[ii] These attacks generally garner significant media attention. While they are annoying, embarrassing, and disruptive to victims, they seldom result in meaningful losses or damage, beyond costs associated with website repair.[1] More worrisome are sophisticated probes and attacks that exfiltrate sensitive data for malicious use, or plant software designed to disable systems. Attacks such as these may be conducted by state-sponsored actors or organized criminal enterprises, and may inflict greater damage and losses.

- (U//FOUO) On 23 June, hacker group LulzSec released information taken from the Arizona Department of Public Safety – including personal information of law enforcement officers – to protest a controversial immigration law.[2]
- (U) A multi-phase attack between March and June 2011 against RSA, a secure token provider, and three major defense contractors, saw hackers use stolen and cloned token keys to breach and remove data from networks at the defense firms.[3,4,5]
- (U) The mid-2009 targeted Stuxnet virus temporarily disabled a uranium enrichment plant in Iran.[6]

---

[i] (U) InfraGard is an information-sharing partnership between the Federal Bureau of Investigation and the private sector, comprising businesses, academic institutions, state and local law enforcement agencies, and other participating agencies.

[ii] (U) *Hacktivism* involves breaking into a computer or system for a politically- or socially-motivated purpose. For example, in December 2010 the group Anonymous launched distributed denial of service (DDOS) attacks against MasterCard and PayPal in retaliation for withdrawing financial services from the WikiLeaks site (a website that published anonymous submissions and leaks of sensitive governmental, corporate, organizational, or religious documents, while attempting to preserve the anonymity of its contributors).

(U) Different Targets, Different Methods

(U//FOUO) A successful cyber attack can be detrimental to targeted systems, computers or individuals. Hackers may install programs that steal personal information, flood a browser with pop-up advertising, slow Internet connections, fill e-mail with advertisements and/or crash the system.[7] They may take control of a computer, commit fraud or identity theft, or cause an individual to lose all data stored on that system. This can impact both personal and work systems, and can affect all aspects of an individual's life.

(U//FOUO) Cyber threats can involve any aspect of communications and data infrastructure, but can be broadly categorized as threats to users, systems, and access devices, including mobile devices.

(U) Threats to Users

(U//FOUO) Social engineering[iii] schemes pose the greatest threat to users, and include techniques such as phishing[iv], counterfeit e-mails and websites, and targeted attacks. Perpetrators follow a cycle of information gathering, relationship development, exploitation of a target, and execution of a plan, usually for profit or information gain.[8] Popular social networking sites provide a wealth of freely-posted information in order to support launching an attack.[9]

- (U//FOUO) In June 2011 a phishing attack originating in China targeted White House personnel. It is unclear as of yet how many, if any, staff members were affected.[10]

(U) Threats to Systems

(U//FOUO) Perpetrators in 2011 utilized distributed denial of service (DDOS) attacks[v], cyber extortion[vi], malware[vii], botnets[viii], zero day exploits[ix], rootkits[x], and targeted attacks[xi] that combined several of these techniques.[11,12,13,14,15,16]

[iii] (U) *Social engineering* involves the use of deception or trickery to manipulate individuals into divulging confidential information or performing actions that circumvent or compromise security protocols.

[iv] (U) *Phishing* is a social engineering tactic whereby the attacker attempts to coax a group or individual into releasing sensitive information (ranging from bank account numbers to personal information), or to visit a malicious website where such information may be gained. Phishing usually involves hoax e-mails and/or websites. *Spear phishing* targets a specific person, usually by mentioning personal information, such as an address or name. *Whaling*, another variation, targets high-profile individuals who are expected to have very specific information.

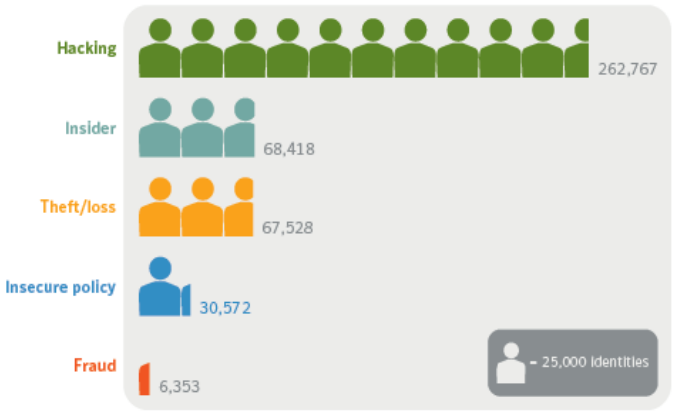
[v] (U) *(D)DOS*, sometimes called a "storm" or "flood", is a form of attack that disables the targeted computers and resources by overwhelming a system with traffic. Typical targets include large or high-profile systems such as banks.

[vi] (U) Cyber extortionists use a variety of attacks, including DDOS, to disable a network; once disabled, they demand payment to cease the attack and restore normal functioning to the website or network.

[vii] (U) *Malware* is a general term for malicious software that infects a computer. Often intended to provide illegal access to a system, programs may be attached to e-mail (i.e. viruses or "Trojan horses").

[viii] (U) *Botnets* are created by undetectable malicious software that infects the computer, turning it into a 'bot' (short for 'robot') that performs tasks over the internet without the owner's knowledge. Botnets are groups of

(U//FOUO) In the previous year, hacking attacks exposed, on average, 260,000 identities per security breach. In 2010, one major computer security provider encountered more than 286 million unique variants of malware.[17] These threats to systems directly affect those who use them by doing everything from stealing personal information to slowing Internet connections and crashing computers.



(U) Average number of identities exposed per data breach, by cause. Source: Symantec.

(U) Threats to Mobile Devices

(U//FOUO) Like stationary systems, mobile devices are vulnearable to social engineering, exploitation of social networking, botnets, malware, vishing[xii], smishing[xiii], and exploitation of mobile applications and mobile commerce (m-commerce.)[18]

- (U//FOUO) In 2010 there were 163 known vulnerabilities in mobile devices – a 42 percent increase from 2009.
- (U//FOUO) Legitimate applications ("apps") sold in app stores often contain hidden Trojans. [xiv,19] Hackers make efforts to exploit smartphones in much the same manner as they would computer systems and networks. One known Trojan, the 'DroidDream', affected over 50 free downloadable applications. After rooting the phone[xv], the Trojan installed a malicious application designed to send information from the phone to a remote command-and-control center; this enabled the center to gain unlimited control of the infected phone.[20]

---

compromised machines harnessed to work together, and may be used to send out e-mail, spread viruses, attack computers or servers, or commit other crimes.

[ix] (U) *Zero-Day exploits* are viruses or other programs used to take advantage of a vulnerability in a computer application before a fix for said vulnerability has been released, sometimes before the developers are even aware of the flaw.

[x] (U) *Rootkits* are malicious programs that hide in operating systems and spread malicious software while remaining undetected.

[xi] (U) Targeted attacks use a variety of techniques to achieve specific ends, such as network penetration (e.g., Stuxnet, which compromised operations at an Iranian uranium enrichment facility) or intellectual property theft (e.g., the InfraGard attacks).

[xii] (U) *Vishing* is a subset of social engineering that utilizes voice communication.

[xiii] (U) *Smishing* is a form of social engineering that exploits SMS (text) messages.

[xiv] (U) *Trojans* are destructive programs that impersonate legitimate computer applications.

[xv] (U) *Rooting a phone* is a similar process to *jailbreaking*; both allow the owner to make the phone faster, tether it to a computer and download applications otherwise not available to the phone.

(U) Government Role in Cyber Security Still Developing

(U//FOUO) The Department of Homeland Security's (DHS) National Cyber Security Division (NCSD), working alongside domestic and international governmental, public, and private entities, handles the securing of cyberspace and America's cyber assets. The NCSD is divided into three programs containing subsets, all with the objective to build and maintain an effective national cyberspace response system and implement a cyber-risk management program for the protection of critical infrastructure.[21] Contracted companies also partner with federal agencies to provide cyber security.[22,23,24]

- (U//FOUO) According to congressional testimony from February of this year, government and private sector groups are concerned by the lack of overall authority and strategic direction in regards to cyberattack defense.[25] There is no clear agreement between Congress, the White House, Pentagon, Central Intelligence Agency, Department of Homeland Security, and other stakeholders regarding where responsibilities lie with regard to various networks, and which department should respond to cyberattack scenarios.[26]

(U) Outlook

(U//FOUO) Cyber threats will likely continue to increase and evolve in 2011 and beyond. User vigilance is the first line of defense in protecting information and assets. Appendices A, B and C contain detailed lists of threats and possible mitigation techniques; some areas may contain overlap. Follow your agency's protocol for handling cyber threats and attacks, and report all major incidents to the JRIC via e-mail at leads@jric.org, or by phone at (562) 345-1100.

(U) Appendix A: Threats to Users

Method of Attack	Attack Details	How to Spot	If Affected	Prevention/Mitigation
Social Engineering	The methods cybercriminals use to trick individuals into sharing sensitive information or allowing access to a computer through deception.	Remain wary of requests from unknown individuals; criminals use fear, curiosity, greed and sympathy to trick individuals. Other tactics include impersonation of individuals known to their targets.	Review these appendices for applicable symptoms and possible solutions.	Consider using a search tool that determines if a website is safe; use updated security software and anti-spam filters from security providers.
Phishing	Phishers use SPAM[xvi], malicious websites, e-mail messages and instant messages to trick people into divulging sensitive information.	E-mail and websites used by phishers tend to have the copyright information from the original; messages are often not personalized, and may use emotional language or scare tactics.	If affected by phishing, assume that you will become a victim of credit card fraud, bank fraud, or identity theft. The Anti Phishing Working Group has advice based on what information you have given out.	View an e-mail that asks for personal information as a potential fraud attempt and do not respond. Do not click links or open attachments; type the organization's web address directly into the browser or call the company directly.
Scareware	Illegitimate anti-virus software may lure users into fraudulent transactions, victimize them through social engineering, install malware, corrupt files or disable legitimate anti-virus software.	Unexpected virus alerts from products that were not installed; website pop-ups while browsing the internet.	Scan the system using known valid anti-virus software; check accounts to see if personal information is compromised. Contact a security expert.	Up to date software, firewalls and virus protection. Exercise caution when clicking links.

[xvi] (U) *SPAM* is unsolicited e-mail sent to large groupings of individuals.

(U) Appendix B: Threats to Systems

Method of Attack	Attack Details	How to Spot	If Affected	Prevention/Mitigation
Botnets	Remote-controlled software, or Rootkit, is installed on the system; it then performs automated tasks over the internet without the user's knowledge. Botnets may be used to modify personal information, attack other computers or commit crimes, and may be installed via e-mails, messages, or websites.	See Malware and/or Rootkit.	See Malware and/or Rootkit.	See Malware and/or Rootkit.
Cyber Extortion	Threats to system, or business; attacks range from (D)DOS, data theft, website defacement, hard drive encryption and data obfuscation.	An attack on your computer/system/site comes coupled with a demand for money.	See various terms based on the method of attack.	Up to date software, firewalls and virus protection.
(Distributed) Denial of Service (DDOS)	Typical attacks flood the server or network, causing its resources to be consumed to the point where the service is no longer responding	A network or server is suddenly overwhelmed with traffic.	Contact the appropriate technical professionals for assistance such as your home provider or network administrator.	There are no effective ways to prevent an attack: anti-virus software, firewalls configured to restrict traffic, and the use of good security practices are all recommended.
Malware	Utilizes popular communication tools to spread, including worms sent through e-mail and messages, Trojan horses downloaded from websites, and virus-infected files downloaded from peer-to-peer connections[xvii],[27] May also result from removable media including CD's, thumb drives and mobile devices that are connected to computers.	No standard way of knowing: be aware of unusual or unexpected behaviors of the computer.	If available, contact technical professionals immediately. If not, disconnect from the internet. Perform a scan using anti-virus software.	Install, use and maintain the following: anti-virus software, firewalls and anti-spyware tools. Frequently change passwords and follow good security practices.
Rootkits	A rootkit is a piece of software installed on your computer. Using rootkits, attackers may be able to access information, monitor your actions, modify programs, or perform other functions on your computer without being detected.	The computer may be running slow with the computer processing unit (CPU) being low on resources – an indication the system is doing background work for the rootkit. The system may also crash frequently.[28]	Some, though few, security programs are designed to remove rootkits; the software needs to run from a drive that is not affected (CD or USB[xviii]). Effective, though drastic, is the reformatting of the hard drive.[29]	Use anti-rootkit software from well known companies and avoid opening e-mails from unknown sources; use firewalls and up to date anti-virus software and anti-spyware programs.
Zero Day Exploits	An exploit for a vulnerability is created before, or the same day as, the vulnerability is discovered; viruses or worms take advantage of a vulnerability that the vendor is not yet aware of.	Odd computer behavior; slower, more network activity, less stable, etc.	See various terms based on results of attack.	Follow good security policies; install and update anti-virus software, block file attachments in e-mails which may be harmful and keep the system patched against already known vulnerabilities.

[xvii] (U) *Peer-to-peer* connections are computer networks in which each computer can act as a server for the others, allowing shared access to files.

[xviii] (U) *USB* (universal serial bus) is a computer port used to connect the computer with external devices.

(U) Appendix C: Threats to Mobile Devices

Method of Attack	Attack Details	How to Spot	If Affected	Prevention/Mitigation
Social Networking Exploitation	Posting shortened Uniform Resource Locators (URLs) to popular networking sites; shortened URLs prevent the user from knowing what site they are being redirected to – legitimate URLs are indistinguishable from malicious ones.	See Phishing.	See Phishing.	Avoid selecting links unless you are certain of their destination.
Mobile Botnets	Takes over the phone much in the same way a Botnet works. See Botnet for details.	See Mobile Malware.	See Mobile Malware.	Anti virus protection for smartphones.
Mobile Application Exploitation	Jailbreaking[xix] a smartphone allows the user to install third-party applications, some of which may contain Malware; markets outside of trusted sources are also at risk.	Exercise caution when browsing alternative application stores; always check permissions of apps before downloading them – ensure the permissions request matches the application's use.	See various terms based on the result of the attack, or type of information given away.	Anti virus protection for smartphones.
Mobile Malware	May be hidden in downloadable applications; for other methods see Malware.	No standard way of knowing: be aware of unusual or unexpected behaviors of the phone; more likely if the phone has downloaded rouge/third party applications.	Smartphone vendors offer various fixes and applications based on the phone's platform.	Anti virus protection for smartphones.
Vishing	Individuals utilize the phone network in attempt to steal money; attackers use caller-ID spoofing[xx] to appear legitimate, directing individuals to call a toll-free number where they are asked to disclose information.	See Phishing.	See Phishing.	Be aware of vishing scams, do not place full trust in caller ID, be suspicious of all unknown callers and register on the National Do Not Call registry.
Smishing	A phishing attack sent via text messaging.	See Phishing.	See Phishing.	See phishing.

[xix] (U) Installing a software application and transferring it to the smartphone, where it 'breaks open' the file system allowing the user to modify it. Different phone platforms offer various terms and methods. More details can be read here.

[xx] (U) *Caller ID Spoofing* is causing the telephone network to display a number which is not that of the actual originating station.

(U) Endnotes

[1] (U) Internet site; David Morgan; MSNBC.com; "'Hacktivists' Make Noise, Not War on US Sites"; 16 June 2011; http://www.msnbc.msn.com/id/43433428/ns/technology_and_science-security/t/hacktivists-make-noise-not-war-us-government-websites/; accessed on 25 May 2011; MSNBC is an established news site.

[2] (U) Internet site; CNN Wire Staff; CNN.com; "Hacker Group Targets Arizona Law Enforcement"; 24 June 2011; http://www.msnbc.msn.com/id/43433428/ns/technology_and_science-security/t/hacktivists-make-noise-not-war-us-government-websites/; accessed on 24 June 2011; CNN Is an established news site.

[3] (U) Internet site; William Jackson; FCW.com; "Hackers Might Have Skeleton Key to Defense Contractor Systems"; 1 June 2011; http://fcw.com/articles/2011/06/01/defense-contractors-l3-lockheed-hacked.aspx; accessed 14 June 2011; Federal Computer Week is a strategic technology site.

[4] (U) Internet site; Fahmida Y. Rashid,; E Week.com; "Northrop Grumman, L-3 Communications Hacked via Cloned RSA SecurID Tokens"; 2 June 2011; http://www.eweek.com/c/a/Security/Northrop-Grumman-L3-Communications-Hacked-via-Cloned-RSA-SecurID-Tokens-841662/; accessed 14 June 2011; E Week is an IT security and network security news site.

[5] (U) Internet site; William Jackson; GCN.com; "Hackers Gain Access to RSA's SecurID Security Tokens"; 18 March 2011; http://gcn.com/articles/2011/03/18/rsa-securid-hacked-apt.aspx; accessed 25 May 2011; GCN is an online site for government IT professionals.

[6] (U) Internet site; New York Times.com; "Stuxnet"; 15 January 2011; http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html; accessed 26 May 2011; New York Times is an established news site.

[7] (U) Internet site; Paul Gil; About.com; "Spyware-Malware 101: Understanding the Secret Digital War of the Internet"; March 2011; http://netforbeginners.about.com/od/antivirusantispyware/a/malware101.htm; accessed 25 May 2011; About.com is an established publisher of independent subject matter guides.

[8] (U) Online Publication; SANS; *Social Engineering: A Means To Violate A Computer System*; June 2006; http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529; accessed 25 May 2011; Report detailed how social engineering may be used to violate a computer system.

[9] (U) Internet site; Andrew Whitaker; InformIT.com; "Top 10 Social Engineering Tactics"; 11 June 2011; http://www.informit.com/articles/article.aspx?p=1350956&seqNum=7; accessed 14 June 2011; Inform IT is the online presence for Pearson, the world's largest publisher of technical books.

[10] (U) Internet site; David Sanger; New York Times.com; "Hacking of White House E-Mail Affected Diverse Departments"; 3 June 2011; http://www.nytimes.com/2011/06/04/technology/04hack.html?_r=2; accessed 14 June 2011; New York Times is an established news site.

[11] (U) Online Publication; Symantec; Internet Security Threat Report, Volume 16; *Symantec Internet Security Threat Report; Trends for 2010*; April 2011; https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf; 26 May 2011; threat report which gives a detailed overview of 2010's activity; Symantec is an established provider of Internet security software solutions.

[12] (U) Internet site; Darril Gibson; InformIT.com; "The Explosion of Cybercrime"; 23 May 2011; http://www.informit.com/articles/article.aspx?p=1713590; accessed 25 May 2011; Inform IT is the online presence for Pearson, the world's largest publisher of technical books.

[13] (U) Internet site; Safety & Security Center; Microsoft.com; "What is a Botnet?"; http://www.microsoft.com/security/resources/botnet-whatis.aspx; accessed 24 May 2011; Microsoft is a known computer company.

[14] (U) Internet site; SND.com; "Hacktivsts – Who Are They and How Do We Defend Against Them?"; 5 April 2011; http://www.softwarenewsdaily.com/2011/04/hacktivists; accessed 25 May 2011; Software News Daily is an established site reporting on software news.

[15] (U) Internet site; Carnegie Mellon University; Mysecurecyberspace.com; "Encyclopedia: Zero Day Attack"; http://www.mysecurecyberspace.com/encyclopedia/index/zero-day-attack.html; accessed 25 May 2011; Carnegie Melon is an established university.

[16] (U) Internet site; Internet Security Centre; Bullguard.com; "All the Information You Need on Rootkits and How to Remove Them"; http://www.bullguard.com/bullguard-security-center/security-articles/what-is-a-rootkit.aspx; accessed 25 May 2011; Bullguard is a computer security software provider.

[17] (U) Online Publication; Symantec; Internet Security Threat Report, Volume 16; *Symantec Internet Security Threat Report; Trends for 2010*; April 2011; https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf; 26 May 2011; threat report which gives a detailed overview of 2010's activity; Symantec is an established provider of Internet security software.

[18] (U) Online Publication; US-Cert; United States Computer Security Emergency Readiness Team; *Cyber Threats to Mobile Devices*; 15 April 2010; http://www.us-cert.gov/reading_room/TIP10-105-01.pdf; 26 May 2011; technical information paper which details cyber threats to mobile devices; the US CERT team is a known Government cyberthreat response team.

[19] (U) Online Publication; Symantec; Internet Security Threat Report, Volume 16; *Symantec Internet Security Threat Report; Trends for 2010*; April 2011; https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf; 26 May 2011; threat report which gives a detailed overview of 2010's activity; Symantec is an established provider of Internet security software.

[20] (U) Internet site; Tony Bradley; TechWorld.com; "DroidDream Autopsy: Anatomy of an Android Malware Attack"; 3 March 2011; http://www.techworld.com.au/article/378957/droiddream_autopsy_anatomy_an_android_malware_attack/; accessed 25 May 2011; TechWorld is an established IT and technology news and help site.

[21] (U) Internet site; Homeland Security; DHS.Gov; "National Cyber Security Division"; http://www.dhs.gov/xabout/structure/editorial_0839.shtm; accessed 1 June 2011; the Department of Homeland Security is a known government website.

[22] (U) Internet site; DC Tech Source.com; "ManTech Awarded $9.2 Million Contract to Provide Cyber Security Services to the Federal Bureau of Investigation"; 20 January 2011; http://www.dctechsource.com/mantech-awarded-9-million-contract-to-provide-cyber-security-to-fbi.aspx; accessed 14 June 2011; DC Tech Source is a business technology site related to the D.C. metro area.

[23] (U) Internet site; David Hubler; WashingtonTechnology.com; "CSC to Prop Up Air Force Cybersecurity Services"; 18 January 2011; http://washingtontechnology.com/articles/2011/01/18/csc-air-force-cybersecurity-services.aspx; accessed 14 June 2011; Washington Technology is an online news source for government contractors and partners.

[24] (U) Internet site; David Hubler; WashingtonTechnology.com; "CSC to Prop Up Air Force Cybersecurity Services"; 18 January 2011; http://washingtontechnology.com/articles/2011/01/18/csc-air-force-cybersecurity-services.aspx; accessed 14 June 2011; Washington Technology is an online news source for government contractors and partners.

[25] (U) Internet site; Henry Kenyon; GCN.com; "In Event of Cyberattack, Who's in Charge?"; 14 February 2011; http://gcn.com/articles/2011/02/14/congress-concerned-about-cyber-defense.aspx; accessed 14 June 2011; GCN is an online site for government IT professionals.

[26] (U) Internet site; Kevin Baron; Stars and Stripes.com; "Lawmakers: US, DOD Still Not Taking Cybersecurity Seriously"; 11 February 2011; http://www.stripes.com/news/lawmakers-u-s-dod-still-not-taking-cybersecurity-seriously-1.134503; accessed 14 June 2011; Stars and Stripes is an independent news site for military affiliations.

[27] (U) Internet site; Norton.com; "Malware"; http://us.norton.com/security_response/malware.jsp; accessed 26 May 2011; Norton is a known computer security provider.

[28] (U) Internet site; R. Kayne; WiseGeek.com; "How do I Check my Computer for Rootkits?"; http://www.wisegeek.com/how-do-i-check-my-computer-for-rootkits.htm; accessed 26 May 2011; WiseGeek is a computer help site.

[29] (U) Internet site; G. Wiesen; WiseGeek.com; "What Are the Best Tips for Rootkit Removal?"; http://www.wisegeek.com/what-are-the-best-tips-for-rootkit-removal.htm; accessed 26 May 2011; Wisegeek is a computer help site.