# JOINT REGIONAL INTELLIGENCE CENTER

**BULLETIN** 

# (U//FOUO) Situational Awareness: Steganography: A Lesser Known Method of Concealing Electronic Information, Attacking Systems

(U//FOUO) Steganography—the practice of concealing data within a carrier<sup>i</sup>—may be used to obscure malicious or criminal information and activity from law enforcement. While steganography dates to the fifth century BC, it has long been regarded as, and remains, one of the most advanced forms of clandestine communication. In modern usage, the Internet allows accessibility to, and broad dissemination of, steganography tools, and its application continues to evolve with technology. Understanding steganography in its current state is essential to its identification and detection.

# (U) Detection

(U//FOUO) Detecting steganography is challenging; in fact, determining whether media contains extraneous data is nearly impossible. Generally, detection occurs only through direct knowledge of its existence, evidence of steganography tools, or chance. Some indicators of steganography may include: <sup>1</sup>

- (U//FOUO) Conspicuous and unusual sharing of digital media files via peer-topeer<sup>ii</sup> (P2P) clients, e-mail, or uploads to Web sites
- (U//FOUO) Repeated sharing of the same file
- (U//FOUO) Possession of steganography software, or visiting sites known to contain steganography

### (U) Steganography: The Basics

• (U) Modern steganography is the practice of hiding information within a form of media (that is, an image, audio, or text file) in a way that it is difficult to discern. 11 January 2012

- (U) Legitimate uses of steganography include watermarking images; tagging notes to online images; or maintaining information confidentiality, such as protecting data from sabotage, theft, or unauthorized viewing.
- (U) Steganography tools are widely available online and are easy to use.
- (U) For more information, visit <u>Symantec</u>.
- (U//FOUO) Sharing of content that is inconsistent with a subject's life, such as pictures of children when he or she is not known to have any

www.jric.org

<sup>&</sup>lt;sup>i</sup> (U) Modern digital steganography may use a number of electronic carrier file formats to conceal information, including but not limited to, BMP, JPEG, GIF, WAV, and MP3 files.

<sup>&</sup>lt;sup>ii</sup> (U) In a P2P network, computer systems are connected to each other via the Internet and files are shared directly between systems without the need of a central server.

<sup>(</sup>U) Law enforcement can report tips and leads to the JRIC via the Web site at <u>www.jric.org</u>, by e-mail at <u>leads@jric.org</u>, or by telephone at (562) 345-1100 or (888) 705-JRIC (5742).

# UNCLASSIFIED // FOR OFFICIAL USE ONLY



- (U//FOUO) Possession of two or more copies of a file that do not look/sound identical, that is, the same image but of varying sizes and hash values<sup>iii</sup>
- (U//FOUO) Presence of files whose large size is unusual for the type of content<sup>iv</sup>
- (U//FOUO) Possession of books or articles on—or, expression of interest in cryptography or steganography

(U) Note that traditional security devices (for example, firewalls) do not detect steganography; a file containing a concealed message presents as a legitimate file.<sup>2</sup>

## (U) Tools for Detection

(U) Steganalysis, the method of detecting steganography and destroying the hidden message, is possible through free online tools. Deciphering and viewing the original message is challenging without the encryption keys, and some detection software may only identify steganography within a specific medium.<sup>3,4</sup>

## (U) Illicit Uses of Steganography

### (U) Covert Communication

(U) Steganography can be used to hide communication behind seemingly innocuous files to pass messages without fear of detection.

- (U) According to an indictment unsealed in June 2010, an accused Russian spy network in New York began to use steganography as early as 2005. After a raid on the home of an alleged spy, law enforcement found a program on a computer that allowed group members to embed data in images on publicly available Web sites.<sup>5</sup>
- (U//FOUO) The second issue of *The Technical Mujahid*<sup>v</sup> details the benefits of using steganography over encryption;<sup>vi</sup> the magazine includes instructions for and examples of steganography.<sup>6</sup>

## (U) Concealing Illicit Activity

(U//FOUO) Criminals use steganography to hide materials or information for the purpose of

- (U) Trafficking in child pornography<sup>7</sup>
- (U) Committing fraud<sup>8</sup>
- (U) Evading government censorship abroad<sup>9</sup>

#### Tel 562.345.1100

www.jric.org

<sup>(</sup>U) Hash values are numerical identifiers assigned to a file, group of files, or part of a file.

<sup>&</sup>lt;sup>iv</sup> (U) This may be an indication of *appending variants*, in which data are posted after the end of the file marker, adding to its size; use of this technique makes it possible to use almost every file type as a carrier.

<sup>&</sup>lt;sup>v</sup> (U) *The Technical Mujahid* is a 2007 electronic periodical published by al-Qa'ida -affiliated or -inspired individuals that teaches the use of technology.

<sup>&</sup>lt;sup>vi</sup> (U) *Encryption* is the act of converting data or information into code.



• (U) Conducting industrial espionage<sup>10</sup>

### (U) VoIP Steganography

(U) Voice over Internet Protocol (VoIP)<sup>vii</sup> steganography, also known as network steganography, is one example of adaption to new technology. Use of a proprietary VoIP service eliminates the need for a carrier to conceal data, and extends the message length.<sup>11</sup> The longer the conversation or data exchange, the longer or more detailed the hidden message can be.<sup>12</sup> The brief time period the VoIP data exists for makes this nearly impossible to detect or prevent.

## (U) Attacking Computers and Systems

(U//FOUO) In the same way steganography may hide one file within another, it may also be used to conceal malicious programs.

- (U) In September 2011, a leading international technology corporation encountered a new variant of the Alureon<sup>viii</sup> Trojan<sup>ix</sup> and bootkit<sup>x</sup>: the malware<sup>xi</sup> applied steganography to its actions, downloading images from the Internet that contained an updated configuration file, providing the malware an extra layer of protection, and hiding its commands.<sup>13</sup>
- (U) Operation "Shady RAT," a cyber-espionage campaign beginning in July 2006, hooked victims with phishing<sup>xii</sup> e-mail and used steganography to hide malware commands in photos and images.<sup>14</sup> The attacks compromised 72 organizations, 49 of them in the United States.<sup>15</sup>

Т	el	50	52.	.3	45	5.	1	1	0	0
	•••	~		~	-	•	-		v	v

www.jric.org

<sup>&</sup>lt;sup>vii</sup> (U) *VoIP*, also called Internet telephony, is a category of hardware and software that enables use of the Internet as a transmission medium for telephone calls by sending voice data in packets via Internet Protocol (IP) rather than by traditional circuit transmissions on the public switched telephone network (PSTN).

<sup>&</sup>lt;sup>viii</sup> (U) The *Alureon* was designed to, among other things, steal data by intercepting a system's network traffic to seek and capture usernames, passwords and credit card data.

<sup>&</sup>lt;sup>ix</sup> (U) *Trojans* are destructive programs that impersonate legitimate computer applications.

<sup>&</sup>lt;sup>x</sup> (U) *Bootkits* are variants of *rootkits* (malicious programs that hide in operating systems and spread harmful software while remaining undetected) used primarily to attack full-disk encryption systems.

<sup>&</sup>lt;sup>xi</sup> (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 (that is, viruses or "Trojan horses").

<sup>&</sup>lt;sup>xii</sup> (U) *Phishing* is a social engineering tactic whereby the attacker attempts to get a target to release sensitive information (ranging from bank account numbers to personal information), or to visit a malicious Web site where such information may be gained. Phishing usually involves hoax e-mail and/or Web sites. *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.

### UNCLASSIFIED // FOR OFFICIAL USE ONLY



BULLETIN

11 January 2012

# (U) Further Reading

(U//FOUO) For additional information on methods of cyber attacks and preventative measures, see the JRIC bulletin *Awareness Detection and Mitigation of Cyber Threats and Attacks*, published 5 July 2011.

# (U) Contact Information

(U//FOUO) For questions or comments regarding this bulletin, please contact the JRIC at <u>analysis@jric.org</u>.

(U//FOUO) To provide feedback regarding this product please complete this <u>survey</u>.

Tel 562.345.1100

www.jric.org

### UNCLASSIFIED // FOR OFFICIAL USE ONLY



BULLETIN

## (U) Endnotes

<sup>1</sup> (U//FOUO) Intelligence Bulletin; Federal Bureau of Investigation; "Continued Terrorist Interest in Steganography"; 12 June 2008; accessed 15 November 2011.

<sup>2</sup> (U) Online news article; Tim Greene; Tech World; "Steganography Meets VoIP in Hacker World"; 14 September 2009; <u>http://www.techworld.com.au/article/318301/steganography meets voip hacker world/</u>; accessed 18 November 2011; Tech World is an IT service and information site.

<sup>3</sup> (U) Online reference article; Kristy Westphal; Symantec; "Steganography Revealed"; 2 November 2010; <u>http://www.symantec.com/connect/articles/steganography-revealed; accessed 26 December 2011</u>; accessed 26 December 2011; Symantec is a computer protection resource.

<sup>4</sup> (U) Steganalysis resource; Niels Provos; OutGuess; "Steganography Detection with StegDetect:" 2004; <u>http://www.outguess.org/detection.php</u>; accessed 26 December 2011; OutGuess is a steganography site.

<sup>5</sup> (U) Online news article; Noah Shachtman; Wired; "FBI: Spies Hid Secret Messages on Public Websites"; 29 June 2010; <u>http://www.wired.com/dangerroom/2010/06/alleged-spies-hid-secret-messages-on-public-websites/</u>; accessed on 16 November 2011; Wired is an established technology news site.

<sup>6</sup> (U//FOUO) Intelligence Bulletin; Federal Bureau of Investigation; "Continued Terrorist Interest in Steganography"; 12 June 2008; accessed 15 November 2011.

<sup>7</sup> (U) Online article; Brad Astrowsky; ACPO; "Steganography: Hidden Images, A New Challenge in the Fight Against Child Porn"; date unknown; <u>http://www.antichildporn.org/steganog.html</u>; accessed 29 November 2011; ACPO is an organization dedicated to fighting child pornography.

<sup>8</sup> (U) Online article; Unknown author; National Institute of Justice; "Digital Evidence Analysis: Steganography Detection"; 5 November 2010; <u>http://www.nij.gov/topics/forensics/evidence/digital/analysis/steganography.htm</u>; accessed 29 November 2011; The NIJ is government resource.

<sup>9</sup> (U) Online article; Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski; "Voice Over IP: The VoIP Steganography Threat"; February 2010; <u>http://spectrum.ieee.org/telecom/internet/vice-over-ip-the-voip-steganography-threat/0</u>; accessed 17 November 2011; Spectrum is a technology site.

<sup>10</sup> (U) White paper; Joann Kennedy; SAS Institute; "Steganography in the Corporate Environment"; 9 April 2004; <u>http://www.giac.org/paper/gsec/4078/steganography-corporate-environment/106511</u>; accessed 29 November 2011; SANS Institute is a computer security organization.

<sup>11</sup> (U) Online article; Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski; "Voice Over IP: The VoIP Steganography Threat"; February 2010; <u>http://spectrum.ieee.org/telecom/internet/vice-over-ip-the-voip-steganography-threat/0</u>; accessed 17 November 2011; Spectrum is a technology site.
 <sup>12</sup> (U) Online article; Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski; "Voice Over IP: The VoIP

<sup>12</sup> (U) Online article; Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski; "Voice Over IP: The VoIP Steganography Threat"; February 2010; <u>http://spectrum.ieee.org/telecom/internet/vice-over-ip-the-voip-steganography-threat/0</u>; accessed 17 November 2011; Spectrum is a technology site.

<sup>13</sup> (U) Online new article; unknown author; Virus Bulletin; "Alureon Trojan uses Steganography to Receive Commands"; 26 September 2011; <u>http://www.virusbtn.com/news/2011/09\_26.xml?rss</u>; accessed 5 December 2011; VirusBTN is an online resource dedicated to fighting malware and spam.

<sup>14</sup> (U) Online news article; Kevin McCaney; Government Computer News; "How 'Shady RAT' Espionage Attacks Spread"; 12 August 2011; <u>http://gcn.com/articles/2011/08/12/shady-rat-steganography-malware-</u>

images.aspx?sc lang=en; accessed 17 November 2011; GCN is a news site covering cyber security.
<sup>15</sup> (U) Online news article; Kevin McCaney; Government Computer News; "How 'Shady RAT' Espionage Attacks Spread"; 12 August 2011; <u>http://gcn.com/articles/2011/08/12/shady-rat-steganography-malware-</u>

images.aspx?sc lang=en; accessed 17 November 2011; GCN is a news site covering cyber security.

Tel 562.345.1100

www.jric.org