19 March 2015

(U//FOUO) SWATting and Voice over Internet Protocol (VoIP) Technology

(U) Scope

(U//FOUO) This bulletin was created by the Northern California Regional Intelligence Center (NCRIC) to address the practice of "SWATting"—described by the FBI as calls to an emergency service that fake an emergency to draw a response from law enforcement[1]—and the implications for local law enforcement and first responders. This bulletin focuses on SWATters' use of telecommunications—in particular, Voice over Internet Protocol (VoIP) technology—to hide their identity. The NCRIC bases its analysis on known SWATting incidents in the United States from 2008 to the present with a focus on the 15 counties within the NCRIC's Area of Responsibility (AOR).

(U) Key Judgements

- (U//FOUO) Advancements in encryption and anonymization techniques are increasing the ability of perpetrators to hide their identities when placing SWATting calls.[a]
- (U//FOUO) The complexity of a SWAT hoax depends on steps taken by the perpetrator to hide his/her identity. A perpetrator's use of VoIP in addition to other anonymization measures, for example, reduces the ability of law enforcement to successfully investigate.
- (U//FOUO) To date, the NCRIC is not aware of any information regarding the use of SWATting hoaxes as a tactic to divert law enforcement away from a planned illicit operation or as a method to test first responder responses. However, we cannot rule out the possibility that malicious actors might see the technique as a viable option to divert law enforcement or security personnel from the location of planned criminal activity.

[a] (U) A variety of techniques exist to stage a SWATting incident. These come in the form of caller ID spoofing, social engineering, teletypewriter (TTY) for hearing or speech impaired individuals, prank calls from public phones, phreaking (a term used to describe individuals who manipulate various frequencies of analog or digital phone systems), and hacking telecommunication systems.

(U) SWATting Overview

(U//FOUO) SWATting is considered a federal offence under 47 U.S.C. § 227(e). The phenomenon known as SWATting gained notoriety in 2008 when a phone hacker who was capable of manipulating and faking various in-band phone signals used the technique to harass his adversaries. The perpetrator was able to spoof his number by manipulating the caller ID to display an alternative number, eliciting a SWAT response to a person's house whom he disliked.[2] The case made international headlines when the perpetrator was sentenced the following year to more than 11 years in prison for his attacks.

(U//FOUO) SWATting has since gained popularity, and VoIP in recent years has become the most popular method of caller ID spoofing. According to open source consumer reports, the number of VoIP services has multiplied to several hundred service providers, 10 of which are US-based.[3]

(U) VoIP Technology

(U) VoIP is essentially phone service through the internet. Instead of a typical carrier signal operated through a phone company, a call can be made through a digital connection. An individual can use VoIP on a cellular smartphone since most phones have a data connection, or calls can be made through the use of an adapter connected to an analog telephone by converting to a digital signal. VoIP interacts with other media services such as phone applications, selective call forwarding, phone portability, service mobility, web-based user control interfaces, and selective area or country codes. These capabilities not only allow users to encrypt their communications, but also enable them to anonymize their communications by, for example, selecting the area from which they are calling.

(U//FOUO) SWATting Incidents in Northern California

(U//FOUO) SWATting is occurring on occasion within the NCRIC's AOR. Local media has reported at least three SWATting incidents in the San Francisco Bay Area in the past three years, while hundreds of hoaxes have taken place across the country. Although many recent episodes of SWATting nationwide have been perpetrated by online gamers against rival gamers, targets vary and there is not enough information to suggest a definitive target profile.[4]

- (U) On 19 August 2014, the San Rafael Police Department responded to a call from a man who claimed to have four bombs in addition to holding a family hostage. The caller stated he would begin executing the family. When officers arrived, they learned the call was a hoax after evacuating the area.[5]

- (U) On 8 January 2014, Santa Clara County Sheriff's deputies responded to a call from an individual claiming he had killed two people and had planted bombs inside a San Jose home. Some 25 to 30 deputies responded in addition to SWAT and a nearby medical center kept on standby, but the call was determined to be a hoax. There was no motive revealed in the investigation.[6]

- (U) On 14 February 2013, a San Mateo woman was victim to a SWATting hoax. Officers received a call that shots were fired at the woman's residence and a suspect was barricaded inside the house with several hostages. Once officers arrived at the home and detained the woman, it was revealed the call was a hoax.[7]

(U//FOUO) How a Subject SWATs a Target Using VoIP and Stays Hidden

(U) The NCRIC has identified the following steps to show how an individual might employ VoIP and other anonymization techniques to SWAT a target using a cellular smartphone or desktop software. These steps are not intended to serve as a comprehensive guide but rather to illustrate one of several possible approaches.

1. (U) Register all smartphone and desktop applications with a throw-away e-mail account using a fake name. Enter misleading information upon registration should the service provider require identifying information.

2. (U) Install Orbot for mobile devices or The Onion Router (TOR) for a desktop computer.[89] When correctly installed, these applications create a private connection by encrypting all of the phone's traffic and bouncing it through computers located around the world on the TOR network—a network used to encrypt and hide the activity of a user.[10]

3. (U) Install a VoIP application such as SMSListo[11], MagicJack,[12] Silent Circle,[13] TORFone,[14] Burner[15] or Skype.[b] There are a wide variety of VoIP services provided by carriers such as Verizon, Comcast, AT&T, and Vonage that an individual could use for mobile phones and desktop computers, and many are free of charge or charge only a small monthly fee.

4. (U) Install a GPS spoofing application (mobile only).[c] This application will fake the phone's location and, if combined with steps 1-2, will spoof the phone's E911 position.[d]

(U//FOUO) Steps Law Enforcement Can Take To Identify and Investigate a SWATting Event

(U//FOUO) The NCRIC recommends the following steps to identify and investigate possible SWATting events based on our understanding of advancements in VoIP technology and guidance from partner organizations on phone number investigations. Depending on the skill set of the caller and sophistication of his/her phone setup, these steps may or may not yield results for an investigator. A combination of investigative techniques may be required to go beyond typical phone number tracking methodology.

1. (U//FOUO) Identify the caller's service provider at the Number Portability Administration Center (NPAC):[1617] www.npac.com.

2. (U//FOUO) If the number has been ported or the phone carrier has been switched repeatedly, these activities can be accessed through the Local Number Portability Enhanced Analytical Platform (LEAP).[18] LEAP will help identify alternative service providers' service type (wireless, VoIP) and a range of numbers through an automatic subpoena process.

---

[b] (U) For a list of VoIP smartphone applications, visit http://www.androidauthority.com/best-android-apps-voip-sip-calls-wi-fi-calling-internet-calling-87396/

[c] (U) "Spoofing" is the act of misleading or masquerading identifying characteristics such as an IP address or GPS location to mislead a receiving or investigating party.

[d] (U//FOUO) E911 uses a Public Safety Answering System (PSAP) to geolocate cellular and VoIP calls based on service provider's database which is not required at the time of E911 registration. At the time of registration with the VoIP service provider, an individual may post false or misleading information.

3. (U//FOUO) Determine if the case involves "exigent circumstances." If the situation involves immediate danger of death or serious injury, a provider can verify and send a report via fax. A Court Order may be required by the provider in order to process a request.

4. (U//FOUO) Verify the provider is the actual provider of the account. Service providers may recycle numbers, including VoIP, and databases may not reflect if a number has changed hands.[19] Popular VoIP providers include Vonage, MagicJack, Google, and Skype.[20]

5. (U//LES) File the appropriate paperwork with the provider. This includes a preservation letter USC 2703(b)(2) used to preserve the data associated with the number before it is discarded, a subpoena for transactional records, and a court order for detailed records.[21]

6. (U//FOUO) A last resort for an investigator may be tracking the IP address associated with a call. LEAP can include IP addresses with requested data.[22] An investigator may use an IP address or domain lookup tool to identify a name associated with this information.[23]

(U) Possible Indicators of a SWATting Attack

- (U) Considerable delays in phone conversation responses.
- (U) Caller has little detail about the event or too much detail.
- (U) Caller's speech may sound rehearsed or scripted, or the tone of the caller or background noise may not match the alleged situation. If the caller is emotional, it may sound forced.
- (U) Caller's number is not associated with the area and does not receive incoming calls or the caller refuses to give up this information.

(U) Outlook and Implications

(U//FOUO) The NCRIC assesses that the use of VoIP in SWATting hoaxes will likely continue as technologies that can hide and obfuscate caller identification continue to be developed. Improvements in anonymization techniques and encryption standards will hinder efforts by law enforcement to identify perpetrators and may exceed local law enforcement's capabilities. SWATting hoaxes will continue to be used by pranksters who believe they are beyond the reach of law enforcement, and successful hoaxes where a caller is not identified may inspire others to also apply the tactic.

(U) Tracked By: HSEC-1.3, HSEC-1.4, HSEC-1.8

(U) Endnotes

[1] (U) "Don't Make the Call: the New Phenomenon of 'Swatting,' FBI, 02/04/08. http://www.fbi.gov/news/stories/2008/february/swatting020408, [Accessed: 11/20/2014].
[2] (U) "Notorious phone phreaker gets 11 years for swatting," 06/29/2009. http://www.theregister.co.uk/2009/06/29/phone_phreaker_sentence/, [Accessed: 11/20/2014].
[3] (U) VoIP Providers USA, http://www.voip-info.org/wiki/view/VoIP+Providers+USA. [Accessed: 11/20/2014].
[4] (U) "On Twitch, SWAT teams are becoming dangerous props for trolls," 08/22/2014. http://www.dailydot.com/esports/swatting-twitch-trend-prank/, [Accessed: 3/6/2014].
[5] (U) "Hoax 911 calls a troubling trend," 10/10/2014. http://www.marinscope.com/ross_valley_reporter/news/article_23440888-3948-11e4-9c37-2ba11cc7964b.html, [Accessed: 21/1/2014].
[6] (U) "San Jose: Hoax call involving shooting, explosives leads to large emergency response," 1/8/14. http://www.mercurynews.com/crime-courts/ci_24875068/san-jose-hoax-call-involving-shooting-explosives-leads, [Accessed: 12/1/2014].
[7] (U) "San Mateo Woman Vitcim of 'Swatting' Prank," 09/15/2013. http://www.nbcbayarea.com/news/local/San-Mateo-Woman-Victim-of--Swatting-Prank-191390561.html, [Accessed: 11/20/2014].
[8] (U)Tor product line, https://www.torproject.org/. [Accessed: 3/9/2015].
[9] (U) Orbot Application description page, https://play.google.com/store/apps/details?id=org.torproject.android, [Accessed: 11/20/2014].
[10] (U) "Granting Anonymity," 12/17/2014. http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html?pagewanted=all, [Accessed: 11/20/2014].
[11] (U) https://play.google.com/store/apps/details?id=finarea.SmsListo, [Accessed:11/20/2014].
[12] (U) MagicApp smartphone application for Android, https://play.google.com/store/apps/details?id=com.magicjack&hl=en, [Accessed: 11/20/2014].
[13] (U) https://silentcircle.com/technology, [Accessed: 11/20/2014].
[14] (U) TOR Fone: p2p secure and anonymous VoIP tool, http://torfone.org/
[15] (U) Burner smartphone application for Android, https://play.google.com/store/apps/details?id=com.adhoclabs.burner&hl=en, [Accessed: 10/20/2014].
[16] (U) Alternative number lookup service: http://www.fonefinder.net/.
[17] (U) Number Portability Administration Center IVR System, http://www.npac.com/the-npac/access/law-enforcement-agencies-psaps/ivr-system
[18] (U) Local Number Portability Enhanced Analytical Platform Website, http://leap.neustar.biz/index.html. [Accessed: 12/2/2014].
[19] (U) "Wrong Number? Blame Companies' Recycling," 12/1/2014. http://online.wsj.com/articles/SB10001424052970204012004577070122687462582, [Accessed: 11/24/2014].
[20] "Top 100 VoIP Providers World Ranking," http://www.myvoipprovider.com/en/Top_100_VoIP_Providers. [Accessed: 11/2/2014].
[21] (U//LES) Ohio Law Enforcement Telephone Investigations Resource Guide, 3/12/2012.
[22] (U) FRS Document Only Change – NSAP Field Size, Number Portability Administration Center. http://www.npac.com/lnpa-working-group/nanc-change-orders/nanc-315, [Accessed: 2/16/2015].
[23] (U) WHOIS home page, http://cqcounter.com/whois/, [Accessed: 2/16/2015].