Quick Response Guide to Internet-Based Threat Investigations

(U//LES) FBI Boston has developed this response guide to assist law enforcement officers in their investigation of Internet-based threats.

Reporting Procedures *See* *“Characteristics of Swatting Calls” guide*

YOU ARE NOT ALONE! Swatting calls and bomb threats typically come in clusters. Situational awareness is key. Knowing you are not the only one receiving the threat informs your actions and response, reducing the risk to first responders and innocent victims.

- **Immediately report the details of the call to your Fusion Centers.**
- Fusion Centers collate the information and distribute to the stakeholders, as well as the FBI.

E-mail Threats

- Inform recipient of the e-mail to keep the e-mail open on the computer until assistance arrives. Instruct the recipient to save the e-mail and avoid deleting the e-mail at all costs.
- Do not delete the e-mail. Save the e-mail.
- Print, photograph, or copy the e-mail.
- Obtain full e-mail header data from original e-mail.
- Obtain IP address visitor logs to the school’s website. In the past, perpetrators have obtained the targeted e-mail addresses of bomb threats via the school public Internet website.
- Research all IP addresses to determine the telecommunications provider that owns the IP address. If applicable, serve legal process to these providers.
- Utilize available open-source social media search tools to determine if the e-mail or username that sent the threat has a social media presence.

Swatting/Phone/VoIP Threat

- Obtain a recording of the call.
- Identify the date/time and victim number called, as well as the telecommunication provider for the victim.
- Subpoena popular VoIP providers (Google, Skype, TextNow) and ask them for any accounts that called the targeted number on a specific date and time. Submit an Emergency Disclosure Request (EDR) to the appropriate provider, utilize www.search.org/resources/isp-list/ to find the provider)

- Identify the subject inbound number (even if spoofed or caller ID is not displayed). If the call was directed to a non-emergency dispatch line and routed through multiple extensions, attempt to provide the original receiving line number and extension.
- Identify **if** a specific name was utilized during the call (typically a victim of the swatting call, not the subject).
- Determine if there are any publicly accessible web cameras in the vicinity of the identified swatting location and identify the owner of those cameras.
- Conduct a thorough interview of the victim. In many cases, the victim is not randomly chosen but instead is familiar with the subject placing the call. Victims may be able to provide information useful for identifying the perpetrator through an interview.
- Contact your local FBI field office regarding the tools and techniques they have available for tracking back to the source.

Indicators of a Swatting Call *See "Characteristics of Swatting Calls" guide*

This is not an exhaustive list:

• The swatting call is the only incoming call reporting the incident. In a real incident multiple calls would be received. (Call the location to corroborate the details)

• Swatting calls are received by the non-emergency line. Swatters using VoIP services cannot dial 911 directly so they must call the non-emergency number.

• Swatting calls using VoIP services will appear as all zeros or nines, blocked, unavailable, or one of the default VoIP numbers. Skype, TextNow, Google Voice, etc.

• The caller's demeanor is inconsistent with the claimed crisis or threat. For example, the caller claims to have witnessed the shooting of several students, but they appear calm and with no background noise.

• Background noises include computer mouse clicking and/or typing. Callers use mapping tools and internet searches to answer follow-up questions or provide building address or names.

• The caller mispronounces names such as city, street, or building names. Swatting calls are commonly conducted by foreign perpetrators with thick accents who are unfamiliar with the local areas they target.

• The caller's story changes or escalates when challenged with follow-up questions.

• "Call of Duty Speak" - caller uses exotic or specific names of weapons from playing video games.

• Gunshots or explosions heard in the background are inconsistent with other noise or sound fake.

(U) Subpoena Verbiage

(U//LES) When issuing legal process to social media platforms, VoIP providers, or ISPs, the FBI recommends that you include a full description of information you are seeking. This may include, but is not limited to, subscriber names, usernames, addresses, length of service, types of service used, telephone number and e-mail addresses associated with the account, billing records, and date range of the data you are requesting.

Additionally, subjects have been known to create fake accounts on their own computer. Many service providers like Google will link accounts through cookies. Be sure to ask for: **"Accounts linked to one or more of the Subject Accounts by machine cookies."**

When issuing legal process to telecommunication carriers, ensure that you ask for a "carrier identification code, AKA CIC." In the event the telephone number was spoofed, the CIC would identify other telecommunication providers that accessed a local telephone exchange.

Search.ORG (ISP List)

(U//FOUO) "ISP List" is a frequently updated database of Internet service and other online content providers that stores legal contact information and instructions needed to serve subpoenas, court orders and search warrants.

www.search.org/resources/isp-list/