Swatting: Mitigation Strategies and Reporting Procedures

Thank you to the **NJCCIC**[1] which has provided the following information to aid schools and public and private sector partners in mitigating *swatting*, a pervasive threat impacting schools, hospitals, shopping malls, and private residences throughout the nation.

Due to the ease by which perpetrators are able to conceal their location and identity, and the obstacles limiting law enforcement's ability to investigate these crimes, swatting threats are likely to persist and the targeting scope may expand to other venues.

Therefore, proactive mitigation strategies and coordination between the public and private sector, state and federal law enforcement, and the intelligence community is essential to preventing and limiting the impact of these incidents.

Overview

Swatting *is defined as a false report of an ongoing emergency or threat of violence intended to prompt an immediate tactical law enforcement response.* **Swatting** is not a new threat; it has evolved over the last decade or so and includes a range of tactics and techniques used to cause false public alarm and divert law enforcement resources to a hoax threat. Certain incident types and tactics have tended to receive more media coverage than others. **Swatting** scenarios include bomb threats, active shooter scenarios, threats of an imminent shooting rampage, hostage scenarios, and threats involving chemical, biological, radiological, nuclear, or explosives agents.

- The motivations for swatting vary and include the attention gained from national media coverage and discussions on social media or online forums, revenge against gamers or those responsible for previous swatting incidents, and financial gain. Perpetrators post advertisements in online forums and black market sites *offering to conduct swatting for a fee* and to boast of their previous swatting successes.
- Incidents of swatting across the country are commonly linked, and investigations often lead to groups of perpetrators outside the US. These foreign actors are often contacted and paid to conduct the swatting act by a student of the targeted school or a video game player who provides the name and address or workplace of another gamer against whom they are seeking revenge.
- Many incidents involve the targeted location receiving the swatting call, as opposed to reporting the emergency directly to law enforcement agencies, and an anonymous caller using a computerized text-to-speech voice. Swatting incidents in which the caller does not provide a name, and there are no claims of responsibility following the incident, differ from historical cases and indicate a potential shift away from motivations of revenge and recognition.

Indicators

The following are indicators which can be used to identify a potential swatting incident. This is not an exhaustive list, and public and private sector partners are encouraged to contact local law enforcement with lessons learned or success stories of tactics used to dispel a swatting attempt.

- The swatting call is *the only incoming call* to report an active shooter or ongoing emergency situation. If a shooting has occurred or an active shooter scenario is unfolding, multiple calls to dispatch from witnesses or victims are likely.
- The incoming telephone number *is spoofed or blocked*. Swatting calls using Voice over Internet Protocol (VoIP) services will appear as all zeros or nines, blocked, unavailable, or one of the default Skype numbers: (661) 748-0240, (661) 748-0241, or (661) 748-0242.
- The swatting call is *routed through a non-emergency dispatch line*. Swatters using VOIP services cannot dial 9-1-1 directly so instead they look up non-emergency lines of dispatch operations.
- The caller's tone and background noise is *inconsistent with the claimed emergency* or threat. For example, the caller claims to have murdered a family member, coworkers, or innocent bystanders, yet their demeanor is suspiciously calm, with minimal background noise.
- The caller can be heard *typing or clicking a computer mouse* in the background. Swatters will conduct internet searches or use online mapping and geospatial tools during the call to answer follow-up questions and provide exterior descriptions of buildings or residences.
- The caller is *unable to answer follow-up questions* requesting details such as their full name, phone number, or current location. Swatting callers may attempt to provide descriptions of interiors or exteriors of buildings gleaned from photos on social media or internet searches.
- 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* throughout the course of questioning. When challenged by follow-up questions or doubts that their claims are true or legitimate, the swatting caller may intensify their threat or change key details of their story.
- The caller uses *specific gun names* or terminology to identity their weapon. Swatting callers often refer to weapons commonly depicted in video games, such as an AR-15 assault rifle.
- Gunshots or explosions heard in the *background are inconsistent* with other noise or sound fake.
- Swatting callers may play recordings of gunshots or live firefights from video games or the internet in order to sound as if they are shooting a weapon while on the call.
- The caller *claims to be armed or suicidal* and willing to shoot law enforcement.

Mitigation

Swatting calls can be successfully mitigated using follow-up questioning to identify inconsistencies or weaknesses in the caller's storyline or to make the caller feel their attempt is failing. Call receivers should ask **multiple questions** in quick succession, and repeat questions later in the call to identify inconsistencies.

Suggested questions include:

- "What is your full name?" (ask again later during call, and specifically ask for a middle name)
- "Where are you calling from?"
- "What is your phone number?"
- "Why didn't you call 911 directly?" (for VoIP calls to non-emergency dispatch line)
- "I need a call back number in case we get disconnected. What is your mobile or home number?"
- "Why are you reporting yourself?"
- "Why is there no noise in the background?"
- "What is that noise in the background?" (when background noise is inconsistent with the story)
- "Why does it sound like you are typing on a computer keyboard?"
- "Are you targeting anyone in particular?"

Caller claims to be inside, near, or on the roof of a *school*:

- -"How did you get on the roof?"
- -"Where exactly are you on the roof?"
- -"How are you going to get inside the building?"
- -"Do you know a student at the school?"

Caller claims to be inside or near a *mall, hospital, or other commercial venue*:

- "Where are you in the building?"
- "What are you near?"
- "Which building are you in/on?" (when there are multiple buildings in a complex)
- "Do you know an employee?"

Caller claims to be at a *residence*:

- "Where are you in the house?"
- "Is it a one or two story house?"
- "What color is the house?"
- "Who owns the house?"
- "Who else lives in the house?"
- "What are your parents' names?"

Caller claims they are *on their way or planning to target* a location:

- "Where are you coming from?"
- "Are you in a car?" "When will you get here?"

Reporting

Public and private sector partners should ensure staff and employees are trained on swatting mitigation strategies and reporting procedures for swatting incidents or attempts. First, targeted locations should call 9-1-1 in the event of a reported emergency or threat of violence and clearly indicate if there is suspicion of swatting. If possible, try to keep the caller on the line and ask follow-up questions while another individual speaks to the dispatcher.

Reporting information will aid in the coordination of investigations between local, state, and federal law enforcement, as well as in analysis of trends and the further development of best practices, which will be shared with all partners. Detailed information includes::

1. **Exact time and date** the call was received.
2. **Victim telephone number** that received the incoming swatting call.
   - 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.
3. **Victim's telecommunications provider** (for example, Verizon, AT&T, or another carrier).
4. **The incoming (swatting) telephone number**.
   - Was the calling number identified as one of the default Skype numbers: (661) 748-0240, (661) 748-0241, or (661) 748-0242?
   - Was the call number unavailable, blocked, or displayed as all zeros, ones, or nines?
5. **Detailed description of the nature of the threat**.
   - Incident Type: For example, bomb threat, active shooter, hostage situation, or CBRNE threat.
   - Did the caller provide a motivation or reason for the threat?
   - Did the caller specify a timeline for imminent or future threats?
   - Where did the caller claim to be calling from?
   - Was any background noise heard during the call?
6. **Detailed description of caller**.
   - Did the caller provide a name to identify themselves?
   - What was the caller's gender and accent?
   - Was the caller's voice computerized or masked in any way?
   - What was the caller's demeanor and tone (for example, calm, agitated, excited, hysterical, emotional, or confused)?
   - Did the caller seem prepared with a script or preplanned responses?

This information was adapted from a document developed by the New Jersey State Police Cyber Crimes Unit, the Intelligence and Analysis Threat Unit at the Regional Operations Intelligence Center, the Office of Homeland Security and Preparedness, and the FBI. Comments or questions about this document can be directed to the NJCCIC at njccic@cyber.nj.gov.

[1] New Jersey Cyberbsecurity & Communications Integration Cell