



GOV. CHRIS CHRISTIE | LT. GOV. KIM GUADAGNO | DIR. CHRIS RODRIGUEZ

NJOHSP

OFFICE OF HOMELAND SECURITY AND PREPAREDNESS

NJOHSP Podcast *Intelligence. Unclassified.* Episode 4: Swatting – Not Just a Prank

Rosemary Martorana, Director of Intelligence, New Jersey Office of Homeland Security and Preparedness:

Hello. I am Rosemary Martorana, Director of Intelligence here at the New Jersey Office of Homeland Security and Preparedness (NJOHSP) and you are listening to *Intelligence. Unclassified.* This podcast is exactly what the title states: unclassified information about current trends in homeland security for the state of New Jersey, as well as educational information and resources for your awareness. Although it is produced every month, we aim to stay on top of current events and will often offer additional content. If this is your first time listening, then thanks for coming! Please feel free to add this podcast to your RSS feed or iTunes. You can also follow NJOHSP on Twitter @NJOHSP and Facebook. All links can be found in the show notes and on our website www.njohsp.gov.

Rosemary Martorana, Director of Intelligence, New Jersey Office of Homeland Security and Preparedness: Hello. I am Rosemary Martorana, Director of Intelligence here at the New Jersey Office of Homeland Security and Preparedness, and today I am speaking with Paige Schilling, an Intelligence Analyst here at the Office. We are going to be discussing swatting. Paige, to begin with, what is swatting?

Paige Schilling, Intelligence Analyst, New Jersey Office of Homeland Security and Preparedness: Swatting is the act of falsely reporting an ongoing emergency or threat of violence, in order to prompt an immediate tactical law enforcement response. Throughout New Jersey, we have seen a variety of different types of threats. We have seen bomb threats, active shooter scenarios, hostage situations, and even threats involving chemical, biological, radiological, or nuclear weapons. Swatting has its roots in the online gaming community. Gamers had the added incentive of swatting each other because often they would see their opponents be swatted in real time since many chose to live stream their game play over the internet. Many of you may remember, in August 2014, a professional gamer in Colorado was actually swatted and that video received a lot of different airplay throughout the United States. Celebrities throughout the United States, including Lil Wayne, Ashton Kutcher, Miley Cyrus, and Tom Cruise, have also been swatted. Swatters definitely have it out for celebrities and those that I just named are a few of many.

Martorana: That being said, are there any consequences for swatting?

Schilling: There are three primary consequences for swatting. First and foremost, swatting is dangerous. It is dangerous to not only first responders, but to the victims of these incidents. Each and every time law enforcement rushes to the scene of an incident that turns out to be a hoax,

they are putting their lives in danger. And there have been reports of officers being injured in car accidents in their rush to respond. In January 2015, we had a police officer in Oklahoma, Chief Louis Ross, He was actually shot when he entered the home of an individual named Dallas Horton at 4 a.m. in the morning because of a swatting incident. Dallas Horton had nothing to do with the threat or the swatting itself. And so he shot at the police chief and injured him. Luckily, everyone came out OK. The individual was not charged, obviously. But this is just an example of how these situations can really escalate when both the victims and first responders are unaware that it is a hoax. The second consequence of swatting is that it is a drain on resources. Each and every time law enforcement is at a prank or hoax, it takes them away from actual real emergencies that do need their attention. And lastly, swatting is expensive. It can cost thousands of dollars every single time a swat team is called out. And although we do not have any national statistics on how many swatting incidents occur annually, the number may be in the thousands. In April 2014, one single swatting call in Staten Island cost law enforcement \$100,000 after 60 officers responded. And that swatting incident was actually prompted by an individual who called the police and said they had just killed their mother and brother and threatened to fire upon first responders.

Martorana: That's scary. What motivates swatters to conduct these types of attacks?

Schilling: We have seen a wide range of motivations for swatters. We have seen it be used at just a simple prank. We have seen it be used as revenge or even the desire for notoriety. In May of 2014, a teenager in Canada was arrested after he was harassing young women using swatting as a tactic. He targeted individuals that had turned down his advances and along with swatting them, he was doxing them, which is the release of personally identifiable information on the internet. He was calling them and texting them over a longer period of time. That is where we see swatting go from just a simple prank or act of revenge to actually being a tool of harassment. We have even seen some gamers admit that they would make these calls if they lost a game. Or, if they felt they needed to pay other people back in the gaming community, they would place these calls. Although the motives range for swatters, the consequences are very serious for each of these motivations.

Martorana: How exactly is swatting done, or how is it conducted?

Schilling: I might get a little technical here, and I would just ask you all to just stay with me. There are a few different tools that swatters use to anonymize themselves. The first of which is social engineering. This is the technique that uses certain tools and psychological manipulation in order to get enough information about a target in order to make a swatting attack successful. For example, if I identify someone on the online gaming community who I want to swat, but I do not know much about them, I may use social engineering to acquire more information about them. I may pretend to be the target, call the internet service provider that individual uses, and try to trick the representative into giving out sensitive information, like the target's home address or phone number. The second technique is called VOIP and we see this a lot - Voice Over Internet Protocol software. Skype and Google Hangout are the most popular VOIP applications that swatters use. These applications are generally free and they basically make the swatter anonymous. The third technique involves different spoofing services, which conceal the true telephone number of the individual. These services are usually paid and there is a whole array online that you can purchase, but these numbers will show up as legitimate numbers. The last technique is called text-to-speech services, which is basically a system and software that was

invented for people with hearing disabilities, so they could communicate by typing text and having a spoken voice output of that information. Swatters are capitalizing on this technology to disguise their voices.

Martorana: Interesting. Have we ever had any swatting incidents here in New Jersey?

Schilling: Yes. We have actually, in the past year, in 2015, we had over 200 cases reported to the New Jersey Suspicious Activity Reporting System (NJSARS). The NJSARS is run by NJOHSP and it is basically all of the suspicious activity throughout the state that is submitted by our partners, our law enforcement partners, and also private residents, and organizations throughout New Jersey. Those 200 cases include a variety of different threats. They include telephonic threats, in-person threats, and threats made via social media. The targets in 2015 were primarily schools, malls, and retail establishments, and lastly, hospitals. And speaking to schools, a few weeks ago we had a very large incident in New Jersey that seemed to be a coordinated incident throughout several states. Here in New Jersey alone we had 26 schools in one day that received telephonic threats. So, this problem definitely is not going away. New Jersey is not alone in this struggle. It seems that there have been swatting incidents reported throughout the United States, as well.

Martorana: With so many swatting incidents taking place nationally, are there any penalties in place for people that use this tactic?

Schilling: Recently, New Jersey Governor Chris Christie has signed into law a bill that upgraded the crime of false public alarm from a crime of the third degree to the second degree. By signing the law, it increases the penalties for a swatter to spend up to ten years in prison and also they are liable for the cost of the law enforcement response up to \$150,000. New Jersey is doing its part to catch these swatters and punish them and hopefully deter other people that are looking to pull this type of prank. Federally, there has also been legislation introduced. It is actually called the [Interstate Swatting Hoax Act](#) and it is trying to tighten up some of the loopholes that currently exist for telephonic threats.

Martorana: Great. Thank you, Paige. And thanks for tuning in!

Outro:

Again, all links can be found in the show notes and on our website at www.njohsp.gov. Thanks for listening and don't forget to subscribe to *Intelligence. Unclassified*.