Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-072325-3-PSA
July 23, 2025

The Com: Theft, Extortion, and Violence are a Rising Threat to Youth Online

The Federal Bureau of Investigation is warning the public about a growing and evolving online threat group known as The Com, short for The Community. The Com is a primarily English speaking, international, online ecosystem comprised of multiple interconnected networks whose members, many of whom are minors, engage in a variety of criminal violations. The FBI estimates thousands of individuals identify as current or recent members of The Com with varying levels of associated activity. Criminal activity conducted by members of The Com includes, but is not limited to, swatting[1]/hoax threats, extortion/sextortion of minors, production and distribution of child sexual abuse material, violent crime, and various types of cyber crimes. The latter category is broad and includes distributed denial-of-service (DDoS) attacks, subscriber identity module (SIM) swapping[2], ransomware, intellectual property theft, extortion, cryptocurrency theft, and money laundering. The motivations behind the criminal activity vary, but often fall within one of the following: financial gain, retaliation, ideology, sexual gratification, and notoriety.

The sophistication of The Com criminal activity has grown over the last four years, with subjects employing increasingly complex methods to mask their identities, hide financial transactions, and launder money. An underlying theme within the entirety of The Com is its members' interest in and proficiency with cyber related tactics, techniques, and procedures. The Com members have also demonstrated knowledge of the UK and US criminal justice systems. For example, subjects involved with The Com have been known to intentionally recruit juveniles within the United States to perform criminal acts based on their misperception that juveniles cannot be pursued by the US criminal justice system.

The deployment of swatting and hoax bomb threats to facilitate other illicit criminal activity is an underlying theme across subgroups within The Com. Members of The Com will engage in swatting when conducting cryptocurrency theft to distract from the ongoing crime. Of note, swatting is the most visible violation that occurs within The Com and often acts as the entry point into the larger Com ecosystem. While subgroups of The Com have different recruitment tactics, in general they target young and impressionable individuals using minor-friendly

[1] Swatting is the act of reporting a false emergency situation with the intention of eliciting a law enforcement or SWAT response.

[2] Subscriber identity module (SIM) swapping is a method in which a cyber criminal performs an unauthorized account takeover of a victim's wireless account held with the mobile phone carrier. This is accomplished by linking the victim's mobile phone number to a different SIM card within the same carrier's network but installed in a device the cyber criminal controls.

applications such as social media platforms or gaming sites and indoctrinate them into their ideology. Members of The Com typically range between 11 and 25 years old. Young people are often recruited on gaming sites and social media platforms based on shared interests, or through other members of The Com.

SUBSETS OF THE COM

There are currently three known primary subsets within The Com: Hacker Com,[3] In Real Life (IRL) Com,[4] and Extortion Com.[5] Each subset has a distinct focus; however, members of The Com often participate in criminal activity encompassed in more than one subset and maintain relationships with members in multiple subsets simultaneously, in case their skills are beneficial. The members within these subgroups typically have a shared interest, ideology, or goal and work together, adding others to the group and splintering when necessary, to achieve their mission.

RECOMMENDATIONS

The FBI urges the public to exercise caution when posting or messaging personal information, photos, or videos on social media, dating sites, or other online platforms. Posting seemingly innocuous information online may provide threat actors with content to exploit for malicious purposes, including targeting and extortion.

The FBI recommends the public consider the following when sharing information or engaging online:

- Monitor children's online activity and discuss risks associated with engaging with others in online platforms.
- Exercise discretion when posting personal information, videos, or photos online, especially content that includes minors.
    - Once information is shared online, it can be very difficult, if not impossible to remove, particularly if it has been shared by other individuals.
    - Avoid posting personal information online, such as mobile phone number, address, or other personally identifying information.
- Apply privacy settings to social media accounts to limit public view of photos, videos, and personal information.
- Exercise caution when accepting friend requests, engaging in video calls, and sending images to individuals you do not know personally.

---

[3] For additional information on Hacker Com, please see PSA Alert I-072325-PSA: Cyber Criminal Subset of The Community (Com) is a Rising Threat to Youth Online

[4] For additional information on In-Real-Life Com, please see PSA Alert I-072325-2-PSA In Real Life (IRL) Com: Violent Subset of The Community (Com) is a Rising Threat to Youth Online

[5] For additional information on Extortion Com, please see PSA Alert I-030625-PSA, Violent Online Networks Target vulnerable and Underage Populations Across the United States and Around the Globe.

- Run searches of your information/your child's personal information to determine the level of exposure and spread of information.
- Do not provide money or other valuable items to individuals you do not know online. Complying with extortion or threats does not guarantee sensitive content will not be shared.
- Enable multifactor authentication on financial accounts, social media sites, and other applications.
- Do not reply to emails, text messages, or calls that request personal information, such as your password, PIN, or One Time Password sent to your email or phone. If someone claiming to be a company "representative" contacts you and asks you to provide personal information or to verify your account by providing a code, initiate a new call to the company by dialing the verified customer service line.
- Do not post or advertise information about financial assets, including ownership of or investment in cryptocurrency, on social media websites or forums.

VICTIM REPORTING AND ADDITIONAL RESOURCES

If you or someone you know may be a victim of a crime using the tactics outlined above, the following resources may help:

- If it is an immediate, life threatening emergency, dial 9-1-1.
- Consult a health care provider who can provide an initial evaluation or referral to a mental health professional.
- Connect to a mental health resource who can help learn health coping skills for intense emotions and help reduce the risk of a serious injury.
- The National Center for Missing and Exploited Children (NCMEC) provides a free service known as **Take It Down**, which helps minor victims, or adults who were victimized as minors, with removing or stopping the online sharing of nude, or sexually explicit content taken while under 18 years old. For more information, visit https://takeitdown.ncmec.org
- Contact your account providers immediately to regain control of your accounts, change passwords, and place alerts on your accounts for suspicious login attempts and/or transactions.
- Retain all of the information regarding the incident (i.e. usernames, email addresses, monikers, websites, platforms used for communication, names, photos, videos, etc.) and immediately report it to:
    - FBI's Internet Crime Complaint Center: www.ic3.gov
    - FBI Field Office: www.fbi.gov/contact-us/field-offices or 1-800-CALL-FBI (225-5324)
    - National Center for Missing and Exploited Children (NCMEC): 1-800-THE-LOST or https://report.cybertip.org/.