Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-072325-1-PSA
July 23, 2025

Hacker Com: Cyber Criminal Subset of The Community (Com) is a Rising Threat to Youth Online

The Federal Bureau of Investigation is warning the public about Hacker Com, one of three subsets of the 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. Members of Hacker Com typically have a shared interest, ideology, or goal and work together, adding others to the group and splintering when necessary, to achieve their mission.

Hacker Com involves a broad community of technically sophisticated cyber criminals, some of whom are linked to ransomware-as-a service (RaaS) groups. Members of Hacker Com often sell technical services for a profit and use their technical capabilities to steal cryptocurrency to fund other criminal activity. Computer-related criminal activity within Hacker Com includes, but is not limited to, distributed denial-of-service (DDOS) attacks, compromise of personally identifiable information, sale of government email accounts, ransomware attacks, phishing, malware development and deployment, cryptocurrency theft, computer intrusions, and subscriber identity module (SIM) swapping[1]. Hacker Com actors use tools such as: remote access trojans, phishing kits, voice over internet protocol (VOIP) providers, voice modulators, virtual private networks (VPNs), spoofing technology, cryptocurrency cash out services, live streaming services, and encrypted email domains to facilitate their criminal activity and conceal their true identities. While many of these tools and methods are used throughout the entirety of The Com, some are more prevalent within Hacker Com subgroups. Open-source information indicates Hacker Com groups are responsible for high-profile attacks and intrusions and have affiliations with ransomware organizations.

Cryptocurrency theft is the primary motivator for many Com actors, which often leads to internal conflicts and Com members themselves becoming the targets of SIM swaps and other cyber-related crime. Perceived slights, membership in a rival group, or boasts about cryptocurrency balances can provoke Com actors to attack each other. Notoriety and perceived status within Hacker Com groups are derived from a member's skill sets and account balances. Members screen share and brag about profits resulting from cryptocurrency thefts, which sometimes

[1] 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.

exceed millions of dollars. In many cases, this leads to a member becoming a target of cryptocurrency theft. In addition to SIM swapping and network intrusions, physical extortion is another means of stealing cryptocurrency. This can involve kidnapping, torture, threats of violence toward family members, and the use of firearms. The intensification of these online conflicts has resulted in the emergence of a new layer of The Com known as In Real Life (IRL) Com, which includes subgroups that aim to facilitate real world acts of violence, oftentimes resulting from online conflicts. Members may start their Com participation in IRL Com, make friends with other members in Hacker Com, develop the necessary cyber skills, and then begin participating in Hacker Com while continuing their association with IRL Com. Others may use funds gained through participation in Hacker Com to participate in Extortion (Extort) Com. Extortion Com primarily involves the exploitation of children. Members extort minors, typically females, through threats of doxing[2], swatting[3], and IRL violence if member demands are not met.[4]

SWATTING AND HACKER COM

Some Com subgroups offer swat-for-hire services via communication applications and social media platforms. Infighting among Com subgroups often leads to targeted swatting and doxing of members. The Com actors who offer these swatting services use platforms and technologies to obscure their true identities and are often paid in cryptocurrency.

Hacker Com groups use swatting to divert attention away from mobile devices or company networks during cryptocurrency thefts or corporate intrusions. The relative ease with which swatting is arranged makes it an attractive retaliation option.

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 with 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

[2] Doxing is the public posting of an individual's personal identifying information online.

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

[4] 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.

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 the information regarding the incident (e.g. usernames, email addresses, monikers, websites, platforms used for communication, names, photos, or videos) 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/.