BTAC BULLETIN

BEHAVIORAL SCIENCE | LAW ENFORCEMENT & COUNTERINTELLIGENCE | CYBERSECURITY | EMPLOYEE MANAGEMENT RELATIONS | THREAT ASSESSMENT & MANAGEMENT

VIRTUAL CHILD SEXUAL ABUSE MATERIAL

A National Security Vulnerbility

Engagement with Virtual Child Sexual Abuse Material (VCSAM) is a high-risk activity that creates significant national security vulnerabilities from an insider threat perspective. This material, which includes computer-generated or synthetically altered media like cartoons, animations, or AI-generated images depicting child sexual abuse, presents a critical concern for any organization. Those who download and view these images are prime targets for blackmail and coercion by adversaries and demonstrate profoundly poor judgment that makes them unreliable, and risk introducing malware and other vulnerabilities onto sensitive government networks when they look at these images from unvetted sources. Regardless of whether the activity meets a criminal threshold, viewing and/or collecting VCSAM fuels a criminal market, signals untrustworthy behavior, and represents a clear behavioral indicator of a potential insider threat that must be addressed to protect the mission and the organization.[1]

10,000

The average offender possessed over 10,000 images/videos, an activity that requires significant time and technical effort, which could overlap with work hours or use of government equipment.[2]

In the majority of all adjudicated insider threat cases, co-workers admitted they observed concerning behaviors but failed to report them. The risk is not the material itself, but the behaviors and vulnerabilities of the individuals who seek it.

Legal Considerations

Federal Law & Penalties

Engaging with VCSAM is a federal felony under 18 U.S.C. § 2252A. Even viewing content can be legally considered "possession," leading to severe criminal penalties.

Military Justice (UCMJ)

A UCMJ conviction can lead to severe penalties, including confinement and a dishonorable discharge.

Security Clearance Impact

Under SEAD 4, strong grounds for security clearance revocation include criminal conduct, high risk activities, and conduct that creates a vulnerability to coercion.

Fueling Harm

Engaging with VCSAM fuels a cycle of harm and creates direct threats to the organization and its mission in the following ways:

- **Coercion and Blackmail:** Creates a critical vulnerability where an insider can be forced to compromise sensitive information to hide their illicit activity.
- **Network Exploitation:** Introduces malware, ransomware, or spyware onto secure government systems when individuals download illicit files from unvetted sources like the dark web.
- **Reputational Damage:** Causes severe harm to the agency's reputation, eroding public trust and distracting from the core mission upon discovery. [3]

Threat Mitigation

The insider threat community's role is to identify and mitigate these risks. Key mitigation strategies include:

- **Recognize Behavioral Indicators:** Train the workforce to identify observable warning signs, such as secretive online activity, use of anonymizing software, inappropriate comments, increased and secretive use on cellphones or unexplained changes in behavior.
- **Enhance User Activity Monitoring (UAM):** Insider threat programs should tune UAM strategies to detect network anomalies and unauthorized software that correlate with these high-risk behaviors.
- **Promote Reporting:** Foster a culture where personnel understand their duty to report concerning behaviors through established channels, allowing for early intervention before a threat escalates.

Role of Threat Manager

- **Joint Task Forces:** InT programs should understand the role of JTFs and other LE capabilities to combat VCSAM/CSAM and tailor mitigation recommendations accordingly. This includes active partnership with key organizations like the National Center for Missing & Exploited Children (NCMEC) and regional FBI Child Exploitation Task Forces.
- **Secure Information Sharing:** InT programs should use secure channels and standardized forms to share data with law enforcement while protecting sensitive information.
- **Training and Education:** InT programs and local law enforcement must participate in joint training programs to enhance awareness and reporting skills.

The BTAC Podcast "Beyond the Bulletin" featured on DVIDS is now streaming on Apple and Spotify

1. Christensen, L. S., Moritz, D., & Pearson, A. (2021). Psychological perspectives of virtual child sexual abuse material. Sexuality & Culture, 25(4), 1353–1365. 2. U.S. Department of Health & Human Services, Administration for Children and Families, Administration on Children, Youth and Families, Children's Bureau. (2024). Child maltreatment 2022. 3. Christensen, L. S., & Vickery, N. (2023). The characteristics of virtual child sexual abuse material offenders and the harms of offending: A qualitative content analysis of print media. Sexuality & Culture, 27(5), 1813–1827.