LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

MARCH 2025

DANGERS OF ONLINE GAMING; FOREIGN INTELLIGENCE GATHERING AND CONTACT REPORTING

Social media platforms in modern society create unique vulnerabilities to Insider Threats. Platforms like dating sites, social media communication, online gaming, and content sharing can be exploited for adversarial purposes, ethical violations, and unauthorized disclosures.

Foreign Intelligence Entities (FIEs) actively exploit trusted insiders through tailored psychological and digital tactics to gain access to sensitive information.

Gaming platforms act as fertile ground for influential operations by FIEs and extremist groups:

- Social Engineering and Honey Trapping: Use of psychological manipulation to exploit insiders' vulnerabilities, including impersonation and trust-building.
- Recruitment: Gaming environments are leveraged for the Recruitment Cycle and/or elicit information.
- Gamified Propaganda: Embedding ideological content in games to influence vulnerable users.

Dating applications like Tinder, Bumble and Grindr, which are designed to facilitate personal connections, have been increasingly exploited by adversaries to engage with individuals in sensitive circumstances. Here are several ways in which individuals can be exploited:

Exploitation of Personal Information

- Adversaries utilize dating apps to gather detailed personal data from targets, such as their whereabouts, job roles, and social circles.
- This information aids in building trust and manipulating individuals for espionage activities.

Grooming and Blackmail

- By establishing romantic or intimate relationships, adversaries can groom insiders, leading to the unintentional disclosure of sensitive information.
- In some cases, the relationship may be used to blackmail the individual into providing classified data.

Growing Popularity

Online games and platforms like Discord and Twitch provide real-time communication for millions, including those in sensitive roles. FIEs engage with insiders through in-game chats or gaming forums to build trust and extract operational information.

Attraction for Adversaries

Gaming platforms offer anonymity, encrypted messaging, and large user bases, making them ideal for exploitation.

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

General Risks

- Adversarial grooming and trust-building.
- Use of gamified strategies to influence behavior.
- Covert communication using private chats.

Online Exploitation Methods

Gamification of Espionage
Avatars are used to foster friendly rivalry and build rapport with the target through shared in-game experiences while subtly gathering information.

Identity Exploration and Anonymity
Leverage the lack of accountability and perceived invisibility to establish trust and manipulate behavior.

Social Validation and Peer Influence
Pose as influential community members, offering in-game benefits or recognition in exchange for sensitive information or compliance.

Emotional Regulation and Escapism
Exploit vulnerabilities by offering companionship or camaraderie, steering the target toward divulging sensitive information.

Cognitive Load and Decision-Making
Adversaries time their manipulations during peak cognitive strain or during a Dopamine rush, which pushes the target toward impulsive actions.

Reporting Online Foreign Contacts

Review the list below so that you know when to report these online contacts to your FSO at **security@lissol.com**:

- Has anyone asked for information about your professional duties?
- Has anyone asked about your clearance or work access or work associates?
- Has there been an uptick of social media friend request (especially from foreign individuals)?
- Report profiles suspected to be fake, or AI generated.
- Report profiles attempting to move the conversation to another platform.
- Do not click links, save all conversations via screenshots.
- Even if not sure, **REPORT!!!**

Foreign actors will likely not ask sensitive information at first contact, they may try to build a relationship first or not ask anything sensitive for months, so they do not seem "alarming." This is a reminder to be aware and cautious of all your online contacts.