EXPRESS COMPUTER

Seqrite uncovers rising digital honey trap attacks that steal confidential information by targeting emotions over technology

Seqrite, the enterprise security arm of Quick Heal Technologies Limited has uncovered concerning details about the growing threat of digital honey traps. These sophisticated scams use fake romantic relationships to steal sensitive information from government officials, corporate employees, and other high-value targets. According to research conducted by the team at Seqrite Labs, India's largest malware analysis facility, these attacks have moved beyond traditional espionage tactics and now exploit human emotions through social media platforms and dating apps, bypassing security systems by manipulating people directly rather than targeting technical vulnerabilities.

Researchers at Seqrite Labs identified the primary targets as government officers with access to classified documents, employees in IT, finance, defense, and research divisions, and anyone with access credentials or decision-making power. The company warns that vulnerability knows no bounds, whether you're an ordinary citizen or a high-profile target, you could be at risk of these emotionally-driven cyberattacks that pose serious threats to national security and corporate data integrity.

Honey Trap attacks follow a predictable pattern that begins on social media platforms like Facebook, LinkedIn, and dating apps where attackers research their victims' online presence. Scammers initiate contact that gradually shifts from professional to personal conversations on private messaging platforms like WhatsApp. They build trust through flattery, regular chats, and video calls, giving victims unnecessary attention and care while exchanging photos that are later used as blackmail material if victims try to expose the scam. The final stage involves requests for confidential data, such as project details or passwords to encrypted workplace domains, with this stolen information often sold on black markets.

Several recent incidents highlight the severity of this threat. In 2023, an Indian Army soldier was arrested for leaking sensitive military information to a Pakistani intelligence operative posing as a woman on Facebook, and a senior DRDO scientist who was honey-trapped by a foreign spy through WhatsApp and social media, leading to the sharing of classified defense research. Between 2019-2022, Indian Navy personnel were arrested for

being honey-trapped by ISI agents using fake female profiles, resulting in the theft of sensitive naval movement data that compromised national security operations.

Seqrite advises individuals and organisations to watch for warning signs including someone online getting close quickly and asking for work details, flirty messages appearing too soon in conversations, sudden shifts from friendly to romantic communication, refusal to participate in real-time video calls, requests for financial support or sensitive information, and attempts to isolate victims from friends and colleagues. The company emphasises that these emotional manipulation tactics are designed to exploit human psychology rather than technical system vulnerabilities.

To defend against honey trap attacks, Seqrite advises users to avoid sharing personal information online, verify profile photos through reverse image searches, and never send money or explicit content to online contacts. It is also important to remain cautious with unknown links and files, and implement zero-trust access control in organisations. Enterprises should conduct employee awareness sessions focused on psychological manipulation and emotional engineering, as these scams can lead to severe consequences including insider threats where employees leak confidential data, espionage by state-sponsored actors, and intellectual property loss that can compromise national security.

Together with ongoing efforts to combat digital threats, Seqrite continues to work towards making cybersafety a fundamental right for all and creating a cyber-safe nation through comprehensive security solutions that protect against both technical vulnerabilities and human-targeted attacks. The company's commitment to simplifying cybersecurity extends beyond traditional protection methods to include education and awareness about the psychological aspects of modern cyber threats.