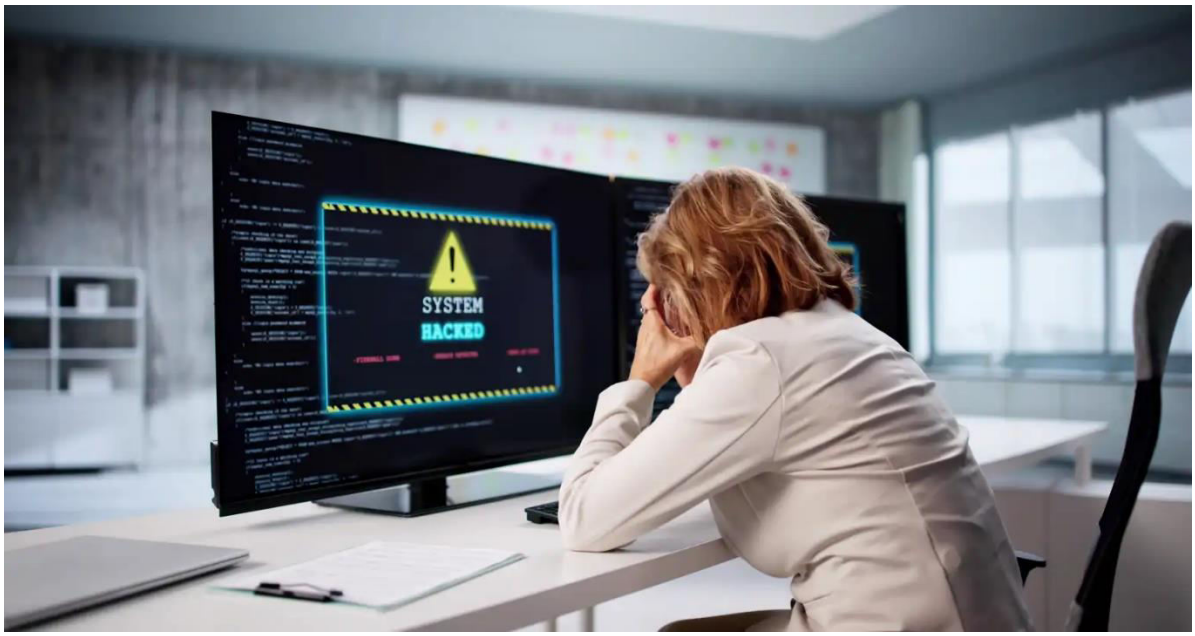
Quote by Devroop Dhar, Co-Founder & Managing Director, Primus Partners

Published in CSO Online
15th October, 2026

Ransomware extortion gets personal as attackers target employees' families

Threat actors are applying pressure beyond the enterprise by doxing employees, targeting family members, and manipulating AI systems to force ransom payments.

Authored by Nidhi Singal



Read on: Ransomware extortion gets personal as attackers target employees' families | AI cybersecurity, social engineering, cyberattacks, AI agents, data protection

Article Content:

Ransomware attackers are expanding their tactics beyond encrypting corporate systems and threatening to leak stolen data. They are increasingly using AI in attacks, exploiting organizations' own AI systems and even using physical intimidation by threatening employees and their families to pressure companies into paying ransoms.

The Semperis' 2026 Ransomware Risk Report found that 84% of surveyed ransomware victims experienced attacks involving AI, while 87% reported attacks targeting identity infrastructure. It also highlighted that attackers are exploiting technology and extending pressure beyond corporate networks to the people connected to their targets.

While 41% of respondents reported physical or psychological intimidation, 37% said employees' friends or family members had been threatened. The survey in the first half of 2026 covered 1,200 IT and security professionals across nine countries, spanning eight sectors including finance, healthcare, manufacturing, critical infrastructure and government.

Extortion is moving beyond corporate networks:

Ransomware initially relied on encrypting files and demanding payment for a decryption key. As organizations improve their ability to recover from ransomware attacks using backups and recovery systems, attackers increasingly adopt double extortion, combining encryption with data theft and threats to expose or sell stolen information.

Now, they are adding personal intimidation to their tactics. These include threatening texts, letters or packages, threats against family members and friends, physical intrusion, abduction, bodily harm and stalking.

The report found that 25% of respondents said employees or family members had been doxed (their identities were revealed online without their consent), while 23% reported swatting, where they were harassed by fabricated emergency reports resulted in law enforcement being dispatched to a victim's location. About 25% reported that employees or their family members required medical or psychological treatment, while 24% said they had hired additional security. And around 14% were even forced to change jobs, office locations, or move to a new home.

"Threats that target corporate employees beyond corporate borders are an unusual new phenomenon that distracts employees from being laser-focused while at work on the job at hand. Now you're trying to figure out how to protect yourself and loved ones against a threat that has crossed the boundary from work to personal life," Chris Inglis, former US national cyber director and Semperis Strategic Advisor, noted in the report.

Despite the fact that an organization might agree to suffer financial losses and restore their servers while rejecting ransom, the threat to hurt one of their employees' spouse or kid creates additional pressure to decision making due to the fact that it involves more people than just a business.

"Attackers do this by trying to build up a picture of an employee's personal life using the information that is already available or leaked somewhere else before. It can include public information posted on social media accounts, professional networks, data broker databases, previously leaked information, and even information available in the attacked company's network. Artificial intelligence can help speed up the process of correlating

this information and thus create a personalized threat for a person," said Devroop Dhar, MD and CEO at Primus Partners.

Exploiting enterprise AI:

As enterprises connect AI agents to corporate data, applications, and identity systems, these tools are becoming another potential attack surface. Semperis found that 44% of respondents experienced attacks involving the manipulation of their own AI agents or systems.

Courtney Guss, Semperis AVP of Crisis Management, said that if a company is adopting AI agents, one should consider that at some point, those agents will try to compromise identity systems, even if that action isn't meant to be malicious. She added, "AI agents typically try to accomplish their assigned tasks by any means they can. One way they can gain more ability to operate in the environment is by getting permissions to other systems. The fastest path to get those permissions is to compromise your identity system, which effectively puts the agent into 'god mode,' enabling it to grant itself whichever permissions it needs to accomplish its task. Unfortunately, the agent then becomes a ticking time bomb."

Dhar noted that AI can be used by attackers to speed up the processes of reconnaissance, personalize social engineering, and accelerate the processing of information. Besides, weakly secured AI agents are another entry point for hackers into systems. In most cases, AI serves as an accelerating tool but does not stand alone behind attacks. While organizations increase their capabilities for restoring encrypted data, attackers continue to become even more aggressive in exploiting weaknesses of people and organizations.

Closing the security gaps:

The evolving threat landscape raises questions about whether existing security controls and incident response plans are equipped to handle attacks that exploit AI systems and extend to employees' personal lives. Experts suggest CSOs should take care of identity security, test recovery and limited access to AI systems. They should ensure robust, phishing-proof two-factor authentication of privileged accounts, least privilege approach, safe backups of identity systems and testing restoration.

"AI agents used by the organization should have clearly defined owners and limited permissions. They should have human approval for all high-priority actions. The organization should also minimize information retention and access to sensitive personal information of employees," added Dhar.

In case an employee's family is attacked, they should have a confidential channel to report intimidation, while HR, legal, cybersecurity, and corporate security teams should know when and how to escalate cases to law enforcement. Even tabletop exercises should simulate scenarios involving compromised identity systems, threatened data leaks, and threats against employees' families.