Loyal Employee ... or Cybercriminal Accomplice?

Can the bad guys' insider recruitment methods be reverse-engineered to reveal potential insider threats? Let's take a look.

(Image: Andrea Danti via Adobe Stock)

While most employees don't join their companies with the intent to do harm, some end up doing exactly that. Whether from discontent, activism, malintent, or mere opportunity, employees who go bad create significant harm to their employers. Cybercriminals are good at finding such people to serve as their accomplices, so the question becomes: Why aren't employers good at that, too?

Keep in mind that it's not just employees who populate the field of insider threats. This threatscape "extends to partners, contractors, and related third parties that are integrated with the organization and quickly becomes a difficult problem to solve," says Greg Foss, senior cybersecurity strategist at VMware Carbon Black.

Unfortunately, no company is immune to a threat coming from within.

"It would be bold for any company to say, 'There's no one ever on my staff who would take a $1 million to plug a thumb drive in," says Marcus Fowler, director of strategic threat at Darktrace, in an October interview with Dark Reading. "That's a bold statement unless, I mean, maybe if you're a company of one."

Related Content:

An Inside Look at an Account Takeover

9 New Tactics to Spread Security Awareness

60% of Insider Threats Involve Employees Planning to Leave

Insider threats are increasing and resulting in costly damages. According to a 2020 Ponemon study, the average global cost of insider threats rose by 31% in two years to $11.45 million, and the frequency of incidents spiked by 47% in the same time period. The highest overall cost center is in containment, at an average of $211,533 per company annually. The fastest-growing cost is in investigations, which is now costing 86% more than investigations cost three years ago.

And, according to a Carnegie Mellon, US Secret Service and CSO magazine survey, "since about 2004, 40 to 45% of all incidents are insider incidents," says Randy Trzeciak, director of the National Insider Threat Center, which is in the CERT division of the Software Engineering Institute at Carnegie Mellon University. "It's not the majority, but it's just less than half of the incidents that an organization experiences are insiders, whether that be accidental or malicious insider incident."

In addition, nearly three out of four malicious insider incidents are handled internally, with "no legal action or no law enforcement activity taken," he adds. "Thus these incidents are significantly underreported."

Although various technologies can be helpful in the search for potential and active insider threats, many fail for the simplest reasons.

"While most traditional security tools are looking for outright malicious behavior, it's the users who are simply leveraging systems as they're intended for nefarious purposes that are simultaneously the most impactful and the hardest to detect pre-compromise," Foss says.

The challenges are myriad, but here are a few considerations in detecting employees who may turn on their company.

Look for Suspicious Behaviors by Otherwise Straightlaced People
"I wouldn't call them traitors, but I would say they are in an unfortunate situation," says Josh Rickard, security research engineer at Swimlane, which offers a security orchestration, automation, and response (SOAR) platform that investigates suspicious incidents, alerts, and user behavior.

Technologies such as user behavior analytics can help organizations find insider threats, "but working closely with human resources, legal, and direct line managers will give organizations insights that technology won't," Rickard says.

Examine What the Bad Guys Are Looking At
Cybercriminals know that recruiting insiders is often a long game, but not always. Knowing what the bad guys are looking for, and where they're looking for it, is essential to finding and using these same clues.

"Threat actors that are targeting your organization will perform [open source intelligence] or reconnaissance on individuals that may be vulnerable because of financial pressures, disgruntlement, social engineering, or other reasons," Rickard says. "For example, if an employee posted information about being in financial debt or being upset about their employer on social media, a threat actor may then take advantage of these statements. At this point, they may begin to build a relationship with this individual."

The good news is, not all employees will fall for it. For example, an employee at Tesla rejected a $1 million bribe to install malware for an attacker, said Fowler, who recently joined Darktrace after a career in the CIA. He faults the attackers for not doing their homework.

"Before they even offered the money, they should have gotten to a place to know that this is a type of person that would take the money," he said. "And it shouldn't have been a question. If you're bringing along a [human] asset, by the time you kind of do the 'reveal,' you should already know, 'You're joining us. We all know what's happening here.'"

Know the Bad Guys' Recruitment Tools and Tactics
Malicious actors will research an organization to identify employees by using tools such as LinkedIn, ZoomInfo, Maltego with Social Links, and Jigsaw, according to Daniel Wood, associate vice president of consulting at Bishop Fox. More advanced attackers will even use pay services such as Pipl API, LexusNexis Westlaw, and TransUnion TLOxp.

"Once they have a target list, they will usually refine the list by researching individual employees, paying close attention to current role, skills, and technical knowledge, as well as more personal attributes, such as location, arrest records, family, social media presence, and other publicly available data people tend to expose," he says.

With their soft targets selected, attackers then have to devise a plan to compromise them "in order to carry out an attack with a specific purpose, whether it's obtaining confidential nonpublic information about an organization, or person or asking the compromised employee to provide working credentials to a service, or a myriad of other things," Wood adds.

Shine a Light in Dark Places
Monitoring the Dark Web should be a given. But dark data also should be closely monitored.

"The information that is often most difficult to protect is dark, unstructured data that cannot easily be translated into zeros and ones," says Kon Leong, CEO and co-founder at ZL Technologies. "Instead, dark data is information created by humans for humans, including emails, file shares, and messages. Over 80% of a typical company's data is unstructured, and despite the wealth of information stored within, few have taken proper measures to protect it or harness its full potential."

Be Realistic
Ultimately, be aware that even these tips have limited value. Your best bet is to reinforce the human bonds between employee and employer and to address issues before they become vulnerabilities or openings for enticements.

"Insider threats have been an unfortunate reality for a long time," says Rolf von Roessing, partner and CEO at Forfa Consulting AG and ISACA board vice chair. "While historic methods such as background checking, monitoring behavioral patterns, and analyzing credit histories may have been commonplace in the past, we simply cannot 'reverse engineer' the human mind to predict whether a breach might occur through one person or another."

A prolific writer and analyst, Pam Baker's published work appears in many leading publications. She's also the author of several books, the most recent of which is "Data Divination: Big Data Strategies." Baker is also a popular speaker at technology conferences and a member ... *View Full Bio*