Not so IDLE hands: FBI program offers companies data protection via deception

Enlarge / The FBI’s IDLE program uses “obfuscated” data to hide real data from hackers and insider threats, making data theft harder and giving security teams a tool to spot illicit access.
Getty Images

reader comments

5 with 5 posters participating

Share this story

The Federal Bureau of Investigations is in many ways on the front lines of the fight against both cybercrime and cyber-espionage in the US. These days, the organization responds to everything from ransomware attacks to data thefts by foreign government-sponsored hackers. But the FBI has begun to play a role in the defense of networks *before* attacks have been carried out as well, forming partnerships with some companies to help prevent the loss of critical data.

Sometimes, that involves field agents proactively contacting companies when they have information of a threat—as two FBI agents did when they caught wind of researchers trying to alert casinos of vulnerabilities they said they had found in casino kiosk systems. “We have agents in every field office spending a large amount of time going out to companies in their area of responsibility establishing relationships,” Long T. Chu, acting assistant section chief for the FBI’s Cyber Engagement and Intelligence Section, told Ars. “And this is

really key right now—before there's a problem, providing information to help these companies prepare their defenses. And we try to provide as specific information as we can."

But the FBI is not stopping its consultative role at simply alerting companies to threats. An FBI flyer shown to Ars by a source broadly outlined a new program aimed at helping companies fight data theft "caused by an insider with illicit access (or systems administrator), or by a remote cyber actor." The program, called IDLE (Illicit Data Loss Exploitation), does this by creating "decoy data that is used to confuse illicit… collection and end use of stolen data." It's a form of defensive deception—or as officials would prefer to refer to it, obfuscation—that the FBI hopes will derail all types of attackers, particularly advanced threats from outside and inside the network.

Going proactive

Enlarge / A recent FBI Private Industry Notification (PIN) warned of social engineering attacks targeting two-factor authentication.

In a discussion about the FBI's overall philosophy on fighting cybercrime, Chu told Ars that the FBI is "taking more of a holistic approach" these days. Instead of reacting to specific events or criminal actors, he said, "we're looking at cyber crime from a key services aspect"—aka, what are the things that cybercriminals target?—"and how that affects the entire cyber criminal ecosystem. What are the centers of gravity, what are the key services that play into that?"

In the past, the FBI got involved only when a crime was reported. But today, the new approach means playing more of a consultative role to prevent cybercrime through partnerships with both other government agencies and the private sector. "If you ever have the opportunity to go to the courtyard at FBI Headquarters, there's a quote there. 'The most effective weapon against crime is cooperation, the efforts of all law enforcement and the support and understanding of the American people.' That can not be more true today, but it expands from beyond just law enforcement to the private sector," Chu said. "That's because we're facing one of the greatest threats that our nation has ever faced, arguably, and that's the cyber threat."

An example of that sort of outreach was visible in a case Ars reported on in March—that of the casino kiosk vendor Atrient. FBI Las Vegas field office and FBI Cyber Division agents picked up on Twitter posts about an alleged vulnerability in Atrient's infrastructure, and the agents connected the company and an affected customer with the researchers to resolve the issue (which, in Atrient's case at least, went somewhat awry). But in these situations, the FBI now also shares information it gathers from other sources, including data gathered from ongoing investigations.

Sharing happens a lot faster, Chu said, when there's a

“preexisting relationship with our partners, so we know exactly who we need to call and vice versa.” And information flows faster when it goes both ways. “Just as we’re trying hard to get the private industry information as fast as possible, it’d be a lot more effective if we’re getting information from the private industry as well,” he said. Exchanging information about IP addresses, indicators of compromise, and other threat data allows the FBI to aggregate the data, “run that against our databases and all our resources, and come up with a much stronger case, so to speak, against our adversaries,” Chu noted, “along with trying to attribute or identify who did it will prevent further attacks from happening.”

Some information sharing takes the form of collaboration with industry information sharing and analysis centers (ISACs) and “Flash” and “Private Industry Notice” (PIN) alerts on cybercrime issues. And to build more direct relationships with companies’ security executives, the FBI also offers a “CISO Academy” for chief information security officers twice a year at the FBI Academy in Quantico, Virginia. Attendees are indoctrinated on the FBI’s investigation approaches, and they learn what kind of evidence needs to be preserved to help spur investigations forward.

But for some sectors of particular interest, the FBI is now trying to get a deeper level of collaboration going—especially with companies in the defense industry base (DIB) and other critical infrastructure industries. The FBI sees these areas as crucial industry-spanning networks, and it hopes to build a defense in-depth against cyber-espionage, intellectual property theft, and exposure of other data that could be used particularly by other nations in a way that could impact national security or the economy.
That’s precisely where IDLE comes in.

https://arstechnica.com/?p=1632381