THE WALL STREET JOURNAL.

MONDAY, DECEMBER 7, 2020

JOURNAL REPORTS: TECHNOLOGY

In Battle Against Hackers, Companies Try to Deceive the Deceivers

The idea is to convince the attackers they have been successful, so that they will then reveal their methods

By Heidi Mitchell

An increasing number of companies are looking at an innovative approach to deal with hackers that break into their computer networks. They lure cybercriminals into thinking they're getting close to the good stuff—and then they trap them.

That's what Land O'Lakes, the suburban Minneapolis agricultural giant, is doing.

"Manufacturing-plant technology is difficult to protect, because those mills, generators and turbines were built 20 years ago with little consideration for security," says Land O' Lakes Chief Information-Security Officer Tony Taylor. If a hacker shuts down a dairy plant, "we lose hundreds of gallons of milk that we've already paid for. And we can't make any butter."

So, the company uses a tool called DeceptionGrid, created by Boston-based cybersecurity shop TrapX. The technology deploys an array of decoys and booby traps throughout the Land O' Lakes network that mimic crucial information, to convince hackers that they have gotten access to the company's crown jewels.

"Once any of the [decoys] are accessed or probed in any way, one centralized console alerts us, so we know to start investigating the source of that activity," says Mr. Taylor. His team can then contain the intruder.

It is a method known as deception technology—and it is gaining momentum as cyberattacks become more sophisticated, and the world moves to less-secure work-from-home models and cloud computing.

This new method doesn't try to bar intruders from getting in, like firewalls. Instead, deception technology scatters fake information—such as false credentials that can be used to access vital information—throughout a company's network to lure attackers.

Then, when the false information gets hacked, the company is alerted and can either kick out the bad guys or isolate them from the rest of the network to study their methods—and better identify them in the future.

Land O' Lakes says the technology has helped shield it from attack. For instance, the company had a contractor whose laptop was infected with malware that began scanning the network, recalls Mr. Taylor. But the malware hit many of the decoys, and his security team was able to locate the source and disable the intruder quickly.

Land O' Lakes hasn't had an attack from an unauthorized outsider since it implemented deception technology, Mr. Taylor says. "We still have the older defenses like firewalls in place," he says, "but we layer deception tech on top of it."

Beyond honey

Deception technology is the evolution of another idea called "honey pots": fake servers that mimic a company's actual server. They sit passively and wait for an attacker to climb in.

The problem with these baits is that they allow security teams only to monitor and learn the behavior of bad actors as they attempt to move closer to high-value targets. Studying patterns is useful, especially if that intelligence can be fed into a machine-learning system to adapt to hackers' tricks, but it doesn't capture the attackers.

Those honey pots can be linked together into a sophisticated network called a honeynet to make them even more effective, but that isn't cheap, says Raj Badhwar, CISO at Voya Financial, who created such a network for the financial-services company last year. A large bank, for instance, could pay up to $1 million in subscription fees alone for such a setup, he says, "plus you have to hire human monitors," which brings up the price substantially.

Enter deception technology. Unlike honey pots, it isn't just designed to study attackers but to stop them outright. As soon as a

(over please)

malicious actor interacts with a decoy, an alarm is raised, and the cybersecurity team can go into active-defense mode, isolating attackers or ejecting them before they have escaped with any valuable property.

And because deception technology operates within the main network and requires very little hardware or infrastructure to implement, it can be a much more cost-effective solution.

But that simplicity brings more risk. Since deception technology lives inside the main network, there is always the chance that hackers who are inside could get their hands on real assets instead of decoys.

So, most users couple deception systems with traditional defenses like firewalls, anti-malware solutions, encryption and authentication systems, which aim to keep attacks out of networks in the first place.

"I'm adamant about [defenses like deception technology] being only one component of the security strategy," says Wade Woolwine, principal security researcher at deception-technology maker Rapid7 in Arlington, Va. For instance, he says, he builds defenses into his systems to look for suspicious credential uses, such as employees logging in from new locations.

A growing effort

Ofer Israeli, chief executive of deception-technology firm Illusive Networks, says the technology is more widespread than many assume, especially in highly regulated industries like banking, insurance and government.

Mr. Israeli believes that to stop an attack, you have to think like a cybercriminal. "If I'm an attacker, I'm going to dig into your browser history and find your saved login credentials. And I'll go unnoticed because I'm using the same pathway that you use to log into the cloud as part of your daily routine," he says.

Illusive's technology plants dozens of fake but believable data points into every company-issued laptop or cellphone. If the attacker exploits an administrator's credentials, the system disorients them with deceptive data and lets defenders know there is an unauthorized presence on the network. Setting up the system takes less than a second, Mr. Israeli says, "and we have a 95% true-positive rate, meaning almost no false alarms."

Among Illusive's competitors is Attivo Networks, of Fremont, Calif., which in 2018 helped supplemental-insurance giant Aflac install deception technology. Aflac Global CISO Tim Callahan is rolling out the system to subsidiary networks now. "Fortunately, we haven't caught a criminal, but that means we have a high belief that so far we have had no theft," Mr. Callahan says.

Steve Preston, vice president of growth and strategy at TrapX, says people would be surprised to see exactly how and where companies are hacked. "A lot of times it's a third party that comes in with a USB to service a machine, and it has [ransomware] on it," he says.

He knows of a petrochemical plant in Europe that wasn't connected to the internet but was infected with ransomware through a coffee pot in a break room that was online. "Attackers are agile and fast. They're adapting to the new-normal chaos, taking advantage of remote workers and new security gaps," says Mr. Preston. "When security analysts can focus on real threats detected through deception technology, they waste less time chasing false alarms—and a quicker response means reduced loss."

Ms. Mitchell is a writer in Chicago.