West Texas Cyber Security Consortium

Operation Stop the Exfiltration

Determined cybercriminals and cyberspies will find their way to the data they want, but there are ways to trip them up as they try to make their way out.

Second installment in an occasional series on a new sense of urgency for incident response after a cyber attack. Read part 1, "Incident Response Now Shaping Security Operations," here.

The sophisticated cybercriminals who stole some 40 million payment card accounts from Target had to work harder than most bad guys. Not only did they have to first gain a foothold into the retailer's network via its HVAC contractor in order to infect its POS system, but they also had to set up shop inside the Target network on one of its computers in order to siphon and then ship out the data from the POS to their own machines.

"They had to move laterally and needed a control node. So they had to set up a command-and-control inside Target" and attack the POS at the time the cards were swiped and the data briefly unencrypted, says Mike Lloyd, CTO at RedSeal Networks. "Target raised the bar, so the attackers had to. This is an endless game. Yes, Target did lose in the end, but you can learn from what they did well: they forced the attackers to put a command and control inside their [Target's] network."

What could have made the difference in Target's breach -- and in that of other victim organizations -- is if they had in place more hoops for the attackers to jump though so they could first stopped them from commandeering their internal machine, or at the least, or altogether deterred them from exfiltrating the stolen data, he says. Target apparently had blocked outbound paths on its POS, so the attackers couldn't just send the data out, he says, so they instead did so via an internal system at the retailer.

"You try to make it so they can't simply walk out of the building," he says. "It's not literally putting tar or glue on packets. But if the number of locations [machines] that could talk to the POS is very limited," for example, then the chances of the attackers exiting the building with stolen data is greatly reduced.

"How can you make it harder for them to get data out?" he says. "You can build a better maze."

There are no specific tools or sure-fire techniques for tripping up attackers trying to grab data. There are, however, ways to configure and architect the environment to slow them down and potentially stop them in their tracks, or even shut them down before they manage to pilfer anything. It's a matter of closing unnecessary conduits to sensitive and at-risk data, and becoming intimately familiar with the normal and acceptable goings-on in the network so you can spot the outliers.

Cris Ewell, chief information security officer at Seattle Children's Hospital, says there is no easy answer for how to stop an attack from becoming a breach, but a solid and well-rehearsed incident response (IR) plan can go a long way. Ewell, who reports to the hospital's general counsel as well to a Board-level committee, oversees the security operations as well as IR. "Incident response is one of my top four activities for the hospital," he says. "We are very proactive at looking at things and stopping them before they happen because they could become a breach."

Knowing the risks facing key machines and how they communicate with other machines helps. "You have to really focus on narrowing that scope as much as you can," he says. The hospital has been executing that strategy for the past four years, narrowing holes in firewalls, for example, and closing any risky or unnecessary ports on its nodes.

Seattle Children's monitors its traffic closely, and none of its internal systems have direct access from the Internet. That access goes through a portal, he says, with Citrix virtualization and two-factor authentication. "That decreases the risk pretty significantly," he says.

At the least, you need to understand when an incident has occurred, Ewell says. "There's nothing you can do to stop someone from coming in. Our adversaries are incredibly bright and well-funded, and if they want our data, they are able to get it. That's the first premise," he says.

The hospital's regimented and proactive incident response operation is more the exception than the rule today among enterprises. Incident response represents less than 10 percent of the overall IT security budget at most organizations, according to a recent study by The Ponemon Institute, and more than one-third of organizations do not have a fully operational IR team.

"We collect terabytes of data," Ewell says. "Unfortunately, it's that little blip... [determining] what's important or not. That's where my team is focusing on: How do we do the analytics to build that intelligence in?"

Ewell belongs to multiple ISACs and regularly swaps threat information and experiences with other CISOs in his region. " We are sharing things like certain IPs, 'I just saw this and it looks unusual. Did you?' We are talking," he says. "That's the first part to how you stop this. That's what makes us different" than other organizations, he says.

The missing link in his organization -- and one that is common among many others -- are the tools to help security and IR analysts more accurately sift through monitoring events and find the real problems or potential ones, and to not miss that one tiny blip that could be the attack. "I know my high-risk targets ... we are watching those every day," Ewell says. "That's how we're successful in stopping incidents quickly." Ewell's team is working on developing its own custom tools to drill down even more on the "blips," he says.

Measuring the baseline of your servers and PoS terminals and setting security policies and alerts around that can lock out a lot of attacks, says Dan Hubbard, CTO at OpenDNS. "There's not much reason for your POS or other servers to be connecting to servers in Russia and downloading data," he says. "Context of identity and the baseline are key," because it may be just fine for an end user to download a white paper from a Russian website, for example.

Monitoring can help spot an attacker moving from one machine to another inside your network. Host IPS systems also can help stop malware from running on machines, experts say.

In Target's case, it may have been a matter of limiting the number of locations the POS could communicate with, or cranking up the levels of the host IPS on its servers, notes RedSeal's Lloyd. "You could put that [sensitive system] in a controlled network zone. But you don't see many commercial companies doing this," he says.

At the least, it's locking down with tighter controls the machines that communicate with critical data. "It's slowing them down through architecture, ahead of the attack," he says.

Meanwhile, attacks are more precise now because cyberspies and the more sophisticated cybercriminals are conducting more reconnaissance prior to breaking in, says a security and IR team member at a large US manufacturer. "It's sniper hacking now," he says. "They know exactly where they want to go. There's no poking around. They already know what our network looks like."

Next installment: How to conduct a smooth incident response operation
Kelly Jackson Higgins is Senior Editor at DarkReading.com. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise Magazine, ...
http://www.darkreading.com/informationweek-home/operation-stop-the-exfiltration/d/d-id/1204263