Hewlett Packard Enterprise

FireEye

by MIT Technology Review Custom
In Partnership with Hewlett Packard Enterprise Security Services and FireEye Inc.

Once More Unto the Breach: What It Takes to Defeat Cyberattackers

Cyberattacks are a fact of life across the world, as intruders breach more and more organizations each day. Why are we so vulnerable? And what can we do to make our systems more secure?

146 days

Average time an attacker spends inside a network before being detected.

Source: *M-Trends 2016 Report,* Mandiant

Picture this: It's the evening before a big holiday. Family and friends descend upon your home to enjoy a relaxing meal and time away from the office.

But not everyone is taking a break.

In the middle of the night, the phone rings. There's an emergency at work—a network breach. "I've received calls at the most inopportune times," says Marshall Heilman, vice president and executive director, incident response and red-team operations at the cybersecurity firm Mandiant, a FireEye company. "In 2014, I got a call just before Thanksgiving. I had to go in to help a company that had been hit by an advanced attacker, and it was serious," Heilman recalls, adding that his team battled another breach on Christmas Eve in 2015. Team members also have plenty of stories about, for instance, being so busy on holidays that employees were working "while trying to baste a turkey at the same time," Heilman says: "Hackers are strategic about the holidays. They compromise organizations at those times because that's when they expect the defenses to be down."

But as Heilman knows all too well, hackers don't need to wait until the holidays to catch their targets off guard. Organizations of all sizes are vulnerable to breaches year-round.

There was a time when cybersecurity experts used a castle analogy to describe such attacks—where enemies cross a "moat," scale a "wall," and sneak in undetected by the "knights." But Chris Leach, chief technologist for Hewlett Packard Enterprise (HPE) Security Services, calls that perspective obsolete. "The older tactics of having the knights watching the perimeter is not the best use of resources. Because of changing threats and the ways the camouflaged soldiers get in, we need to detect intruders more quickly, before they can find the crown jewels."

Andrzej Kawalec, chief technology officer for HPE Security Services, also sees an evolution in cybersecurity. "Today, there is a huge asymmetry in the capabilities of the attackers and the defenders," he says. "Most organizations today rely on the walls and moats of yesteryear, thinking they're defending against catapults and cannons, while attackers instead use drones and highly targeted stealth technology." And in today's digital enterprises, he notes, employees and customers are often outside a company's walls—for instance, in coffee shops and collaborative spaces without

strong perimeter defenses. Meanwhile, as HPE's Cyber Risk Report 2016 finds, 86 percent of organizations currently lack adequate cybersecurity capabilities.

Months on the Inside

On average, an adversary spends 146 days beyond the perimeter and inside a network before being detected, according to the M-Trends 2016 Report by Mandiant. While most attacks won't turn into major breaches, constant cybersecurity threats are a fact of life these days, Heilman says. "A successful attacker can gain network access over the course of a week, or even in just a couple of days," he says. "So if you can't prevent an attack—if you know the attacker is going to get in no matter what—then you want to detect it as fast as possible, and then respond to it." HPE's Kawalec agrees. "People need a robust security partner, or set of partners, who understand how to respond in real time," he says.

$7.7M

Mean one-year loss to cybercrime at 252 organizations in 2015.

Source: *2015 Cost of Cyber Crime Study*: Global, Ponemon Institute

> "Most organizations today rely on the walls and moats of yesteryear, thinking they're defending against catapults and cannons, while attackers instead use drones and highly targeted stealth technology."
>
> **—Andrzej Kawalec, Chief Technology Officer, Hewlett Packard Enterprise Security Services**

That's where FireEye and HPE come in. In a first-of-its-kind alliance, the two companies offer incident response, compromise assessment, and threat detection services to enterprises worldwide. Most organizations will face many attacks over the course of a year, but just one or two hugely disruptive breaches during that time, Kawalec says. Together, HPE and FireEye respond to thousands of such breaches annually, typically handling 30 to 40 concurrently at any one time. "So there's a need for real learning and understanding about the cadence—the sequence of events—and how they operate," Kawalec says.

That cadence includes research and reconnaissance, infiltration, discovery, capture, and exfiltration or data extraction. It is paramount, Kawalec says, to understand your organization's risk profile: "You should start with a simple question: What are your digital assets and the cyberthreats facing them? Without that answer, you're going to be woefully underprepared to respond in real time to a potentially devastating cyberattack."

The Attack Lifecycle

Regardless of whether the perpetrator is a "hacktivist," a cybercriminal, or a state-sponsored threat actor, the cadence (or attack lifecycle) remains essentially the same, Heilman says. His team's work skews toward advanced persistent threats (APTs), which are situations where perpetrators gain access to a network and stay there for a long time.

After they have researched a target company's systems and people, attackers take the next step: infiltrating a network by tapping into a weakness—in 80 percent of cases, by sending a "spear-phishing" email, Heilman says. "By making a human click on a link or open up a file, the attackers exploit that to run their own malicious code, which often creates a back door into the network." That establishes a foothold from which attackers can control their activities in that environment.

Next comes "privilege escalation," Heilman explains: "They take the rights that they've gained from the systems that they've compromised and escalate them to a local administrator or a main administrator, to root access, or to whatever they may need for greater access to systems and data." That's often accomplished by stealing credentials, cracking passwords, or exploiting vulnerable software.

Once the attackers have obtained administrative rights, they've reached APT status. They undertake reconnaissance, moving laterally throughout the company's computer systems, taking stock of what they're seeing, noting the roles and responsibilities of key individuals and the location

6%

Percentage of business and IT leaders surveyed who believe their organizations are "extremely well prepared" for a security breach involving serious information loss.

Source: *Cybersecurity Challenges, Risks, Trends, and Impacts Survey,* MIT Technology Review Custom in partnership with Hewlett Packard Enterprise Security Services and FireEye Inc.

of information they want. Perpetrators often maintain presence, or "persistence," by installing multiple back doors throughout the environment. "Then they're going to try to accomplish whatever they came to do, which is often stealing information—intellectual property, financial data, merger and acquisition details or personally identifiable information, for example," Heilman says. When they've completed their mission, attackers retain access where possible in case they want to return.

Tips for Targets: Think Like the Bad Guys

In Heilman's view, the best approach to defeating attackers is adopting their mindsets—not responding to their next moves, but anticipating them. You must also recognize and detect anomalous behavior in your organization.

> "If you can't prevent an attack—if you know the attacker is going to get in no matter what—then you want to detect it as fast as possible, and then respond to it."
>
> **— Marshall Heilman, Vice President and Executive Director, Incident Response and Red-Team Operations, Mandiant**

Kawalec, of HPE, also encourages enterprise executives to become acquainted with their company's threat landscapes. Knowing which assets are most critical, and thus must be vigilantly protected, is a significant offensive advantage against cyberthreats. "Understand what is valuable in your organization. Who is going to try and get those major assets? That gives you a view of risk," he says. "Then understand whether you've been compromised and where you're vulnerable." Finally, the biggest issue: "Do you know exactly what you're going to do when the phone rings in the event of a breach?" Kawalec asks. "Those are the big questions that any cybersecurity leader or chief information security officer should be able to answer on behalf of their organization—because if they can't, they're in trouble."

As with many other crimes, the first 48 hours following a breach are the most critical. But how quickly and how well an organization responds and recovers is determined by what has been done *before* the incident. "Your initial emergency response is dependent entirely and fundamentally upon the work you did months earlier: Write and understand a breach-response plan, identify the roles and responsibilities of the people involved, especially the first responders, and then train people," Kawalec explains. Drills are crucial as well: "Run scenarios and red-team reviews—or realistic simulations—and take the company board through a real-life experience of a cyberattack," he says. "That way, when they do experience it for real, it's not for the first time."

And it won't be the last time. As HPE's latest Cyber Risk Report documents, the volume of breaches has increased, and although attackers are still using relatively old methods to scale firewalls and bypass antivirus software and other traditional defenses, they're also becoming more sophisticated. They're adjusting their techniques to circumvent newer cybersecurity technologies, such as the use of deep learning to detect possible fraud. In addition, they're developing intricate business models in which they collaborate on attacks, and they're expanding their reach into everything else connected to the Internet, including cell phones, tablet computers, cloud services, and the Internet of Things. It all adds up to massive expenses for organizations: A 2015 Ponemon Institute study of 252 companies estimates their mean annual loss to cybercrime at $7.7 million for just one year, with the security-research firm reporting that some lost as much as $65 million.

Dealing with increasingly sophisticated adversaries requires correspondingly sophisticated lines of defense. With that in mind, HPE has developed an industry-standard cyber reference architecture (CRA) that provides customers with a blueprint for advanced threat protection services and incident response capabilities. The CRA incorporates FireEye's most current insights regarding APTs—that is, those attackers who establish a strong foothold and wreak havoc over long periods of time.

Essentially, the CRA is a "cybersecurity cookbook," says Leach, of HPE. "The reference architecture articulates what your organization should look like: the key areas, the span of responsibilities, and the metrics. It ranges from the strategic part—including running response drills inside a company—to the people, to the ops, to what you should do in an actual breach," he explains.

The architecture also includes specific use blueprints, synthesizing the common events and mapping them back to the CRA to see whether it addresses risk and operational risk, Leach adds. "The chief information security officer (CISO) is probably addressing risk as proactively as he or she can. But a CISO may not hold all of the pieces of that reference architecture and, therefore, needs to partner with others" to get the whole picture, he says. "The CRA really is a valuable end-to-end guide."

Partner With the Experts

Statistics indicate that companies need outside help with cybersecurity. Only 47 percent of the 2015 breaches Mandiant addressed were discovered internally, by a company's own employees; in 53 percent of cases, companies learned about breaches from external sources, such as law enforcement, the media, customers or suppliers—or even the attackers themselves. Kawalec says such outside notification puts company leaders in a difficult, reactive position. "It means that they find it very hard to control the situation, to command and direct the appropriate response, and also to communicate from a position of strength," he says. "They have to focus on understanding and tracking the behaviors of users and systems, and then match a pattern against something they know is not right."

More and more global companies are turning to HPE for cybersecurity remediation services underpinned by FireEye's advanced threat detection, intelligence, methodologies, and incident-response expertise. The HPE-FireEye alliance provides 24/7 security monitoring for indications that a cyberattack has evaded traditional technology defenses. HPE-FireEye threat analysts engage as an extension of an organization's cybersecurity team, providing insight and intelligence from the frontlines. In addition to responding to incidents, HPE and FireEye proactively hunt for indicators of compromise in their clients' environments.

With 10 security operations centers around the world, and 5,000 security professionals serving 10,000 clients, HPE offers unparalleled global reach. Additionally, FireEye has six global security operations centers providing constant detection and response to 4,400 customers. Together, the two companies form a powerful partnership in cybersecurity, Kawalec says. "When you consider the resources of a typical security team in a pretty big organization, even large security teams would only be 15 to 100 people. HPE and FireEye are able to project cybersecurity capability around the world. That's why people turn to us for that help."

For more information on cybersecurity, please explore this HPE-FireEye resource website.