DIGITAL **SPOTLIGHT** | cybersecurity

CSO

BUSINESS RISK LEADERSHIP

Danger Lurking
What APT really means, and what to do about it
PAGE 4

APT in Action
Heartland Payment Systems CTO Kris Herrin on the HPS breach
PAGE 9

Beneath the Surface

Advanced Persistent Threats: Don't let the hype disguise the real dangers
PAGE 2

www.csoonline.com $9.00 February/March 2012

A Clear-Eyed Look at APT

BY DEREK SLATER

Security is occasionally susceptible to two afflictions:

1. Hype.
2. Semantic arguments.

"Advanced persistent threat," or ATP, hits the exacta, to borrow a horse-racing term. Because victims, marketers and journalists alike seized the term APT with gusto (hype), an inevitable backlash has occurred (semantic arguments).

Anyone who has suffered a breach has great incentive to characterize the perp as both advanced and persistent. After all, admitting you've been hacked at random by a casual script kiddie might be looked upon unfavorably by your CEO, or a civil judge, or the Securities and Exchange Commission, or your shareholders.

And anyone selling a security product has great incentive to say it can stop a tank.

Plus, stories about the bogeyman sell newspapers.

So, amid the flurry of press releases and articles and blog posts touting APT attacks, some folks have concluded that the term is meaningless.

The thing is, some threats really are advanced, and some are persistent, and some are both. State-sponsored cyberespionage is clearly emerging from the shadows. Organized hacking syndicates do exist, and do target specific companies in specific industries. Disorganized hacktivist syndicates do want to embarrass corporations and governments.

So in this special Digital Spotlight edition from *CSO*, Michael Fitzgerald digs beneath the semantics in the hope of finding a reasonable basis for calling something (or someone) an APT. Then CISOs offer advice on confronting the abstract bogeyman with concrete defensive actions. And Heartland Payment Systems CTO Kris Herrin offers some details about the hackers who infiltrated his company's systems in 2008.

I take away a few key points.

First, if your adversaries are advanced, make sure you are doing the basics. The basics include not just mounting the old standby network defenses (guard your perimeter, segment your networks, monitor your logs, educate your employees), but also knowing what kinds of information your organization produces and retains, what the value of that information is, and how to interconnect your technical defenses with the right policies, physical security measures and legal defenses. Ten years ago, that kind of holistic approach was advanced. Now, it absolutely has to be considered basic.

Tim Llewellyn

Second, if your adversaries are persistent, make sure you are even more persistent. Persistence means constantly evaluating your defensive posture, adjusting your toolkit of processes and technologies, staying on top of the threatscape and mapping it to your controls.

And third, these kinds of targeted attacks are going to continue to yield results for the attackers. So, if not all incidents can be prevented, you must be well prepared to detect and respond to them. Industry leaders such as Bruce Schneier and Richard Bejtlich have been making this point for years: First-rate incident response capabilities mean you are able to detect a breach quickly, limit the damage suffered, and rapidly restore full business functionality. Incident response excellence is a fiduciary responsibility.

–Derek Slater, dslater@cxo.com

CSO

Editor in Chief Derek Slater
Contributing Editor Sara Shay
Copy Editor Colleen Barry
Editorial Administrator Pat Josefek
Contributors Michael Fitzgerald, Mary Brandel

DESIGN
Exec. Director, Art and Design Mary Lester
Art Director Steve Traynor

RESEARCH
Research Manager Carolyn Johnson

EDITORIAL/ADVERTISING/ BUSINESS OFFICES
492 Old Connecticut Path, P.O. Box 9208, Framingham, MA 01701-9208
Main phone number: 508 872-0080

IDG Enterprise
An IDG Communications Company

INTERNATIONAL DATA GROUP
Chairman of the Board Patrick J. McGovern
IDG COMMUNICATIONS, INC.
CEO Bob Carrigan
Chief Content Officer John Gallant

President and CEO Michael Friedenberg
Group Publisher Bob Melk
Publisher Bob Bragdon
Senior National Sales Manager Per Melker
East Coast Regional Director, Integrated Sales Roz Burke
West Coast Regional Director, Integrated Sales Michelle McHugh
Sales Associate Sarah Nadeau

INTEGRATED MEDIA AND ONLINE SALES
SVP, GM, Online Operations Gregg Pinsky
SVP, Online Sales Brian Glynn
East Coast Online Regional Sales Manager Richard Hartman
West Coast Online Regional Sales Manager Erika Karr
Central Online Regional Sales Manager Stacy Bryne
Director, Online Account Services Danielle Tetreault

CUSTOM SOLUTIONS GROUP
Vice President Charles Lee
National Sales Directors Brett Ferry, Karen Wilde

PRODUCTION
VP/Manufacturing Chris Cuoco
Production Manager Heidi Broadley

EXECUTIVE PROGRAMS
SVP, Executive Programs Ellen Daly
Sr. Director, Event Operations Deb Begreen
VP, Content Development & Events Derek Hulitzky

MARKETING
Vice President, Marketing Sue Yanovitch
Marketing & PR Manager Lynn Holmlund

LIST SERVICES
Contact Steve Tozeski of IDG List Services at 508 820-8106 or *stozeski@idglist.com*

REPRINTS & PERMISSIONS
For information about reprints and copyright permissions, please contact The YGS Group, 800 290-5460, ext. 100, *cso@theygsgroup.com*

BPA WORLDWIDE

Danger Lurking

What APT really means, and what to do about it

BY MICHAEL FITZGERALD

Flickr Creative Commons

Every couple of years the security world faces its version of Jason or Freddie or Ghostface, some malevolent force that aims to end life as we know it. From the worm to the virus to the Trojan horse to phishing to SQL injection to the Zero Day Exploit, these serial killers build on one another and torture the dreams of CSOs. Now, we face a malicious threat made worse by its malignant name: the Advanced Persistent Threat.

Clearly, the names of these security threats have gotten less interesting with time. But every CSO can spell APT. So can every security marketer, and they tend to stamp the label on everything in sight.

Partly that's because a string of high profile companies have suffered losses from APTs. Google, among the most vaunted names in technology, suffered an APT. RSA—a fabled name in security itself—confessed that some advanced and very persistent hackers not only threatened it but also made off with information related to its SecurID line of products. The Internet Security Alliance told companies in the defense industry that APTs were "a near-existential threat," back in 2009.

Despite such dire words, the defense industry persists, thrives even. And at least one CSO dismisses the term "APT" as a lot of marketing hype.

"The phrases that security vendors want to scare you to death with are kind of new, but this is stuff you should've been worried about as a CSO eons ago," says Ken Pfeil, CSO at Pioneer Investments, an investment management firm in Boston.

Notice that Pfeil does not say advanced persistent threats don't exist. They do, and he thinks CSOs should be worried about them. What gets him going is the idea that there's a simple product one can buy to keep a company safe. When he talks with CSOs, he says, "a lot of them are not very technical, and they buy into vendor speak: 'If you buy this product it's going to protect you from APTs.'"

It's a natural human reaction to think that when a problem arises, a clever technologist will come up with a product to counteract it. Unfortunately, no single product can stop an advanced persistent threat. "What it means, in layman's terms, is, 'we got hacked,'" Pfeil says. He says advanced persistent threat gives CSOs public relations cover; something like, "they used an advanced persistent threat to compromise some insecure channels to gain access to blah blah blah" sounds more forgivable than "we got hacked, and they got all our data."

What is an APT?

The National Institute of Standards and Technology provides a detailed definition: "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating (i.e., transporting it from internal networks to external drop servers) information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out

these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives."

All that boils down to one simple phrase: APTs are about stealing data over time.

Hackers capable of carrying off advanced persistent threats seem to share a few characteristics: They are bright. They are talented enough to write sophisticated viruses, worms and other malware programs, and to disguise them so that the myriad firewalls and AV and IDS and other tools do not find them, even when they are siphoning information back out of the network. In some cases, particularly those involving banks, the hackers have to organize groups of people to do things like withdraw money from ATMs and deposit it into other bank accounts. And, like good CSOs, these hackers have to understand the whole IT environment, not just the network.

APTs are about stealing data **over time.**

They are methodical. They probably buy and run all the significant antivirus tools, using them to test their code before they let it out in the wild, to make sure it won't get caught quickly or be noticed by future updates.

They are patient. Unlike on the SciFi channel or in the movies, hackers don't typically break into corporate networks with a few keystrokes, although some automated attacks might make it seem that way. Hackers may also slip in via social engineering. Skill with people is an underrated aspect of hacking. Breaking into a network through a human link can be easier than figuring out a way past technology, particularly if a company has done a good job blocking its network's doors and windows.

Such attacks have always been part of the computing world, says Greg Shipley, until recently CTO of Neohapsis, a security consultancy in Chicago. Shipley says Neohapsis saw "multiple breaches" in the late 1990s and early 2000s that would have fit the current definition of an advanced persistent threat: previously unknown toolkits used in a sophisticated way to penetrate an organization's network undetected, and to stay that way despite the hacker coming back again and again.

What has changed about such attacks, he says, is volume. "There's definitely more of this going on. There are more people at it," Shipley says. Some of that increased action comes from governments ramping up cyber espionage. But, "cut out the nation-state thing for a minute and look at just straight-up criminals. I don't think anybody would argue that there aren't more criminals involved in computer-based attacks today than there were just 10 years ago."

Shipley says an increase in the number of attacks makes sense, given that Western society is far more technologically oriented—and dependent—than it was a decade ago. Mobile devices such as cell phones are now widespread, and consumers are broad adopters of digital technologies, many of which were not available in the past.

Pfeil says another difference is that business-side executives will sidle up and ask him what to do about buzzword security problems. They don't necessarily come offering money. He says the hard truth for CSOs when it comes to advanced persistent threats is that "from [the business] perspective, this is not really a new type of attack. It's stuff that they can say 'I funded you eight years ago against these types of things, and now you're telling me you did not provide adequate resources against them?'"

Plenty of CSOs, though, are finding business execs are willing to add some money for protection against sophisticated hacks. An August 2011 Enterprise Strategy Group survey of 244 security professionals who work at large enterprises (companies with at least 1,000 employees) found that 77 percent of large companies would increase security spending, including spending on training, because of the APT phenomenon. Half of those surveyed called APTs a new kind of threat, unique to the security industry. "I was surprised that more people weren't dismissive about them," says Jon Oltsik, an analyst who led the survey for Enterprise Strategy Group.

Persistent little buggers

These three different kinds of attacks are usually lumped into the category of advanced persistent threat:

Hacktivism attacks, such as the releases of confidential information by WikiLeaks, or highly targeted attacks by groups like Anonymous and LulzSec.

Attacks by nation states. Espionage is as old as politics. Governments are widely thought to organize long-term, patient attacks on rivals. Such attacks have traditionally been on other nations' agencies, a kind of cyber James Bond action. Hence the Stuxnet attack that damaged Iran's power grid, notably two of its nuclear reactors. The United States, possibly working with Israel, is thought by many to have been behind the Stuxnet attack (the United States claims Russia did it).

For CSOs, the danger of nation-state attacks appears to be the advantage of being highly targeted and backed by the most patient kind of money. It's fun to sneer at the competence of governments, but look at the alleged exploits of the Chinese. China was accused of compromising Google, was fingered indirectly in the RSA attack, and recently was alleged to have infiltrated more than 760 companies worldwide, including one that provides Internet access to hotels, giving its hackers access to guests' e-mail threads. China denies any such behavior. But one report put China's APT success in 2010 at $500 billion worth of information stolen in the United States alone.

Not all CSOs work at companies that make good targets for cyber espionage, of course, but any CSOs at companies engaged in cutting-edge research or in businesses that matter to a nation's well-being should consider themselves targets.

Attacks by organized crime networks. Organized crime leaders see the money out there in cyberspace. They have the resources to employ top-notch people and give them the time they need to work a good hack.

Of these three, hacktivists seem to be the least likely perpetrators of APTs. "They're advanced and a threat," says Marc Maiffret, CTO at eEye Digital Security in Irvine, Calif. But they aren't trying to hide their actions, which means their attacks aren't persistent.

Some businesses are more likely targets for attacks than others. As noted, firms with defense contracts, financial services firms and companies with important intellectual property, including not-so-visible assets like groundbreaking manufacturing processes, make more lucrative targets than those that don't.

Whoever they are, and whatever their motives, hackers capable of pulling off a successful attack like the ones on Google, RSA Security and Heartland are clearly out there. CSOs need more than just a buzzword to beat them back.

Fight or flight?

Advanced persistent threats are the sort of thing Sun-Tzu would have loved: an attack that happens without its victim knowing. How does a company defend itself against the invisible? "That's the gazillion-dollar question," says Shipley.

The only easy answer: go offline.

Shipley says almost all the simple ways to track network intrusions and anomalies are already pretty well known and available. "We've solved most of the easy stuff," he says. What's left? Strategies like these:

- Do a better job of assessing technology before adopting it.
- Hold technology vendors accountable for introducing vulnerabilities into systems, or introducing products that come with vulnerabilities.
- Make risks clearer to non-technology executives.

Maiffret says that while advanced persistent threats are difficult to stop, some simple precautions can help. He notes that if companies had followed Microsoft's best practices for dealing with file permissions, they wouldn't have needed to worry about Stuxnet. "Just by having good file permissions, you would have mitigated that vulnerability, and Stuxnet would've failed to exploit that [vulnerability]," Maiffret says.

In the wake of Stuxnet, he says, a large bank asked eEye to do a risk assessment to see if it would have to patch a few hundred thousand Windows computers, which would have been very costly. Maiffret says the bank had in fact implemented those permissions properly by following Microsoft's best practice guide.

Oltsik says CSOs need to look at every layer of security infrastructure as well as examine their security policies and employee training practices. "The people who are most prepared are consistent in so many areas," he says.

Whether you think all the talk about APTs is mere noise or a megaphone call, the business side has heard it. Oltsik says that this gives CSOs an opportunity. They can no longer complain that executives don't understand security. "Execs are coming back and saying, 'you need to tell me where we are,'" he says. He advises CSOs to respond with metrics and third-party assessments of their network configurations.

APT might be just a new acronym for a threat that's persisted since before CSO was a title. But in technology, a slight twist to an old idea can be enough to reshape a landscape. It's happened in personal computers, in social networks, in speech recognition, to name just a few. Oltsik says the rise of APT as a buzzword might mean the same shift for CSOs.

"We are on the cusp of major changes," he says. "Security will become more integrated into business processes. CSOs will need to work more closely with CIOs so there is oversight when a company is bringing in mobile applications or new devices. And there's going to be real pressure on security vendors to come up with integrated enterprise end-to-end kind of tools." ■

Michael Fitzgerald is a freelance writer based in Massachusetts. Send feedback to editor Derek Slater at dslater@cxo.com.

APT in Action

Heartland's Kris Herrin talks about the attack that changed his views on data security

BY MARY BRANDEL

In late 2008, a group of hackers successfully broke into the network of Princeton, N.J.-based payment processing giant Heartland Payment Systems. The hackers stole data from more than 100 million credit and debit cards on the company's network that serves the card-processing needs of restaurants, retailers and other merchants.

The hackers spent weeks gathering intelligence on Heartland's networks, systems, corporate structure and employee roles, according to Kris Herrin, the company's chief technology officer. This level of persistence defines the new threat landscape for all businesses today, Herrin says, and dramatically changes how organizations need to think about data security. Security leaders today need to assume their systems and networks are compromised and begin focusing on securing—or getting rid of—the data itself, he says.

We spoke with Herrin recently about the new threat landscape and how the 2008 breach transformed his outlook on data security.

Tell us what tactics hackers used to successfully infiltrate Heartland's systems.
Ukrainian hackers, led by Albert Gonzalez, spent about six months on our corporate network, mapping out who does what in terms of employee roles, the network layout and design, as well as our security defenses. They were essentially gathering intelligence to get from our corporate network to our processing network, which are very different and separate from each other.

Was this a combination of social engineering and technology-based hacking?
The initial breach was through SQL injection, but they also used social mining and data gathering to

figure out, for instance, who the developers were who had access to code and systems.

Would you classify this as an advanced persistent threat (APT)?
As a security guy, I don't like the term APT. I think it misses the point and gets overused quite a bit. So, no—our breach was not an example of APT the way the media uses that term. What's more interesting to me—and what's changed the security landscape—is not how advanced the attack is; it's the persistence that's the important part of attacks today, and that quality was absolutely part of our breach.

We know that the very first breach to our corporate network was December 2007. It was detected at the time, and we believed it was cleaned up, but it wasn't completely. It turned out to be much more persistent than anyone thought. They spent a lot of time avoiding detection and finding new ways to move around laterally and get into information.

It shows that "advanced" is not the concern—it's the resources, time, effort and energy that hackers are willing to spend to try to get to your data. They won't just try a few times, quit and give up. They'll spend months and years mapping information about the network, mining data, studying the personnel database, finding the right person to spearfish. That's the critical part of the threat landscape today.

So to me, APT refers to any hacker that will spend a lot of time, effort and energy finding weaknesses, and once they're in, they'll insert multiple hooks and multiple ways to get back in.

Who is at risk?
Gonzalez broke into hundreds of companies, and some were our customers and merchants. They'll target Joe's Pizzeria with 10 tables if they find the point of sale system is insecure, or they'll put a card skimmer on a gas pump to siphon data. The majority of compromised credit cards comes from small companies, not large. For everyone, APT is now the norm. Attacks will become more persistent, harder to detect and more difficult to get rid of.

> *"When* **hackers have a bag of tools**, *they won't change them for every job they do."*
>
> –KRIS HERRIN, CTO, HEARTLAND PAYMENT SYSTEMS

How do threats from Eastern Europe and the Ukraine differ from those from China?
They're very different kinds of threats, but there are common threads. Both will come up with creative ways to target individuals through social engineering and placing multiple hooks in your environment. But Ukrainian threats—and by this I'm also referring to Eastern Europe and Russia—are more "smash and grab." They're after a specific set of data, and after they get it, they're out. In our case, they were looking for track data [the information encoded on the magnetic strip on the back of a credit card]. They knew how to monetize it, so once they found it, they were finished because that's what they were after.

Reuters

Chinese threats are more geared toward espionage and intelligence-gathering. They're hanging around the network for a long, long time and working to steal intellectual property or economic information—they don't have one thing they're after. They tend to target the defense industry and possibly have more state sponsorship, depending on what you read.

How does APT change how companies should approach data security?
Companies need to start from the premise of, "assume your systems are compromised." Stop trying to keep the bad guys out—assume you're compromised and get rid of the data they're after.

You can replace sensitive data with tokens, encrypted values or other enabling technologies. These approaches will protect against threats not only from APT but also consumerization of IT, people bringing in their own iPhones, data moving to the cloud or employees getting into social media.

I'm not saying to do away with the antivirus, network security, identity and access management systems—those are the minimum standard. But you're kind of saying, "I can't protect all the

iPhones and Androids that can download everything from an app store." Instead, you need to focus your limited resources on ensuring that valuable data is safely handled so you don't have to worry about it being lost.

This also means getting rid of the data you don't need to be handling. Look at your legacy processes and find ways to reduce the scope of the data. Remember when Social Security numbers were used for everything? Now, we have to do the same thing with the rest of the data the business handles. Merchants and call centers should be asking, "Why do I need the full credit card number?" They don't—they just need a reference or a token.

them. All that old logic in the application still works.

This sounds like a big job for the smaller companies that, as you say, are also at risk of APT breaches.

Joe's Pizzeria doesn't care about security; it cares about selling pizza. So we took the concept of "assume you're compromised and stop trying to keep the bad guys out," applied that to merchants and came up with end-to-end encryption, which encrypts data as soon as the card is swiped at the POS terminal. You can take the credit card data away from the merchant so they no longer have to worry about it. And that's a big deal for our merchants. They don't want to worry about

"Joe's Pizzeria doesn't care about security; it cares about selling pizza."

–KRIS HERRIN, CTO, HEARTLAND PAYMENT SYSTEMS

So, the focus needs to move to encryption and key management?

Key management is actually a much harder problem than trying to protect servers and networks. You need to look at your applications and how they use the data so you can protect the data in a way that the application can still use it. For instance, how do you search for something if the data is encrypted? But that's where it's going—finding ways to keep data usable for business processes but taking away the data's value from the bad guys.

Our E3 technology uses a format that encrypts a credit card number so it still looks like a credit card number. We do that for the legacy applications out there so you don't have to rewrite Ukrainian hacker stuff. We now have merchants banging on our doors to get rid of this data.

Lots of people want to do payments through mobile devices. If you encrypt the data as soon as the card is swiped, you don't have to worry about the device at all because the technology ensures it's encrypted before it gets to the device.

Are there new APT security solutions that can also help?

There are lots of good technologies that try to find APT threats and do sandboxing of executables. We use those technologies, but none of it actually solves the problem. The solution is getting rid of the data where it's not needed and taking the data out of scope.

Can you ever fully solve the problem? For some merchants with just credit card processing functions, you can. For more complex process, no. But you can get to a much, much smaller risk profile if you focus on the data.

How can law enforcement agencies around the world help with APT?

They can play a very important role, but there are limitations. If you believe you've had an attack or see threat indicators, plugging into law enforcement is critical—they need this kind of stuff reported to them, and they get federal dollars to help protect us. So the more we educate them on the threats out there, the better.

On the flipside, if they're working on an investigation like a Gonzalez-style case, there are realities having to do with jurisdictions and victim organizations that we've seen. Setting up partnerships with other companies is just as important.

What types of partnerships can be effective?

This is something we took leadership on and that others are focusing on, too. Historically, as payment processors, we all shared the same threat, but we didn't share information on these threats. It was all very siloed because of the legal and competitive implications. But it reached the point where we could either get picked off one by one, or we could come together and work against these threats.

That's why we formed the Payments Processing Information Sharing Council. We've opened the kimono and even shared a sample of the malware that was part of our breach. We can report when we see a certain kind of phishing attempt or share tactics and techniques of how to better defend ourselves from attacks. We also do table-top exercises, where we conduct an attack and see how we'd respond.

We saw in our breach that Gonzalez and crew made changes to the malware as they went along, but they were fairly small changes. There were definitive indicators that did not change. When hackers have a bag of tools, they won't change them for every job they do. So just sharing that is helpful to other companies to know this is the known bad stuff to look for.

Two years in, this is a phenomenal group that shares threat intelligence on a daily basis. Now, when there's an incident, there are people to reach out to, both for help and to see if they're also seeing things. Many other groups—even in the defense industry—are doing the same thing now. Tearing down the walls and barriers is a must. We can't be silenced—the bad guys are talking to each other all day long. ■

Mary Brandel is a freelance writer based in Massachusetts. Send feedback to editor Derek Slater at dslater@cxo.com.

White Paper

Choosing a Cloud Hosting Provider with Confidence

Symantec SSL Certificates Provide a Secure Bridge to Trusted Cloud Hosting Providers

Symantec

Norton SECURED
powered by VeriSign

Click here to download this free white paper.

For more information on Symantec SSL certificates visit www.symantec.com
Or call 1-866-893-6565, option 3.