APTs

New waves of advanced persistent threats are vastly improved and smarter than ever.

ebook

An SC Magazine publication

Sponsored by

APTs

Formerly associated more with nation-state attackers, APTs are now, increasingly, following the money, reports Alan Earls.

Advanced persistent threats (APTs) are not new, nor have they changed much from a purely technical standpoint. Using such tried-and-true methods as social engineering to gain entry to enterprise networks, cybercriminals can easily siphon off identities and other information. That's because these adversaries will go to great lengths to identify weakness within a high-value target.

What does seem to be changing in this particular threat landscape, though, is who is at the controls and what is being targeted. Now, instead of mere disruption – or a hunt for intellectual property goodies – APTs are often putting financial institutions in their sights and simultaneously leveraging the unique security problems of mobile technology.

What's so worrisome about APTs? For one thing, APTs remain challenging to find. They are always stealthy and patient and rarely have an obvious symptom. As the threat and the actors have evolved, the attractiveness of banks and financial transactions as targets has grown – particularly the growing financial transaction volume transmitted via mobile devices. But the picture is by no means entirely bleak. Organizations that pay attention to the APT threat, assisted by more sophisticated security technologies and training, are helping to ensure that no matter how advanced or how persistent, APTs may eventually be less of a threat.

Who's in the cross hairs these days? While no one industry is being targeted, financial organizations are a growing focal point. In fact, attacks on banks are often in the headlines, and attacks on alternate payment companies, such as PayPal in 2014, are also growing.

"Attacks follow money, pure and simple," says Andrew Braunberg, research director at NSS Labs, an independent analyst firm in Austin, Texas.

APT attacks are typically committed by organized criminal groups or federated groups of individual criminals that each add value to the operation. This amounts to work specialization, where some criminals focus on developing exploits, some on creating malware packages and some on data extraction, he explains.

"The hardest part has always been figuring out the clues that point to a real threat versus simply the unexpected behavior of legitimate systems," says Todd Inskeep, the global security assessments vice president, global security services, at Samsung in Charlotte, N.C.

Inskeep, an advisory board member for the RSA Conference who has more than 20 years of experience in information security, including a period with Bank of America, says he learned first-hand the challenges that APTs present. "After details from the Google APT attacks started trickling out and new intrusion detection systems were revealing evidence of something unexpected in various systems, we started looking for APTs," he says.

The biggest challenge with APTs is ambiguity. For instance, is that unexpected occurrence in an activity log something to

OUR EXPERTS: APTs

Andrew Braunberg, research director, NSS Labs

Charles Gaughf, information security manager, (ISC)²

Adam Harder, director of mobile access engineering, Endgame

Todd Inskeep, global security assessments vice president, global security services, Samsung; advisory board member, RSA Conference

John Pescatore, director, emerging security trends, SANS Institute

Michael Versace, global research director, IDC Financial Insights

87%

of the top 100 paid apps for the Apple iOS have been hacked.

–Arxan, "State of Mobile App Security" (Nov. 2014)

Follow the money: Where the attackers go

Like the famous bank robber Willie Sutton, reputed to have justified his choice of careers "because that's where the money is," APT attackers have discovered the obvious: Money doesn't grow on trees but it definitely flows freely across the cyber landscape.

According to a recent mobile apps report issued by Arxan Technologies, a Bethesda, Md.-based provider of anti-hacking products, the financial sector has real concerns to face up to, such as:

- Hacking or malware has been the predominant method of credit card data breaches that occurred from 2005 to 2014
- Most apps have been hacked. Research on top financial apps reveals that 95 percent of Android apps have been hacked and 70 percent of iOS apps have been hacked

The research also reveals a growing trend of financial app hacking: Android app hacking increased from 76 percent of apps to 95 percent, from 2013 to 2014 while iOS app hacking increased from 36 percent to 70 percent over the same period.

worry about or just something no one noticed before? Is it something happening on just one device or several? Is the code new or something that's been seen before? For a CISO or anyone else trying to detect and thwart, answers are hard to come by, he explains.

But, like others before and since, he had to struggle to find those answers and select the best response. Frequently, the process starts with reverse engineering to try to find what an APT does. But beyond that there are crucial decisions that need to be made about whether it makes sense to make a change in configurations that could better protect systems, but might also alert the attackers to try another attack approach. Similarly, he notes, APT victims need to weigh whether to bring in the help of outsiders or people from law enforcement.

Todd Inskeep, global security assessments vice president, global security services, Samsung

Furthermore, given the tenuousness involved in diagnosing an APT, security decision-makers have to wrestle with whether – or how – to assign blame. "There are lots of pointers, but without someone really taking responsibility [for an attack], it's difficult to make a case you could prosecute," Inskeep says.

While APTs were once mostly the domain of nation-states, there are plenty of new players – such as the recently discovered Carbanak group, which has used a widespread APT to siphon millions of dollars from banks around the globe. "Approaches through spear-phishing and malware will continue, but targeted and broad attacks on equipment will [increasingly] provide attackers access to systems they didn't know existed," says Inskeep.

He is not alone in seeing a new kind of threat. "I would say the clear trend is toward a lot more attack paths; attacking infrastructure, hard drives and SSL certification authorities rather than just the standard missing patches in Windows machines," says John Pescatore, director, emerging security trends, at SANS Institute, a security training organization based in Bethesda, Md.

At issue, ultimately, is that IT organizations are largely built on a range of fairly standard components. When attackers master one organization's infrastructure, other organiza-

97%

of the top 100 paid apps for the Android OS have been hacked.

–Arxan, "State of Mobile App Security" (Nov. 2014)

tions suddenly become just as vulnerable. On the plus side, Pescatore says many organizations seem to have gotten better with traditional housekeeping issues, like patching, but, with phishing so effective, there is an enormous potential field for APTs to exploit. If, as now appears to be a possibility, attackers may even have access to most hard drives,

> "...the clear trend is toward a lot more attack paths..."
>
> *– John Pescatore, director, emerging security trends, SANS Institute*

then structures once imagined to be safe, like secure "wallets" for storing passwords, may turn out to be highly vulnerable, he adds.

Perversely, Pescatore notes, APTs now sometimes use encryption to thwart analysis and detection. As a consequence, given the fact that so few organization use encryption broadly, APT hunters have taken to looking for anything that is encrypted on the assumption that it could be part of an APT, he says.

Mobile security

The APT threat is further complicated by concerns about the potential vulnerability of mobile devices. In recent years, mobile banking and financial services have flourished globally, particularly in emerging economies where large populations have never previously had a bank account, notes Adam Harder, director of mobile access engineering at Endgame, an Arlington, Va.-based security intelligence company. For many of those users in the developing world, a cash balance is maintained with their phone service which functions much like money in a bank.

Andrew Braunberg, research director, NSS Labs

In the U.S., although mobile banking still represents but a fraction of retail banking and retail sales, there's still plenty of money moving around. ApplePay and the upcoming re-launch of Google Wallet, for example, are emerging while a range of other organizations – such as Starbucks, Amazon and Uber – see consumers channeling billions of dollars via devices.

Given the dramatic growth in transactions moving through mobile devices, it's safe to assume APT organizations are eyeing them as potential attack vectors. However, Braunberg at NSS Labs says mobile devices are not inherently less secure than traditional computing devices – particularly as application hardening and the creation of enterprise-class security features gets more attention.

Indeed, many in the security field say mobility is actually remarkably safe. Having come to maturity in the age of the hacker, mobile devices have more built-in security than traditional desktop or laptop computers and are far harder to exploit. For instance, according to Harder, from a user perspective, mobile banking and credit actually offers a more secure form of payment than a physical credit card. Credit card numbers can be stolen from end-users via hardware skimmers and phone and email scams (social engineering), he explains. And credit card numbers can be stolen en masse from merchants and credit processors. By contrast, mobile banking actually adds a layer of security by allowing the credit card processor to communicate directly with the phone, requiring a PIN or password and generating one-time credit card numbers.

Still, if you were an attacker, could you resist that stream of commerce just a few clicks away? Indeed, from an attacker's perspective, Harder admits, mobile applications offer the irresistible potential of a direct pipeline to someone's bank and credit ac-

80%

of the most popular free Android apps have been hacked.

–Arxan, "State of Mobile App Security" (Nov. 2014)

counts, ripe for bogus charges or transfer to the attacker's account.

And, end-users in the developed world – many with significant funds on tap – are growing more comfortable connecting a credit account to their individual apps. "This means the attack space is increasing in two dimensions," says Harder. "There are more phones running apps that can be attacked to steal money and there are more apps running on any given phone."

The issues don't stop there. Loyalty programs from retail stores, airlines and hotels all store credit card information. "Just a few weeks ago, the Marriott mobile app was found to have made unauthenticated calls that could allow an attacker to steal member credit card information," says Harder.

So, the overall vulnerability picture is mixed, according to Pescatore. And drilling down a bit, while IoS is a much tougher nut to crack than Windows, Android is less so. And the recent revelation by Dutch SIM card maker Gemalto that the American NSA and the UK's Government Communications Headquarters (GCHQ) may have compromised the security of its products, should serve as a wake-up call to the mobile world, he says.

A big positive, however, is that users of mobile devices are not generally expecting their friends to send them executable files – a common APT attack vector with traditional computing devices, Pescatore explains. What's more, links can't really download software the same way. On an IoS device, software needs to come through Mac App Store, while Android users usually access downloads through Google Play.

Putting trust back in the system

While a return to a pre-APT Eden may be impossible, there are things that organizations and the industry as a whole can do to rebuild a more generally trustworthy environment.

At least one analyst, Michael Versace, global research director at IDC Financial Insights, Framingham, Mass., thinks he knows how. "I have been writing about the need to secure mobile platforms by helping developers to build secure mobility – for the enterprise users and for end customers." Versace's concept is to deliver secure mobility through a platform approach that sees the challenge in infrastructure terms.

Already embraced by some vendors, Versace says the approach can provide all the things developers need to make applications resistant to APTs. It would have a whole set of functions – everything from being able to access the state of mobile device (showing whether it is infected or not), as well as the apps and whether the operating system has been changed in any way. "It would look to see if there is an anomaly in how the software resides that could be an indication of malware or an APT," he explains.

APT fight: Starts with fundamentals

There is no magic formula that can provide protection against advanced persistent threats (APTs), notes, Andrew Braunberg, research director at NSS Labs, an independent analyst firm in Austin, Texas. What can help, however, he says, is to start with security fundamentals, including:

- Keep threat surface area to a minimum – for example, restricting the number and variety of mobile devices allowed on a network.
- Review current incident response processes – do they permit rapid answers to "was that important"?
- Consider a breach detection and continuous forensic analytic product for post-incident analysis.
- Incorporate digital signatures for email
- Keep anti-spam policies up to date and applicable to current traffic.

75%

of the most popular free iOS apps have been hacked

–Arxan, "State of Mobile App Security" (Nov. 2014)

ATP (Adequately Trained Personnel): Fighting APTs

Creating an arc from problem to solution can be a challenge in any business situation. And when it comes to advanced persistent threats (APTs) the amorphous and changeable nature of the problem creates even more difficulties.

However, according to Charles Gaughf, information security manager of (ISC)², a company in Clearwater, FL that provides IT skill certification services, an invaluable tool in the APT fight is training. Specifically, he notes, the best defense against APTs is to produce what he calls ATP (Adequately Trained Personnel). "The majority of recent, highly-publicized security breaches originated from attackers using simple social engineering tactics," says Gaughf. Those tactics will continue to work until staff learns how to recognize phishing attacks and acquires the instinct to alert security to suspicious activity. And, he says, it takes more than annual security awareness training, it requires an effort to build a strong, security-minded culture. "Communication should not just include tips on corporate security, but also how end-users can protect themselves, their families and their technology at home," he says.

Encouraging what Gaughf calls continuous security awareness, as opposed to something employees only practice at work, can help raise the level of security awareness for end-users in their everyday lives. And that can make a difference in uncovering and fighting APTs

Gaughf says there are low-hanging fruit concepts that can be easily implemented and contribute to establishing a culture of security aware end-users. Examples include sending a simple advisory related to security issues that are relevant to staff, such as IRS phishing scams or examples of emails others have flagged as phishing attempts. "This kind of effort should empower end-users not to fear technology, but rather to become hyper-aware of the risks and the types of attacks that malicious users use to bypass security and gain access to systems," he says.

"It would also have the capability to secure the physical device at a point where the risk and threat might be neutralized or mitigated," says Versace. "If there is a piece of malware, the device can then be secured such that those risks would be minimized for those interacting."

That, he emphasizes, would create a basis for trust.

In the meantime, though, many experts say much more can be done to tame the APT onslaught. Standing on the front lines, Inskeep, for instance, says simply having a plan can help. One needs to be ready to deal with every aspect of APTs – from thinking about how to react, both publicly and privately, to what critical business information on would most want to prevent APTs from accessing, he says. That means engaging with business decision-makers and other key stakeholders, such as legal advisers.

Planning becomes more actionable with practice. That could mean staging a war game to test out how you and your organization would respond to an APT. "Think about your reactions," says Versace. "Do you call the police, collect evidence, follow the bad guys or just rebuild the systems and ignore it?"

These are all potentially legitimate reactions...and they might all be wrong, he says. In fact, though, at least in a practice situation, there is no right or wrong approach. Every option needs to be considered.

And, guess what? Inskeep says it's a good idea to go right from testing an APT response to implementation because "there's a good chance you are already hosting an APT without knowing it."

"My best practice is to assume your systems have been hacked and to start managing information risk through system architecture,

720

major data breaches in the U.S. during 2014.

– Identity Theft Resource Center

policy, technology and personnel training," advises Inskeep. Specifically, he notes, separating critical business operations from less critical systems and managing the most important business information can help make you more attack-resistant. "Whatever separates a company from its competition and potential competitors, that's the information that needs to be protected," he says

The next steps involve looking at ways to share attack information, indicators and warnings with others. "Set up a security operations center capability that's sized to support realistic activity levels in your organization," he says. It can be easy to set up a large threat intelligence-based security operations center with lots of people and round-the-clock activity. But it's harder to make that activity pay off in reduced threats and better risk management. So, be prepared to work with fewer resources and plan to contribute to the organizations you work with on threat intelligence.

Michael Versace, global research director, IDC Financial Insights

For any mobile payment, credit or deposit system, the phone operating system must provide a base level of security relative to APTs, says Endgame's Harder. If the operating system is compromised, then an attacker can access the private data of any application – and network connections to the banking service can be manipulated by a man-in-the-middle attack.

"App makers that maintain banking apps must take responsibility for securing their customers' data. If possible, nothing sensitive should be stored on the device at all," Harder says. "Credit card or bank information can be requested from the cloud when needed." Furthermore, any data that must be stored locally on the phone should be encrypted and inside the application itself, and access to sensitive data should be protected via a PIN or Apple Touch ID.

So, in the final analysis, while APTs are clearly a growing danger, attackers are neither invincible nor all knowing. As Inskeep explains, every organization should take a look at its own threat profile and risk tolerance to identify the right technologies, processes and training needed to manage the APT risk for that organization. They need to assess the effectiveness of what they have and determine where they need to better manage risk, he says. Furthermore, last year's introduction of the NIST Cybersecurity Framework [Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013] provided companies with a great starting point to consider a more comprehensive view of security maturity and risk management.

In reality, notes Braunberg, attacks do not need to be advanced or persistent to be effective. Malware, spam, phishing and social engineering continue to be common threats. Social engineering, in particular, is exceptionally dangerous and without malicious attachments (either an attached file or URL), an email can more easily bypass traditional email security tools, yet yield rich content if successful.

Therefore, APTs can and should be considered within a spectrum of threats. And, fortunately, while finding and stopping an APT can be challenging, general improvements in security practices can be a big step toward making APTs less of a problem. ■

For more information about ebooks from SC Magazine, *please contact Illena Armstrong, VP, editorial, at illena.armstrong@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, sales, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

56m

cards were exposed during more than five months of attack on Home Depot's network.

sponsor

HP is a leading provider of enterprise security solutions designed to mitigate risk and defend against today's most advanced threats. With market-leading products, services and innovative research, HP Enterprise Security Products enables organizations to take a proactive approach to security, integrating information correlation, application analysis and network-level defense.

For more information, visit www.hpenterprisesecurity.com.

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
ASSOCIATE EDITOR Teri Robinson
teri.robinson@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
PRODUCTION MANAGER Krassi Varbanov
krassi.varbanov@haymarketmedia.com

SALES
VP, SALES David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
REGION SALES DIRECTOR Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*

When it comes to advanced cyber threats, every second matters

The average threat goes undetected for 229 days. The HP TippingPoint Advanced Threat Appliance can slash that to less than one day. By detonating the malware in a safe, sandbox environment and analyzing the threat, we can map its attack plan and block communication to the command and control server. That neutralizes patient zero, the first infected system, and stops lateral movement across the organization to prevent future attacks. You can't let your guard down for a minute, so TippingPoint makes every second matter to protect your business.

Learn more at hp.com/go/ATA

Make it matter.

003:55:18:122 \ Malware Detected \ Name: Trojan horse