

security

# Attack of the Bots

*The emergence of botnets and other off-the-shelf cyber-crime tools has transformed hacking into a point-and-click process. To fight these 'advanced persistent threats' Wall Street firms including Raymond James Financial are adopting new detection technologies. By Anne Rawland Gabriel*

**H**ACKING THROUGH A FINANCIAL firm's multilayered defenses once required considerable effort. But now it takes just a few mouse clicks. By exploiting gray areas in the legal code, yesterday's attention-seeking hackers have morphed into today's capital-motivated entrepreneurs.

These "black hat" businesses have reshaped the threat landscape in two critical ways. First, they create and sell malware tool kits, making the process of unleashing potent attacks as simple as choosing from a menu of options. And second, they build and operate sophisticated distribution systems called botnets, permitting cyber criminals to launch attacks with such speed and stealth that it's impossible to warn users in advance.

According to security experts, today's preferred infiltration method is via a single bot (a tiny automated software program). "These bots send a signal to a C&C [command-and-control] server," explains veteran networking security specialist John Pescatore, who is a distinguished analyst with Gartner. "While they can perform other functions, their primary purpose is acting as a conduit for the malware that subsequently carries out an attack."

Such bots silently hitch a ride on a user's computer during visits to legitimate, but breeched, websites. And it's nearly impossible to detect which websites are affected, according to

experts. "It's not about visiting porn or other shady websites anymore," stresses Pescatore. Bots and botnets are now so widespread that "virtually any website" can be infected, he says.

## Fortifying the Defenses

This toxic combination of botnet ubiquity and the simplicity of unleashing an attack makes every financial firm a top target — which is exactly why Raymond James Financial began considering in the latter half of 2009 enhancements to its existing malware defenses. "Malware attacks had become almost completely for-profit or to obtain intellectual property," affirms Todd Ferguson, enterprise information security architect for Raymond James. "So we started looking at the emerging category of advanced persistent threat (APT)-detection vendors to further fortify our security posture."

The St. Petersburg, Fla.-based financial services firm quickly rejected several solutions as insufficient. "Some seemed more like whitelist/blacklist solutions," comments Ferguson. "We needed something more robust that could handle dynamic threat environments and minimize the noise for us to wade through."

This left two contenders, according to Ferguson, who says Raymond James took a novel approach to assess them. "We evaluated them side by side with our existing solutions," Ferguson explains. "We wanted to see where there was overlap and where we might need more visibility. In addition, we wanted to identify whether there were opportunities within our existing tools to improve their protective posture."

To accomplish its evaluation goals, Raymond James conducted a 13-week bake-off, using production traffic, beginning in April 2010, Ferguson reports. During this time, existing and prospective solutions ran head-to-head, which allowed Raymond James to see which ones best filled security gaps. "In other words, from an operating expense perspective, we could determine which tool — existing or prospective — would give us the most bang for the buck," Ferguson says.

Upon analyzing the trial's findings, Raymond James decided that adding Failsafe from Atlanta-based Damballa to its existing mix provided clear advantages. "Failsafe gave us greater visi-



## The Changing IT Security Paradigm

**W**hereas security solutions were once thought of as prevention systems, today's advanced threat landscape requires a mind-set shift and a new focus on detection, according to IT security experts, who point out that chances are good that your firm already is affected.

In fact, Gartner estimates a minimum of 4 percent to 8 percent of the computers on most enterprise networks could contain at least one bot that is actively phoning home. For companies with business-to-consumer relationships, the analyst firm says, the numbers can be higher since consumers' computers are estimated to be contaminated at a rate of about 25 percent.

Gunter Ollmann, research VP for Damballa, a solution provider to "technology elite customers" with as many as

"30 to 50 layers of security," concurs. "We regularly see 3 to 7 percent of all assets not only compromised but actively communicating with criminal operators," he reports. "Within the ISP marketplace, 20 to 24 percent are actively under control."

Given today's realities, security infrastructures are evolving to include detection and mitigation alongside traditional prevention. "We're seeing a shift away from highly paid rapid-response teams to technology solutions that give help desks the tools for managing incidents and the workflows to remediate affected systems," Ollmann explains. "With the right solutions, the tools can automate and drive the response."

In addition, financial firms should consider compliance implications, advises Gartner distinguished analyst John Pescatore. "Think through all of the

processes you'll need, beyond physical threat removal," he emphasizes. "For a disclosure event, incident response procedures and forensics are critical."

To choose the right solution, Pescatore recommends considering reputation-based and binary-based advanced persistent threat (APT) solutions. "Reputation-based systems compare outgoing traffic to known malicious and compromised sites," he explains. "Binary-based solutions examine incoming executable files and perform an on-the-fly analysis to identify which are dangerous."

Ideally, financial firms will adopt a solution, or a combination of solutions, that provides both reputation- and binary-based detection, Pescatore says. "For the best security posture, I always recommend both," he insists. —A.R.G.

bility into certain areas. Plus, it provided accurate and actionable information as well as having a low false-positive rate," according to Ferguson. In addition to the Damballa solution's detection capabilities, the vendor was "very receptive to candid feedback and has already incorporated some of it into their production product," he adds.

### A Shifting Response Paradigm

Having already tested Damballa in production, the process of deploying the solution was simply a matter of acquisition and installation, according to Ferguson. However, updating security policies and procedures to incorporate Damballa was another matter.

"It required a paradigm shift from typical antivirus response," Ferguson says. With Damballa, he explains, an alert necessitates investigating whether the flagged traffic is actually malicious or just benign.

Consequently, Raymond James overhauled its operational response. "We rewrote our entire response procedure," reports Ferguson, adding, "We not only accommodated Damballa but also addressed lessons learned during the bake-off with respect to our existing systems."

Perhaps most significant, Raymond James no longer just neutralizes threats — it now shares data acquired during the remediation process with the appropriate threat-detection vendors. "By sharing data with our vendors we can challenge them to improve their solutions," Ferguson asserts. "Ultimately, this enhances our defensive posture as our vendors introduce

new features and functions."

In addition, the firm also updated various existing systems "to provide additional benefits and improve our protective stance," Ferguson adds.

Since completing the transformation in September 2010, Raymond James' security posture has palpably improved, Ferguson says. "We're absolutely addressing threats at an accelerated pace," he contends. "This is because the data we receive from Damballa generally provides enough evidence for us to take action on first look."

With less work required to locate and research potential malicious activities, the efficiency of Raymond James' security operations also has improved. "With malware versions changing so quickly, today's threats are a moving target," Ferguson says. "But our visibility into those threats is vastly better than before; so we're definitely more productive."

But solutions like Damballa are hardly substitutes for existing deterrent layers, emphasizes Ferguson. "Investing in this new detection technology isn't a replacement," he stresses. "It has given us another security component because Damballa looks at threats from a communication perspective, which is different than traditional protection solutions."

Going forward, Ferguson expects to continue evolving Raymond James' security infrastructure. "As an organization we don't just install something and quit," he says. "We evaluate new tools and solutions on an ongoing basis. Given the fluid threat landscape, I don't think that will ever stop." ■



www.damballa.com  
(404) 961-7400