Feature

Security Vendors: Trend-Setters, or Trend Followers?

06 October 2011
Danny Bradbury

How far ahead of the curve – or behind it – are vendors when it comes to identifying security trends? Danny Bradbury finds out that the curve may not matter at all

Deep in a grim former Soviet city somewhere, with a stack of copied credit cards on one side of his desk, some enterprising young blackhat 'researcher' is working on something that will change the face of security. Not just another zero-day malware attack, but something game changing that 'ups the ante' with an entirely new technique. What it is, we don't know. But when it hits, it will make headlines.

Who's going to stop him? You would hope that security vendors, staffed as they are with experts in their field, would be one step ahead of him. But is that true? Brian Bourne, founder of the Toronto-based security conference SecTOR, doesn't think so.

Security vendors are far too reactive, Bourne argues. "You're only worthwhile if your product reacts to what's on the street, and then you need a research team just to keep up with what's going on", he says. "To do any forward thinking, you need your research team to invent attacks."

Staying Within A Comfort Zone

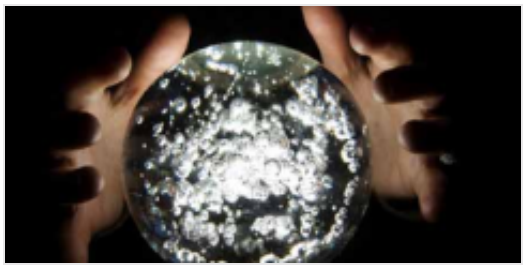
Rather than winning kudos among your peers, focusing on attacks that might happen one day reduces your overall return on investment, Bourne argues. Moreover, finding ways to break the internet can create a PR problem, he warns.

Dr Prescott Winter agrees. Formerly at the National Security Agency, Winter knows a thing or two about security – he has seen it from both sides of the fence. Following his public sector career, he became CTO for the public sector at ArcSight, a company that provides security and compliance products and services. One of the problems is that vendors tend not to move outside their core areas of interest, leading to a fragmented effort, he says.

"Instead of working together to create a common operational picture as we described it in the defense and intelligence community, they are

"It's been a long time since I saw a vendor report that was either useful or not supporting their own product"

ArcSight's Winter says one of the problems within the vendor community is that they tend to remain within their core areas of interest, leading to fragmented views on the entire security landscape



Many security researchers employed by vendors are adept at foreseeing the next generation of attack techniques

Share

More services

Related Stories

Comment: It's Time to Take APTs Seriously
Ross Brewer of LogRhythm explores the danger posed by advanced persistent threats, the rash of high-profile data breaches that have been making headlines this year, and the steps organizations should be taking to protect IT assets

Please Feed the Bear: The Growing Russian Infosec Market
The Russian information security market is thriving, fueled by a rise in cybercrime. Some foreign security firms, however, have found it difficult to break into the market. Fred Donovan explains why

Cashing in on Security Training
At long last, a cybersecurity career field has

maintaining separate pictures where they should be integrating", Winter worries.

> Brian Bourne, founder, SecTor Conference

This is why many of the vendor reports that come out focus on specific areas. Anti-spam vendors issue histrionic press releases fretting that China has exceeded the US for spam this month. Anti-malware vendors urgently report that one botnet has trumped another in terms of infection vectors. Who cares? "It's been a long time since I saw a vendor report that was either useful or not supporting their own product", Bourne complains.

New Dog, Same Tricks

John Stock, senior security consultant at web vulnerability scanning firm Outpost24, argues that there's very little new under the sun. Modern SQL injection attacks, for example, are simply rehashed versions of attacks that appeared when websites first became interactive.

"New generations of attacks can be deemed to be such things as Stuxnet, which attacks SCADA systems, but such attacks are very targeted and not generally seen 'in the wild'", he says. "This therefore makes it difficult for vendors to anticipate new generations of attacks, as so much time has to be spent responding to those in existence already, or working on ways to fix/detect new ways of doing old tricks."

emerged. The (ISC)² US Government Advisory Board Executive Writers Bureau examines where employment opportunities lie and how much you can expect to be paid in this very important sector

Researching the Security Researchers

The security industry doesn't have it easy. For every virus it detects and prevents, several new ones are being designed for maximum impact and damage. Information security researchers are up against a deluge of malware writers. Wendy M. Grossman reports on how they keep up

Top 5 Stories

1. Private Facebook messages on Timeline? The social network says no

2. Anonymous #OpVendetta set for 5th November

3. Europe says ICANN's proposals are illegal

4. Identity theft on the rise as only 5% of mobile devices are physically protected

5. White House targetted by spear-phishing attack

Perhaps that is part of the problem: all of the interesting stuff is happening at a state level, where state actors or their affiliates craft independent attacks to hit specific targets. Stuxnet was an orchestrated attack that required simulation servers, specialist equipment, and months of manpower. It isn't so much a new attack as a series of existing techniques, painstakingly and methodologically applied. Anti-Stuxnet protection isn't going to show up in the next edition of Norton Anti-Virus.

But does this mean that vendor research really all goes into the kind of PR fodder that bores journalists to tears? That's unfair, says Catalin Cosoi, head of the BitDefender Online Threats Lab. "Based on past experience, vendors can estimate what services will be targeted next and by which threats", he says, adding that BitDefender anticipated a boom in social media scams as the phenomenon grew online. "Indeed, a hoard of fake apps started to trick users into installing them under various pretences." The firm also predicted Android malware.

> **"I've seen situations where product teams won't even allow the security team to test their products!"**
>
> Chris Eng, Veracode

"The next step is for researchers to delve into the intricacies of the platform/system and identify possible vulnerabilities. Most of the time, security researchers are able to predict what tricks scammers could use", Cosoi says.

ESET's chief research officer, Juraq Malcho, points out that companies like his program their software to be proactive rather than reactive when recognizing threats. Moving from signature-based attacks to heuristic and behavioral analysis is one example of how vendor research has progressed. "We also actively monitor several botnets so that we see where the attacker is trying to move. This helps us to be prepared when new features and techniques are implemented in new malware variants", he says.

Making Positive Contributions

Condemning vendors roundly for myopia does seem a little harsh. Many of them are involved in real operations that have dramatic results, even if they're not discovering the next big attack vector.

Microsoft, for example, worked with academic and law enforcement partners to take down the Rustock botnet last year. Before that, it orchestrated a similar action against the Waledec network. Malware protection company FireEye, which also worked with Microsoft on the Rustock takedown, was instrumental in killing Mega-D. These actions undoubtedly saved internet users' data.

Others produce groundbreaking reports on specific exploits and advanced persistent threats. Vendors issued extensive technical reports on Conficker when it appeared. McAfee heavily documented what it called Operation Aurora, the attack on Google and tens of other high-tech firms, when it first came to light in late 2009.

Where companies make significant inroads, they tend to stretch across multiple product categories, commentators suggest. For example, security researcher Dan Kaminsky suddenly discovered in 2008 that the internet was broken thanks to a fundamental flaw in

> **"One big customer in the US government told me, 'we have bought a lot of your stuff but**

DNS. The flaw could have spelled disaster.

Kaminsky gave up six months of his life pulling together a huge consortium of stakeholders in secret to fix it. They didn't pay him for the privilege (although he was working for security consulting firm IOActive at the time). Kaminsky published the details, and a fix, and the world breathed again. Many of the stakeholders were DNS vendors, who kept quiet and diligently worked on a solution until it was solved.

we don't think we're getting any traction' "

Prescott Winter, ArcSight

Bridging the Gaps

While vendors focus on operational investigation, who is plugging the gap in terms of tactical and strategic research? Academics spring to mind, because they are not driven by commercial considerations.

However, this also makes it difficult to connect academic research to commercial products. Bridging the gap between theoretical and applied research can be tricky. Nevertheless, there is some excellent investigation happening. For example, the Citizen Lab, an interdisciplinary laboratory based at the University of Toronto's Munk School of Global Affairs, participated in research that led to the uncovering of the Ghost Net cyber espionage ring, with servers located mainly in China.

And we also see the occasional link between more abstract research and commercial activities. In the past, for example, senior researchers at Symantec have conducted psychological and social studies on blackhats to try and understand what makes them tick.

Perhaps the problem lies at a more fundamental level. Chris Eng, research VP at Veracode, argues that there is a worrying internal disconnect at many security vendors. Their researchers focus on tracking the latest botnets or deconstructing malware, and they are often woefully removed from development teams.

"The security experts rarely control the types of testing and the extent of testing required before a product ships. They may be asked for input at certain stages of the secure development lifecycle (such as threat modeling, or design review) but they are not driving the process", Eng says. "I've seen situations where product teams won't even allow the security team to test their products!"

The upshot? Seventy-two percent of security products and services analyzed in the Veracode 'State of Software Security' report were deemed unacceptable, which is far above the cross-sector average. This indicates that while vendors may be adept at pushing out spam and malware statistics, many of them could do a better job keeping their own house in order.

"We actively monitor several botnets so that we see where the attacker is trying to move. This helps us to be prepared when new features and techniques are implemented in new malware variants"

Juraq Malcho, ESET

A Bit of Personal Responsibility

But it isn't just vendors who need to get their act together. ArcSight's Winter points an accusatory finger at customers, too. "The customers aren't putting in place the protective tools and processes that they need", he warns. "They're relying on technology, rather than process and technique."

Enterprises are failing to identify their most important assets, he says. That means that they can't establish technical frameworks for security, leaving them rudderless when it comes to security. "One big customer in the US government told me, 'we have bought a lot of your stuff but we don't think we're getting any traction'", Winter concludes. "I get worried about that."

Vendors may be largely reactive, but that's the nature of the market. And in any case, throwing their technology at a solution won't be enough to solve your security problems. It takes some insight and organization on the part of the customer, too. And isn't it more empowering to take responsibility for our own actions?

This article is featured in:
Application Security • Cloud Computing • Compliance and Policy • Data Loss • Encryption • Identity and Access Management • Industry News • Internet and Network Security • IT Forensics • Malware and Hardware Security • Wireless and Mobile Security

Comment on this article

You must be registered and logged in to leave a comment about this article.


Reed Exhibitions