NETWORKWORLD

January 26, 2012

6 Security Companies to Watch

Young companies' offerings range from content delivery networks to securing BYOD to multi-factor authentication

By Tim Greene

This group of security companies includes several that want to capitalize on technology ideas that were originally devised to serve communities of special interest but could now take on a wider cybersecurity role. Fixmo, for example, has its roots in the National Security Agency where its mobile security makes it possible to run critical applications in sandboxes that are insulated from the rest of the machine, making them less likely to fall victim to malware that might have infected the device.

Or Emerging Threats Pro, which started off as an open source intrusion detection project that needed better-quality assurance to make the leap to widespread use in businesses and as an element of other security products.

And as is often the case with young companies, they form around individuals whose creative spark and energy bring new products to life. Sticking with Emerging Threats Pro, its founder, Matt Jonkman, is also president of the Open Information Security Foundation (OISF), which is working on the Suricata intrusion detection engine on which the commercial venture is based.

Also in this crop of companies to watch, Kenneth Weiss, the daddy of two-factor SecurID authentication, is hoping to make another winner with Universal Secure Registry's three-plus factor authentication. And Matthew and Prince Lee Holloway, both alumni of open source anti-spam Project Honeypot, are continuing their efforts to block junk Internet traffic with their content delivery network, CloudFlare.

Cisco Fellow Patrick Peterson is behind Agari, an email security company based on work Peterson started at IronPort before Cisco bought it. Still a Cisco fellow, he spends most of his time on the new venture.

Here are brief descriptions of a half-dozen security companies to watch, what they can do for enterprises and why they are worth keeping an eye on.

Agari

Headquarters: Palo Alto, Calif.
Founded: 2009, as Authentication Networks
Funding: $2.5 million Series A funding from Alloy Ventures with participation from Battery Ventures, First Round Capital and Greylock Partners
Leader: Cisco Fellow Patrick Peterson
Fun fact: The idea for Agari came out of research being done by IronPort when Cisco bought the company. Also, Agari means "to win" in Japanese.

Why we're following it: This email security service will block fake emails, a valuable means for cutting down on successful phishing attacks, but the company gets a leg up because it has support for its portal from AOL,

Google, Microsoft and Yahoo, which will be put in place for their customers. Millions of customers will be using it without knowing it.

Key to the service is its accuracy in nailing malicious email without blocking legitimate messages, which company founder Patrick Peterson estimates at one false positive per million blocked messages.

The service can block emails being spoofed under the domain names of legitimate businesses, but also notifies businesses when their domain names are being hijacked to send phishing messages and emails with malicious attachments.

It's worthy of note because it plans to develop support for enterprise-grade email platforms such as Microsoft Exchange. And the company is working to expand support for its filtering to ISPs and telecom carriers in Europe to block the source of more malicious emails.

Success relies on cooperation of major service providers, and Agari has secured that broadly in the U.S. and is seeking it out in other regions. It is also being offered to the financial services industry via the financial services information sharing and analysis center (FS-ISAC), and the Financial Services Roundtable. Information about URLs that are sending illegitimate emails can be sent to takedown services, making a contribution to cleaning up the Internet in general.

Given its leadership, current industry support, road map and financial backing, Agari can be looked to as a means to help better control email-borne threats.

CloudFlare

Headquarters: San Francisco
Founded: 2010
Funding: $22.1 million from New Enterprise Associates, Pelion Venture Partners and Venrock
Leaders: Its three founders are CEO Matthew Prince and Lead Engineer Lee Holloway (both veterans of Project Honeypot), and Customer Experience executive Michelle Zatlyn.
Fun fact: The company started as a Harvard Business School project, and when its founders graduated they moved via U-Haul cross-country to San Francisco.

Why we're following it: There are lots of content-delivery networks, but this one offers a significant number of services free, weeding out bad traffic to websites, mitigating DDoS attacks and in the process cutting load times, on average, in half.

Preparation to use the service requires a simple change to customers' DNS settings to direct traffic through CloudFlare's network. No hardware, no software.

The company stores customers' static Web page content in its 13 nodes worldwide so it's closer to requesters and lowers latency. The service can store a limited version of Web pages that it can continue to serve from CloudFlare nodes should a customer's Web servers fail.

The company claims its filtering of bad requests can reduce the amount of traffic Web servers handle by 65%, making better use of Internet bandwidth.

Part of what's attractive about CloudFlare is that the founders come at CDN after it has already been well defined as a service network category, but they have the luxury of starting fresh with hardware and custom software that optimizes what they want to do.

Toss in that the founders have a demonstrated passion for eliminating spam and improving Web performance as shown by their participation in Project Honeypot, which tracks the IP addresses used to harvest email

addresses that are then spammed. And they've managed to attract the attention of respected venture firms who have contributed more than $20 million.

Given all that, it's worth keeping an eye on CloudFlare to see what it comes up with in its planned enterprise version that was supposed to launch at the end of last quarter, but didn't. Nevertheless, when it does appear, it will be worth a look.

CO3 Systems

Headquarters: Cambridge, Mass.
Founded: 2010
Funding: Fairhaven Capital, amount undisclosed
Leader: CEO John Bruce
Fun fact: The actual founder is shrouded in mystery, partly because he still works for a firm that had a need for the type of service CO3 offers due to repeated breaches, and he doesn't want to bring all that up again publicly. The company name is based on its three goals, all of which start with the letters "C-O": contain, control and comply.

Why we're following it: CO3 fills an ever-increasing need: how to respond quickly to all the legal reporting requirements that come into play after a business suffers a data loss.

The company offers software as a service that generates an action list of what businesses have to do to meet those requirements, drawing on its constantly updated database of what 46 states, three commonwealths and 14 federal agencies demand.

When customers suffer losses, they enter the nature of the breach into the service's Web portal, and the portal produces a list of what agencies need to be notified, how soon and the penalties if the deadlines aren't met. It also details how to contact the pertinent parties and the actual language of legislation and regulations that apply.

The alternative is to manually piece together the same information and map it to a spreadsheet, something that CO3 says is virtually impossible to do while also hitting all the deadlines; there just isn't enough time.

Given the trauma of having to make a public disclosure about a data loss, this service can get organizations quickly on track to do the requisite reporting, meeting their obligations and avoiding fines.

Breaches became commonplace and high-profile in 2011, and they are now viewed more as inevitabilities than they are as something that can be avoided. CO3 offers a service that could help businesses do the right thing in the eyes of the law. It bears watching to see what customers who fall victim and wind up having to use the service have to say about it.

Emerging Threats Pro

Headquarters: Lafayette, Ind.
Founded: 2010
Funding: Private
Leader: CEO Matt Jonkman, also president of the Open Information Security Foundation (OISF)
Fun fact: Suricata, the IDS engine developed via OISF and that underlies Emerging Threats, is funded by the Department of Homeland Security.

Why we're following it: Intrusion detection is a must-have in any layered network defense, and Emerging Threats Pro is weaving its way into the fabric of open source intrusion detection software, with the company's CEO Matt Jonkman as the driving force.

The IDS is based on the open source Suricata engine. The open source ruleset that goes along with Suricata comes from the Emerging Threats project. That is different from Emerging Threats Pro, which is a commercial enterprise set up to apply quality assurance to the Emerging Threats ruleset so it is more likely to find its way into commercial products. Jonkman says an open source community alone could not afford the equipment needed to do top-notch QA.

That sounds a lot like the relationship between the Snort IDS engine and Sourcefire, and it is. But Emerging Threats Pro touts its multi-threading support that effectively boosts the potential line speed of IDSs that use it. And the Emerging Threats rules are compatible with the Snort IDS engine, so they can be used to augment Snort as well as other IDS rulesets that incorporate Snort.

The company has a number of partners including Bridgeway Security, Critical Intelligence, Digital Pathways, Kaspersky Labs and Nitro Security, among others, which use Emerging Threats in various ways. Kaspersky, for instance, partners with Emerging Threats Pro to help expand its ruleset based on new malware it detects in its labs. It also uses the ruleset for its internal research.

Given its potential to work its way into a variety of commercial security platforms and its open source community that provides quick responses to new threats, Emerging Threats Pro is a company to watch.

Fixmo

Headquarters: Sterling, Va., and Toronto
Founded: 2009
Funding: $29.5 in Series B and C funding in 2011 from Extreme Venture Partners, Horizons Ventures, iNovia Capital, Kleiner Perkins Caufield Byers, Panorama Capital and Rho Ventures Canada
Leader: CEO and founder Rick Segal
|Fun fact: Core Fixmo technology was developed by the National Security Agency.

Why we're following it: As mobile devices increasingly make their way into corporate networks, it becomes more important to make sure they comply with security policies and stay that way.

Fixmo addresses this concern with software that continuously monitors mobile gear so it remains in authorized, trusted states, helping to prevent data loss and other security breaches. It also sets down audit trails to prove that devices maintained trusted state in order to satisfy regulators.

Perhaps more important, Fixmo addresses the problem of bring your own device: How does a business allow employees to access corporate resources via their personal device (smartphone, tablet, etc.) without exposing those resources to the dangers inherent in unrestricted private use of the device? An employee hitting websites in the absence of URL filtering and downloading unvetted apps could compromise the gear and therefore valuable company information. Or a compromised device could be used as a means to compromise the network to which the device connects.

Fixmo can partition these devices and create a secure sandbox in which corporate data is handled, ensuring that data can't be accessed by the rest of the machine, blocking it from potentially being compromised. The products are already being used by the Department of Defense to secure Android devices.

With these solid credentials and an infusion of $29.5 million last year, the company should have noteworthy expansion and enhancements soon.

Universal Secure Registry

Headquarters: Newton, Mass.

Founded: 2007
Funding: Private
Leader: Founder is Kenneth Weiss
Fun fact: Weiss is the creator of what is now the RSA SecurID two-factor authentication token.

Why we're following it: You can't have enough factors in multi-factor authentication, and Universal Security Registry is boosting the number to three-plus.

Kenneth Weiss, the founder of Universal Secure Registry, brings an impressive credential to the venture: He is the father of the two-factor authentication tokens known as SecurID.

With USR, he's upping his game with an additional biometric authentication factor that would be used to support electronic wallets. With the technology that he calls three-plus factor authentication, critical data used in transactions aren't stored on the phones. Rather, the multi-tiered authentication enables a connection to a server that stores customer data such as credit card numbers. That data is transmitted via a secure channel to a point-of-sale device.

Using the system, customers in the checkout line punch in passwords (something they know) followed by a randomly generated number from their phone (something they have) followed by reciting a phrase into the phone to create a voiceprint (something they are). If all three line up, customer data is sent to the point-of-sale device including a photo of the customer for the clerk to verify against the person standing there with the phone (that's the "plus").

The Universal Secure Registry could just as well be used for network logins. The constantly changing PIN generation is based on SecurID patents that are now in the public domain.

With the wide interest in digital wallets and Universal Secure Registry's goal of licensing the technology to others, it has the chance to become a widespread authentication tool that could give SecurID a run for its money.

The company is privately funded and has competition against some formidably well-heeled adversaries including Google, Visa, AT&T, Verizon and T-Mobile, the latter three of which are teaming up on a scheme called Isis.

###

Article: http://www.networkworld.com/news/2012/012612-security-companies-255358.html
Corresponding slideshow: http://www.networkworld.com/slideshow/28461