the cyberwire

The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

RSA 2013

February 25 - March 1, 2013 San Francisco, California

February 26

Congratulations to Remotium, named the Most Innovative Company at RSA for their BYOD security technology. Congratulations, also, to the other competitors—it was a tough cut to make it into the sandbox in the first place.

Several interesting studies appear at RSA. HBGary reports that investors increasingly expect (and demand) more disclosure about corporate cyber attacks. Palo Alto Networks outlines SSL's current role as both a security tool and masking agent. Other reports cover cloud security and overviews of global cyber threats.

The Deputy Undersecretary for Cybersecurity at the US Department of Homeland Security pitched his "cyber 911 plan" yesterday. He cited last year's attack on Saudi Aramco as an inspiration for the proposed system.

Two debates roil attendees. First, are security certifications like CISSP worth pursuing? Second, do pentesting tools contribute more to enterprise security than they detract from the overall "health" of the Internet?

McAfee takes note of the limitations of signature-based malware detection (a field in which it is surely a leader) and announces a shift in direction by adding heuristics to its detection products. Whether or not heuristics go far enough to keep pace with malware's rapid evolution remains an open question. In any case, the register calls McAfee's change more modification than departure.

The state of the cyber security labor force continues to draw concern (see, for example, (ISC)2's trend study reported yesterday). Today, a platform for growing that labor force—LifeJourney—premieres at RSA.

Many other interesting products debut this week—see the links below for details.

February 27

Several interesting discussions are taking place at RSA. Adi Shamir (of RSA crypto algorithm fame) challenges Rivest and Diffie over the continuing utility of cryptography. Shamir thinks that, since "even the most secure, isolated systems have been penetrated," cryptography has seen its day. He believes APTs in particular, which can lurk and observe over the long haul, have made cryptography obsolescent, and that it's time to turn our attention elsewhere (making files too large to be surreptitiously exfiltrated, etc.). Whit Diffie counters that Shamir's suggested measures would make systems harder to use without yielding a significant payoff.

And the long-running debate between libertarians and dirigistes over security awareness training also surfaces—is an informed user the best defense, or do users need the paternalistic protections of devices and controls to save them from their inattention and irrationality?

In a discussion that straddles both schools of thought with respect to users, testing company Spirent argues that stopping "data mishaps" is more important than fending-off zero-days.

Proofpoint describes "Longlining": a phishing technique that combines spearphishing with mass customization, generating large numbers of malware-carrying emails that evade signature- and reputation-based security measures.

Crowdstrike did a live takedown of the Kelihos botnet yesterday, sinkholing scads of bots for the delectation of the assembly.

If you're around the Moscone Center, the pub-crawls are worth a look. In particular CyberMaryland's meet-and-greet with Cyber Hall-of-Famers at 4:40 this afternoon (booth #216) should be fun.

And, of course, take a look through the products launching at RSA.

February 28

China can protest all it wants, but RSA symposiasts are unconvinced: PLA cyber espionage is, well established and unlikely to abate.

CounterHack describes three trends in offensive cyber operations: offensive forensics (enabling precise targeting), misdirection (including mimicking national coding styles), and kinetic effects (via attacks on critical infrastructure).

An FBI presentation sharply distinguishes hackers from insider threats, and argues that insider threats are best predicted, recognized, and neutralized using traditional personnel security disciplines.

Some panels suggest ways of balancing risk and reward when choosing security investments. If, as Adi Shamir argued yesterday, all systems eventually get breached, perhaps rapid response and active defense give a better return on investment than traditional perimeter security. And software security, as sensible an approach to development as it seems, may not make economic sense for all companies.

RSA and Detica discuss big data's potential contribution to cyber security. They see, in particular, opportunities for fraud detection through big data analytics.

Sophos draws a gloomy lesson from the Matt Hoban and Cloudflare hacks: you now need to worry not just about your own system but about everyone else's, too. (Or, as Network World puts it, "Cloud security forecast: murky with an 80% chance of finger pointing.")

Enjoy the booths and new product launches.

March 1

FBI Director Muller advocates more industry-government partnership (an evergreen proposal) but also argues that counterterrorism holds a lesson for cyber security: you defeat a threat not through passive defenses, but by identifying and disrupting it. This naturally suggests a move toward offensive security, and Crowdstrike leads the discussion of how to achieve an active defense without slipping into vigilantism ("hacking back," in this context). TechWeek Europe listens and advises its corporate readers to lawyer up. (Compare two articles in our main section below: Anonymous hit the Bank of America to expose the bank's hacker profiling effort, and the Center for a New American Security urges the US Government to clarify what it means by "cyber offensive operations.")

Symposiasts and booth-boulevardiers sniff at the "advanced" in "advanced persistent threat," noting that the APTs Mandiant found in its investigation of Chinese attacks on US media outlets weren't really that advanced. But the critics dismiss such APTs as "script kiddy" work too glibly—they may have been inelegant and manpower-intensive hacks, but they did their damage nonetheless. (And note the Ponemon report on how long attacks go undetected by the victims.)

IT security managers scoff at predictions that big data will have a big impact on cyber security. “Garbage data,” as one hyperbolically calls it, but they may have a point. Collection of information has, for almost a century, outstripped the ability to analyze it into intelligence; big data will face a big burden of proof.

Congratulations to Naked Security, named best corporate blog.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com

@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 8.4.15