McAfee Labs’ 2016-2020 Threat Predictions

The newly released *McAfee Labs Threat Predictions Report* offers short- and long-term trend insights for organizations racing to keep pace with and perhaps overtake business and technological change, while continuously fending off a growing variety of cyber threats.

The report predicts key developments on the cyber threat landscape in 2016 and provides unique insights into the expected nature of that landscape through 2020, as well as the IT security industry’s likely response.

Here are some key threat predictions from the report for 2016:

- **Hardware.** Attacks on all types of hardware and firmware will continue, and the market for tools that make them possible will expand and grow. Virtual machines will be targeted with system firmware rootkits.

- **Ransomware.** As it has come to pass in other areas of cybercrime, the true accelerator of ransomware growth will be the availability of ransomware-as-a-service offerings on the dark Web.

- **Attacks through employee systems.** Attackers are likely to shift their focus to increasingly attack enterprises through their employees by targeting, among other things, employees’ relatively insecure home systems to gain access to corporate networks.

- **Cloud services.** Cyber criminals could seek to exploit weak or ignored corporate security policies established to protect cloud services.

- **Warehouses of stolen data.** The coming year will see the development of an even more robust dark market for stolen personally identifiable information such as usernames and passwords.

- **Integrity attacks.** One of the most significant new attack vectors will be stealthy, selective compromises to the integrity of systems and data. In 2016, we could witness an integrity attack in the financial sector in which millions of dollars could be stolen by cyber thieves.

- **Sharing threat intelligence.** Threat-intelligence sharing among enterprises and security vendors will grow rapidly and mature. Legislative steps may be taken that make it possible for companies and governments to share threat intelligence.
Legislative Updates

Bloomberg - “Target Settles With Banks Over 2013 Breach for $39 Million,” by Christie Smythe: “Target Corp. will pay about $39 million to banks and credit unions to resolve losses from a 2013 holiday-season data breach, as retailers and financial institutions continue to grapple with the costs of major hacker attacks. Financial institutions sued the Minneapolis-based retailer to recover an estimated $200 million in losses stemming from the hack, in which as many as 40 million payment cards were exposed. Lawyers for the banks argued the retailer failed to take precautions to protect the customer data.”

“Regulators Show Interest in Blockchain to Monitor Systemic Risk,” by Stephen Joyce: Regulators are looking at whether blockchain technology that uses encrypted databases or ledgers to record and authenticate transactions can help monitor global financial systems for systemic risk. R3 CEV, a financial services technology company backed by JPMorgan Chase & Co., Bank of America Corp., Wells Fargo & Co. and other large banks, has discussed with regulators the possibility of using blockchain technologies, said Charley Cooper, the firm's managing director. Cooper told Bloomberg BNA that regulators in jurisdictions around the world have raised the issue at meetings scheduled for other purposes.

The Hill – “DHS hacks businesses for free to test cybersecurity,” by Cory Bennett: “The Department of Homeland Security (DHS) is peppering U.S. businesses — mostly banks and energy firms — with cyberattacks to test their digital defenses. The little-known program, offered to companies free of charge, is part of an ongoing effort to help critical infrastructure companies bolster their cybersecurity.”

Bank Info Security – “Congress Probes Mobile Payments Security,” by Tracy Kitten: “Mobile payments are expected to reach an all-time high in the U.S. this month as more consumers turn to mobile services such as Apple Pay and Samsung Pay to make their holiday purchases. Two-thirds of U.S. adults now own smartphones, and more than 36 million Americans are expected next year to use mobile payments options to conduct $27 billion in transactions, according to statistics from Juniper Research and CNET that were gathered for a Dec. 1 hearing of the House Energy & Commerce Committee.”

“Cybersecurity Bills Would Add Secrecy to Public Review,” by Tami Abdollah: A proposed law meant to encourage companies to share information about cyberthreats with the U.S. government includes measures that could significantly limit what details, if any, the public can review about the program through federal and state public records laws. The legislation — already passed with broad bipartisan support in both houses of Congress but not yet finalized — would keep secret any information a company hands over to the Obama administration under a new cybersecurity agreement, including specifics the firms decide themselves shouldn’t be disclosed. It’s not clear whether that secrecy would extend to learning whether particular companies are even participating.

Reuters – “U.S. retailers hunt for attacks after warning on stealthy malware,” by Jim Finkle: “U.S. retailers are hunting for evidence of new breaches leading into the holiday shopping season after a cyber intelligence firm privately warned them about payment-card-stealing malware that it said evades almost all security software. “This is by far the most sophisticated point-of-sale malware seen to date," said Maria Noboa, lead technical analyst for privately held iSight Partners, which uncovered the malware and was due to release a technical report about it on Tuesday.”
Making Headlines

- Pearson VUE has disclosed that intruders infected its certification credential manager system with malware. The system supports certification tracking programs for Cisco, F5 and other technology companies. In the wake of the security breach, Pearson VUE has taken the system offline as works with law enforcement to investigate the incident.
- Starwood Hotels (Sheraton, Westin and other chains) announced that malware was found on more than 50 of its hotels in North America, exposing payment card information.
- Secretary of State-Brian Kemp’s office inadvertently released more than 6 million records of personal voter information to the media.

Technical Corner
Patches & Vulnerabilities

- **MS15-112** - Resolves vulnerabilities in Internet Explorer.
- **MS15-117** - Resolves vulnerabilities in Microsoft Windows NDIS.
- **MS15-120** - Security Update for IPSec to Address Denial of Service
- **MS15-123** - Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure.

**CVE-2015-5501** - The Hostmaster (Aegir) module 6.x-2.x before 6.x-2.4 and 7.x-3.x before 7.x-3.0-beta2 for Drupal allows remote attackers to execute arbitrary PHP code via a crafted file in the directory used to write Apache vhost files for hosted sites in a multi-site environment.

**CVE-2015-3761** - The kernel in Apple OS X before 10.10.5 does not properly validate pathnames in the environment, which allows local users to gain privileges via unspecified vectors.

**CVE-2015-4534** - Java Method Server (JMS) in EMC Documentum Content Server before 6.7SP1 P32, 6.7SP2 before P25, 7.0 before P19, 7.1 before P16, and 7.2 before P02 allows remote authenticated users to execute arbitrary code by forging a signature for a query string that lacks the method_verb parameter.

**CVE-2015-2442** - Microsoft Internet Explorer 8 through 11 and Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2444.

Sources: US Cert, Microsoft

---