IBM Tackles Advanced Malware with Expanded Endpoint Protection Software
Wednesday, May 21, 2014 03:45:00 PM (GMT)

Trusteer Apex Helps Block and Shut Down Cyber Attacks that Begin with Malware Exploits

ARMONK, N.Y., May 21, 2014 /PRNewswire/ -- IBM (NYSE: IBM) announced new security software that helps stop threats at the weakest link, the endpoint, including laptops and desktops which are most susceptible to malware. IBM's Trusteer Apex software is the newest offering in the company's Threat Protection System announced earlier this month, which leverages security intelligence and behavioral analytics to go beyond traditional anti-virus approaches and firewalls to disrupt attacks across the entire attack chain - from break-in to exfiltrate.

Advanced threats are attacking organizations at an alarming and ever more costly rate. Data breaches caused by such threats have cost on average $9.4 million in brand equity alone per an IBM Trusteer-commissioned Ponemon study on Advanced Persistent Threats. The same study says targeted attacks are the greatest threat with only 31 percent of respondents believing adequate resources are available to prevent, detect and contain these threats. Organizations are faced with a myriad of point products that do not provide complete protection and also create manageability challenges. Java applications are particularly targeted and carry a high risk as a pervasive part of the corporate environment.

The **Trusteer Apex** endpoint protection software blocks attempts by cyber criminals to exploit vulnerabilities on the endpoint that lead to data breaches. It provides an easy to deploy automated threat analysis capability to prevent attacks that is less burdensome than the many, disparate point solutions in the market. Since the product is easy to manage and maintain, it helps the Chief Security Officer and the IT Security team be more resourceful and effective.

IBM's new Trusteer Apex software blocks attacks and shuts them down when they occur on the endpoint. New capabilities include:

Employing Multi-layered Defenses

These defenses combine several methods to break the attack chain. IBM has identified strategic chokepoints where cybercriminals focus their attention, take hold of a user's endpoint and infect it with malware. For example, Java is the target of half of the application vulnerability attacks. Per the IBM X-Force Q2 2014 report, 96 percent of Java exploits are applicative, meaning rogue Java applications that are not controlled.

Trusteer Apex can stop attacks that are embedded into Java applications and lock them from wreaking havoc on the enterprise. Trusteer Apex prevents malicious Java applications through assessing application trust and activity risk, and blocking untrusted apps from doing high-risk activities.

Stopping Theft of Sensitive Corporate Credentials

Despite the best end user education, there are still cases where employees open emails that appear to be legitimate but are actually spear phishing attacks that do not always go to spam folders. If a phishing email is inadvertently opened, Trusteer Apex can identify there is malware and stop it from exploiting the endpoint.

Trusteer Apex also prevents employees from re-using corporate credentials on untrusted sites that are against corporate policy. For example, a new employee sets up an email and password to access corporate sites. If the employee tries to use the same password on Facebook or other social networks, Trusteer Apex stops it.

Reducing the Ongoing Burden on IT Security Teams

Organizations can offload the analysis of potentially suspicious activity to the IBM/Trusteer threat analysis service, which can help an organization assess suspicious activities and provide protection recommendations. The service looks at an organization's specific threats and helps them take action on them.

IBM also has a dynamic intelligence feed from more than 100 million protected endpoints – a database that has more than 70,000 vulnerabilities categorized. This threat research and intelligence is translated into security updates that are automatically sent to protected endpoints.

"Through extensive research, IBM has identified specific stages of the attack chain where cyber criminals have relatively few options to execute their malicious content," said Yaron Dycian, Vice President of Marketing, Products & Services at Trusteer, an IBM company. "Current point solutions in the market offer narrow protections against specific attack vectors and create significant workload on overstretched security teams, making it difficult to manage against cyber threats. Our strategic chokepoint technology introduces a fresh approach for breaking the threat lifecycle and preempting cyber attacks."

An example of this approach is a major healthcare provider that recently deployed Trusteer Apex on more than 20,000 endpoints to protect sensitive patient data. Apex detected more than 100 high-risk infections, despite the existence of an anti-virus solution and a next-generation firewall. Apex mitigates these infections

with minimal operational impact, and provides the IT Security team with event analysis and solution tuning.

The IBM Trusteer Apex multi-layered approach also:

- Disrupts the exploit chain – Attackers must gain persistency of their malware on the endpoint. Apex monitors the key methods used by attackers to install malware by exploiting vulnerabilities and blocks those methods.
- Blocks malicious communication – To compromise the endpoint, gain control and exfiltrate data, advanced malware must communicate with the attacker, often through a command and control server. Trusteer Apex prevents untrusted communication channels from the endpoint outside of the corporate network.
- Offers new integration with IBM QRadar and IBM Endpoint Manager.

About IBM Security
IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. IBM monitors 15 billion security events per day in more than 130 countries and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Video - http://www.youtube.com/watch?v=7per8XtO-cQ&feature=youtu.be
Photo - http://photos.prnewswire.com/prnh/20140521/90016
Logo - http://photos.prnewswire.com/prnh/20090416/IBMLOGO

SOURCE IBM

Contacts: Mitchell Derman, IBM Media Relations, mderman@us.ibm.com, 571-216-8712
Countries: United States
Industries: Computer Electronics, Hardware & Software, High Tech Security
Languages: English
Primary Identifiers: IBM-US
Related Identifiers: IBM-US
Subjects: New Products & Services