

ADVANCED PERSISTENT THREATS SUMMIT

MOUNTING DYNAMIC DEFENSE TO COMBAT SOPHISTICATED THREATS

Presented By  

APT SUMMIT FINDINGS

On July 13 and 14, 2011, RSA and TechAmerica hosted an Advanced Persistent Threats Summit in Washington, D.C. The Summit brought together senior leaders from government and business to address both the impact of APTs and strategies for defense and mitigation. During the Summit, detailed perspectives on protecting against today's most menacing information security threats surfaced. These findings, which are highlighted below, will be expanded upon in an in-depth report, scheduled to be published in the coming months.

ATTACK VECTOR SHIFTING FROM TECHNOLOGY TO PEOPLE

- Social engineering is now the #1 threat vector.
- The new perimeter is the human being.
- Anyone can be phished given the right context – and attackers have growing access to information about would-be targets through social networking sites that help them identify the right people to go after within the organization and also personalize their attacks.
- User training alone does not entirely neutralize spear-phishing or other targeting. Training coupled with user restrictions and visibility can be more effective: control their online exposures and then educate users on why those working in sensitive environments might have their access to social networking sites tightly managed.

ORGANIZATIONS MUST LEARN TO LIVE IN A STATE OF COMPROMISE

- Determined adversaries can always find exploits through people and in complex IT environments. It's not realistic to keep adversaries out. Organizations should plan and act as though they have already been breached.
- Organizations should focus on closing the exposure window and limiting damage through efforts to compartmentalize systems, stop sensitive data egress and go back to the core principles of IT security such as "least privilege" and "defense in depth."
- The key is to know what digital assets are important to protect, where they reside, who has access to them and how to lock them down in the event of a breach.

Key Findings



SITUATIONAL AWARENESS IS ESSENTIAL TO DETECTING THREATS EARLY

- Security improves through greater situational awareness: gaining the ability to understand what's happening beyond our network boundaries to detect threats on the horizon. We get smarter by looking beyond our infrastructure and observing the ecosystem.
- Telltale signs of APTs can be identified through attacks on others: attendees observed a rise in “beta attacks” – adversaries attacking third parties simply to beta test techniques to be used on actual targets.
- We must work more closely together than ever before: international cooperation and collaboration between companies and the public sector are essential to developing advanced “indicators” that will help identify and mitigate threats.

SUPPLY CHAIN POISONING IS ON THE RISE

- We're only as strong as the weakest link in our supply chain. Adversaries will take the time and care to cultivate vulnerabilities through trusted vendors. Attendees noted that attackers have moved further upstream in the supply chain to get to a target.
- Monitoring suppliers' security is a huge need and challenge. Contractual attestations are not enough. Attendees proposed various solutions that companies can utilize to reduce their risk, including reputation rating services, third-party audits of vendors (paid for by the vendor) and doing external monitoring of vendors to evaluate their security posture.

INCIDENT RESPONSE SHOULD BE AN ORGANIZATIONAL COMPETENCY, NOT A SECURITY FUNCTION

- Incident response should not be considered exclusively a security function. It is an organizational competency that must be developed long before you are attacked and must be continually honed. If organizations are planning responses as an attack unfolds, they are too late.
- A competency approach allows remediation activities to kick in automatically – like a reflex. Incident response plans are in place and tested before attacks happen.
- It pays to model and drill incident response exercises and ensure that working relationships between functional teams and key personnel are well established.

CUSTOMIZATION – AN APT'S CALLING CARD – DEFIES TRADITIONAL SIGNATURE-BASED APPROACHES

- APT techniques are custom-developed to work against a target's specific weaknesses. Malware used in a recent attack was compiled just hours before used to exploit a zero-day vulnerability, defying identification by generic signatures.
- Attackers are increasingly agile and can take advantage of vulnerabilities more quickly than signature-based approaches can remediate.

TODAY'S ATTACKERS ARE BETTER AT REAL-TIME INTELLIGENCE SHARING THAN TARGETS – FIXING THIS IS A TOP PRIORITY

- Audience members observed attackers seem to share intelligence more effectively than legitimate enterprises do. Attackers are not impeded by the legal restrictions and other rules that govern corporations and government organizations.

- Attendees find value in sharing threat information through informal, personal networks, but results are uneven and unscalable – there are many apples to oranges barriers
- Fear of legal risks appears to be one of the biggest impediments to sharing actionable threat information. Attendees discussed liability protection measures, including a pending bill in the Senate.
- The industry needs better frameworks for communicating threat information. Again and again, attendees identified information-sharing as a strategic capability that the security community needs to prioritize. According to the attendees, information sharing frameworks should include:
 - Standardized reporting processes and lexicons
 - Indemnifications against liability for information sharing or directed action for cyber security purposes
 - Technical infrastructure to share and analyze threat information at “machine speed”

ORGANIZATIONS MUST GET CREATIVE TO DETECT ATTACKS EARLY AND DISRUPT ATTACKERS OFTEN

- Focus on early detection of breaches to minimize your window of vulnerability. The key is actively preserving, aggregating and reviewing data to detect a potential intrusion but also for post-event forensics.
- Don’t underestimate the power of disruption. Damage from APTs can be minimized or prevented by simply interrupting attackers’ work flow at multiple points. Organizations should strive for a disruptive approach to defense in order to match the rapidly evolving threat environment.

APT HEADLINES ARE THE TIP OF THE ICEBERG

- Although the term APT may be overused, there is no question that sophisticated, targeted cyber attacks are more widespread than even today’s frequent headlines suggest.
- We need to think beyond data theft: poisoning, disruption or embarrassment can also be end goals of an APT.
- Companies get inducted into “the club” after an attack and only then realize the wealth of information available.

SIMPLICITY IS THE PATH TO BETTER SECURITY

- Many of the holes that exist today come from an unmanageably complicated IT infrastructure.
- We need to simplify our technology environment. Given that security is a weakest link problem, only through understanding assets, processes and endpoints is there a chance at real defense. Use the minimal technology needed to achieve your objectives – decommissioning outdated systems.

Key Findings