Understanding information security threats: Expert Models

Thu, 03/31/2011 - 11:17 | by **Jim Lippard**

Yesterday, I briefly recounted Rick Wash's research on "folk models" of information security threats; today I'd like to do the same for a more advanced threat model. Last December, Timothy Casey gave a presentation at the first Phoenix SecureWorld Expo on the library of threat agents that he and others have developed at Intel and made available for general use. In his presentation, he noted that "threat" is often not well defined, and Intel decided to address the issue by identifying the personas of the humans behind information security threats, creating a taxonomy of agents and their respective attributes. For each agent, their access, intent, limits, primary goal, methods, resources, skills, and visibility were identified; associated with each agent is a matrix of exploits that can be matched against vulnerabilities. The current published version of the library identifies 22 agents, though Casey said they are now up to 24.

The library provides a common language for senior executives, security specialists, and other employees to discuss threats and how to respond to them. It also can be used to perform a variety of threat assessments, including agent-specific trending. Casey pointed out two broad types of assessment, a targeted threat assessment for a narrow target or specific domain, and a domain-wide threat assessment. In the former case, subject matter experts for the particular domain meet with information security experts to discuss the types of agents from the library most likely to be a threat to their domain, and thereby identify what defenses are appropriate. In the latter, all threats and all agents are considered, assigned weights, and used to find the most pressing risks. This can be done within a risk assessment framework such as OCTAVE or the U.S. National Infrastructure Protection Plan's Baseline Risk Assessment Framework.

Agent trending is performed by periodically (every six months at Intel) updating the ratings of each agent on a low/medium/high scale based on recent activity and its relevance to the target company. Agents which are trending upward over time may provoke a review and improvement of controls relevant to countering that threat.

By putting this threat agent library into the public domain, Intel has provided a useful tool to organizations for understanding threats and prioritizing responses to them.

Intel Threat Agent Library white paper by Timothy Casey (2007)
Prioritizing Risks with Threat Agent Risk Assessment (2009)
Information Technology Sector Baseline Risk Assessment
Tim Casey video on use of the threat agent library

Tags: Defense in Depth Security Expert Models OCTAVE Security threats Tim Casey

Request new password

Recent blog posts

- Global Crossing Genesis Solutions International Events Part 2 of 2 - "Operationalizing the deal"
- Global Crossing Genesis Solutions International Events Part 1 of 2 "Winning the deal"
- IPv4 Addresses for Sale?
- Recap at IBC 2011 - Global Crossing Genesis Solutions
- Regional and global bandwidth expansion boom
- Tips to prevent voice communications systems fraud
- PSN Cost Savings in the UK Government Sector
- Advanced Cyber Attacks Require Sophisticated Technology
- Application management on Data Center critical enviroments
- Crowning glory for Global Crossing (UK) Telecommunications Limited

more

Legal Disclaimer