



CIO/CTO Perspective Policy and Regulation Defense in Depth Security Business Insights Voice and Collaboration Solutions IP Solutions
Virtualization & On-Demand

Home » Blogs » lippard's blog

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](#)

Like

Like

5

Add New Comment

[Login](#)



Type your comment here.

Showing 0 comments

Sort by oldest first

[M](#) [Subscribe by email](#) [S](#) [RSS](#)

Trackback URL

[Jim Lippard's blog](#)

Follow Global Crossing

Subscribe to our
Level 3 Blog



Languages

English

Search

Connect on Facebook

Like

Jake Khuon, Paula McElmeel and 1,809 others like this.



Cloud Services Suite

Click Again for Full Screen

User login

Username: *

Password: *

[Log in using OpenID](#)

[Create new account](#)

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 environments](#)
- [Crowning glory for Global Crossing \(UK\) Telecommunications Limited](#)

[more](#)



Legal Disclaimer

Disclaimer: Opinions expressed here and in any corresponding comments are the personal opinions of the original authors, and do not necessarily reflect the views of Global Crossing. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Global Crossing or any other party. This site is available to the public. No information you consider confidential should be posted to this site. By posting you agree to be solely responsible for the content of all information you contribute, link to, or otherwise upload to the Website and release Global Crossing from any liability related to your use of the Website.