

TRACK: InfraGard Track / Cyber-crime, terrorism, and information warfare
SESSION #: TBA
DATE: TBA
TIME: TBA
SESSION TITLE: "2010 Cyber Threats and Trends"
SPEAKER(S): Ralph Thomas – Deputy Director and Manager Malware Intelligence
ORGANIZATION: iDefense and VeriSign, Inc.

ABSTRACT: "2010 Cyber Threats and Trends"

This presentation is a description of the current cyber security landscape from the iDefense perspective. It discusses emerging trends that occurred in 2009 from a technical and a geopolitical perspective, makes some predictions about what may occur in 2010 and then looks over the horizon to the next 5 to 10 years to outline emerging technological and cultural trends that will impact the defense of the enterprise in the future. This white paper represents a snapshot of everything that iDefense understands about the cyber security landscape to date. Throughout 2009, two major themes emerged in terms of cyber security: a steady evolution of malicious tools of the trade (tactics) and a shift in the center of gravity from typical network defenders and commercial security companies to government policy makers in terms of security thought leadership and spending (strategy).

In terms of ongoing and new tactics, this presentation covers increased speed in exploit code development, alternative hosting and command infrastructure for malware, manipulating search engine results to distribute malware, and new business practices in the carding underground.

After a series of well-publicized breaches in corporate and governmental networks during the past two years, governments from around the world have begun to understand that counter-tactics alone will not solve the problem. Many geo-strategically powerful governments have taken steps to implement or refine official cyber warfare policies and capabilities. They have begun forming the nexus for strategic thinking and dedicating large sums of money to the problem. This is a shift. Heretofore, financial institutions, information technology (IT) departments and global security companies provided thought leadership for the security industry and the impetus to spend money. As more and more governments waded into the fray, the center of gravity for these activities is shifting away from private enterprise and into the government sector.

SPEAKER BIO(S): Mr. Thomas serves as deputy director for iDefense, and heads the iDefense Malware Intelligence Group, responsible for malware research and outbreak response. Mr. Thomas also directs the malware research lab in iDefense, which is tasked with the development of tools for discovery and analysis of malicious code and related threats. Before joining iDefense, Mr. Thomas worked as Principal Computer Forensics Consultant in several data acquisition and litigation support

projects and regularly served as an expert witness in federal court. Early in his career, Mr. Thomas designed hardware and real-time software in the controls and digital television sectors before turning his attention to enterprise software. A Certified Lotus Specialist, he has expertise in e-mail archiving, document imaging, Siebel, SAP and Oracle Applications. Mr. Thomas holds an MS in Electrical Engineering from the University of Dortmund in Germany.