

TRACK: IT Security
SESSION #: TBA
DATE: TBA
TIME: TBA
SESSION TITLE: "Sniper Forensics – One Shot, One Kill"
SPEAKER(S): Chris Pogue – Senior Security Analyst
ORGANIZATION: Trustwave

ABSTRACT: "Sniper Forensics – One Shot, One Kill"

"Sniper Forensics – Changing the Landscape of Modern Forensics and Incident Response"

At one time, computer forensics consisted of pulling the plug, imaging everything in sight, and loading those images into EnCase or FTK. As computer hackers became more resourceful, the complexity of computer forensics increased exponentially. Add to that the growing size of data storage devices, and it becomes infeasible to even consider imaging tens of hundreds of terabytes, let alone load those images into EnCase or some other forensic software. So what's the answer? How can incident responders hope to remain relevant in today's operating environment? With Live Analysis!

Live Analysis tools and techniques have exploded onto the incident response scene in the last two years. By gathering and reviewing volatile data and RAM dumps, incident responders can use time proven theories like, "Locard's Exchange Principle", "Occam's Razor", and "The Alexiou Principle" to target only the systems that are part of the breach. What used to take hours of analysis can now be done in minutes! What used to take weeks, can now take days!

By using sound logic and data reduction based on forensic evidence extracted from Live Analysis, incident responders can introduce accuracy and efficiency into their case work at a level not available through any other means. This is truly the cutting edge of modern computer forensics, and not something to be taken lightly! Don't miss the opportunity to learn tips, tools, and hear real world examples of how Live Analysis is literally changing the landscape of modern forensics!

Reason why this material is innovative or significant or an important tutorial.

This information is CRITICAL for all incident responders and computer forensic analysts! It combines cutting edge forensic tools and techniques with time proven principles. Successful integration of the material contained in this presentation will without question, reduce the time spent on cases and increase accuracy! It's a targeted approach to forensics which I have dubbed, "Sniper Forensics" rather than the old school, "Shotgun forensics" approach.

SPEAKER BIO(S): Chris Pogue is a Senior Security Analyst for the Trustwave SpiderLabs Incident Response and Digital Forensics team. He has over ten years of administrative and security experience including three years as an Incident Response/Forensic Analyst for the IBM ISS X-Force Emergency Response Services Team, and five years with IBM's Ethical Hacking Team. During his tenure with the X-force and now the SpiderLabs, Chris worked with some of the largest organizations in the world.

As an Ethical Hacker, he was tasked with emulating the actions of a malicious attacker with the intention of assisting customers to identify and eliminate probable attack vectors. Chris has worked on over 3000 exploitation attempts on both internal IBM systems as well as those of third party customers. Bringing that knowledge and experience to bear within the SpiderLabs, Chris specializes in incidents involving intrusion, unauthorized access, and malware reverse engineering.

Chris is also a former US Army Warrant Officer and has worked with the Army Reserve Information

Operations Command (ARIOC) on Joint Task Force (JTF) missions with the National Security Agency (NSA), Department of Homeland Security (DHS), Regional Computer Emergency Response Team-Continental United States (RCERT-CONUS), and the Joint Intelligence Center-Pacific (JICPAC).

Chris holds a Bachelor's Degree in Business Management, a Master's degree in Information Security, is a Certified Information Systems Security Professional, (CISSP), a Certified Ethical Hacker (CEH), a Certified Reverse Engineering Analyst (CREA), a GIAC Certified Forensic Analyst (GCFA), and a PCI Qualified Security Assessor (QSA). Chris is also the primary author of the book, "Unix and Linux Forensic Analysis", from Syngress/Elsevier. Chris's book is currently being used as a textbook at Saginaw Valley State University and Illinois State University for their computer forensics courses.