FALL TECHNOLOGY SERIES

Ransomware

SEPTEMBER 7, 2016

SPEAKER BIOS

Panel 1: Overview of the Ransomware Threat

Craig Williams is senior technical leader and manager of the Talos Outreach team, and guides some of the most experienced threat researchers in the world. Their collaborative research and analysis work is intended not only to continually enhance the quality and efficacy of Cisco's security products, but also, provide actionable intelligence that helps all Internet users defend against both known and emerging network threats. Mr. Williams' research over the past decade has included running the Cisco malware lab and trying to outwit the very security products he has helped Cisco to design. Among Mr. Williams' significant contributions to Cisco include an issued patent and 2 Google bug bounties. He is also the recipient of a distinguished speaker award.

Joseph Opacki is the Vice President of Threat Research at PhishLabs in Charleston, South Carolina. Prior to joining PhishLabs, Mr. Opacki was the Senior Director of Global Research at iSIGHT Partners and was also an adjunct professor at George Mason University where he taught malware reverse engineering in the master of computer forensics program. Mr. Opacki has also participated in numerous industry advisory councils including the Cybersecurity Curriculum Advisory Council at the University of Maryland University College and the Cyber Crime Industry Advisory Board at The Citadel in South Carolina. Before his career in the private sector, Mr. Opacki was the malware reverse engineering Subject Matter Expert (SME) and the Technical Director of advanced digital forensics in the Operational Technology Division at the Federal Bureau of Investigation.

Lance James is Chief Scientist at Flashpoint where he heads up research and development and engages in thought leadership. Prior to joining Flashpoint, Mr. James was the Head of Cyber Intelligence at Deloitte & Touche LLP. An internationally renowned information security specialist, Mr. James has more than fifteen years of experience in programming, network security, digital forensics, malware research, cryptography design, cryptanalysis, counterintelligence, and protocol exploitation. He provides advisory services to a wide range of government agencies and Fortune 500 organizations including America's top financial services institutions. Credited with the identification of Zeus and other malware, Mr. James is an active contributor to the evolution of security practices and counterintelligence tactics and strategies.

Georgia Weidman is the Founder and CTO of Shevirah Inc. She is a penetration tester, security researcher, speaker, trainer, and author. Ms. Weidman holds a MS in computer science as well as CISSP, CEH, and OSCP certifications. Her work in mobile exploitation has been featured internationally in print and on television. The conferences she has presented at include NSA, West Point, and Black Hat. Her DARPA Cyber Fast Track grant resulted in the release of the Smartphone Pentest Framework (SPF). She founded Shevirah Inc. to commercialize SPF for enterprise customers. Ms. Weidman is the author of Penetration Testing: A Hands-On Introduction to Hacking from No Starch Press. She was the recipient of the 2015 Women's Society of CyberJutsu Pentest Ninja award.

Presentation by Office of Technology Research & Investigation

Joe Calandrino is the research director of the FTC's Office of Technology Research and Investigation. His office's research explores the evolving impact of technology on consumers, examining topics such as consumer fraud, online advertising, financial technologies, and connected devices. He is the author of numerous refereed research publications, and he has spoken on security, privacy, and consumer protection issues in a variety of venues. Dr. Calandrino received his doctorate in Computer Science from Princeton University, where his research focused on security and privacy. He holds a BS in Computer Science and Mathematics from the University of Virginia.

Anthony Masi is a graduate student pursuing a MS in Cybersecurity at New York University, where he is a CyberCorps Scholarship for Service recipient. His coursework and projects have explored key concepts in securing systems and data. He interned with the FTC's Office of Technology Research and Investigation in the summer of 2016. At the FTC, Mr. Masi studied the behavior and impact of ransomware. He received a BS in Computer Science from Manhattan College.

Panel 2: Best Defense Tactics Against Ransomware

Lorrie Cranor joined the Federal Trade Commission as Chief Technologist in January 2016. She is on leave from Carnegie Mellon University where she is a Professor of Computer Science and of Engineering and Public Policy, Director of the CyLab Usable Privacy and Security Laboratory (CUPS), and a co-director of the MSIT-Privacy Engineering masters program. Dr. Cranor also co-founded Wombat Security Technologies, an information security awareness training company. She has authored over 150 research papers on online privacy and usable security, and has played a central role in establishing the usable privacy and security research community, including her founding of the Symposium on Usable Privacy and Security. She was previously a researcher at AT&T Labs-Research. Dr. Cranor holds a doctorate in Engineering and Policy from Washington University in St. Louis. She is a Fellow of the ACM and IEEE.

Bill Wright is the Director of Cybersecurity Partnerships at Symantec. Mr. Wright leads the Norton Cybersecurity Institute program and manages a number of global cybercrime and cybersecurity operational and policy partner relationships with governments and industry. Mr. Wright has more than twenty years of experience spanning the legal, policy, and operational spectrums of national security, law enforcement, and international partnerships. Prior to joining Symantec, he was Staff Director and General Counsel for two U.S. Senate Subcommittees focused on homeland security,

government IT and oversight. He also served as the chief advisor to Senator Scott Brown for cybersecurity, national security and intelligence issues. Prior to the Senate, Mr. Wright worked in the Intelligence Community as a Senior Operations Officer at the National Counterterrorism Center Operations Center (NCTC). Mr. Wright holds a BA in Political Science from Hampden-Sydney College and a JD from DePaul University College of Law.

Keith McCammon is the Chief Security Officer and a co-founder of Red Canary, which specializes in endpoint security and threat detection. Mr. McCammon leads Red Canary's security organization and is responsible for the company's security strategy as well as its innovative approach to threat detection and security operations. He has almost two decades of technology experience, much of it focused on identifying and solving complex security problems. Prior to joining Red Canary, Mr. McCammon served in roles ranging from offensive information operations and signals intelligence to executive leadership.

Jim Walter is a senior member of Cylance's SPEAR team. He focuses on next-level attacks, actors, and campaigns as well as "underground" markets and associated criminal activity. He specializes in long-term campaign and actor trending/analysis with a sharp focus on the organized crime aspects of the modern threat landscape. Mr. Walter is a regular speaker at cybersecurity events and has authored numerous articles, whitepapers, and blogs specific to advanced and low-level threats. He has also created and participated in multiple information security podcasts for over a decade. Mr. Walter joined Cylance following 17 years at McAfee/Intel Security running their Advanced Threat Research and Threat Intelligence teams and content streams.

Chad Wilson, with 24 years of progressive leadership, is the Director of Information Security at Children's National Health System. Children's National, based in Washington, DC, has been serving the nation's children since 1870 and was ranked among the top 10 pediatric hospitals by *U.S. News & World Report 2015-16*. Mr. Wilson joined Children's National in 2013, where he leads its cyber security strategy and execution focused on providing service excellence to patients, clinicians, and co-workers through innovative and secure solutions.

Panel 3: What Happens If You Become a Victim?

Will Bales entered on duty as a Special Agent with the FBI in 2008. SSA Bales was assigned to the Los Angeles FBI field office where he worked on criminal cyber investigations and intellectual property rights crimes. In 2014-2015, SSA Bales served as the Cyber ALAT in Seoul, Korea. Since then he has been promoted to Supervisory Special Agent and is currently assigned to the Major Cyber Crimes Unit, Cyber Division, where he is responsible for leading the FBI's effort against ransomware. Prior to the FBI, SSA Bales worked in private industry for eight years providing technical support and network administration. SSA Bales holds a Bachelor's Degree in Computer Information Systems.

Serge Jorgensen is President and a founding partner of The Sylint Group. He provides technical development and guidance in the areas of Computer Security, Counter Cyber-Warfare, eDiscovery, System Design and Incident Response. Mr. Jorgensen is a patented inventor in engineering and math-related fields. Prior to co-founding The Sylint Group, Mr. Jorgensen ran the Research and Development Department for Locast Corporation developing a HIPAA-compliant patient location- and status-tracking device. Since co-founding Sylint, Mr. Jorgensen has, among his other accomplishments, directed

development of DNS (Dynamic Name Server) tracking applications, provided response and remediation guidance to multi-billion dollar international espionage and cyber-security attacks, and directed, tasked and managed multi-million dollar litigation, forensic and electronic discovery efforts.

Adam Malone is a Director in PwC's Cyber Crime and Breach Response Practice. He leads PwC's Incident Response teams and focuses on the development of world class incident response service and cybercrime investigations and capabilities. He leads cybercrime investigations on behalf of clients and ensures value through integrated and targeted threat intelligence and aggressive completion timelines. His breadth of experience covers multiple adversaries; nation-state actors committing cyber espionage and cyber warfare; financially motivated international organized crime groups; domestic and international Hacktivists; as well as institutional insiders. Prior to joining PwC, Mr. Malone was a Supervisory Special Agent for the FBI where he investigated cybercrime, acts of terrorism, and economic espionage. He was the case agent on several high profile investigations and received distinguished recognition within the U.S. Government for his investigative results and acumen. Prior to joining the FBI, Mr. Malone was a Senior Systems Engineer for BAE Systems, and is a veteran of the U.S. Air Force. Mr. Malone is a Certified Information Systems Security Professional (CISSP).

Bill Hardin, Vice President and Cyber Crime Solution Leader at Charles River Associates, has worked on hundreds of forensic engagements in the areas of data breach and cyber incident response, theft of trade secrets, white collar crime, FCPA investigations, and enterprise risk management. Many of his cases have been mentioned in The Wall Street Journal, Financial Times, Forbes, and Krebs on Security, amongst other publications. With a background in finance, operations, and software development, he brings valuable insights to clients from multiple dimensions. In addition to his forensic engagement assignments, Mr. Hardin has served in numerous interim management roles for organizations experiencing disruption. He has assisted companies with various management consulting assignments pertaining to strategy, operations, and software implementations. Mr. Hardin is a CPA/CFF, Certified Fraud Examiner (CFE), Project Management Professional (PMP), and has a MBA from the Chicago Booth School of Business. Mr. Hardin has spoken at numerous events on cybercrime, risk management, and strategy/operations consulting. He serves on the board for Legal Prep Charter Schools and is an adjunct professor at DePaul University in Chicago.

Päivi Tynninen is a Researcher at F-Secure's Security Labs. She primarily focuses on monitoring the threat landscape by doing threat intelligence, malware analysis, and reverse engineering. More specifically, her expertise lies in following prevalent threats such as botnets, banking Trojans, and ransomware. Päivi has a MS in Computer Science with a major in Information Security from Aalto University in Finland.