STEVEN R. OCEPEK, CISSP

1639 Ohio Avenue Cuyahoga Falls, OH 44223 330-289-4140 socepek@fastmail.net

CERTIFICATIONS

- CISSP, #91033, May 2009
- GIAC Reverse Engineering Malware (GREM), #3833, Feb 2014

PATENTS

- Security Apparatus and Method for Local Area Networks (US Patent 7,124.197).
- Peer Connected Device for Protecting Access to Local Area Networks (US Patent 7,448,076).
- Security Apparatus and Method for Local Area Networks (continuation) (US Patent 7,499,999).
- Detection of Wireless Devices (US Patent 7,570,625).
- Sled-Based Injection – method of testing network protocol for resilience to specific method of attack (US Patent 8,756,697).

PRESENTATIONS & WORKS

- Thotcon, "Synspotting for Teenagers and Real Swinging Adults" Exploration into network traffic visualization, utilizing low-fidelity visuals that depict the entire Internet address space by Autonomous System Numbers, 2015. https://github.com/nosteve/synspot
- RSA Security Conference, "Cloudy with a Chance of Sploits" Research presented on code supply chain security concerns, including live demonstration of malicious app injection, 2013.
- Black Hat USA, "BeEF Injection with MITM" Released "shank" tool to demonstrate attackers' ability to takeover systems connected to insecure networks, 2012. https://github.com/SpiderLabs/beef_injection_framework
- DEF CON, "Blinkie Lights" Empowering users to monitor and detect malicious behavior, 2011. https://github.com/SpiderLabs/cerealbox/
- Black Hat Europe, "Oracle Interrupted" Released "thicknet" tool to intercept and manipulate Oracle database traffic, 2010. https://github.com/SpiderLabs/thicknet

CORE COMPETENCIES

- Security Research
- Penetration Testing / Security Tools
- Incident Readiness and Response
- Patents / Intellectual Property
- Prototyping / Software Development
- Documentation / Technical Writing
- Training / Team Building
- Communication / Presentation

PROFESSIONAL EXPERIENCE

SCATTER
Washington, DC 2015 Oct - Present
Threat Intelligence and Privacy Product Development
CTO / Professional Services

- Startup company focused on development and integration of intelligence and privacy solutions
- Providing professional services in the areas of threat intelligence, security research, and tool development

SECURESTATE
Cleveland, OH 2014 Jul – 2015 Oct
Information security management consulting firm.
CTO / Incident Response Manager

- **Technology leadership** across all internal and client-facing systems.
- **Incident Response** manager and subject matter expert, providing proactive and on-demand triage and investigation services to clients.
- **Increased Incident Response revenue** through technical and business development.
- **Developed Cloud Platform** for interaction with clients, speeding delivery and revamping monetization model of platform using Amazon Web Services.

FIDELITY INFORMATION SYSTEMS
Jacksonville, FL 2013 – 2014 Jul
Multibillion dollar provider of banking software and information technology solutions.
U.S. FIS Incident Response Team (FSIRT) Manager

- **Led and expanded** U.S. FIS Incident Response Team (FSIRT) to include strategic focus areas
- **Reduced Time-to-Close** by 80% by empowering staff and streamlining processes
- **Achieved executive compliance goals** through execution of revised **Incident Response Plan**
- **Created Security Intelligence Program**, offering **proactive security awareness** to lines of business and executive staff

TRUSTWAVE SpiderLabs, (Mirage Networks, Wholepoint Corporation),
Chicago, IL 2001 – 2012
Multimillion dollar developer of network access control solutions for Fortune 500, education, financial, healthcare, high tech, and government entities. (Mirage acquired by Trustwave in 2008.)

Director of Security Research, Trustwave SpiderLabs, Chicago, IL	2010 – 2012
Senior Security Consultant, Trustwave SpiderLabs, Chicago, IL	2008 – 2010
Senior Software Engineer, Mirage Networks, Austin, TX	2004 – 2008
Chief Technology Officer, Wholepoint Corporation, San Francisco, CA	2001 – 2004

NETWORK SECURITY SOFTWARE / DEVICE / PATENT DEVELOPMENT

- Ensured **viability** and **profitability** of start-up of Wholepoint Corporation (network security company) by **inventing innovative software, devices,** and **solutions,** facilitating **valuation** and **acquisition** of Mirage Networks by multibillion dollar **Trustwave.**
- **Awarded 5 patents,** with one patent pending, and served as **trusted advisor** with patent attorney on developments for Trustwave / SpiderLabs.

NETWORK SECURITY RESEARCH MANAGEMENT / TESTING / PROBLEM SOLVING

- Directed startup and growth of **Security Research Department,** from **7 to 30 researchers** and **1 to 6 teams**, **positioning as trusted expert in network security** by developing, introducing, and enhancing:
  - Replacement of third-party with **in-house**, **more effective, higher quality scanning platform**, **saving hundreds of thousands of dollars** annually in licensing fees for **1+ M clients**.
  - Payment Card Industry **Authorized Scanning Vendor Certification** (ASV).
  - **Intelligence feeds** with **daily email alerts** (new stream of revenue) based on risk gathering, and commercial support of ModSecurity, most widely deployed web application firewall in world.
- **Supported SpiderLabs Incident Response** capability, working closely with Forensics unit to **reverse malware and perform technical forensics work** as needed.
- **Collaborated**, as network security expert, with company **Forensic / Incidence Response Team** and **US government protection** and **security agencies** to **enable detection** and **resolution of malware**.