Brown R. Farinholt

CONTACT

Voice: (804) 814-9556 *Email:* brown@farinholt.com *Web:* https://brownfarinholt.com

INTERESTS

I enjoy system building and data analysis with a focus on eCrime and computer security. My graduate research and recent professional experience center around building complex pipelines for data acquisition, processing, and analysis. I find the challenge of developing practical, data-driven solutions to security problems rewarding, particularly towards understanding and preventing eCrime.

EDUCATION

University of California, San Diego, La Jolla, California USA

Ph.D., Computer Science (Computer Engineering), 2019 – Advised by Dr. Kirill Levchenko
M.S., Computer Science, 2015

Clemson University, Clemson, South Carolina USA

B.S., Computer Engineering, 2013 – Magna Cum Laude with General & Departmental Honors

RESEARCH EXPERIENCE

University of California, San Diego, La Jolla, California USA

Malware & eCrime Research **June, 2014 - September, 2019**

Analyzed remote access trojan (RAT) malware and associated operator behavior and criminal activity. Reverse engineered RAT C&C protocols. Studied the criminology of eCrime actors. Built and still operate a system that perpetually collects new RAT IoCs from various sources online and performs **Internet-wide scans** for their RAT C&C servers, probing them for attribution information. Designed and implemented a system for poaching malicious dynamic DNS (DDNS) domains and **sinkholing** their traffic, analyzing it for latent malware infections and other active participants. Designed and operated a system to continuously **dynamically analyze** manually-operated malware, constructing behavioral profiles of malicious actors from API logs and network traces.

Avionics & IoT Security Research **August, 2013 - September, 2019**

Investigated security topics related to consumer and commercial avionics. Built a containerized system to monitor and analyze ACARS and ADS-B traffic, and deployed using Kubernetes and GCP. Conducted security analysis of consumer-grade IoT ADS-B receivers, forced malicious firmware updates and developed traffic-spoofing iOS and Android applications. Built http://aerosec.org.

Industrial Control Systems Security Research **August, 2014 - December, 2015**

Monitored and processed DNP3 microwave traffic from power grid SCADA devices to develop a method of passive grid device identification. Presented an analysis of state-of-the-art computer-based attacks on components of the U.S. power grid for Master's thesis.

Clemson University, Clemson, South Carolina USA

Internet Censorship Circumvention Research **August, 2012 - June, 2013**

Developed a system for reporters in oppressive countries to anonymously and securely access the Internet, mimicking botnet behaviors like DNS tunneling and fast flux.

PROFESSIONAL EXPERIENCE

Lastline, Inc., Santa Barbara, CA USA

Software Engineer, Anti-Malware Backend Group **June, 2017 - August, 2019**

Back end development for the Anti-Malware and the Cloud and Networking Infrastructure teams. Designed and implemented production-grade machine learning pipeline for detection of certain malicious files based on state-of-the-art research in the area. Gained experience with technologies including Docker, Kubernetes, Elasticsearch, HDF5, and scikit-learn.

QTS Data Centers, Dulles, VA USA

Security Engineering Intern **June, 2016 - October, 2016**

Learned the challenges of securing distributed data centers from intrusion. Evaluated and oversaw the test deployment of Bromium Endpoint Protection to select company devices. Explored implementing visualization platform for IDS logs to be made available to customers.

Shockoe Mobile App Development, Richmond, VA USA

Mobile Application Developer **June, 2013 - September, 2013**

Full stack mobile application development for Android and iOS devices using Appcelerator's Titanium Mobile Development Environment. Worked on a small team of developers meeting demanding deadlines, and gained experience in graphical design and user interfacing.

Federal Reserve Information Technology, Richmond, VA USA

Information Technology Intern **May, 2012 - August, 2012**

Developed tools using Excel and VBA that expedited compilation, reformatting, and analysis of large amounts of data pertaining to application development. Produced metrics simplifying the application design lifecycle for improvement. Redesigned and implemented department website.

Currency Technology Office Engineering Intern **May, 2011 - August, 2011**

Researched and produced a whitepaper on design structure matrices, and applied my findings successfully to two major, long-term Fed projects. Worked with design engineers to improve the efficiency of certain supply chain distribution networks, focusing on complex feedback loops.

Publications

Brown Farinholt, Mohammad Rezaeirad, Damon McCoy, Kirill Levchenko. *Dark Matter: Uncovering the DarkComet RAT Ecosystem.* In submission.

Sam Crow, Brown Farinholt, Brian Johanessmeyer, Karl Koscher, Stephen Checkoway, Stefan Savage, Aaron Schulman, Alex C. Snoeren and Kirill Levchenko. *Triton: A Software-Reconfigurable Federated Avionics Testbed.* In *Proceedings of the USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, Santa Clara, CA, August 2019.

Brown Farinholt. *Understanding the Remote Access Trojan malware ecosystem through the lens of the infamous DarkComet RAT.* Dissertation, UC San Diego Computer Science and Engineering. San Diego, CA, May 2019.

Mohammad Rezaeirad, Brown Farinholt, Hitesh Dharmdasani, Paul Pearce, Damon McCoy, Kirill Levchenko. *Schrdingers RAT: Profiling the Stakeholders in the Remote Access Trojan Ecosystem.* In *Proceedings of the 27th USENIX Security Symposium (USENIX Security 18)*, Baltimore, MD, August 2018.

Brown Farinholt, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharmdasani, Haikuo Yin, Stevens LeBlond, Damon McCoy, Kirill Levchenko. *To Catch a Ratter: Monitoring the Behavior of DarkComet RAT Operators in the Wild.* In *Proceedings of the 38th IEEE Symposium on Security and Privacy (Oakland 2017)*, San Jose, CA, May 2017.

Brown Farinholt. *The U.S. Electrical Power Grid as a Cyber-Physical System: Understanding Exposed Attack Surfaces.* Research Exam, UC San Diego Computer Science and Engineering. San Diego, CA, December 2015.

Devin Lundberg, Brown Farinholt, Edward Sullivan, Ryan Mast, Stephen Checkoway, Stefan Savage, Alex C. Snoeren, Kirill Levchenko. *On The Security of Mobile Cockpit Information Systems.* In *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2014)*, Scottsdale, AZ, November 2014.