Paul Benoit

Security & Development

Work Experience

The Crypsis Group · McLean, VA

Full Stack Developer · June 2019-Present
Junior Security Engineer · March 2018-June 2019
Technical Intern · May 2016-March 2018

Development
Live Response Collector and Processor — Developed a Ruby web interface that generates executables to collect live response data from victim Windows, Linux, or OS X systems. The executables upload the data to AWS S3 where it is distributed to a managed Docker cluster to be parsed into plaintext logs for Splunk ingestion.
Crypsis used this tool to collect forensic data from over 100,000 systems.

Large Scale IR tool — Worked on an agile team to develop a large scale incidence response tool. Mostly responsible for agent development.
Made Go parsers for forensic artifacts including:
Shimcache, UserAssist, Recentfilecache, and Shellbags

Helped develop a PowerShell tool that uses the Office 365 API to collect relevant logs for breached mailboxes.

Created a Python script that looks for suspicious RDP connections in event logs.

Host Based Forensics
Conducted forensic examinations of Windows, Linux, and OS X systems.
Timelined Indicators Of Compromise (IOCs), and wrote reports to give to clients about forensic findings.

Analyzed PHP web shells and malicious PowerShell scripts.

Business Email Compromise Analysis
Used Splunk to analyze Microsoft Office 365 logs from breached mailboxes.

Data Discovery
Used Spirion and regex to find PII on breached systems and mailboxes.

Contact

Vienna, VA
(703) 887-0443
benoitpaul6@gmail.com
github.com/thepaulbenoit

Education

May 2019 **Bachelor of Science**
Cyber Security Engineering
George Mason University

Activities

Mason Competitive Cyber · 2016-2019
Founder & Vice President

Founded a club at GMU for participating in cyber competitions like CTFs, CNDs, and wargames. By the time I graduated we had 600+ members in our Slack

Cyber Competitions
Virginia Cyber Fusion 2018 - 1st place
Capital One GMU Wargame 2017 - 1st place
Sevatec GMU Hackathon 2018 - 1st place
Multiple Top 100 placements in online CTFs

Side Projects
Python tool that automatically solves simple steganography CTF challenges

paulbenoit.com
Serverless personal website in Go

Technical Skills

Languages
Python, PowerShell, Ruby, Visual Basic, PHP, Go, HTML, SQL, C

Applications/Frameworks
Git, VMware, AWS, Docker, Splunk, Nmap, Nessus, FTK, Wireshark, Spirion, EnCase, Osquery, GRR

OS Experience
Linux (Ubuntu, Debian), OS X, Windows