Jacob Pimental

Sr. Incident Response Analyst—GCIH Certified

Summary and Objective

I am an Incident Response analyst at T. Rowe Price. My typical responsibilities include handling security incidents for the SOC. I am looking to shift my focus towards malware analysis and reverse engineering. In my free time I maintain the blog Goggle Headed Hacker where I publish malware analysis reports and CTF writeups.

Contact Info

717-574-5092

Jacob16682@gmail.com

JacobPimental

@Jacob_Pimental

/in/jacobpimental

goggleheadedhacker.com

Experience

- **Sr. Incident Response Analyst: T. Rowe Price (June 2019—Present)**
  - Investigate host-based and network-based intrusions across the global enterprise utilizing disk and memory forensics, PCAP Analysis, and log review in Splunk
  - Designs and implements Carbon Black watchlists, Yara Rules, Splunk alerts and dashboards based on previous incidents, threat hunting, and threat intelligence
  - Analyze malware samples to identify new tactics and techniques, pull out suspicious IOCs, and develop alerting for techniques used
  - Work with Splunk as a SIEM to hunt for suspicious activities, design alerting, and identify threats across the global enterprise
  - Lead the Blue Team during Red Team exercises to test controls and provide feedback for current visibility across the network
  - Utilize data analytics skills to develop advanced Splunk controls for tactics such as beaconing hosts and possible DDoS attacks
  - Develop workflows and process documents to assist IR Analysts in triaging different ticket types

- **Sr. Cybersecurity Engineer: T. Rowe Price (June 2018– June 2019)**
  - Manage Nessus Scanners firmwide to schedule vulnerability scans across the firm's networks to create tasks for app owners to remediate findings
  - Used terraform to automate the deployment of applications to the cloud and easily document infrastructure in a git repository
  - Developed new IR Ticketing System using ServiceNow's SecOps platform
  - Automate Nessus Scanner Deployment across the firm using terraform, Tenable IO's API, and Python
  - Automate the process of standing up Elasticsearch cluster to ingest flow log data

Skills

- **Reverse Engineering/Malware Analysis**
  - Uses Radare2/Cutter or Ghidra to statically analyze malware samples collected from public sandboxes or honeypots
  - Uses Ollydbg, x64dbg, and GDB to dynamically analyze and debug malware and applications in a virtual environment
  - Uses Wireshark and Tcpdump to monitor network traffic caused by running malware and applications throughout the reversing process
  - Developed plugins for Radare2/Cutter to automate analysis processes such as string decryption or anti-obfuscation
  - Developed scripts to automatically unpack applications to speed up analysis
- **Incident Response**
  - Knowledge of using a SIEM, such as Splunk
  - Familiar with Carbon Black Response to perform endpoint investigations
  - Created workflows to help guide IR analysts through different incident types
  - Worked on SOAR projects to automate response tasks such as IOC blocking
  - Performed PCAP Analysis to identify different web attacks
  - Utilized basic data analytics skills to develop alerts for beaconing activity and potential DDoS attacks
  - GCIH Certified for incident handling
- **Development Experience**
  - Learned to design video games from scratch using C/C++ and the OpenGL, SDL frameworks
  - Uses Python extensively for most development work for classes, work, and malware analysis
  - Used Javascript at T. Rowe Price to develop automation workflows and IR Ticketing system in Service-Now
  - Learned Assembly from books to become better at Reverse Engineering, also uses it to develop shellcode for exploits
  - Developed webscraping tools to identify and report on potential Magecart infections on e-commerce websites
- **CTF**
  - Was a part of Team Contagion, RIT's CTF group
  - Specializes in Reverse Engineering and CrackMe challenges
  - Part of UltraMegaChicken, a local CTF group in Maryland
    - Recently came in 1st place at Parsons CTF
  - Part of UMGC's CTF Team
    - Recently came in 1st place at MAGIC CTF

Jacob Pimental

Sr. Incident Response Analyst—GCIH Certified

Summary and Objective

I am an Incident Response analyst at T. Rowe Price. My typical responsibilities include handling security incidents for the SOC. I am looking to shift my focus towards malware analysis and reverse engineering. In my free time I maintain the blog Goggle Headed Hacker where I publish malware analysis reports and CTF writeups.

Contact Info

717-574-5092

Jacob16682@gmail.com

JacobPimental

@Jacob_Pimental

/in/jacobpimental

goggleheadedhacker.com

Trainings and Conferences

- **SANS GIAC Certified Incident Handler (Oct. 2019)**
  - Received certification for handling security incidents
  - Demonstrated knowledge of red team tools and techniques during CTF challenge
  - Won the final day's CTF challenge and was awarded the course's challenge coin
- **Speaker at SourceDefense Webinar (2020)**
  - Spoke about techniques used to hunt for Magecart infections in the wild
  - Created tool to automate the task of scraping the web for Magecart infections
  - https://youtu.be/N61_aX8uXI4
- **BSidesRoc (2018 and 2017)**
  - **Save Our Splunk (April 2018)**
    - Learned how to set up Splunk to view logs and search for threats. We also learned how to output the information as graphs to display to clients or management.
  - **YARA Training (April 2017)**
    - Learned how to set up Yara to detect malicious files and write signatures for Host-Based Indicators of Compromise.

Education

- **University of Maryland Global Campus (2019-Present)**
  - Completing Bachelor's of Science in Cyber Security and Development
  - Participating in the UMGC CTF Team

- **Pennsylvania College of Technology (January 2018-June 2018)**
  - Pursuing Bachelor's of Science in Computer Security
  - **Clubs**
    - Information Security Association (ISA)
    - Association for Computing Machinery (ACM) where I gave presentations on exploits and malware analysis.

- **Rochester Institute of Technology (2016-2017)**
  - Studied Computer Security and participated
  - **Clubs**
    - Rochester Cybersecurity Competition Club (RC3)
    - Security Practices and Research Student Association (SPARSA)
    - Team Contagion, RIT's own Capture the Flag group.