

# Joseph Giron

6611 N 89<sup>th</sup> Ave • Glendale, AZ 85305 • (512) 902-3787 • [joe@gironsec.com](mailto:joe@gironsec.com)

## Objective

Dedicated Problem Solver, looking for exciting new challenges. Brings strong background in programming languages and application security, looking for an opportunity to work with a team to lead and teach new skills. Strong malware analysis and reverse engineering background with emphasis on x86/x64 Intel assembly. Excellent background in exploit development.

## Certifications

- Security+
- CEH
- CEMA

## Speeches

- InfoSec Southwest 2012 – Writing your own debugger in C
- Toorcon 2012-2016 – Malware reverse engineering how-to
- CactusCon 2013- 2017 – Exploit / Reverse engineering how-to
- HOPE 2014 – Exploiting McAfee

## Technical Skills

### Software:

HyperV, MSSQL, MySQL, FireEye, Visual Studio, Hailstorm, BurpSuite, IDA Pro, Ollydbg, Immunity Debugger, Metasploit Framework, Apache, IIS, Active Directory, ColdFusion, McAfee EPO, LastLine, Vmware / VirtualBox / Qemu, Volatility, Bindiff, HP Fortify, Checkmark, AWS, Cloud based computing, Azure

### Operating Systems:

Windows Server 2k-2k12 / Linux (FreeBSD, Ubuntu, RHEL, Debian, CentOS, FreeDOS, etc)

### Programming Languages:

C, C++, C#, PHP, Perl, Visual Basic, Python, Intel asm (x86/x64), Ruby

### Special Skills:

Reverse Engineering (malware), Source code analysis, Incident Response, PCI compliance testing, vulnerability management, risk assessment, penetration testing, software development.

### Github:

<https://github.com/joseph-giron>

## Professional Experience

### **LunarLine Inc**, Washington, DC

Senior Penetration Tester

Mar 2016 – Present

- Worked primarily performing penetration tests on various government clients.
- Made extensive use of SQLMap, BurpSuite, Metasploit, Nexpose, masscan, nmap, SoapUI, WebScarab, and SET, depending on the engagement.
- Performed social engineering engagements, phishing attacks, recon, physical assessments, and web based attacks.
- Trained lower level employees on the basics of security, reverse engineering, and penetration testing.
- Threat intelligence gathering
- Worked on Mobile app pen testing on android and IOS devices.
- Source code analysis of Perl and .Net technologies
- Worked with the federal government and US Court and PACERNET systems.

### **Wells Fargo**, Phoenix, AZ

Red Teamer (Contractor / part time)

Sept 2018 – May-2019

- Web application pen testing utilizing BurpSuite and W3AF.
- Performed external network discovery and OSINT for Wells Fargo's external assets
- Did programming and scripting for projects related to the red team for the purposes of discovery and acquisition of new targets / attack surfaces

### **Megaplan-IT**, Phoenix, AZ

Senior Penetration Tester (Contractor / part time)

Jun 2016 – Sept 2018

- Source code review in many languages including; java, python, php, C#, perl
- Web application and network penetration testing
- Mobile application penetration testing as well as mobile code review
- Performed Incident response and forensic investigations
- Heavy usage of BurpSuite and HP Fortify
- Worked on cloud-based environments such as MS Azure and Amazon Web Services.

### **LastLine** , Santa Barbara ,CA

Malware Reverse Engineer

Mar 2015 – Feb 2016

- Primarily work with IDA pro, qemu, and ollydbg to reverse engineer malware and exploits threats in both the user-land and kernel mode space.
- Develop signature matching algorithms in python, YARA, and FLIRT for binary matching and differential analysis of malware signatures.
- Dissect 0day threats and malware from APT's and threat actors across the world to deliver the latest and greatest threat research.
- Publish blog posts about malware analysis and threat research.

### **Synack Inc**, San Diego,CA

Security Red Team

Dec 2014 – Jan 2016

- Performed web app penetration tests and collect bug bounties for various clients.
- Work primarily with BurpSuite and NetWitness.
- Have collected bounties for various items such as SQLI, XSS, CSRF, and code injection.

**American Express**, Phoenix, AZ  
Malware and Forensics Security Investigator

Dec 2013 – Oct 2014

- Was the chief malware / reverse engineer for Amex.
- Regularly performed training for analysts and engineers alike.
- Did special projects and research and performed penetration tests within the internal network.
- Performed threat intelligence gathering from various APT's and
- Developed internal malware database as well as internal tools for the analysts to aid in the detection / prevention of malware.
- Worked with various departments to implement policy changes to strengthen defenses and limit compromise.
- Performed forensic investigations for special cases / management compromises.

**American Express**, Phoenix, AZ  
Security Analyst

Jun 2013 – Dec 2013

- Administered full disk encryption with Open PGP on all assets.
- Monitored network for DDOS traffic with trending tools like FrameFlow and Prolexic.
- Worked with FireEye and EPO to document and analyze malware for incident reporting and root cause analysis.
- Wrote snort rules and administered McAfee IPS / HIPS policies.
- Reverse Engineered malware and trojans using both static analysis tools (like IDA and BugDB) as well as dynamic analysis with tools like Immunity Debugger, Exe Suite, and various unpacking frameworks.
- Tested IPS / HIPS / IDS rules with Metasploit framework for tuning and adjustment of rules & alerts.