

EXHIBIT 1

Rodelio G. Fiñones

529 Ewen Avenue,
New Westminster, BC, Canada
V3M 5B7
Office: +1 (604) 247-6064
Mobile: +1 (604) 551-1294
Personal: rfinones2015@gmail.com / rodelfinones@jilcanada.com
Office: rfinones@microsoft.com

Objective:

To acquire a rewarding career in the field of computer and internet security where my expertise, experience, and knowledge in malware security will be utilized to contribute to the success of the company.

PROFESSIONAL EXPERIENCE:

Senior Antivirus Researcher / Strategist (September 2014 – Present)

Microsoft

- Handle customer samples to provide analysis, detections, advice, and remediation.
- Lead the team on focus research of different categories of malwares such Botnets, Clickfraud, MSIL, and Spambots to provide different kind customer protection such as sourcing, protections (File, memory, and cloud-based, behavior-based, and etc.). Also includes identifying the malware infection chain and monetization.
- Design and develop tools and automation projects for unpacking and tracking botnets.
- Utilize big data to analyze malware treat landscape and to better protect the customer.
- Lead team and hands on research on prevalent malwares for CME (MS Collective Malware Eradication) to disrupt/eradicate malwares.
- Drive research to improve Windows platform features.

Senior Antivirus Researcher (June 2009 – September 2014)

Microsoft

- Handle customer samples to provide analysis, detections, advice, and remediation.
- Focus research on different categories of malwares such Botnets, Clickfraud, MSIL, and Spambots to provide different kind customer protection such as

sourcing, protections (File, memory, and cloud-based, behavior-based, and etc.). Also includes identifying the malware infection chain and monetization.

- Utilize big data to analyze malware treat landscape and to better protect the customer.
- Reverse engineering various types of malwares and exploits.

Principal Software Developer / Researcher (Dec 2007 – June 2009)

Fortinet Technologies (Canada), Inc.

- Improved signature-based detection algorithm to support more complex malwares. Detection methods such as x-raying and behavioral and characteristics detections.
- Research and develop AV engine features to support packer through script-based. Generic unpacker coupled with script-based unpacker will be a powerful and effective solution for most malwares.
- Handle complex malwares analysis and detection through script-based or hard-coded.
- Improvements and optimizations for Fortinet's AV detection algorithms.
- Provide technical knowledge to new AV analyst.

Senior Antivirus Analyst / Engine developer (May 2004 – Dec 2007)

Fortinet Technologies (Canada), Inc.

Analysis, Research and Development Projects

- Research, design, and develop the clean engine for Fortinet's desktop Antivirus product. It supports cleaning Win32 PE, Office, DOS, and script formats.
- Improve the scanning technology through research and development of new scanning algorithm that suits for complex viruses.
- Fix bugs and AV scan and clean engine limitations
- Participate in the research, development, and improvements of Win32 emulator engine.
- Create detection module for hard to detect viruses such metamorphic, polymorphic, and EPO viruses.
- Improved the scanning technology for scripts malwares.
- Research, design, and develop an automated system to replicate, analyze, and heuristically detect known and unknown malwares through sandboxing technology.
- Handle complex malwares.
 - Analysis
 - Creating detection signatures
 - AV Engine support (if necessary)

Other Tasks:

- Provide malware related technical expertise to analyst and product development team.
- Create documentation for developed systems.
- Conduct trainings regarding virus analysis, detection and disinfection algorithm.
- Provide quick and quality solution to customer problems.
- Configure replication system for any kinds of malware

Senior Anti-Virus Researcher / AV Engine Developer (Nov 1999 – April 2004) Trend Micro, Inc. (Anti- Virus and Internet Security)

AV Trainee

- 3-month extensive virus / malware training. Include analysis and creation of detection and clean signatures.

AV Technical Support Engineer

- Provides complete solution to the customer.
 - Provides scan and clean solution. Includes signature to remove system infections such as registry, system files, process, services, and files.
 - Create detailed / comprehensive virus description and manual removal instructions.
 - Provides other assistance needed by the clients.

AV Research Engineer

- Focus on the detailed / comprehensive analysis of Windows viruses.
- Process escalation cases from Virus support engineers.
- Conduct technology upgrade trainings to Virus support team (New virus technology; new Scan / Clean feature).
- Respond to Virus Alerts
- Develop removal tools for specific malware.
- Design and develop TSC (Trojan System Cleaner). Engine module to detect and restore system infection through registry, process, system files, and services.
- Process Scan / Clean Engine related cases.
- Analyze exploits and system vulnerabilities (Windows & Linux).
- Research and develop a system for automating the replication of malware that covers controlled and simulated Internet environment
- Research and develop Scan/Clean Engine modules:
 - Metamorphic virus support
 - Win32 virus clean modules
 - New file formats support
 - Trojan System Cleaner
 - Compression / Packer engine support (UPX, Petite, and PEPack)

Extra

- Develop a network scanner tool that runs in either a gateway mode or as personal IDS. This is a company-wide contest and we were able to get in the final 6 out of 15 contestants.

TECHNICAL SKILLS:

- Advance knowledge and experience in reverse engineering any kinds of malware using debugger (Soft-ice, IDA Pro, OllyDbg, and Immunity debugger)
- In-depth knowledge and experience in exploits and vulnerabilities.
- Strong knowledge and experience in creating comprehensive virus description.
- Strong experience in developing detection and cleaning engine for different kinds of malware such as virus, worms, Trojans, and spywares.
- In-depth knowledge in windows operating system internals.
- In-depth knowledge and experience in virus, Trojans, worms, and spywares behaviors.
- Experience in TCP/IP networks, Unix/Linux networks (AIX, Redhat, Slackware, Ubuntu), Windows network (Windows 9X/NT/2K), Novell Netware. Background knowledge in Windows CE, Palm, and EPOC operating system.
- Advance experience in C and DOS/Win32 Assembly, VB Script, JavaScript.
- Experience in C++, Linux shell scripts, PowerBuilder, and SQL programming.
- Intermediate experience in analyzing and testing various Anti-virus products.
- Experience in using soft-ice debugger, IDA Pro, OllyDbg, Snort, and Ethereal.
- Intermediate knowledge in network protocols like TCP/IP, IPX/SPX, SMTP, FTP, HTTP, DNS, NTTP, and MAPI32.
- Intermediate knowledge in Windows and Unix/Linux system and network security.
- Knowledge in ASP, MS Access, FoxPro, and HTML.
- Knowledge in IP chains/tables, Ethereal packet sniffer, Snort IDS, Tripwire integrity checker.
- Knowledge in Lotus Notes and Domino server
- Have a strong problem-solving ability, reliability, team player and hard working.
- Experience in python and Django web framework.

PREVIOUS EMPLOYMENT:

System analyst / Programmer (July 1999, October 1999)

Gestalt Consulting Inc. (PowerBuilder and MS SQL)

- Create, maintain, and improve Inventory system and Accounting system.
- Provide support to problem of clients.
- Review and document the current application system.

EDUCATION:

Bachelor of Science in Computer Engineering (1995 -1999)
East Asia College of Information Technology, May 1999, 3.2/4.0 GPA

Secondary Education (1991 - 1995)
Gregorio Perfecto High School

Primary Education (1985 – 1991)
Magat Salamat Elementary School