Fyodor Yarochkin, PhD

fygrave | fygrave | www.o0o.nu | fygrave@gmail.com | +886920811510

Summary

Highly motivated Threat Intelligence Data Analyst. Seniour Information Security Researcher with over 20 years in the field including more than 10 years of penetration testing and security assessment experience. Over 20 years in network intrusion detection and data analysis. Cross domain knowlege of large-data analysis and threat intelligence. Strong unerstanding of underground emerging threats and technologies, threat actor and campaign tracking, analysis, attribution and investigation. PhD in Computer Science. Fluency in Russian, Chinese and English (written and spoken)

Work Experience

Trend Micro, Taiwan, Senior Threat Researcher Jan 2017 - present

My primary role at Trend Micro is threat researcher. Being Part of FTR (forward looking threat research) team I focus on cybercrime and targeted attacks investigations, using AWS/big data analysis to process and analyse Smart Protection Network (SPN) feedback and identify, trace and monitor threat actor acitivity. Worked on a number of projects including:

- web3 and blockchain related threats
- investigation and analysis of web3 scam campaigns
- BEC(business email compromise) campaigns investigations and monitoring
- ransomware data science and analytics
- monitoring of prominent ransomware groups
- threat to cloud infrastructure and cloud platform vulnerabilities, including AWS, Azure, Kubernetes.
- large scale twitter analytics, bot detection and disinformation research
- supply-chain attacks against android devices, including investigation of criminal groups, monetization techniques, analysis of fraud from SMS PVA services and pro-active monitoring of the criminal group activities
- monitoring and investigation of several criminal and target groups covering Asia-Pacific and Eastern Europe regions, law enforcement collaboration
- investigation into bullet proof hosting and residential proxies ecosystem
- investigation of threats in 5G and industrial networks
- Investigation into APT campaigns in middle east involving android devices, analysis and profiling of endpoints and identification of CAV (counter-AV) services.

vArmour Inc, Senior Threat Analyst April 2014 - Dec 2016

My primary role at vArmour was research and development of network detection techniques using the feedback logs of vArmour flagship products. My responsibilities at vArmour included:

- Threat Research: monitoring for malware outbreaks, evaluating vulnerabilities, prototyping network detection mechanisms.
- Design and Evaluation of a Scalable Threat and Security Analytics System.
- Maintenance of Threat Analytics Backend Platform.
- Prototyping and Development of Stream Event Processing Security Engine.
- Handling of Incident Response and Forensic Analysis cases.

Plurk, Network and Security Engineer December 2012 - April 2014

My primary interest of joining Plurk was to learn more about big data analysis and social networks. My responsibilities included everything from database management, system administration, firewall configurations, configuration recovery and intrusion detection and monitoring. This was my part-time role.

Academia Sinica, Research Assistant December 2012 - April 2014

Responsibilities: Primarily resposible for Research and Development of Information Security Portal, including development malicious software analysis platform, threat assessment platform, automation for vulnerability assessment platform.

- Developed a scalable platform for risk assessment of large network infrastructures.
- Developed an evaluation platform for malicious software analysis using sandboxing technology.

Armorize Technologies, Security Analyst January 2007 - December 2011

Responsibilities: Develop and support components of Automated Vulnerability Assessment Platform, support Malware Analysis Team (building and evaluating automated malicious software components), Support Penetration Testing team (building automated tools for penetration testing and results processing), Support Static Source Code Analysis Team (security policies review, customer support, manual source code audits)

- Developed components for automated scalable Vulnerability Assessment Platform (python/C/ custom scripting languages/Java/Erlang).
- Built automated javascript deobfuscation components (python/C).
- Developed ICAP integration with Anti-Virus scanning platforms (python/C).
- Built various protocol integration components (SOAP, SMTP) (python).
- Buiilt and maintain Information Security Assessment Data Management System (ruby on rails/ HTML/AJAX/Javascript).
- Conducted several information security training courses (Code Auditing and Code Security, Disk Forensics, Network Forensics, Information Security for a pen-tester, Wireless Security, RFID and Bluetooth Security, Telecom Security)

Guard-Info, Security Analyst January 2003 - January 2007

Asia-Pacific regional responsibility, performing Information Security consulting for large Banking and Finance Institutions, Insurance, Telecoms, Education, Military and Government organizations across the region with primary focus on supporting Taiwan based clients.

- Network Architecture and Application Architecture Security reviews
- Digital Forensics Services
- Remote Network Security Assessments
- System Security Assessments and Hardening
- Vulnerability Research and exploit development
- Application Security Assessments
- Reverse Engineering
- Wireless and Mobile Security Assessments
- Information Security and Web Application Security Training Courses (Instructor)
- Prototyping Security Event Management System

Trusecure Corporation, Security Analyst 2001 - 2003

Asia-Pacific regional responsibility, performing Information Security consulting for large Banking and Finance Institutions, Insurance, Telecoms, Education, Military and Government organizations across the region.

- Conducting network and host security assessments
- Conducting firewall, IDS, and network equipment security reviews
- Vulnerability mitigation and risk assessment
- Handling incident response for customers
- Remote Network Security Assessments
- System Security Assessments and Hardening
- Vulnerability Research and exploit development
- Application Security Assessments
- Reverse Engineering
- Wireless and Mobile Security Assessments
- Information Security Training Courses (Instructor)

Relay Group, Security Analyst 2000 - 2001

The company was aquired by Trusecure.
Conducted remote intrusion tests and provided security consulting services for Finance, Banking and Communication Institutions.

- Conducting network and host security assessments
- Conducting firewall, IDS, and network equipment security reviews
- Threat analysis and vulnerability research
- Research and development of internal-use security tools, innovative defensive and offensive security techniques and methodologies
- Research and development of internal-use intrusion tests automation system

Soros Foundation, Kyrgyzstan, Network and System Administrator 1998 - 2000

This was part-time employment. Responsibilities included design, implementation and system administration of network infrastructure to support regional projects of the Foundation, and covered the following:

- Design and installation of Cisco routers based WANs
- Deployment and configuration of various routing protocols in Cisco hardware-based networks
- Maintenance of Solaris2.X/BSD/Linux based networks
- Installation and security auditing of Solaris2.X/BSD/Linux systems
- Configuration/maintenance of DNS servers
- Installation/configuration of mail delivery system based on deeply customized sendmail daemons
- Installation, configuration and maintenance of news servers, web servers and transparent caching proxy servers
- Development of custom CGI scripts and various custom network daemons

Projects and Publications

Publications to be provided on request

List of publications and conference presentations can be provided on request.

Education

2006 - 2018	PhD in Computer Science at **National Taiwan University, Taiwan**
1995 - 2000	Engineer/M.Sc. Diploma at **Kyrgyz-Russian Slavic University, Kyrgyzstan**
1991 - 1995	Technical Diploma with Honours, Industrial systems and Robotics **Bishkek Technical College**

Skills

Threat Intelligence and Data Analytics	In-depth understanding of campaign tracking and tracing, familiarity with tools including Maltego (avanced use, transforms development) custom tools for campaign monitoring and detection, use of AWS data analysis tools for large scale monitoring
Big Data Processing	Building Parallel Data Processing Systems using distributed and cloud computing technology (Hadoop, JPPF, Erlang)
Red-team Experience	Intrusion testing, internal security audits, authentication and access control, firewalls, intrusion detection systems, secure programming, secure payment systems.
Research	Excellent research and development skills on vulnerability research and exposure (including development of proof-of-concept vulnerability exposure code)
System Administration	Excellent experience with UNIX security on a variety of flavors (SunOS. Solaris, HP-UX, Digital UNIX, AIX, BSD flavors, Linux). Excellent experience with Windows NT/2000 security. Advanced knowledge of Cisco equipment, network protocols and technologies. Excellent experience with various clones of Firewall and IDS systems (CheckPoint, Cisco PIX, Raptor, RealSecure, Dragon IDS, NFR)