Fan (Lily) Wu

(+86)18458308420 | fwu5226@gmail.com

Work Experience

Meituan
Expert Security Engineer 2022.09 – Present

- Establish and maintain systems to capture intelligence and identify potential threats to safeguard, user data, corporate assets, and business operations
- Actively drive the remediation of vulnerabilities by collaborating with cross-functional teams

Alibaba Cloud
Senior Security Engineer 2018.02 – 2022.09

- Detect and analyze network-based threats, perform root cause analysis of security incidents, and provide recommendations for remediation.
- Conduct simulated attacks on infrastructure and defense systems (e.g. WAF) to validate security controls and identify potential risks

Project Experience

Development and Operation of Threat Intelligence Platform 2022.09 – Present

- Collaborate with a team to develop and operate a Threat Intelligence Platform. Implement data sourcing, curation, and filtration processes as part of the platform development
- Utilize LLM chains to effectively label risky information and eliminate noise, significantly enhancing operational efficiency
- Develop and optimize algorithms to enhance the accuracy and effectiveness of threat identification and analysis within the platform

Governance of Misuse and Fraud 2022.09 – Present

- Develop strategies for monitoring and preventing product misuse and fraudulent activities.
- Collaborate with law enforcement authorities to address and investigate serious cases involving criminal activities.

Attack Simulation and Enterprise Security Posture Assessment 2021.04 – 2022.09

- Develop an attack simulation platform, integrating hundreds of attack techniques and tactics, to assess the overall security posture based on the effectiveness of detection alarms and response capabilities
- Randomly test the business with attack scenarios and attempting to bypass defense and detection mechanisms to uncover any failures in security controls and enhance the security posture

Develop Security Capabilities for Network-based Security Products 2019.12 – 2022.09

- Conduct threat modeling and implement defense rules to protect against various attacks
- Design and develop "Smart ACL" functionality with AI technologies to assist clients in adhering to best practices and enforcing safe policies
- Recognition in Gartner Magic Quadrant as one of the "Challengers" and positive reviews received for my featured contributions in industry reports

Threat Detection and Root Cause Analysis of Incidents 2018.02 – 2019.12

- Conduct threat detection and root cause analysis of incidents by analyzing event and network flow logs, including the extraction of signatures to form security rules
- Analyze events and research potential causes using, providing recommendations for remediation plans
- Proactively detect and prevent emerging massive malicious campaigns on the cloud at their early stages

Internship

Qihoo 360 Technology Co. Ltd
Intern Engineer 2015.07 – 2015.09

- Manage and operate a bug bounty platform to assess the effectiveness of vulnerabilities reported by white hat pen-testers.
- Collaborate with relevant enterprises to ensure the timely resolution of identified vulnerabilities

Education

The University of Hong Kong
Master of Science in Computer Science 2016.09 - 2018.02
- Research Assistant (RA) in a project focused on Concurrency Attacks

People's Public Security University of China
Bachelor of Engineering in Cyber Security 2012.09 - 2016.06
- Recipient of the Meiya Pico Scholarship

Skills

- Experienced in cloud infrastructure and business security, including vulnerabilities' cause, impact, prevention methods and remediation. Experienced in red-teaming, reverse engineering, etc
- Experienced in Python (including PyTorch, LangChain, Pandas), Java, C/C++, HiveSQL. Familiar with GoLang, LaTex.
- Fluent in business English, TOEFL 107

Patent & Pivotal Technology

- Attack filtering based on web shell signatures and traffic pattern (patent number CN110943961B)
- A new threat model from attackers' perspective (Recognized as a pivotal technology of the company)

Technical Talks

- < Endoscope: Unpacking Android Apps with VM-Based Obfuscation> @ Black Hat USA Link
- <Security Posture Assessment with Breach and Attack Simulation Platform> @ 2022 FreeBuf Cyber Security Innovation Summit
- <Detection and Defense against Massive Attacks on the Cloud> @ 2021 Beijing Cyber Security Conference Link

Published Technical Articles

- <Breaking the Validation and Exploitation Chain of Log4j RCE Vulnerability> (in Chinese) Link
- <AutoUpdate Botnet is Spreading on the Cloud, Stealing Users' Access Keys> (in Chinese) Link
- <Zero-Day Attack Analysis and Dissemination Method Disclosure for Hadoop Yarn RPC> Link
- <Warning of danger: PHPCMS type.php Code Injection Vulnerability> (in Chinese) Link
- <New Miner Hijacker RDPMiner Adds Malicious Accounts to Victimized Hosts> Link
- <2018 Cloud-Based Cryptocurrency Mining Hijacker Report> Link
- <New ibus Backdoor Exploit Vulnerabilities and Crypto hijack for Profit> (in Chinese) Link
- <Database-Cracking Watchdogs Mining Worm: Issues and Countermeasures> Link
- <ImposterMiner Trojan Takes Advantage of Newly Published Jenkins RCE Vulnerability> Link
- <Xulu: Cryptojacking Leveraging Shodan, Tor, and Malicious Docker Container> Link
- <ProtonMiner Gains Momentum via Expanded Attack Surface> Link

Honors

- Second Prize in recognition of Alibaba Cloud Technical Influencer
- Leaded "Kung Pao Chicken" CTF team to play in multiple Capture-the-Flag competitions. Ranked top15 nationally (2017, according to XCTF)
- Meritorious Prize in Mathematical Contest in Modeling (MCM)
- First prize in Lanqiao Cup programming competition (Java)

0day Vulnerability

Discovered and responsibly reported following vulnerabilities:
- Hadoop RPC Unauthorized Access (2021, can cause Remote Command Execution, captured in-the-wild)
- CVE-2018-19127 PHPCMS Template Injection (Can cause Remote Command Execution, captured in-the-wild)
- CVE-2017-7533 Linux Kernel Race Condition (Local Privilege Escalation), CVE-2017-12193 (Denial of Service)