Kyuhong Park

Security Researcher · Malware Analyst

756 W Peachtree St NW, Atlanta, GA 30308

https://www.linkedin.com/in/davidkpark302/

Summary

Interests: Static and Dynamic Malware Analysis, Runtime Detection, System Security, Cloud Security.

Passionate about developing scalable security solutions through real-world data analysis and advanced research. Specializing in static and dynamic malware analysis, runtime detection, and cloud security, I design and implement proactive defense mechanisms to detect and mitigate sophisticated threats. I enjoy uncovering complex attack patterns that traditional methods often miss by leveraging binary analysis, threat intelligence, and machine learning-assisted detection. My expertise in analyzing large-scale datasets and cloud-based security telemetry enables the development of resilient security solutions, improving detection accuracy and response capabilities in modern computing environments.

Work Experience

Scalable Runtime Detection for Cloud and Linux Security

Atlanta, GA

GuardDuty, Amazon Web Services (AWS) *Feb 2024 – Present*

- Designed and implemented runtime threat detection rules leveraging eBPF-based monitoring to detect privilege escalation, defense evasion, and persistence techniques in EC2, EKS, and containerized environments.
- Correlated security findings into attack chains, identifying multi-stage intrusions and mapping adversary techniques to MITRE ATT&CK for improved detection and response effectiveness.
- Analyzed large-scale runtime security events, refining detection logic to reduce false positives while expanding cloud threat coverage.
- Worked cross-functionally with security researchers, ML researchers, and software engineers to analyze runtime threats and develop actionable detection strategies.
- Researched and tracked emerging attack techniques in cloud environments, including container escapes, privilege escalation, and lateral movement, to enhance detection mechanisms.

Scalable Malware Detection and Threat Analysis for Cloud and Linux Security

Atlanta, GA

GuardDuty, Amazon Web Services (AWS) *May 2022 – Feb 2024*

- Developed scalable malware detection techniques to secure cloud workloads across EC2, EKS, and containerized environments.
- Designed and implemented detection rules and security heuristics to identify sophisticated Linux-based threats, enhancing real-time threat visibility.
- Contributed to a large-scale security detection system processing millions of samples, leveraging extensive datasets for optimization, validation, and deep threat analysis.
- Led malware reverse engineering efforts to uncover evasion techniques and improve detection capabilities.
- Conducted pre- and post-release validation using shadow mode evaluations and large-scale volume testing.
- Collaborated with cross-functional teams, including security engineers, threat researchers, and software developers, to refine detection strategies and enhance system resilience.

Hybrid Malware Binary Rewriting for Penetration Testing

Atlanta, GA

Georgia Institute of Technology *Dec 2019 – Apr 2022*

- Led a research collaboration with Cisco Research to develop a hybrid binary rewriting framework that semi-automatically exposes hidden malicious behaviors in x86 and x86-64 malware.
- Designed and validated penetration testing methodologies using rewritten malware binaries to assess system and network security defenses.
- Built a secure testing environment leveraging Qiling (emulation-based malware sandbox) and DynamoRIO within a virtual machine, ensuring controlled execution by intercepting and monitoring write-related API calls.
- Developed a binary analysis pipeline integrating DynamoRIO, IDA Pro, and Binary Ninja to extract binary insights, identify hidden malicious behaviors, and modify binaries for targeted security assessments.

Automated Detection of Behavior Dispatchers in Malware

Atlanta, GA

Georgia Institute of Technology *Aug 2018 – Dec 2019*

- Developed an automated detection platform to identify triggering conditions in PE and ELF malware, uncovering C&C logic and antivirus evasion tactics through behavior dispatching pattern analysis.
- Integrated static and dynamic analysis tools (DynamoRIO, IDA Pro, Binary Ninja) to enhance malware behavior exposure and improve automated triage workflows.
- Applied the platform to 3,943 real-world malware samples, validating detection accuracy through reverse engineering and manual verification.

Reproducible Malware Analysis and Experimentation Framework

Atlanta, GA

Georgia Institute of Technology

Aug 2015 – Aug 2018

- Led a research collaboration with Lockheed Martin Security Research to develop a reproducible malware analysis framework using Vagrant, virtual machines, and Git.
- Designed and implemented an active containment system to neutralize targeted malware behaviors by isolating network activity, ensuring safe analysis environments.
- Developed detection mechanisms for XOR-based cryptographic algorithms and obfuscated code, enhancing malware decryption and reverse engineering workflows.

Skills

Cloud & DevOps	AWS, Docker, Vagrant
Threat Detection & Analysis	MITRE ATT&CK, YARA, Suricata
Disassembler and Debugger	BinaryNinja, IDA Pro, Ghidra, x64dbg, WinDBG, GDB
Programming	Python, C, C++, LaTeX

Publication

DeepReflect: Discovering Malicious Functionality through Binary Reconstruction

San Francisco, CA

USENIX Security Symposium (USENIX 2021)

August. 2021

- DeepReflect, tool for localizing and identifying malware components within a malicious binary. We use an unsupervised deep neural network in a novel way, and classify the components through a semi-supervised cluster analysis, where analysts incrementally provide labels during their daily work flow. The tool is practical since it requires no data labeling to train the localization model, and minimal/noninvasive labeling to train the classifier incrementally.

BDHunter: Identifying Behavior Dispatchers for Malware Analysis

Hong kong, China

ACM Asia Conference on Computer and Communication Security (ASIACCS 2021)

June. 2021

- BDHunter identifies dispatchers to uncover hidden malicious behaviors. By analyzing dispatching patterns, BDHunter reveals malware decision-making processes and leverages concolic execution to expose hidden malicious behaviors.

Augmenting Cyber Assessment through Dynamic Malware Analysis

Orlando, FL

I/ITSEC 2019

Dec. 2019

- This paper describe an approach on how dynamic malware analysis capability can help design a system with better cyber resiliency against existing and emerging advanced persistent threats (APT). With understanding the capability, we build a simulation enviroment to thoroughtly test and evalutate its ”what-if” cyber defensive postures relative to threats that have not been launched in the real world

Education

Georgia Institute of Technology

Atlanta, GA

Ph.D. Candidate in Computer Science, School of Computer Science

Aug. 2016 – Mar. 2022

- Research focus: Information Security and Malware Analysis under the advisement of Prof. Wenke Lee.
- Completed Ph.D. coursework and qualified as a Ph.D. candidate.

Georgia Institute of Technology

Atlanta, GA

M.S. in Computer Science, School of Computer Science

May. 2015 - Aug. 2018

- Specialty: Computing Systems and Information Security.

Georgia Institute of Technology

Atlanta, GA

B.S. in Computer Science, School of Computer Science

Jan. 2012 - Dec. 2014

- Specialty: Computing Systems and Network.

Extracurricular Activity

CyBoK - MALWARE KNOWLEDGE AREA

www.cybog.org

Writer

Jan. 2019 - PRESENT

- In-depth understanding of Malware and Attack Technologies.