Ilia Mogilin

mogiliniv@gmail.com linkedin.com/in/mogilin/ Yerevan, Armenia 🇦🇲

About me

Detection & Response Security Engineer with 6+ years of experience in threat intelligence, intelligence-driven threat hunting and detection engineering across cloud and enterprise environments.

Strong background in long-term threat tracking, malware research (macOS, iOS) and converting threat intelligence into scalable detections.

Previously at Yandex Cloud and Kaspersky, worked on identifying detection gaps, tracking threat campaigns, and improving security posture through tooling, data analysis, and cross-functional collaboration.

I like automating things using LLMs as a hobby!

Experience

SECURITY OPERATIONS ENGINEER / TI, YANDEX CLOUD; YEREVAN – JULY 2024 - NOW

- Designed and implemented threat hunting and detection rules for cloud-scale telemetry including S3 data exfiltration, IAM abuse, and anomalous network activity leading to identification of malicious and abusive cloud usage patterns;
- Introduced a Data Warehouse–based investigation approach, enabling security engineers to query historical IAM and DNS activity previously unavailable for analysis;
- Worked closely with incident responders, enriching investigations with contextual threat intelligence and translating findings into new detections;
- Deployed and operated Tetragon-based security agents across cloud infrastructure to improve file integrity monitoring and runtime visibility;

SECURITY ENGINEER (SECURITY OPERATIONS & DETECTION), YANDEX CLOUD; YEREVAN – FEB 2024 - JULY 2024

- Focused on improving detection quality and coverage by translating threat intelligence and incident learnings into scalable SIEM correlation logic;
- Worked cross-functionally with Security Product teams to define requirements for SIEM capabilities and detection workflows;
- Supported migration and evolution of SIEM detections, ensuring continuity and quality of security monitoring at scale;
- Worked on custom security agent deployment on cloud infrastructure;

SECURITY ENGINEER, SOC, YANDEX; YEREVAN – 2022 - 2024

- Improved SIEM alerts design and development process: planning, syncing, brainstorming solutions;
- Managed and mentored 2 security engineers working on detection development and log correlation for cloud security use cases; Together with team we managed to develop over 10 detections for cloud environment;
- Acted as a technical contributor in Yandex Cloud SIRT, participating in multiple cloud security investigations and translating incident learnings into new detections;
- Owned technical security controls required for SOX compliance in cloud environments;

SECURITY RESEARCHER, INDUSTRIAL CONTROL SYSTEMS (ICS) CYBER EMERGENCY RESPONSE TEAM KASPERSKY; MOSCOW – 2021 - 2022

- Performed large-scale statistical analysis of threat data to identify anomalous detection patterns and uncover new indicators of compromise;
- Tracked threat campaigns and actor activity over time, contributing to long-term intelligence assessments and threat landscape reports;
- Found new IoCs and targeted industrial users of existing APT attacks such as ShadowPad, Lazarus, GhostEmperor;

MALWARE ANALYST, NON-WINDOWS THREAT RESEARCH, KASPERSKY; MOSCOW – 2019 - 2021

- Conducted malware research and reverse engineering of macOS and iOS threats, identifying and documenting new malware and adware families;
- Developed and maintained detection rules and signatures for production security products, improving detection coverage and reducing false positives;
- Authored public malware reports and SecureList publications, contributing to the broader security community (see Publications / PR section);
- Taught macOS threats reverse engineering skills for newcomers;

JUNIOR SOFTWARE ENGINEER, NETCRACKER TECHNOLOGY; MOSCOW – 2017-2018

- Developed device emulator for T-SDN network controller and supporting components of OSS-system.

Education

- Moscow Institute of Physics and Technology (MIPT), department of infocommunicational networks and systems – Bachelor of Science in applied mathematics and physics, 2018
- Moscow Institute of Physics and Technology (MIPT), department of infocommunicational networks and systems – Master of Science in applied mathematics and physics, 2020

Professional skills

THREAT INTELLIGENCE / HUNTING

- Threat detection engineering (SIEM, hunting, correlation rules)
- Malware analysis (macOS, iOS, Linux)
- Threat intelligence and IoC
- Threat modeling (MITRE ATT&CK)
- Cloud security (AWS, Yandex Cloud)
- Incident investigation and root cause analysis

DATA / DETECTION ENGINEERING

- Python (tooling, automation)
- SQL (large-scale security data analysis)
- Bash (data preprocessing, automation)
- Splunk, Osquery, Tetragon

REVERSE ENGINEERING

- IDA Pro, Binary Ninja
- x86 assembly
- LLDB / GDB debuggers

SOFTWARE DEVELOPMENT

- Developed ycprox tool for pentesting and as a research: https://github.com/chlzen/ycprox (currently archived)

- Learning Rust as a hobby

OTHER

- English - Intermediate

- Native language — Russian

- Passionate about playing drums and music

Publications / PR

- «Securing your Lambda 101» — 13.09.25, OWASP AppSec Days Singapore 2025

- «Securing your Lambda 101» — 14.06.25, BSides Yerevan 2025 — https://blog.chillz.work/posts/securing-your-lambda-101-talk/

- «Threat landscape for industrial automation systems. Statistics for H2 2021» 03.03.22, ICS CERT Kaspersky Portal — https://ics-cert.kaspersky.com/publications/reports/2022/03/03/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2021/

- «Convuster: macOS adware now in Rust» – 18.03.21, SecureList – https://securelist.com/convuster-macos-adware-in-rust/101258/

- «Good old malware for the new Apple Silicon platform» – 12.03.21, SecureList – https://securelist.com/malware-for-the-new-apple-silicon-platform/101137/

- «Shlayer Trojan attacks one in ten macOS users» – 23.01.2020, SecureList – https://securelist.com/shlayer-for-macos/95724/

Looking forward for your feedback and any offers!