Ilia Mogilin

+374-91-593-379 mogiliniv@gmail.com linkedin.com/in/mogilin/ Yerevan, Armenia 🇦🇲

About me

SOC engineer / security researcher with over 6 years of experience in cybersecurity. Worked for global cybersecurity vendor Kaspersky and big-tech company Yandex.

Eager to offer infosecurity and analytical skills to help your team hunt / detect new threats and perform incident response activities.

As a security engineer significantly improved SIEM alerts design and development process by proposing collaborative dashboard for SOC and Yandex.Cloud teams. Also this approach was adopted by other SOC sub-teams in Yandex.

As a macOS malware analyst discovered new malware and adware families such as Convuster, Capip, Padzer, etc.

I like automating things using LLMs as a hobby!

Experience

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

- Adopted Data Warehouse approach to use in Security Operations to support incidents' investigation. Made possible SecOps analysts to look into non-modify IAM operations and DNS resolves.
- Contained / handled incidents in cloud environment as a part of CSIRT team;
- Deployed Tetragon security agent to use cutting edge file integrity monitoring;
- Deployed security agents' updates throughout cloud fleet;

SECURITY OPERATIONS ANALYST, YANDEX CLOUD; YEREVAN – FEB 2024 - JULY 2024

- Created productive cooperation process between SecOps team and Security Product (YCEM) teams; Formulated dozens of product requirements for SIEM product;
- Supported Splunk alerts during SIEM migration period and consulted other workers on issues. Formulated requirements for successful alerts migration.
- Performed incident response. Suggested a technical retro sync to exchange knowledge between team members;
- Continued to support SOX compliance certification for Yandex Cloud;
- Worked on custom security agent deployment on cloud infrastructure;

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

- Improving SIEM alerts design and development process: planning, syncing, brainstorming solutions;
- Managed a team of two L2 SOC security engineers which solved tasks of detection, logs corelation and connecting new log sources for securing cloud infrastructure;
- As a member of Yandex Cloud SIRT investigated over 7 incidents related to cloud infrastructure;
- Leading technical side of SOX compliance certification for Yandex Cloud;

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

- Solved tasks of abnormal spikes detection and explanation in statistics: root cause of high detection rates in some regions and false alarm detections;
- Analysing and preparing half-year detection statistics / threat landscape reports (see my publications);
- Finding 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

- Reverse engineering of malicious samples on macOS and iOS systems;
- Adding detecting rules for antivirus product bases and fixing false alarms;
- Resolving customer support issues regarding possible infection;
- Composing feedback reports during antivirus testing competition;
- Teaching macOS threats reverse engineering skills for newcomers;

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

- Developing 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

CYBERSECURITY

- Splunk SIEM: correlation rules & connecting new log sources
- Incident response
- MacOS and Linux security
- Cloud security
- Familiarity with Yandex Cloud platform (cloud services provider), AWS
- Reverse engineering using IDA Pro, Binary Ninja
- Assembler x86
- Lldb/gdb debugging
- Basic networking knowledge: OSI, TCP/IP, routing protocols

DEVOPS

- Familiarity with JetBrains TeamCity, Spinnaker
- Osquery, Tetragon as agents / log sources
- Packaging code into .deb using fpm

DATA ANALYSIS & AUTOMAING

- Prompt engineering for LLMs
- N8n for automating
- Familiar with Jupyter Notebook

- Basic usage of numpy, pandas, pyplot modules/libraries
- Bash raw data pre-processing using grep, awk, sort, uniq, etc.

SOFTWARE DEVELOPMENT

- Python as a main scripting language
- Bash scripting
- Java on Junior Software Engineer level
- SQL, PL/SQL, Yandex Query Language
- My code snippets and projects can be found on my GitHub: github.com/ilyamogilin

OTHER

- English - Intermediate
- Native language — Russian
- Passionate about playing drums and music

Publications

- «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/

Achievements

- 3-rd place on hackathon «Sberbank Javathon» as part of team «Ctrl+C Ctrl+V»;

- 5-th place in CTF-competition «M*CTF 2018» as part of team «Lights Out»;

- 6-th place in open worldwide university CTF-competition «RuCTF 2019» as part of team «Lights Out»;

Looking forward for your feedback and any offers!