trainsec
where pros train pros.

LIVE WEBINAR

TINY MASTERCLASS SERIES

One Electron to Rule Them All

The Researcher Journey Behind Electron Proxy Execution

DATE	TIME	INSTRUCTOR	DURATION	ADMISSION
June 30, 2026	5:00 PM IDT / 10:00 AM EDT	Uriel Kosayev	4 hours (live)	$49 + $49 voucher

Live event • Google Meet • Joining link sent by email after registration

WEBINAR OVERVIEW

This webinar takes you behind the scenes of Uriel Kosayev's original research into Electron proxy execution. What began as a single intuition, that widely trusted Electron-based applications might expose behavior malware can abuse to evade EDR controls and application allow-listing, evolved into a cross-platform investigation spanning Windows, Linux, and macOS. The research led to a MITRE ATT&CK contribution (T1218.015) and a real-world responsible disclosure case with Cursor IDE that is still unresolved. This session is built around the research journey: the instincts, the validation process, the disclosure experience, and the defender takeaways.

WHAT YOU WILL LEARN

- ✓ Explain what Electron proxy execution is, why it works across Windows, Linux, and macOS, and why it matters for malware evasion and allow-listing bypass
- ✓ Follow the researcher's actual path from a first intuition to a validated, MITRE ATT&CK-recognized finding
- ✓ Apply a structured investigation framework for evaluating whether an application exposes proxy execution behavior
- ✓ Connect the technique to MITRE ATT&CK T1218.015 and understand how it maps to behavior you may already see in your environment
- ✓ Navigate a responsible disclosure process, including how to document, follow up, and respond when a vendor goes quiet
- ✓ Identify concrete detection opportunities and hardening measures that reduce exposure to Electron-based abuse techniques

SESSION AGENDA

TIME	TOPIC	OUTCOME
00:00 – 00:20	**Opening: The story behind the research**	Understand the problem space and why researcher instinct matters
00:20 – 00:55	**Electron as an attack surface**	Understand why Electron applications are everywhere and why their behavior matters for defenders
00:55 – 01:35	**Original research: One Electron to Rule them All**	Learn how the research started, how hypotheses were formed, and how the discovery expanded
01:35 – 01:50	**Break**	Short refresh break

TIME	TOPIC	OUTCOME
01:50 – 02:35	**Proxy execution and MITRE ATT&CK T1218.015**	Connect the research to a recognized attack technique and understand its defensive relevance
02:35 – 03:10	**Cross-platform thinking: Windows, Linux, and macOS**	Learn how to think beyond one operating system and validate patterns across environments
03:10 – 03:35	**Responsible disclosure case study: Cursor IDE**	See how real-world disclosure works, including follow-ups and unanswered vendor communication
03:35 – 03:55	**Defender takeaways: detection, hardening, validation**	Receive practical defensive guidance at a safe, conceptual level
03:55 – 04:00	**Closing and next steps**	Call to action and voucher reminder

PREREQUISITES

- Basic familiarity with cybersecurity concepts: malware, EDR, AV, application allow-listing, and command-line usage
- A computer with a stable internet connection and the ability to join the live session
- Some exposure to Windows, Linux, or macOS internals (recommended)
- Background in malware analysis, reverse engineering, or detection engineering (recommended)

No lab environment or malware execution required.

WHO THIS IS FOR

→ Malware analysts exploring real evasion paths and application-abuse techniques

→ SOC analysts and detection engineers thinking beyond signatures

→ Reverse engineers interested in how legitimate software becomes an attack surface

→ Red teamers who want to understand proxy execution from a research perspective

→ Cybersecurity students learning how a researcher actually thinks

→ Security leaders evaluating allow-listing and EDR control gaps

ABOUT THE INSTRUCTOR

Uriel Kosayev

Co-founder, TrainSec Academy | Cybersecurity Researcher & MITRE ATT&CK Contributor

Uriel is a cybersecurity researcher and reverse engineer with over a decade of experience in malware analysis, offensive security, and incident response. He co-founded TrainSec Academy and authored *Antivirus Bypass Techniques* (8,000+ copies sold) and *MAoS: Malware Analysis on Steroids* (2025). His research contributions to the MITRE ATT&CK framework include the Electron Applications technique (T1218.015).

REGISTER NOW https://trainsec.net/electron-proxy-execution-with-uriel-kosayev-live-4h-masterclass/

trainsec
where pros train pros.

TrainSec Academy is managed by Scorpio Software LLC, 95 Newcomb Rd., Tenafly, NJ 07670, USA
info@TrainSec.net | https://TrainSec.net