SANS | GIAC CERTIFICATIONS

RSAC 2023 Keynote Session Reveals: The Five Most Dangerous New Attack Techniques

moderated by
Ed Skoudis
SANS Technology Institute College President

Each year at RSA Conference, the SANS Institute provides an authoritative briefing on the most dangerous new attack techniques leveraged by modern-day attackers, including cyber criminals, nation-state actors, and more. The annual briefing brings together some of the best and brightest minds shaping SANS core curricula to discuss emerging threat actor Tactics, Techniques, and Procedures (TTPs), assess what they mean for the future, and guide organizations on how to prepare for them.

Katie Nickels
SANS Certified Instructor, Director of Intelligence at Red Canary

ATTACK TECHNIQUE

SEO Attacks & Paid Advertising Attacks

Katie highlighted the emergence of Search Engine Optimization (SEO) and advertising attacks such as Malvertising - tactics which leverage fundamental marketing strategies to gain initial access to enterprise networks. In these instances, threat actors are exploiting SEO keywords and paid advertisements to trick victims into engaging spoofed websites, downloading malicious files, and allowing remote user access. These two attack vectors heighten the importance of incorporating scalable user awareness training programs tailored to new threats.

“Malvertising was just added to MITRE ATT&CK® as a new attack technique.”

Katie Nickels, SANS Certified Instructor, Director of Intelligence at Red Canary

Dr. Johannes Ullrich
SANS Technology Institute College Dean of Research, Internet Storm Center (ISC) Founder

ATTACK TECHNIQUE

Third-Party Developer Attacks

Dr. Ullrich zeroed in on the rise of targeted attacks on third-party software developers to infiltrate enterprise networks through the supply chain. He pointed to the December 2022 LastPass breach, where a threat actor exploited third-party software vulnerabilities to bypass existing controls and access privileged environments. For organizations across sectors, the attack underscored the criticality of effectively working in tandem with software developers to align security architectures and provide the targeted training required to build defensible applications.

“A lot of endpoint protection software is geared towards corporate workstations. They aren’t necessarily designed to protect systems that have developer tools installed, where random code is compiled, and where developers are experimenting with different libraries.”

Dr. Johannes Ullrich, SANS Technology Institute College Dean of Research, Internet Storm Center (ISC) Founder

Stephen Sims
SANS Fellow & Offensive Cyber Operations Curriculum Lead

ATTACK TECHNIQUE

Adversarial AI Attacks

Stephen examined how actors are manipulating AI tools to amplify the velocity of ransomware campaigns and identify zero-day vulnerabilities within complex software. From streamlining the malware coding process to democratizing social engineering, adversarial AI has changed the game for attackers. In response, organizations need to deploy an integrated defense-in-depth security model that provides layered protections, automates critical detection and response actions, and facilitates effective incident-handling processes.

Heather Mahalik
SANS Fellow, DFIR Curriculum Lead, and Senior Director of Digital Intelligence at Cellebrite

ATTACK TECHNIQUE

ChatGPT-Powered Social Engineering Attacks

Heather emphasized how AI-driven social engineering campaigns are now hitting close to home. With the rise of ChatGPT, threat actors are now leveraging generative AI to exploit human risk – targeting the vulnerabilities of individual employees to breach their wide organization’s network, including their families. This development means that everyone is now more easily attackable than ever, and all it takes is one wrong click on a malicious file to put not only an entire company at immediate risk but the victim’s livelihood as well. This widened attack surface requires organizations to foster a culture of cyber vigilance across every fabric of their enterprise to ensure employees are cognizant of ChatGPT-related attacks.

RSAConference™2023