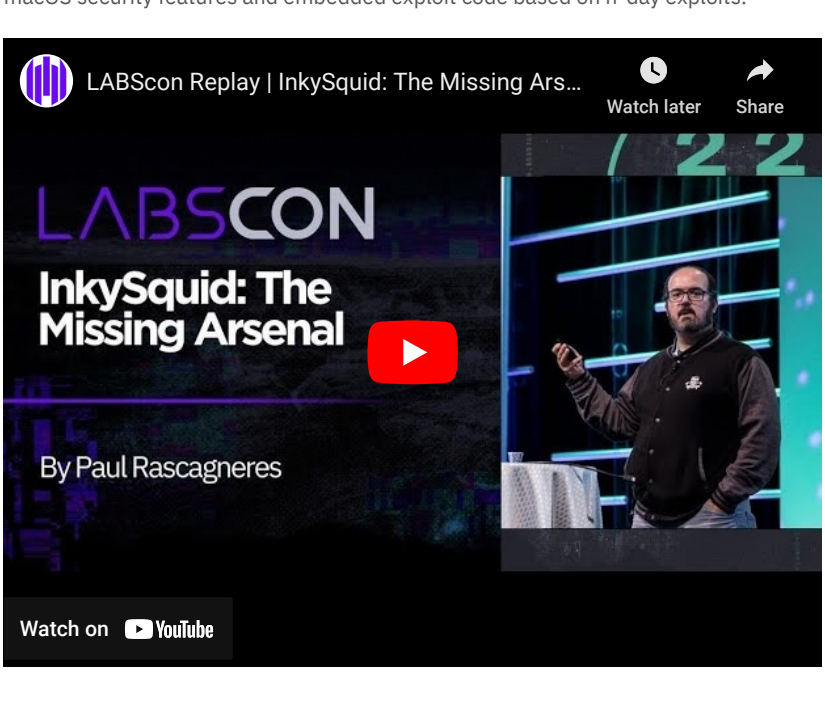
LABSCON

LABScon Replay | InkySquid: The Missing Arsenal

LABSCON / JANUARY 4, 2023

InkySquid (*aka* Group123, APT37) is an infamous threat actor linked to North Korea that has been active for at least 10 years. This actor is known to use social engineering in order to breach targets and exploit n-day vulnerabilities in Hangul Word Processor (HWP), as well as browser-based technologies.

One of the most documented intrusion sets used by this actor is RoKRAT, a Windows RAT using cloud providers as C2 servers. In this presentation, Paul Rascagneres discusses a macOS port of RoKRAT. Paul describes the internal mechanisms and different espionage features of the malware, as well as built-in attempts to bypass macOS security features and embedded exploit code based on n-day exploits.



InkySquid: The Missing Arsenal

Transcript

00:00:05 **Paul Rascagneres**
Yeah. First of all, I'm really impressed to be here in front of you, and the venue is amazing. So thank you for, for the program committee who accept my talk first and for the organizer for for organizing the event. The content is very good, til now, and. And. Yeah, so I'm French. And you, as you can hear and I work at Volexity and I work on the threat intelligence team. Previously I work for Kaspersky Great Cisco TALOS and I mainly work on CTI and malware analysis and this topic will be about this topic, malware analysis, and more specifically about macOS malware. And if you want to contact me after the presentation, if you have questions or if you want some file or stuff like that, you can contact me on Twitter. My DM are open or on Keybase and I would be happy to to share what you need. It's not a problem.

SentinelOne

1.00x

00:00:00 00:18:50

About the Presenter

Paul Rascagneres is a principal threat researcher at Volexity. He performs investigations to identify new threats, and he has presented his findings in several publications and at international security conferences.

About LABScon

This presentation was featured live at LABScon 2022, an immersive 3-day conference bringing together the world's top cybersecurity minds, hosted by SentinelOne's research arm, SentinelLabs.

APT | LABSCON | MACOS

LABSCON

LABScon brings together the world's top cybersecurity minds to share cutting-edge research and push the envelope of threat landscape understanding.