Operation Triangulation

Archived: 2026-04-05 14:29:52 UTC

While monitoring the network traffic of our own corporate Wi-Fi network using the Kaspersky Unified Monitoring and Analysis Platform (KUMA), we discovered a previously unknown mobile APT campaign targeting iOS devices. The targets are infected using zero-click exploits via the iMessage platform, and the malware runs with root privileges, gaining complete control over the device and user data. We are calling this campaign “Operation Triangulation”. MITRE created a page for this campaign as part of its ATT&CK framework.

This is an ongoing investigation, the amount of material we collected is substantial and will take time to analyze. Given the complexity of the attack, we are confident that we are not the only target, and invite everyone to join the research. If you have any additional details to share, please contact us: triangulation[at]kaspersky.com

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT’s infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.

Source: https://securelist.com/trng-2023/