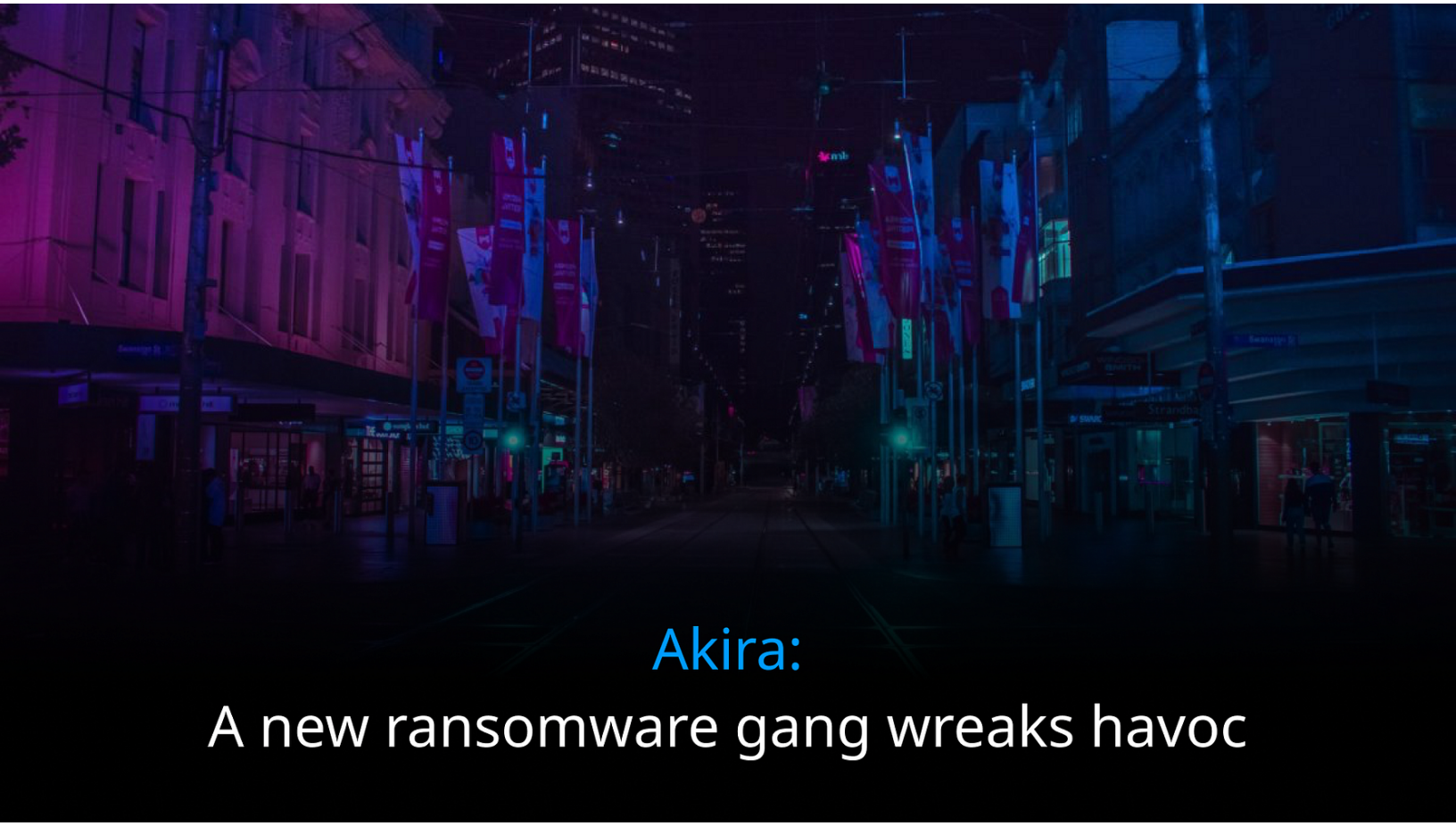

Akira: A new ransomware gang wreaks havoc

Sep 21, 2023 11:13 CEST

Akira: A new ransomware gang wreaks havoc

- **Emerging in March this year, Akira quickly joined the most active ransomware groups as number four.**
- **Logpoint has analyzed the Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise IoCs enabling protection.**

COPENHAGEN, Denmark, September 21, 2023 – The Akira ransomware group has emerged as a tenacious adversary and grabbed widespread notice quickly. The group appeared in March 2023 and became the 4th most active group in August, demanding millions of dollars in ransom from victims. The group primarily targets organizations in the UK and US within various

industries, including education, finance, real estate, manufacturing, and consulting.

“Akira has shown itself as incredibly active and quickly built an extensive victims list. With every campaign, the gang evolves with new features and capabilities,” says Swachchhanda Shrawan Poudel, Logpoint Security Research Engineer. “Since its emergence in March this year, it already has a trail of victims, and there’s no suggestion that the activity level is decreasing. It’s quite the contrary, as the number of victims increases each month.”

Akira ransomware is sophisticated malicious software designed to encrypt files on a victim’s system, delete shadow copies, and provide instructions for ransom payment and data recovery. It employs encryption algorithms, exclusion criteria, and a TOR-based communication system to perform malicious operations.

Logpoint’s research has uncovered the Akira infection chain through malware analysis. Akira actively targets Cisco ASA VPNs without multifactor authentication to exploit CVE-2023-20269 as an entry point for their ransomware. The gang employs several different malware samples in their campaigns, which initiates a series of steps when executed to encrypt victim files, including shadow copy deletion, file and directory search, and enumeration and encryption process.

“The rise of Akira serves as a reminder to get the basic cyber hygiene in order,” says Swachchhanda Shrawan Poudel. “In this particular case, implementing multifactor authentication can make the difference between a devastating cyberattack and an insignificant breach attempt. Organizations must monitor risks and build adequate defenses, such as keeping software and systems updated, auditing privileged accounts, and employing network segmentation.”

Logpoint’s security operations platform, Converged SIEM, contains extensive tools and capabilities for identifying, evaluating, and mitigating the impact of Akira Ransomware. With features like native endpoint solution AgentX and SOAR with pre-configured playbooks, it enables security teams to automate essential incident response procedures, gather vital logs and data, and expedite malware detection and removal operations.

Read Logpoint’s full report about Akira here and get a deep dive into the

infection chain, technical analysis of malware samples, and recommendations to safeguard against the threat.

About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's SIEMand NDRtechnologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit http://logpoint.com.

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98