LOGPOINT

The infamous state-sponsored Advanced Persistent Threat (APT) linked to Russia remains active, posing a severe threat to organizations

Oct 31, 2023 10:00 CET

Cozy Bear: Unmasking the decades-long espionage arsenal

- **The infamous state-sponsored Advanced Persistent Threat (APT) linked to Russia remains active, posing a severe threat to organizations.**
- **Logpoint has analyzed the Tactics, Techniques, and Procedures (TTPs), helping organizations detect the threat actor.**

COPENHAGEN, Denmark, October 31, 2023 – Cozy Bear emerged in 2008 and has gained notoriety for a series of high-level cyberattacks, such as SolarWinds in 2020 and the Democratic National Committee in 2016. The

group is linked to Russia's Foreign Intelligence Service (SVR) and targets governments, non-governmental organizations, businesses, think tanks, and other high-profile targets to spy and steal information and intelligence. Logpoint has collated a report outlining the threat and how to protect against it.

"Cozy Bear has continuously demonstrated a striking level of consistency in their techniques, making only sporadic modifications," says Swachchhanda Shrawan Poudel, Logpoint Security Research Engineer. "What stands out is their ability to carry out successful campaigns repeatedly, evidently without changing techniques or encountering substantial issues or setbacks. Their operations' unwavering resilience and effectiveness emphasizes Cozy Bear's sophistication and adaptability as a threat actor."

As late as September 2023, Mandiant reported that Cozy Bear was active with a phishing campaign targeting embassies in Ukraine. Phishing email is a common element across Cozy Bear's campaigns, but there are variations in how the malware is deployed. The group delivers malware using HTML smuggling and malicious ISO images. MITRE ATT&CK suggests disabling auto-mounting for disk image files and blocking certain container file types.

Cozy Bear's goals are not financially driven. Logpoint's report highlights how the group prioritizes stealthy persistence, allowing them to covertly maintain access for extended periods while exfiltrating confidential and sensitive data, making it challenging for security professionals to detect because the approach limits the availability of telemetry that could trigger detection mechanisms.

"Because of the stealthy nature of Cozy Bear, the only viable way to detect it is to hunt for signs of known persistence techniques proactively," says Swachchhanda Shrawan Poudel. "It's challenging for organizations to conduct effective threat hunting, especially for small and medium-sized ones, because it involves sifting massive amounts of information, but it's important to find ways to keep up to date on the most active APT groups, their tactics, methods and procedures."

Logpoint's security operations platform, Converged SIEM, includes features for detecting, analyzing, and mitigating the effect of threats, including APTs. It allows security teams to automate essential incident response procedures, capture logs and data, and accelerate malware detection and removal

operations with features such as native endpoint solution AgentX and SOAR with pre-configured playbooks.

Read Logpoint's full report about Cozy Bear here and get a deep dive into Cozy Bear activity, security measures and mitigations, and detection.

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