Oct 31, 2023 10:00 CET

Cozy Bear: Afdækning af berygtet cybergruppes arsenal

København, 31. oktober 2023– Cozy Bear blev først beskrevet i 2008 og mistænkes for en række højt profilerede cyberangreb, såsom SolarWinds i 2020 og Demokraternes Nationale Komité i USA i 2016. Gruppen menes at være knyttet til den russiske efterretningstjeneste SVR og målretter sine angreb mod myndigheder, NGO'er, virksomheder, tænketanke og andre højt profilerede mål for at spionere og stjæle information. Logpoint har udfærdiget en rapport, der folder truslen ud og giver råd til beskyttelse.

"Cozy Bear udmærker sig ved gentagne gange at lykkes med at gennemføre kampagner, tilsyneladende uden at ændre deres teknikker eller støde på nogen problemer eller tilbageslag af betydning," siger Swachchhanda

Shrawan Poudel, Logpoint Security researcher. ”Deres modstandsdygtighed og effektivitet understreger, hvor sofistikerede Cozy Bears er, og deres evne til at tilpasse sig som trusselsaktør.”

Så sent som september 2023 rapporterede Mandiant, at Cozy Bear var aktiv med en phishing-kampagne, målrettet ambassader i Ukraine. Phishing-e-mails går igen i Cozy Bears kampagner, men der er variationer i måden malware udrulles på. Gruppen distribuerer malware ved hjælp af såkaldt HTML smuglling og ondsindede (weponiserede) ISO-filer. MITRE ATT&CK foreslår at deaktivere automatisk montering af diskbilledfiler og blokere visse typer containerfiler.

Cozy Bears er ikke økonomisk motiverede. Logpoints rapport understreger, at gruppen prioriterer at skjule sig og bevare adgang i længere perioder, mens de eksfiltrerer fortrolige og følsomme data. Det gør det svært for sikkerhedsfolk at opdage gruppen i systemet, da deres tilgang begrænser mængden af telemetri, der kan sætte gang i alarmer.

"Cozy Bears lyssky karakter betyder, at den eneste holdbare måde at opdage dem på er at søge proaktivt efter indikatorer på, at deres kendte teknikker er i brug i systemet," siger Swachchhanda Shrawan Poudel. "Det er en udfordring for organisationer at jagte trusler effektitv, især for små og mellemstore virksomheder, fordi man er nødt til at gennemgå enorme mængder data. Men det er simpelthen afgørende at at holde sig ajour med de mest aktive APT-grupper og deres TTP’er i en eller anden udstrækning."

Læs Logpoints fulde rapport om Cozy Bear her og få et indblik i Cozy Bears aktiviteter og hvilke sikkerhedsforanstaltninger, der kan afhjælpe truslen.

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
PR Manager
PR & Communications