LOGPOINT

Oct 31, 2023 10:00 CET

Cozy Bear : Démasquer un arsenal d'espionnage vieux de plusieurs décennies

- La tristement célèbre menace persistante avancée (APT) parrainée par l'État et liée à la Russie reste active et constitue une grave menace pour les organisations.

- Logpoint a analysé les tactiques, techniques et procédures (TTP) pour aider les organisations à détecter l'acteur de la menace.

COPENHAGUE, Danemark, 31 octobre 2023 – Cozy Bear est apparu en 2008 et s'est fait connaître par une série de cyberattaques de haut niveau,

notamment contre SolarWinds en 2020 et le Comité national démocrate en 2016. Le groupe est lié au Service de renseignement extérieur russe (SVR) et vise les gouvernements, les organisations non gouvernementales, les entreprises, les groupes de réflexion et d'autres cibles de premier plan pour espionner et voler des informations et des renseignements. Logpoint a rédigé un rapport décrivant la menace et les moyens de s'en protéger.

"Cozy Bear a toujours fait preuve d'une constance remarquable dans ses techniques, n'apportant que des modifications sporadiques", déclare Swachchhanda Shrawan Poudel, ingénieur de recherche en sécurité chez Logpoint. "Ce qui est remarquable, c'est leur capacité à mener des campagnes réussies de manière répétée, manifestement sans changer de techniques ni rencontrer de problèmes ou de revers importants. La résilience et l'efficacité inébranlables de leurs opérations soulignent la sophistication et l'adaptabilité de Cozy Bear en tant qu'acteur de la menace".

En septembre 2023, Mandiant a signalé que Cozy Bear était actif dans le cadre d'une campagne de phishing visant des ambassades en Ukraine. Le courriel de phishing est un élément commun aux campagnes de Cozy Bear, mais il existe des variations dans la manière dont les logiciels malveillants sont déployés. Le groupe diffuse les logiciels malveillants par le biais de la contrebande HTML et d'images ISO malveillantes. MITRE ATT&CK suggère de désactiver le montage automatique des fichiers d'image disque et de bloquer certains types de fichiers conteneurs.

Les objectifs de Cozy Bear ne sont pas de nature financière. Le rapport de Logpoint souligne que le groupe privilégie la persistance furtive, ce qui lui permet de conserver secrètement un accès pendant de longues périodes tout en exfiltrant des données confidentielles et sensibles, ce qui rend sa détection difficile pour les professionnels de la sécurité car cette approche limite la disponibilité de la télémétrie qui pourrait déclencher des mécanismes de détection.

"En raison de la nature furtive de Cozy Bear, le seul moyen viable de le détecter est de rechercher de manière proactive les signes de techniques de persistance connues", explique Swachchhanda Shrawan Poudel. "Il est difficile pour les organisations de mener une chasse aux menaces efficace, en particulier pour les petites et moyennes entreprises, car cela implique de passer au crible des quantités massives d'informations, mais il est important de trouver des moyens de se tenir au courant des groupes APT les plus actifs,

de leurs tactiques, de leurs méthodes et de leurs procédures."

La plateforme d'opérations de sécurité de Logpoint, Converged SIEM, comprend des fonctions de détection, d'analyse et modération de l'effet des menaces, y compris les APT. Elle permet aux équipes de sécurité d'automatiser les procédures essentielles de réponse aux incidents, de capturer les journaux et les données, et d'accélérer les opérations de détection et de suppression des logiciels malveillants grâce à des fonctionnalités telles que la solution native AgentX pour les End-points et SOAR avec des playbooks préconfigurés.

Consultez le rapport complet de Logpoint sur Cozy Bear ici et plongez dans l'activité de Cozy Bear, les mesures de sécurité et d'atténuation, et la détection.

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
mcf@logpoint.com
+45 25 66 82 98