LOGPOINT

Logpoint a compilé un rapport mettant en évidence les TTP et IoC utilisés par Cactus pour créer des règles d'alerte afin de détecter les méthodes utilisées par le groupe

Nov 27, 2023 09:00 CET

Cactus : Se défendre contre un nouveau venu chez les ransomwares

- **Cactus est apparu en mars cette année et a depuis déjà fait des ravages chez plusieurs victimes.**
- **Logpoint a analysé les tactiques, techniques et procédures (TTP) ainsi que les indicateurs de compromission (IoC) pour établir des défenses.**

COPENHAGUE, Danemark, 27 novembre 2023 – Cactus aussi appelé CactusTorch est un groupe d'attaquants par ransomware sophistiqué ayant un impact grave sur ses victimes. Le nouveau venu est apparu pour la première

fois en mars 2023 et a intégré le top 10 des groupes ayant le plus de victimes mensuelles, se classant au septième rang avec 58 victimes au mois de novembre. Le groupe se concentre sur des paiements substantiels et cible de grandes entités commerciales.

« Cactus est un bon exemple de rançongiciel utilisant des TTP de plus en plus sophistiquées dans leurs attaques. Ce qui ressort dans ce cas, c'est que le logiciel malveillant s'auto-encrypte pour éviter la détection, » déclare Bibek Thapa Magar, Ingénieur en Analyse de Sécurité chez Logpoint. « La façon d'éviter les systèmes de défense montre que le groupe est doué dans ce domaine. Cactus a rapidement eu un impact significatif en utilisant l'extorsion double, en compromettant des données sensibles et en laissant les victimes avec peu de choix. »

Cactus est un ransomware sophistiqué avec des fonctionnalités uniques telles que l'auto-chiffrement et un changement consécutif des extensions de fichier après le chiffrement, rendant ainsi plus difficile l'identification des fichiers affectés. Il utilise le packer UPX bien connu et facilement “dé compressible” et divise les fichiers chiffrés en micro-buffers, probablement pour accélérer la gestion des flux de données chiffrées.

Logpoint a compilé un rapport mettant en évidence les TTP et IoC utilisés par Cactus pour créer des règles d'alerte afin de détecter les méthodes utilisées par le groupe. Selon Kroll, Cactus exploite des vulnérabilités connues dans les appliances VPN pour obtenir un accès initial et établit des commandes et un contrôle avec SSH. Le groupe tente de décharger LSASS et les identifiants des navigateurs web pour augmenter les privilèges. En fin de compte, Cactus accède aux ordinateurs cibles en utilisant Splashtop ou AnyDesk et crée un proxy entre les hôtes infectés en utilisant Chisel avant de chiffrer les fichiers.

« Cactus est un bon rappel que l'hygiène de base en matière de cybersécurité est importante, mais cela souligne également que la surveillance et la détection sont essentielles pour se protéger contre les ransomwares plus récents, » déclare Bibek Thapa Magar. « Si une activité est détectée, les analystes de sécurité devraient enquêter et s'assurer qu'elle ne se propage pas en désactivant les réseaux privés virtuels (VPN), les serveurs d'accès à distance, les ressources d'authentification unique et les appareils accessibles au public avant de procéder à la limitation, à l'éradication et à la récupération pour en minimiser l'impact.”

La plateforme Logpoint, Converged SIEM, contient des outils et des capacités étendus pour identifier, évaluer et atténuer l'impact du ransomware Cactus. En plus d'un ensemble de règles d'alerte pour aider à détecter l'activité de Cactus, Logpoint propose des capacités permettant aux équipes de sécurité d'automatiser des procédures essentielles de réponse aux incidents.

Lisez le rapport complet de Logpoint sur Cactus ici et plongez dans la conception des attaques du groupe ainsi que dans la manière de détecter et de répondre à la menace.

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