LOGPOINT

Aug 24, 2023 10:00 CEST

Le groupe de ransomware 8base intensifie considérablement son niveau d'activité

- **8base figure parmi les 5 premiers groupes de ransomware cet été, et Logpoint a identifié les TTP (Tactics, Techniques and Procedures) ainsi que les IoC (Indicators of Compromise) à surveiller.**
- **Le groupe de ransomware se distingue en ciblant les petites et moyennes organisations, moins susceptibles de disposer de mesures de sécurité solides.**

COPENHAGUE, Danemark, 23 août 2023 – Le groupe de ransomware 8base a émergé en tant qu'adversaire persistant et redoutable dans le paysage des menaces cybernétiques, ciblant plusieurs secteurs, notamment les petites et

moyennes entreprises. Le groupe est apparu en mars 2022 et depuis juin, le niveau d'activité a considérablement augmenté, plaçant le groupe parmi les 5 plus actifs.

"En général, les petites et moyennes organisations ont plus de difficultés à allouer des budgets de sécurité et souffrent de pénuries en matière de cybersécurité, ce qui est un cocktail dangereux lorsqu'un groupe de ransomware comme 8base les cible", déclare Anish Bogati, ingénieur en recherche en sécurité chez Logpoint. "Les petites et moyennes organisations, en particulier, devraient se familiariser avec 8base et, plus important encore, renforcer leurs mesures de sécurité pour se défendre contre lui. Comprendre l'adversaire est la clé pour élaborer de meilleures stratégies de défense."

La recherche de Logpoint a mis en lumière la chaîne d'infection de 8base grâce à l'analyse de logiciels malveillants. 8base utilise plusieurs familles de logiciels malveillants pour atteindre leurs objectifs, notamment SmokeLoader et SystemBC, en plus de la charge utile du ransomware Phobos. Le groupe de ransomware obtient principalement un accès initial via des e-mails d'hameçonnage et utilise le Shell de Commande Windows et PowerShell pour exécuter la charge utile. Les adversaires utilisent plusieurs techniques pour assurer leur persistance dans le système, échapper aux défenses et atteindre leurs objectifs.

L'analyse de Logpoint révèle ce que les équipes de sécurité devraient rechercher pour détecter l'activité de 8base dans le système, notamment des processus suspects générés par des produits Microsoft Office, l'exécution de fichiers à l'aide de WScript ou CScript, ou la création de tâches planifiées. Connaître les indicateurs de compromission et les tactiques, techniques et procédures (TTP) aide les organisations à identifier et à atténuer de manière proactive les activités suspectes associées à 8base.

"Les petites et moyennes organisations doivent s'assurer de disposer des capacités nécessaires pour détecter et répondre à l'activité de 8base à n'importe quel stade de l'infection", déclare Anish Bogati. "La journalisation adéquate, la visibilité des actifs et la surveillance sont essentielles à une stratégie de cybersécurité robuste, car elles offrent une vue d'ensemble du réseau et aident à détecter des anomalies telles que des fichiers déposés dans des dossiers accessibles en écriture publique, des modifications de valeurs de registre et des tâches planifiées suspectes pouvant indiquer une menace de sécurité telle que 8base."

Lisez le rapport complet de Logpoint sur 8base ici et obtenez une analyse approfondie des logiciels malveillants, une analyse technique ainsi que tous les moyens de détecter, d'enquêter 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