LOGPOINT

Aug 24, 2023 10:00 CEST

KMU im Fadenkreuz: Die Ransomware-Gruppe 8base steigert ihre Aktivität erheblich

*Von Anish Bogati, Logpoint Security Research Engineer*8Base hat sich in diesem Sommer in die Top 5 der aktivsten Ransomware-Gruppierungen gearbeitet und hat dabei besonders einen Sektor auf dem Radar: kleine und mittlere Unternehmen (KMU). Erstmals auf den Plan getreten ist 8base im März 2022 und seit Juni 2023 zeigt sich die Gruppe aktiver als je zuvor. Entsprechend gilt es nun, zu handeln und sich vor einem Einfall der Kriminellen zu schützen.

Eine brisante Mischung

Im Allgemeinen haben KMU eher mit niedrigen Sicherheitsbudgets und Cybersecurity-Mängeln zu kämpfen, was ein gefährlicher Cocktail ist, wenn eine Ransomware-Gruppe wie 8base auf sie zukommt. Vor allem kleine und mittelständische Unternehmen müssen sich daher mit der Bedrohung durch 8base vertraut machen und, was noch wichtiger ist, ihre Sicherheitsvorkehrungen zum Schutz vor 8base verstärken. Den Angreifer zu verstehen ist dabei der Schlüssel zur Entwicklung besserer Verteidigungsstrategien.

Logpoints Forschung hat die 8base-Infektionskette durch Malware-Analyse aufgedeckt. 8base verwendet mehrere Malware-Familien, um ihre Ziele zu erreichen, darunter *SmokeLoader* und *SystemBC*, zusätzlich zur *Phobos* Ransomware-Nutzlast. Die Ransomware-Gruppe verschafft sich in erster Linie über Phishing-E-Mails Zugang und nutzt die Windows Command Shell und Power Shell, um die Nutzlast auszuführen. Die Angreifer verwenden mehrere Techniken, um sich im System zu halten, die Abwehr zu umgehen und ihre Ziele zu erreichen.

Die notwendige Prävention

Es ist essentiell, dass Sicherheitsteams dazu in der Lage sind, 8base-Aktivitäten im eigenen System rechtzeitig zu erkennen. Das schließt auch verdächtige untergeordnete Prozesse ein, die von Microsoft Office-Produkten gestartet werden, wie die Ausführung von Dateien mit WScript oder CScript oder die Erstellung von geplanten Aufgaben. Das Wissen um die relevanten Indikatoren für eine Kompromittierung (IoC) und die Taktiken, Techniken und Verfahren (TTPs) der Angreifer hilft KMU, verdächtige Aktivitäten im Zusammenhang mit 8base proaktiv zu erkennen und zu vereiteln oder wenigstens abzuschwächen. Die wichtigsten Hilfsmittel für eine robuste Cybersicherheitsstrategie sind in diesem Fall ordnungsgemäße Protokollierung, die Sichtbarkeit von Ressourcen und strenge Überwachung. Diese Komponenten unterstützen dabei, den Überblick über das Netzwerk zu behalten und helfen außerdem, Anomalien wie das Ablegen von Dateien in öffentlich beschreibbaren Ordnern, die Änderung von Registrierungswerten und verdächtige geplante Aufgaben zu erkennen, die auf eine Sicherheitsbedrohung wie 8base hindeuten können. Wer es allerdings versäumt, die notwendigen Sicherheitsbausteine proaktiv vorzubereiten, der läuft Gefahr, ein weiteres Opfer in der immer länger werdenden Liste der Ransomware-Vorfälle zu werden.

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