8base øger aktivitetsniveauet markant

Aug 24, 2023 10:00 CEST

Angreb mod SMV'er: 8base øger aktivitetsniveauet markant

- **8base er blandt de 5 mest aktive ransomware-grupper denne sommer.**
- **Logpoint har offentliggjort TTP'er (Tactics, Techniques, & Procedures) og IoC'er (Indicators of Compromise) knyttet til gruppen.**
- **Ransomware-gruppen skiller sig ud ved at målrette sine angreb mod små og mellemstore organisationer, hvor sikkerheden ofte halter.**

KØBENHAVN, 24. august 2023 – Ransomware-gruppen 8base er en ny og

vedholdende modstander i det evigt foranderlige cybertrussellandskab. Gruppen fokuserer på flere sektorer og målretter især sine angreb mod små og mellemstore virksomheder. 8base, der dukkede op i marts 2022, har øget sit aktivitetsniveau markant siden juni i år, hvilket har rykket gruppen op i top 5 over de mest aktive grupper.

"Generelt set har små og mellemstore organisationer større udfordringer med lave sikkerhedsbudgetter og kritisk mangel på cyberkompetencer, hvilket udgør en farlig cocktail, når en ransomware-gruppe som 8base begynder at gå målrettet efter dem," siger Anish Bogati, Security Research Engineer hos Logpoint. "Særligt små og mellemstore organisationer bør sætte sig ind i, hvad 8base er for en størrelse, og endnu vigtigere styrke deres sikkerhed for at beskytte sig imod angreb. Nøglen til at udvikle bedre forsvarsstrategier er at forstå sin modstander."

Logpoints research har afdækket 8bases angrebskæde gennem malware-analyse. 8base bruger flere typer malware til at opnå deres mål, blandt andet SmokeLoader og SystemBC, udover deres egen Phobos ransomware payload. Ransomware-gruppens angrebsvektor er hovedsagligt phishing-e-mails, og gruppen bruger Windows Command Shell og PowerShell til at udføre selve ransomware-angrebet. 8base bruger flere teknikker til at fastholde adgang til systemet, omgå forsvarsmekanismer, såsom antivirusprogrammer, og opnå deres mål.

Logpoints analyse afslører, hvad sikkerhedsteams skal være opmærksomme på for at opdage eventuel aktivitet relateret til 8base i deres system, herunder mistænkelige subprocesser, der startes via Microsoft Office-produkter, filer der eksekveres via WScript eller CScript, eller tilføjelse af planlagte opgaver. Organisationer kan proaktivt identificere og afbøde mistænkelige 8base-angreb, når de kender IoC'er og TTP'er.

"Små og mellemstore organisationer bør sikre sig, at de er i stand til at opdage og reagere på 8base-aktivitet i hele angrebskæden," siger Anish Bogati. "Korrekt logning, et godt overblik over aktiver på nettet og proaktiv overvågning er afgørende for en robust cybersikkerhedsstrategi, da de giver et overblik over netværket og hjælper med at opdage uregelmæssigheder, såsom filer der uploades til en offentlig skrivbar mappe, ændring af værdierne i registreringsdatabasen og mistænkelige planlagte opgaver, der kan give nys en sikkerhedstrussel fra 8base."

Læs Logpoints fulde rapport om 8base her og se den dybdegående malware-analyse, tekniske analyse samt gode råd til at opdage, undersøge og reagere på 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