LOGPOINT

Logpoint har udarbejdet en rapport, der fremhæver Cactus' TTP'er og IoC'er for at lave alert-regler, som kan hjælpe med at identificere, hvis gruppens metoder er i brug.

Nov 27, 2023 09:00 CET

Cactus: Forsvar mod ny ransomware-trussel

- **Cactus dukkede op i marts i år og har siden opbygget en omfattende portefølje af højt profilerede ofre.**
- **Logpoint har analyseret gruppens taktikker, teknikker og procedurer (TTP'er) samt indikatorer for kompromittering (IoC'er) for at etablere effektive forsvar.**

København, 27. november, 2023 – Den avancerede ransomware-gruppe Cactus har på kort tid skabt alvorlige konsekvens for dens ofre. Gruppe, som først gjorde sin entre i marts 2023, er hurtigt blevet en af de mest produktive

og rangerer nu som nummer 7 på listen over grupper med flest ofre om måneden. Cactus retter sine angreb mod store virksomheder og går efter store summer i løsepenge.

"Cactus er et godt eksempel på, at ransomware-grupper bliver stadig mere sofistikerede i deres angreb. Det bemærkelsesværdige her er, at malwaren krypterer sig selv for ikke at blive opdaget," siger Bibek Thapa Magar, Security Analytics Researcher hos Logpoint. "Gruppens snedige måde at undgå forsvarsmekanismer på viser, at de er dygtige til spillet. Cactus har hurtigt gjort indtryk med double extortion, kompromittering af følsomme data og begrænsede valgmuligheder for deres ofre."

Cactus er en sofistikeret ransomware med unikke funktioner såsom automatisk kryptering og ændring af fileudvidelser efter kryptering, hvilket gør det betydeligt sværere at opdage inficerede filer. Gruppen benytter den velkendte UPX-packer og deler krypterede filer i op i mikro-buffere for at håndtere de krypterede datastrømme hurtigere.

Logpoint har udarbejdet en rapport, der fremhæver Cactus' TTP'er og IoC'er for at lave alert-regler, som kan hjælpe med at identificere, hvis gruppens metoder er i brug. Ifølge Kroll udnytter Kaktus kendte sårbarheder i VPN-enheder for at opnå 'initial access' og etablere 'command and control' med SSH. Gruppen forsøger at udtrække LSASS og loginoplysninger fra webbrowsere for at eskalere privilegier. Til sidst opnår Cactus adgang til specifikke computere ved hjælp af Splashtop eller AnyDesk og opretter en proxy mellem de inficerede værter med Chisel, før filerne krypteres.

"Cactus er en påmindelse om, at grundlæggende cyberhygiejne er afgørende, men det understreger også, at overvågning og detektering er nøglen til beskyttelse mod nyere ransomware-varianter," siger Bibek Thapa Magar. "Hvis en sikkerhedsmedarbejder opdager aktivitet, bør de efterforske det og sørge for, at det ikke spreder sig ved at deaktivere virtuelle private netværk (VPN), fjernadgangsservere, single sign-on-ressourcer og offentligt tilgængelige aktiver. Derefter kan man arbejde på at inddæmme angrebet, fjerne malware og uautoriseret adgang og genoprette systemer."

Logpoints cybersikkerhedsplatform kommer med værktøjerne til at identificere, evaluere og begrænse konsekvenserne af Cactus-ransomware. Udover en pakke med alert-regler til at hjælpe med at opdage aktivitet gør Logpoint det muligt for sikkerhedsteams at automatisere processer til

håndtering af sikkerhedshændelser.

Læs Logpoints fulde rapport om Cactus her og få et indblik i gruppens angrebsdesign, og hvordan man opdager og reagerer effektivt 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
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98