Aktueller Kommentar von SentinelOne vom 09.12.2020:

Ransomware Egregor leakt Daten des Personaldienstleisters Randstad

Statement von Matthias Canisius, Regional Sales Director Central Europe bei SentinelOne

Der international tätige Personaldienstleister Randstad gab Ende vergangener Woche bekannt, dass ihr Netzwerk von der Ransomware Egregor befallen <https://www.heise.de/news/Ransomware-Cyberangriff-auf-Zeitarbeitsfirma-Randstad-4981249.html> wurde, die während des Angriffs unverschlüsselte Dateien gestohlen hat. Das Unternehmen ist Betreiber des Jobportals Monster.com und eines der größten globalen Personalvermittlungsunternehmen mit dutzenden Zweigstellen weltweit.

Laut Angaben von Randstad hat das IT-Team des Unternehmens Malware im Netzwerk entdeckt, die sich als die jüngst immer wieder auftretende Ransomware Egregor herausgestellt hat. Daraufhin wurde der Notfallplan des Dienstleisters ausgeführt: Neben dem internen Incident Response-Team wurden auch externe Forensiker und Sicherheitsexperten herangezogen, um den Vorfall schnellstmöglich zu klären und die Systeme vor weiteren Schäden zu bewahren. Laut eigenen Angaben waren zwar nur wenige Server betroffen, allerdings hat die verantwortliche Hackergruppe infolge des Angriffs ein Archiv mit 184 Dateien veröffentlicht, bei denen es sich wohl um diverse Dokumente und Finanzunterlagen des Unternehmens handelt wie Bleeping Computer <https://www.bleepingcomputer.com/news/security/largest-global-staffing-agency-randstad-hit-by-egregor-ransomware/> berichtete.

Angriffe dieser Art scheinen sich im Zuge der Covid-19-Pandemie zu häufen, was Anlass zur Sorge gibt. Randstad ist nur eine von vielen Organisationen <https://www.zdnet.de/88390072/71-opfer-seit-september-forscher-warnen-vor-ransomware-egregor/>, die Egregor in den letzten Wochen zum Opfer gefallen sind. Es wird vermutet, dass Egregor die Lücke füllt, die von der in letzter Zeit rückläufigen Ransomware Maze hinterlassen wurde. Um sich heute als Unternehmen gegen eine sich stetig wandelnde Bedrohungslandschaft zu behaupten, ist es unerlässlich, Investitionen in die eigene Cybersicherheit zu tätigen. Besonders wichtig ist es, eine moderne Endpunktlösung zu implementieren, die in der Lage ist Gefahren aus dem Netz zuverlässig und automatisch zu erkennen und zu beseitigen – sowohl vor Ort als auch im Home Office, wo sich aktuell eine Vielzahl der Arbeitnehmer befindet.

Fazit
So lange Unternehmen ihre IT-Sicherheit nur halbherzig betreiben, wird es in Zukunft immer wieder zu erfolgreichen Cyberangriffen kommen. Hackergruppen, die Ransomware nutzen, werden Sicherheitsteams sicherlich noch lange ein Dorn im Auge bleiben, denn sie entwickeln ihre kriminellen Methoden stets weiter, um mit ihrer ausgefeilten Malware auf „Großwildjagd“ zu gehen. Wenn wir eines gelernt haben, dann ist es, dass Cyberkriminelle alle Tricks in ihrem Arsenal nutzen, um an schnell verdientes Geld zu kommen – auch wenn dabei Unternehmen zu Schaden kommen. Die beste Abwehr dagegen sind regelmäßige Patches, die Schulung von Mitarbeitern und eine solide Endpunktlösung, die alle Netzwerke und Geräte in Echtzeit absichert.

Kontakt
Kafka Kommunikation GmbH & Co.
Lukas Reck
Dr. Bastian Hallbauer-Beutler
Kafka Kommunikation
089 74 74 70 580
sentinelone@kafka-kommunikation.de