Aktueller Kommentar von SentinelOne vom 28. August 2020:

Ist das der nächste Malware-Trend? Ransomware-Gruppen leaken Daten über eigene Plattformen

Matthias Canisius, Regional Director CE & EE bei SentinelOne

Meldungen über geschlossene Untergrundmärkte im Darknet sind an sich nichts neues, Plattformen wie Hansa und Alpha Bay wurden 2017 mit Hilfe der Ermittlungsbehörden geschlossen, andere wie Dream Market schlossen ihre Pforten aus eher widersprüchlichen Gründen. Der springende Punkt ist auch nicht, wie diese Anbieter heißen, sondern dass jedes Mal, wenn einer nicht mehr verfügbar ist, sofort ein neuer Dienstleister aufmacht und mit einem ähnlichen Geschäftsmodell Millionen an den illegalen Tätigkeiten seiner Nutzer verdient. Lange Zeit schien es, als wenn Cyberkriminelle ihre erbeuteten Daten vor allem auf solchen Marktplätzen vertreiben würden. Doch die weitere Professionalisierung scheint dieses Schema aufzubrechen.

In letzter Zeit häufen sich Informationen <https://www.zdnet.com/article/conti-ryuk-joins-the-ranks-of-ransomware-gangs-operating-data-leak-sites/>, dass die großen und leider erfolgreichen Ransomware-Betreiber so gefährlicher Schadsoftware wie Maze, Emotet und Trickbot sich einerseits zusammenschließen und andererseits sogar eigene Plattformen zur Veröffentlichung der kopierten Daten ins Leben rufen. Der Begriff hinter dieser Taktik nennt sich „Double Extortion“. Damit ist gemeint, dass die Angreifer einerseits die Daten nach einem Ransomware-Angriff kopieren und dann auch noch bei der Erpressung mit einer Veröffentlichung drohen. Eines der letzten Opfer waren die Technischen Werke Ludwigshafen wie Golem im Mai diesen Jahres berichtete.

Für die Cyberkriminellen bedeutet das Leaken von Informationen über eigene Kanäle mehr Sicherheit, so paradox es klingen mag, aber auch diese Gruppen haben ein ausgesprochen großes Sicherheitsbedürfnis. Durch die Unabhängigkeit von Darknet-Märkten müssen sie sich weniger Sorgen darum machen enttarnt und von den Ermittlungsbehörden gefasst zu werden. Das Kommen und Gehen dieser Marktplätze muss sie also nicht mehr interessieren, zumal die Umsätze wie im Fall des kürzlich geschlossenen Empire Markets <https://news.bitcoin.com/sources-say-worlds-largest-darknet-empire-market-exit-scammed-30-million-in-bitcoin-stolen/> auch schnell von den Betreibern der Plattformen sozialisiert werden können.

Setzt sich dieser Trend fort, so müssen Firmen nicht nur fürchten, dass ihre Informationen verschlüsselt werden und unter Umständen verloren sind, sondern auch, dass zunehmend auch personenbezogene und für die Unternehmen selbst sensible Dokumente veröffentlicht werden. Dies zieht dann nicht nur die üblichen DSGVO-Strafen nach sich, sondern erhöht den Reputationsschaden für das Opfer enorm.

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