アサヒを襲ったランサムウェア集団“麒麟”（Qilin）とは？
世界中で被害多発、カルテル結成でさらに勢力拡大も

22161020　露原秀斗

アサヒグループHDのサイバー攻撃

・酒類や飲料など国内グループ各社の受注・出荷業務と、客からの問い合わせを受けるコールセンター業務が停止

・「Qilin」が犯行声明を出していることや、同グループがダークウェブ上のリークサイトで窃取した情報のサンプルを公開したと主張

・10月8日、サイバー攻撃の被害を巡り、流出した疑いのある情報をインターネット上で確認したと発表

Qilinとは

・「サービスとしてのランサムウェア（RaaS）」と呼ばれる犯罪ビジネスを展開する集団

・狙った相手のデータを暗号化するランサムウェアのコードや、恐喝用のデータ暴露サイトなどのインフラを実行犯に提供して分配金を受け取る

・不正侵入を専業とする「イニシャルアクセスブローカー」（IAB）集団と提携

被害

・米国や欧州の大手企業から地方自治体、アフリカのNPOまで多岐にわたる

・2022年に登場し、25年9月21日までに犯行声明を出した件数は792件、25カ国以上の攻撃に関与

・被害額は1件当たり600万～4000万ドル（9億～60億円）

・中国軍や北朝鮮などの国家が関与する集団も顧客としてQilinのサービスを利用していたとの情報も

ランサムウェア3集団が提携

・有力ランサムウェア集団の「LockBit」および「DragonForce」と手を組んで、25年9月3日にカルテルを結成

・各集団の手口やリソース、インフラを共有することで、ランサムウェアビジネスの運営能力を強化し、攻撃の頻度や効率の向上を狙う

・原子力発電所のような施設が標的にされる可能性もあると指摘

コメント

・ビジネスモデル化した以上、確実に収益を上げることを狙ってくることを考えると、より実害の出る攻撃が増えていくのでしょう。

・世の中には様々な犯罪集団がありますが、数多の犯罪集団の中でハッカーは摘発されたり壊滅に追い込まれるケースが少ない様に感じます。更なる国際機関や各国警察の活動を願うばかりです。

・「サイバー空間における安全保障」は、もはや一企業のセキュリティ対策の範疇を超え、国家の存亡と国民の生活基盤に直結する喫緊の課題と捉えるべき。

感想

・個人の犯行ではなく組織化しており、闇フォーラムに広告を出したり、提携関係を築いたりと、企業のような運営を行ってることに恐ろしさを感じた。

・今後はセキュリティ対策がされているかを条件に、利用の有無を考える必要があるのかもしれないと思う。