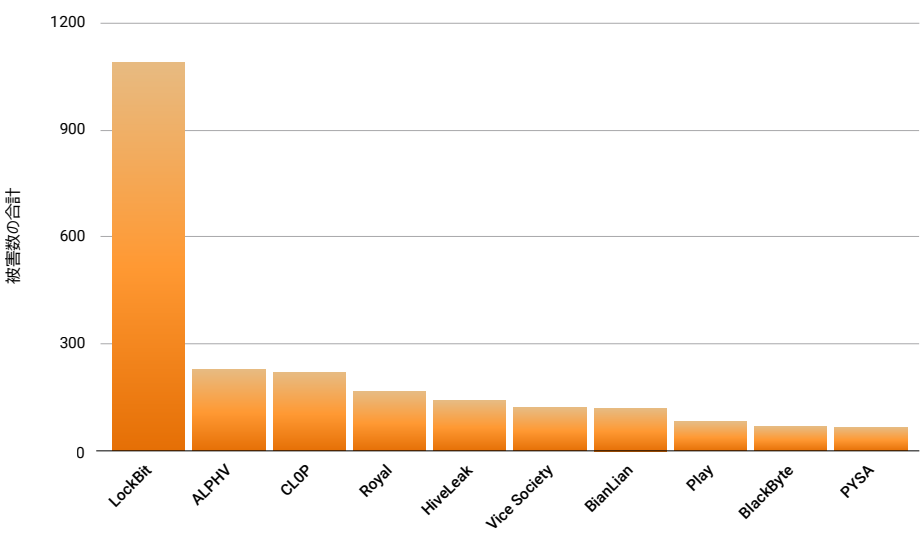
猛威を振るうランサムウェア

進化する悪用手法と執拗なゼロデイの利用

ランサムウェアグループの動きが活発になっています。彼らはゼロデイやワンデイの脆弱性悪用などの積極的な攻撃手法やいくつもの脅迫手法を用いて、企業への損害を最大化しようとしています。

LockBit は企業が受けた被害の 39% を占め、ランサムウェアの上位となる

ランサムウェアグループ別の被害件数
2021 年 10 月 1 日～2023 年 5 月 31 日



LockBit の攻撃が成功している背景には、ソフトウェアを継続的に改良していることが挙げられます。しかしながら、CL0P が支配的な地位を獲得しつつあり、ファイル転送ソフトウェアのゼロデイ脆弱性の悪用によって悪名を高めてきています。

143% ↑

CL0P などのグループによるゼロデイ脆弱性やワンデイ脆弱性の積極的な悪用により、ランサムウェアの被害企業が増加している

複数のランサムウェアグループの攻撃を受けた企業は、**最初の攻撃から 3 か月以内に**後続の攻撃を受ける可能性が **6 倍高い**

77%
ヨーロッパ、中東、アフリカ（EMEA）地域で**ランサムウェアの被害者が増加**

204%
アジア太平洋・日本（APJ）地域で**ランサムウェアの被害が増加**

攻撃者は脅迫戦術をどう最大限に活用するのか？

最初の足がかり
（スピア）フィッシング、セロデイ／ワンデイ脆弱性、Credential Abuse

ラテラルムーブメント
ネットワーク全体に拡散して最大の損害を与えます

データ窃取
貴重なデータを検出して盗みます。これは、脅迫でまず用いられる方法の 1 つになっています

暗号化
効率的かつ強固な暗号化により、復旧を妨げ、業務を中断させます

身代金要求
被害者が身代金を支払わない場合、攻撃者によって機密データがリークサイトに公開されます

ランサムウェアグループは、データ窃取に直接的につながりかねない脆弱性を悪用する可能性があります

直近の数か月で、窃取したデータのみを人質として利用するランサムウェア攻撃者も現れています

DDoS 攻撃
業務を中断させる DDoS 攻撃は、追加の脅迫戦術として機能します

脅迫と嫌がらせ
攻撃者は被害者の顧客やパートナーに対し、電話やメールで圧力をかけます

被害企業に身代金の支払いを迫る、更なる圧力

ランサムウェアのトレンド、攻撃手法の変化、緩和戦略に関する詳細と知見については、レポートの全文をご覧ください。

レポートの全文をダウンロード

 | サポート | 公開日：2023 年 8 月