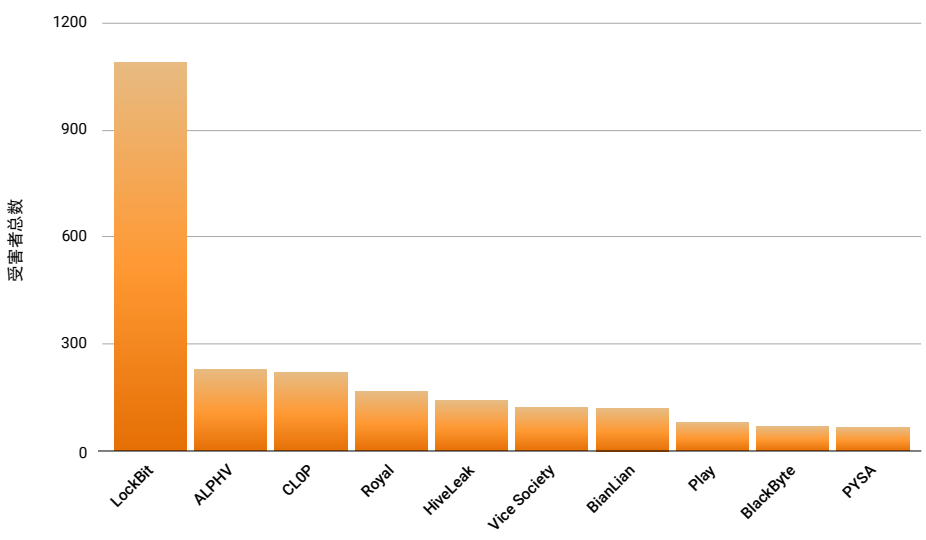
勒索软件异常活跃

漏洞利用技术花样翻新，零日漏洞深受黑客青睐

勒索软件团伙异常活跃，他们使用“零日”和“一日”漏洞滥用等激进的攻击方法以及多种勒索攻击方法，最大限度地增加受害企业的损失。

LockBit 在勒索软件形势中占据主导地位，有 39% 的受害企业受其影响

勒索软件团伙攻击的受害者数量
2021 年 10 月 1 日–2023 年 5 月 31 日



遭受 LockBit 攻击的企业之所以最多，与 LockBit 持续改进软件功能密不可分。但遭受 CL0P 攻击的企业数量也越来越多，这种勒索软件因肆意利用文件传输软件内的零日漏洞而臭名昭著。

143% ↑

由于 CL0P 等团伙对“零日”和“一日”漏洞的积极利用，导致勒索软件受害者出现的增幅

与其他受害者相比，受多个勒索软件攻击团伙攻击的受害者在首次遭受攻击后的前 3 个月内遭受后续攻击的可能性几乎达到 6 倍

77%
欧洲、中东和非洲 (EMEA) 地区的**勒索软件受害者**增幅

204%
亚太地区及日本 (APJ) 的**勒索软件受害者**增幅

攻击者如何最大限度提升其勒索手段造成的损害？

初始立足点
（鱼叉式）网络钓鱼攻击、“零日”和“一日”漏洞、撞库

横向移动
在整个网络中传播，尽可能扩大损害或影响

渗透
寻找并窃取有价值的数据：这正成为主要勒索手段之一

加密
加密方法高效且难以破解，以阻止受害者恢复，并导致运营中断

索要赎金
受害者支付赎金，或者攻击者在数据泄露网站上公布其机密数据

勒索软件团伙可能利用漏洞直接窃取数据

近几个月来，部分勒索软件攻击者仅使用泄露的数据来勒索赎金

DDoS 攻击
通过 DDoS 攻击中断运营；以此作为额外的勒索手段

恐吓和骚扰
攻击者通过电话或电子邮件联系受害者的客户或合作伙伴，以向受害者施加压力

施加额外压力，强迫受害者支付赎金

如需了解勒索软件趋势、攻击技术变化和抵御策略的更多信息和见解，请阅读完整报告。

下载完整报告

扫码关注，获取最新CDN前沿资讯

©2023 Akamai Technologies | 支持 | 发布时间：2023 年 8 月