

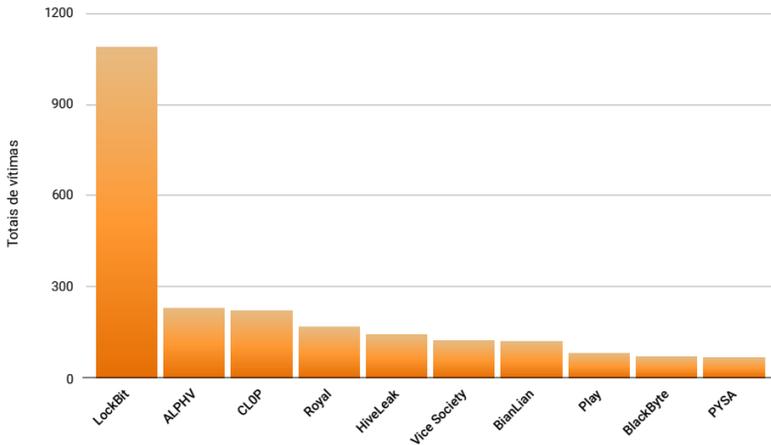
Ransomware à espreita

Técnicas de exploração em evolução e a busca ativa de dias zero

Os grupos de ransomware estão à espreita, usando métodos agressivos de vitimização, como abuso de vulnerabilidade de dia zero e de dia um, e vários esquemas de extorsão para maximizar os danos às organizações.

LockBit domina a cena do ransomware, representando 39% das organizações vítimas

Número de vítimas de grupos de ransomware
1 de outubro de 2021 – 31 de maio de 2023



O sucesso da LockBit pode ser atribuído às constantes melhorias em seu software. No entanto, o CLOP está ganhando domínio e criando um nome para si mesmo com seu abuso desenfreado de vulnerabilidades de dia zero no software de transferência de arquivos.

143% ↑

Aumento das vítimas de ransomware devido ao abuso ativo de vulnerabilidades de dia zero e de um dia por grupos como o CLOP



As vítimas atacadas por vários grupos de ransomware têm quase **6 vezes mais** probabilidade de sofrer um ataque subsequente nos primeiros 3 meses



77%

Aumento das vítimas de ransomware na Europa, Oriente Médio e África (EMEA)

204%

Aumento das vítimas de ransomware na região da Ásia-Pacífico e no Japão (APJ)

Como os invasores maximizam suas táticas de extorsão?

Posição inicial
(Spear) Phishing, vulnerabilidades de dia zero e dia um, abuso de credenciais



Movimentação lateral
Espalhar-se pela rede para obter o máximo de danos ou impactos



Exfiltração
Localizar e roubar dados valiosos: este está se tornando um dos principais métodos de extorsão



Criptografia
Criptografia eficiente e segura para impedir a recuperação e interromper as operações



Exigência de resgate
As vítimas pagam o resgate, ou os invasores publicam seus dados confidenciais em locais de vazamento



Ataques de DDoS
Ataques de DDoS para interromper operações; serve como uma tática de extorsão adicional



Intimidação e assédio
Os invasores ligam ou enviam e-mail a clientes ou parceiros da vítima para aumentar a pressão



Os grupos de ransomware podem explorar vulnerabilidades que podem levar diretamente ao roubo de dados

Nos últimos meses, alguns invasores de ransomware usaram apenas dados exfiltrados para resgate

Pressão adicional para coagir as vítimas a pagar resgate



Para mais informações e insights sobre tendências de ransomware, a mudança nas técnicas de ataque e estratégias de atenuação, leia nosso relatório completo.

Baixe o relatório completo