

---

# Qilin lidera ataques de ransomware à medida que novos grupos surgem n

Data: 2025-09-21 07:44:50

Autor: Inteligência Against Invaders

[Redazione RHC](#):21 Setembro 2025 09:13

Qilin continua a liderar o caminho entre todos os grupos de ataque cripto ativos, *significativamente atrasado em relação aos seus concorrentes no número de incidentes comunicados*. De acordo com [um relatório recente da Cyble](#), o grupo atacou **104 organizações somente em agosto, enquanto seu rival mais próximo, Akira, afetou apenas 56 vítimas**. Todavia *Novos atores surgiram, cuja atividade rápida pode mudar drasticamente o equilíbrio de poder no cenário de ransomware em um futuro próximo*.

O número total de ataques registrados em agosto atingiu **467, marcando o quarto mês consecutivo desse crescimento de incidentes**. O pico registrado em fevereiro permanece insuperável. Particularmente alarmante é a tendência crescente de ataques às cadeias de suprimentos de software: esses incidentes estão se tornando cada vez mais comuns e as consequências de tais invasões podem ser generalizadas.

Após o declínio acentuado em **Resgate Hub** atividade no início de abril, *Qilin conseguiu fortalecer significativamente sua posição: desde então, o grupo relatou atacar 398 alvos, 70% a mais do que Akira no mesmo período*. De acordo com a Cyble, Qilin recrutou com sucesso **muitos ex-parceiros e participantes da infraestrutura do RansomHub**, oferecendo-lhes condições e oportunidades atraentes. Como resultado, **Qilin controla mais de 18% de todos os ataques de abril a agosto, enquanto a participação de Akira é limitada a 10,7%**.

No entanto, a verdadeira notícia nos últimos meses tem sido **a ascensão meteórica do grupo Sinobi**, que surgiu há apenas dois meses e já se tornou o terceiro maior cibercriminoso em termos de ataques. Dos 41 alvos declarados, a grande maioria está localizada nos Estados Unidos. Pesquisadores da Cyble *destacam semelhanças entre a infraestrutura técnica e os dados vazados do Sinobi e de outros grupos ativos, particularmente Lynx e INC Ransom*. No entanto, todos os três continuam a operar de forma independente, lançando dúvidas sobre a hipótese de rebranding e, em vez disso, sugerindo cooperação interna.

Vale a pena notar que *Sinobi relatou apenas um novo incidente desde 24 de agosto*. Isso pode indicar *um mudança de tática ou o alcance de um limite organizacional: um aumento acentuado geralmente segue um declínio igualmente rápido*.

Não menos notável é o surgimento de outro recém-chegado: **Os cavalheiros**. Desde o início de setembro, reivindicou a responsabilidade por mais de 30 ataques e, se seu ímpeto continuar, sua participação de mercado poderá ser comparável à dos atuais líderes até o final do mês.

---

O aumento da atividade do LockBit, anteriormente considerado o maior grupo de ransomware, está aumentando as tensões. O lançamento de uma nova versão da ferramenta, o LockBit 5.0, indica uma tentativa de recuperar a influência perdida e reafirmar sua posição dominante. O sucesso da campanha só será evidente depois de setembro, mas a crescente competição entre veteranos e novos jogadores já é evidente.

Em sua conclusão, a Cyble enfatiza que a constante evolução de grupos e modificações em suas soluções de software continuam sendo a principal ameaça à infraestrutura corporativa e aos serviços de segurança. O impacto de tais ataques afeta não apenas o setor financeiro, mas também a infraestrutura crítica, cadeias de suprimentos, processos de negócios e modelos operacionais corporativos.

Manter a máxima prontidão e monitoramento constante são as únicas medidas eficazes em um ambiente ciberdelinqüente cada vez mais agressivo. dinâmico.

### **Redação**

A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

[Lista degli articoli](#)