Qilin Reivindica Ataque de Ransomware às Escolas de Mecklenburg

Data: 2025-10-07 16:45:00

Autor: Inteligência Against Invaders

Um ataque de ransomware que interrompeu as operações nas Escolas Públicas do Condado de

Mecklenburg (MCPS) no início de setembro foi reivindicado pelo grupo russo de crimes cibernéticos Qilin.

A gangue disse que roubou 305 GB de dados confidenciais do distrito do sul da Virgínia, incluindo registros financeiros, documentos de subsídios, orçamentos e arquivos médicos de crianças.

Ataque cibernético fecha escolas

MCPS alertou as famílias pela primeira vez sobre um incidente de segurança cibernética em setembro de 22025. O ataque forçou os professores a ficarem offline, deixando-os dependentes de caneta, papel e quadros brancos para instrução. Os sistemas de Internet foram restaurados cerca de uma semana depois.

Mais tarde, a Qilin publicou imagens de amostra online, que alegou serem parte dos arquivos roubados. O superintendente Scott Worner confirmou que o grupo estava por trás do ataque, mas afirmou que o distrito escolar ainda está avaliando a extensão da violação.

“Não pretendemos avançar com o pagamento neste momento”, disse Worner.

“A decisão final depende das conclusões da investigação e de quais arquivos foram criptografados e/ou roubados.”

Ele também pediu a outros distritos que se preparem para ameaças cibernéticas.

“Não é se. É quando”, disse ele.

“Quem quer que seja sua seguradora, certifique-se de que sua cobertura de segurança cibernética esteja atualizada.”

O Alcance Crescente do Ransomware Qilin

Qilin é uma operação de ransomware que surgiu no final de 2022 e é executada como um Rede de ransomware como serviço. Os afiliados usam seu malware para lançar ataques e compartilhar os lucros do resgate. O grupo espalha seu malware principalmente por meio de e-mails de phishing.

Até agora, em 2025, Qilin reivindicou a responsabilidade por 103 incidentes de ransomware

confirmados e 470 não verificados. As instituições educacionais têm sido alvos frequentes.

Outras vítimas deste ano incluem:

- Universidade do Oeste do Novo México
- Escolas Públicas do Condado de Botetourt na Virgínia
- Escolas públicas de Fort Smith em Arkansas
- Belmont Christian College na Austrália

Leia mais sobre ameaças de ransomware às escolas: ICO alerta sobre violações de dados lideradas por alunos em escolas do Reino Unido

Impacto crescente na educação

Dados da Comparitech mostram pelo menos 33 ataques de ransomware confirmados em escolas, faculdades e universidades americanas em 2025, com outros 62 reivindicados, mas não verificados.

Somente em setembro, distritos no Texas e no Arizona divulgaram novos incidentes.

O setor educacional enfrenta desafios únicos na resposta a violações, levando em média 4,8 meses para notificar os indivíduos afetados.

Esses ataques geralmente prejudicam operações essenciais, desde frequência e notas até folha de pagamento e sistemas de comunicação, ao mesmo tempo em que expõem funcionários e alunos a possíveis fraudes de identidade.