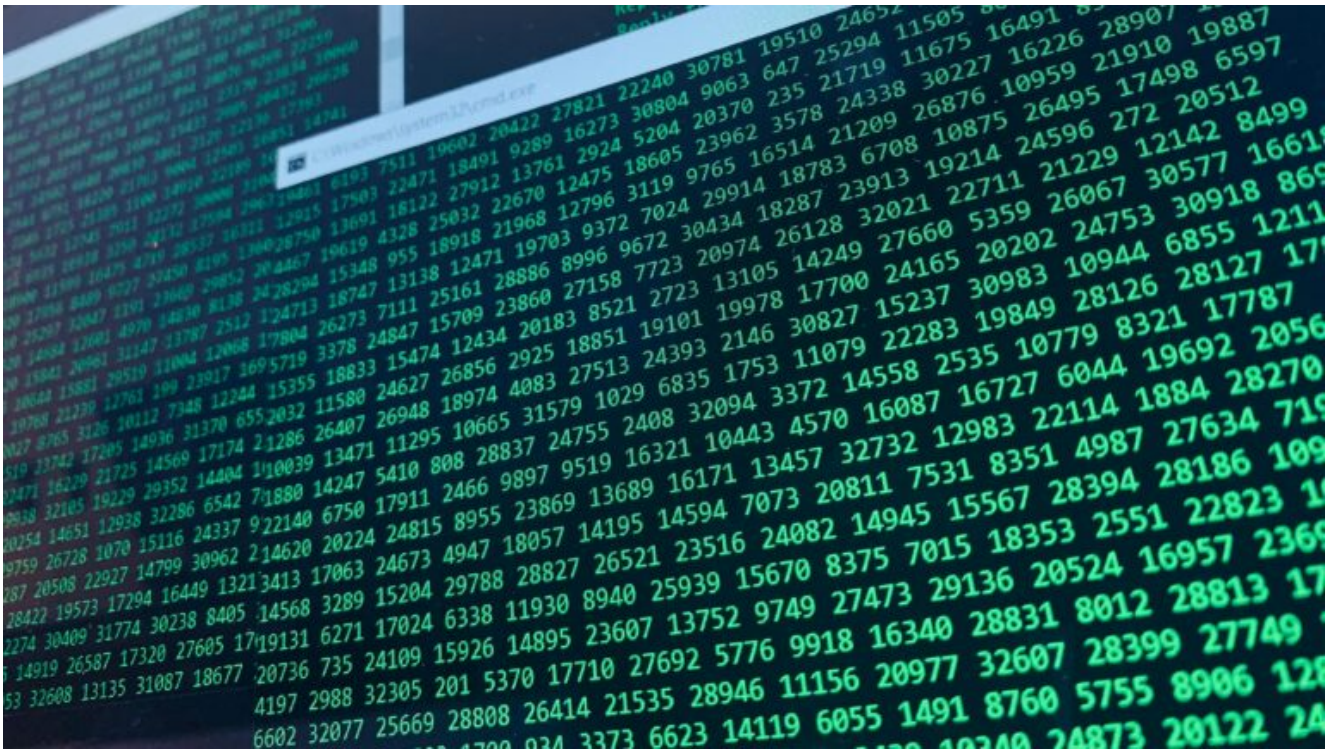
Indústria transformadora tornou-se o principal alvo do cibercrime em 2025

written by O Cidadão | 14 de Abril, 2026



A conclusão é clara, os cibercriminosos deixaram de atingir a indústria por oportunidade e passaram **a fazê lo de forma deliberada.** A forte dependência de processos contínuos, a existência de ambientes operacionais críticos, a interligação entre IT e OT e a crescente complexidade das cadeias de abastecimento criaram um contexto altamente favorável para campanhas de extorsão, sabotagem e roubo de dados.

Em 2025, o ransomware manteve se como o principal vector de ataque no sector industrial, com 890 incidentes registados, seguido de ações de defacement, com 526 casos, de disrupção de sistemas de informação, com 345 ocorrências, e de ataques centrados em violação e fuga de dados, com 144 incidentes. Estes números mostram que a ameaça já não se limita à encriptação de sistemas, estendendo se a campanhas multietapa orientadas para paralisar operações, extrair informação

sensível e maximizar pressão financeira e reputacional sobre as organizações.

O relatório mostra ainda que os Estados Unidos lideraram o número de incidentes de ransomware dirigidos à indústria transformadora, com 713 casos, seguidos da Índia, com 201, da Alemanha, com 79, do Reino Unido, com 65, e do Canadá, com 62. A dispersão geográfica confirma que tanto economias industriais maduras como mercados em forte crescimento estão hoje expostos a níveis semelhantes de risco.

Entre os grupos mais ativos contra o sector destacam se Akira, com 121 incidentes associados, Qilin, com 118, Play e ALOLI01, ambos com 77, e NoName057(16), com 72. Também Chinafans, Clop, Safepay, Mr. BDRK28 e x7root figuram entre os principais actores que têm explorado fragilidades do ecossistema industrial, seja através de ransomware, ataques de negação de serviço, reconhecimento de infraestruturas OT ou compromissos de websites públicos.

Segundo a investigação da Check Point, há três fatores estruturais que ajudam a explicar esta exposição crescente. Em primeiro lugar, muitos fabricantes continuam a operar com sistemas OT legados, incluindo PLCs, SCADA e dispositivos IoT industriais que não foram concebidos com mecanismos modernos de segurança. Em segundo lugar, o aumento da interdependência com fornecedores, prestadores de serviços e plataformas SaaS expandiu a superfície de ataque. Em 2025, os ataques à cadeia de abastecimento quase duplicaram, subindo de 154 para 297 incidentes. Em terceiro lugar, o modelo de ransomware as a service continua a industrializar o cibercrime, permitindo a afiliados escalar operações com rapidez, reutilizar ferramentas testadas e adaptar campanhas por geografia e por sector.

“Os dados deste relatório mostram uma mudança clara no perfil das ameaças dirigidas à indústria transformadora. Os atacantes reconhecem que qualquer paragem operacional neste sector tem

um impacto imediato, tanto financeiro como logístico, o que torna estas organizações alvos especialmente apetecíveis para campanhas de ransomware, roubo de dados e disrupção de sistemas. Numa realidade em que ambientes IT e OT estão cada vez mais interligados, a cibersegurança tem de ser encarada como uma prioridade de negócio e não apenas como uma questão técnica. As empresas do sector precisam de reforçar a sua resiliência com uma abordagem assente em prevenção, visibilidade e resposta rápida, sob pena de enfrentarem consequências cada vez mais graves ao longo de toda a cadeia de valor." Afirma Rui Duro, Country Manager para Portugal da Check Point Software.

A Check Point alerta também para a crescente valorização de credenciais de acesso industrial em mercados clandestinos, bem como para o **uso crescente de campanhas de phishing mais sofisticadas**, reforçadas por inteligência artificial, para acelerar o tempo entre a intrusão inicial e o impacto operacional. O resultado é uma redução da janela de deteção e resposta e um aumento do potencial de propagação entre ambientes IT e OT.

Perante este cenário, a prioridade das organizações industriais deve passar por uma revisão profunda da sua estratégia de defesa. A Check Point recomenda a adoção de arquiteturas Zero Trust em ambientes IT e OT, segmentação rigorosa de rede, reforço da gestão de vulnerabilidades e de credenciais, implementação de MFA e SSO, utilização de backups imutáveis e offline, e controlo mais apertado sobre acessos de terceiros. A formação dos colaboradores continua igualmente crítica, sobretudo num contexto em que o phishing assistido por IA se torna mais convincente e direcionado.

A evolução da ameaça indica ainda que 2026 poderá trazer campanhas mais rápidas, automatizadas e destrutivas contra a **indústria transformadora**, com maior recurso a extorsão baseada em dados e menor tempo de permanência dos atacantes nas redes antes da execução do ataque. Para as organizações industriais,

a cibersegurança deixou de ser uma função de suporte e passou a ser uma condição essencial para garantir continuidade operacional, resiliência e confiança em toda a cadeia de valor.