ANÁLISE DE GRUPOS DE AMEAÇAS AVANÇADAS DIRECIONADAS A INFRAESTRUTURAS INDUSTRIAIS (ICS/OT): TÁTICAS, FERRAMENTAS E INTER-RELAÇÕES

Rodrigo Caio Koelln Alfonsin

Universidade Tecnológica Federal do Paraná, Medianeira, Brasil
alfonsin@alunos.utfpr.edu.br

Resumo: A convergência entre TI/TO ampliou a superfície de ataque em infraestruturas críticas. Este trabalho tem o objetivo de analisar as táticas e procedimentos de 24 grupos de ameaças a ambientes ICS/OT. O método consistiu na análise documental via MITRE ATT&CK e relatórios de inteligência da empresa Dragos, baseando-se na ICS Cyber Kill Chain. Conclui-se que as defesas industriais devem transcender o isolamento de rede, exigindo monitoramento comportamental profundo contra ataques destrutivos.

Palavras-chave: Cibersegurança; Defesa Cibernética; Inteligência de Ameaças; Cyber Kill Chain; Sistemas de Segurança Instrumentada.

INTRODUÇÃO

A crescente convergência entre redes de Tecnologia da Informação (TI) e redes de Tecnologia Operacional (TO) ampliou significativamente a superfície de ataque de infraestruturas críticas. Ambientes que historicamente operavam de forma isolada (modelo *air-gapped*), como usinas elétricas, plantas de manufatura e instalações de tratamento de água, passaram a estar interconectados para otimização de processos, expondo Sistemas de Controle Industrial (ICS) a atores de ameaças cada vez mais sofisticados (Dragos, 2025; Mitre, 2023a).

Para modelar e combater essas ameaças, a indústria de segurança adotou inicialmente a *Cyber Kill Chain*, desenvolvida pela Lockheed Martin, que se provou um modelo altamente bem-sucedido para intrusões em redes corporativas tradicionais (Hutchins et al., 2011). No entanto, ataques direcionados a ambientes ICS exigem um rigor diferente. O adversário precisa adquirir um conhecimento íntimo sobre os processos físicos, os protocolos industriais empregados e as decisões de design do sistema de segurança (Assante e Lee, 2015).

Para refletir essa complexidade, a *ICS Cyber Kill Chain*, divide o ataque cibernético em dois estágios práticos. O Estágio 1 assemelha-se a campanhas tradicionais de espionagem: planejamento, intrusão na rede de TI, movimento lateral e coleta de inteligência. Já o Estágio 2 representa a fase crítica, na qual o invasor desenvolve, testa e implanta cargas úteis (*payloads*) customizadas para interagir fisicamente com controladores industriais, visando degradar, perturbar ou destruir processos físicos (Assante e Lee, 2015).

Este trabalho tem como objetivos descrever e comparar sistematicamente 24 grupos de ameaças relevantes identificados na literatura técnica, mapear suas Táticas, Técnicas e Procedimentos (TTPs) utilizando matrizes padronizadas, analisar as inter-relações funcionais entre eles e, por fim, propor implicações defensivas práticas e estratégicas para organizações que operam ambientes ICS/OT.

MATERIAL E MÉTODOS

A pesquisa caracteriza-se como um estudo exploratório e descritivo, fundamentado na análise documental de relatórios de inteligência de ameaças. A base de dados primária foi composta pelos relatórios anuais e alertas específicos da empresa Dragos, bem como pelas matrizes do framework MITRE ATT&CK for ICS (Dragos, 2025; Mitre, 2023a).
O referencial teórico central é o modelo ICS Cyber Kill Chain, proposto por Assante e Lee, que descreve dois estágios distintos de operações adversariais contra ambientes industriais: o Estágio 1, equivalente a espionagem e intrusão inicial em redes IT/OT, e o Estágio 2, que compreende o desenvolvimento, teste e execução de capacidades capazes de causar impacto físico direto nos processos industriais (Assante e Lee, 2015). Os 24 grupos selecionados foram classificados com base em quatro critérios: (1) nível de capacidade no ICS Kill Chain; (2) atribuição a Estado-nação ou organização criminosa; (3) setor-alvo primário; e (4) relacionamento de sobreposição ou habilitação com outros grupos (Assante e Lee, 2015; Hutchins et al., 2011).

RESULTADOS E DISCUSSÃO

A análise sistemática evidencia uma separação clara no ecossistema adversarial direcionado a ambientes ICS/OT. Apenas um subconjunto restrito de grupos possui as capacidades específicas para operar no Estágio 2 da ICS Cyber Kill Chain, que compreende a execução de ataques para manipular, interromper ou destruir processos industriais.

Destacam-se o grupo CHERNOVITE, desenvolvedor do framework modular PIPEDREAM, focado em redes elétricas e gás natural liquefeito, e o grupo XENOTIME, responsável pelo malware TRISIS, único documentado a comprometer intencionalmente Sistemas de Segurança Instrumentada (SIS) (Dragos, 2018c; 2022b). O grupo ELECTRUM (ligado ao Sandworm russo) também figura neste patamar, sendo o causador do apagão na Ucrânia em 2016 com o malware CRASHOVERRIDE.

A Tabela 1 consolida os 24 grupos analisados, apresentando seus respectivos estágios na Kill Chain, setores-alvo e ferramentas principais, conforme rastreamento pela Dragos e pelo MITRE ATT&CK (Dragos, 2025; Mitre, 2023a).

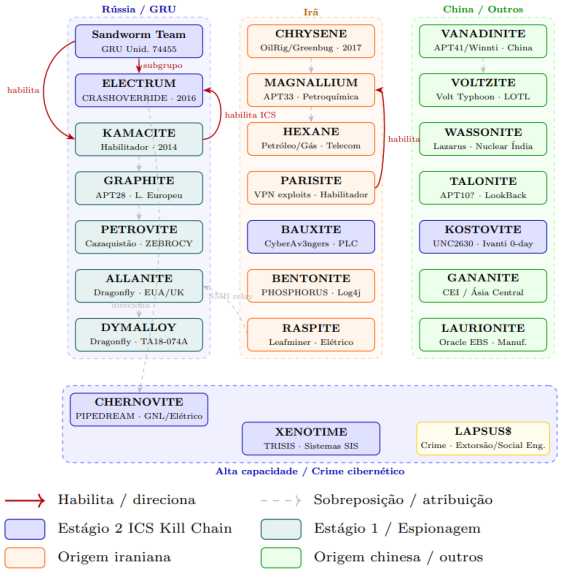
Tabela 1. Comparativo de capacidades dos 24 grupos de ameaças ICS/OT analisados.

Grupo	Kill Chain	Alvo	Ferramenta
CHERNOVITE	Estágio 2	GNL e Elétrico	PIPEDREAM
XENOTIME	Estágio 2	Petróleo e Gás	TRISIS
ELECTRUM	Estágio 2	Elétrico	CRASHOVERRIDE
BAUXITE	Estágio 2	Global (ICS)	Backdoor MQTT
KAMACITE	Estágio 1	Elétrico e Gás	Malware customizado
VOLTZITE	Estágio 1	Elétrico, Telecom (EUA)	*Living off the Land* (LOTL)
KOSTOVITE	Estágio 2	Energia Renovável	*Living off the Land* (LOTL)
CHRYSENE	Estágio 1	Petroquímica, Elétrico	Malware 64-bit, IPv6 C2
PARISITE	Estágio 1	P&G, Utilities	Impacket, MASSCAN
GRAPHITE	Estágio 1	Energia, Logística	HEADLACE, OCEANMAP
MAGNALLIUM	Estágio 1	Petroquímica, Aeroespacial	StoneDrill, PowerShell
HEXANE	Estágio 1	P&G, Telecom	Excel malicioso, DNS C2
VANADINITE	Estágio 1	Manufatura, Energia	Cobalt Strike, Metasploit
WASSONITE	Estágio 1	Nuclear, Manufatura	DTrack, Mimikatz
ALLANITE	Estágio 1	Elétrico (EUA/UK)	Watering hole, Screencap
BENTONITE	Estágio 1	P&G marítimo, Manufatura	PowerShell
DYMALLOY	Estágio 1	Elétrico, P&G	Goodor, Karagany
PETROVITE	Estágio 1	Mineração, Energia	ZEBROCY
TALONITE	Estágio 1	Elétrico (EUA)	LookBack, FlowCloud
RASPITE	Estágio 1	Elétrico	SMB Relay, RDP
STIBNITE	Estágio 1	Energia Eólica	PoetRAT

Em termos de TTPs, o uso de abordagens *Living off the Land* (LOTL), onde o invasor utiliza ferramentas legítimas do próprio sistema da vítima, como ocorreu na campanha do grupo KOSTOVITE, tem dificultado substancialmente a detecção precoce (Dragos, 2021b).

Como implicações defensivas diretas, os resultados indicam a necessidade urgente de: Implementação de monitoramento passivo de tráfego exclusivo para OT; Autenticação multifator resistente a *phishing* (FIDO2) nas fronteiras IT/OT; Isolamento lógico rigoroso de Sistemas de Segurança (SIS); e Monitoramento focado no uso anômalo de ferramentas nativas como PowerShell e WMI.

Figura 1. Mapeamento das inter-relações e capacidades (ICS Kill Chain) dos grupos de ameaças.



Fonte: Elaborado pelo autor (2026) com base em Dragos (2025) e Mitre (2023).

A dependência funcional entre KAMACITE e ELECTRUM demonstra que ataques de alto impacto são resultado de operações colaborativas de longo prazo, e não de incidentes isolados (Dragos, 2025).

CONCLUSÃO

A análise do ecossistema adversarial revela uma clara separação: enquanto a maioria atua como habilitadora de acesso (Estágio 1), uma parcela crítica possui capacidades destrutivas reais no Estágio 2. A consolidação de frameworks modulares e reutilizáveis, a exemplo do PIPEDREAM e do TRISIS, evidencia que os adversários estão evoluindo de ataques customizados para plataformas adaptáveis a múltiplos setores, representando riscos diretos a processos físicos e a vidas humanas. Consequentemente, o modelo tradicional de isolamento de rede não é mais suficiente para garantir a segurança industrial. É importante que as organizações adotem o monitoramento comportamental profundo, capaz de identificar malwares específicos e táticas de *Living off the Land* (LOTL). Para acompanhar essa evolução das ameaças, pesquisas futuras devem focar na aplicação de inteligência artificial para a correlação automatizada de TTPs e na criação de respostas a incidentes moldadas por perfil adversarial.

REFERÊNCIAS

ASSANTE, M. J.; LEE, R. M. The Industrial Control System Cyber Kill Chain. SANS Institute InfoSec Reading Room, out. 2015. Disponível em: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297. Acesso em: 4 maio 2026.

DRAGOS INC. ELECTRUM and CRASHOVERRIDE. Dragos Threat Intelligence, 2017. Disponível em: https://www.dragos.com/threat/electrum. Acesso em: 4 maio 2026.

DRAGOS INC. CHRYSENE Threat Group. Dragos Threat Intelligence, 2018a. Disponível em: https://www.dragos.com/threat/chrysene. Acesso em: 4 maio 2026.

DRAGOS INC. RASPITE Threat Group. Dragos Threat Intelligence, 2018b. Disponível em: https://www.dragos.com/threat/raspite. Acesso em: 4 maio 2026.

DRAGOS INC. XENOTIME and TRISIS/TRITON Malware. Dragos Threat Intelligence, 2018c. Disponível em: https://www.dragos.com/threat/xenotime. Acesso em: 4 maio 2026.

DRAGOS INC. HEXANE Threat Group. Dragos Threat Intelligence, 2019a. Disponível em: https://www.dragos.com/threat/hexane. Acesso em: 4 maio 2026.

DRAGOS INC. MAGNALLIUM Threat Group. Dragos Threat Intelligence, 2019b. Disponível em: https://www.dragos.com/threat/magnallium. Acesso em: 4 maio 2026.

DRAGOS INC. PARISITE Threat Group. Dragos Threat Intelligence, 2019c. Disponível em: https://www.dragos.com/threat/parisite. Acesso em: 4 maio 2026.

DRAGOS INC. TALONITE Threat Group. Dragos Threat Intelligence, 2019d. Disponível em: https://www.dragos.com/threat/talonite. Acesso em: 4 maio 2026.

DRAGOS INC. DYMALLOY Threat Group. Dragos Threat Intelligence, 2020a. Disponível em: https://www.dragos.com/threat/dymalloy. Acesso em: 4 maio 2026.

DRAGOS INC. STIBNITE Threat Group. Dragos Threat Intelligence, 2020b. Disponível em: https://www.dragos.com/threat/stibnite. Acesso em: 4 maio 2026.

DRAGOS INC. VANADINITE Threat Group. Dragos Threat Intelligence, 2020c. Disponível em: https://www.dragos.com/threat/vanadinite. Acesso em: 4 maio 2026.

DRAGOS INC. WASSONITE Threat Group. Dragos Threat Intelligence, 2020d. Disponível em: https://www.dragos.com/threat/wassonite. Acesso em: 4 maio 2026.

DRAGOS INC. KAMACITE Threat Group. Dragos Threat Intelligence, 2021a. Disponível em: https://www.dragos.com/threat/kamacite. Acesso em: 4 maio 2026.

DRAGOS INC. KOSTOVITE Threat Group. Dragos Threat Intelligence, 2021b. Disponível em: https://www.dragos.com/threat/kostovite. Acesso em: 4 maio 2026.

DRAGOS INC. PETROVITE Threat Group. Dragos Threat Intelligence, 2021c. Disponível em: https://www.dragos.com/threat/petrovite. Acesso em: 4 maio 2026.

DRAGOS INC. BENTONITE Threat Group. Dragos Threat Intelligence, 2022a. Disponível em: https://www.dragos.com/threat/bentonite. Acesso em: 4 maio 2026.

DRAGOS INC. CHERNOVITE Activity Group and PIPEDREAM Malware. Dragos Threat Intelligence, 2022b. Disponível em: https://www.dragos.com/threat/chernovite. Acesso em: 4 maio 2026.

DRAGOS INC. GANANITE Threat Group. Dragos Threat Intelligence, 2023. Disponível em: https://www.dragos.com/threat/gananite. Acesso em: 4 maio 2026.

DRAGOS INC. ALLANITE Threat Group. Dragos Threat Intelligence, 2024a. Disponível em: https://www.dragos.com/threat/allanite. Acesso em: 4 maio 2026.

DRAGOS INC. BAUXITE Threat Group. Dragos Threat Intelligence, 2024b. Disponível em: https://www.dragos.com/threat/bauxite. Acesso em: 4 maio 2026.

DRAGOS INC. GRAPHITE Threat Group. Dragos Threat Intelligence, 2024c. Disponível em: https://www.dragos.com/threat/graphite. Acesso em: 4 maio 2026.

DRAGOS INC. LAURIONITE Threat Group. Dragos Threat Intelligence, 2024d. Disponível em: https://www.dragos.com/threat/laurionite. Acesso em: 4 maio 2026.

DRAGOS INC. VOLTZITE Threat Group / Volt Typhoon. Dragos Threat Intelligence, 2024e. Disponível em: https://www.dragos.com/threat/voltzite. Acesso em: 4 maio 2026.

DRAGOS INC. Year in Review: ICS/OT Cybersecurity. Dragos, 2025. Disponível em: https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf. Acesso em: 4 maio 2026.

HUTCHINS, E. M.; CLOPPERT, M. J.; AMIN, R. M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Proceedings of the 6th Annual International Conference on Information Warfare and Security, 2011.

MITRE CORPORATION. ATT&CK for ICS: Tactics and Techniques. MITRE, 2023a. Disponível em: https://attack.mitre.org/matrices/ics/. Acesso em: 4 maio 2026.

MITRE CORPORATION. LAPSUS$ — Group G1004. ATT&CK, 2023b. Disponível em: https://attack.mitre.org/groups/G1004/. Acesso em: 4 maio 2026.

MITRE CORPORATION. Sandworm Team Group G0034. ATT&CK, 2023c. Disponível em: https://attack.mitre.org/groups/G0034/. Acesso em: 4 maio 2026.

MITRE CORPORATION. TEMP. Veles Group G0088. ATT&CK, 2023d. Disponível em: https://attack.mitre.org/groups/G0088/. Acesso em: 4 maio 2026.