Tendências CTI

Inteligência de Ameaças Cibernéticas

Segundo semestre 2025

Índice

Índice

1. Resumo Executivo

O segundo semestre de 2025 (S2 2025) consolidou uma evolução estrutural do cenário de ameaças cibernéticas, marcada pela convergência entre tensões geopolíticas, a profissionalização do cibercrime e a maturidade tecnológica dos agentes de ameaça, em vez do surgimento de técnicas radicalmente novas. O período foi definido por uma mudança profunda na lógica operacional do atacante, orientada para persistência, furtividade e maximização do impacto econômico, estratégico e reputacional.

O ciberespaço foi confirmado como um domínio central de confronto híbrido, integrado de forma estável às dinâmicas geopolíticas globais. Conflitos prolongados e rivalidades estratégicas têm sido projetados sobre infraestruturas digitais, cadeias de suprimentos e ecossistemas tecnológicos, gerando efeitos transversais que afetam governos, setores críticos e organizações privadas. A fragmentação geoeconômica, a soberania digital e a reconfiguração das alianças tecnológicas reforçaram um ambiente mais volátil, menos cooperativo, com maiores dificuldades de atribuição e resposta coordenada.

Do ponto de vista operacional, o semestre mostrou uma redução deliberada do ruído técnico. Os atacantes priorizaram intrusões de baixo perfil baseadas no abuso de identidades legítimas, serviços em nuvem e ferramentas comuns das organizações, reduzindo o uso de malwares tradicionais. Essa abordagem aumenta o tempo gasto em ambientes comprometidos e dificulta a detecção precoce, mudando o foco defensivo de indicadores técnicos óbvios para sinais fracos e distribuídos.

Ransonware e extorsão orientada por dados atingiram um grau avançado de industrialização. A inovação não está mais na criptografia, mas na orquestração abrangente das campanhas: automação, seleção de informações de alto valor, pressão escalonada e exploração reputacional.

Esse modelo reduz a dependência do impacto operacional direto e permite que as intrusões sejam monetizadas mesmo sem interromper completamente os serviços da vítima.

A inteligência artificial (IA) se estabeleceu como um multiplicador operacional. Seu uso foi normalizado para acelerar tarefas específicas, engenharia social, reconhecimento, adaptação de ferramentas; Reduzir custos e barreiras de entrada, sem substituir o operador humano. Por outro lado, uma aceleração sustentada na exploração de vulnerabilidades críticas foi observada após sua divulgação pública, intensificando a assimetria entre capacidades ofensivas e defensivas.

Ao mesmo tempo, o ecossistema criminoso passou por uma fragmentação significativa. A queda de grandes fóruns subterrâneos e mercados centralizados não reduz a atividade ilícita, mas sim a redistribui para mercados especializados, corretores de acesso inicial e canais privados mais opacos, dificultando o monitoramento e a obtenção de inteligência antecipada.

Ao mesmo tempo, o semestre foi marcado pelo fortalecimento do arcabouço legal e regulatório e por operações policiais internacionais de alto impacto, bem como por uma progressiva melhoria nas capacidades defensivas das organizações. No entanto, a adaptabilidade de agentes maliciosos continua superando esses avanços, destacando uma lacuna persistente entre conformidade regulatória e resiliência operacional real.

No geral, a segunda metade de 2025 trouxe um cenário em que a cibersegurança deixou de ser um problema exclusivamente tecnológico, mas um desafio sistêmico, onde identidade, confiança, processos organizacionais e contexto geopolítico são tão decisivos quanto as capacidades técnicas. Uma gestão eficaz de riscos exige uma abordagem abrangente, voltada para a detecção contextual, resiliência e antecipação estratégica diante de ameaças persistentes e altamente adaptativas.

2. Introdução

2.1. Propósito do relatório

Este relatório tem como objetivo fornecer uma análise detalhada das tendências, incidentes e eventos relevantes na área de Inteligência de Ameaças Cibernéticas durante o segundo semestre de 2025. O relatório aborda as ameaças emergentes que estão redefinindo o cenário da cibersegurança, os atores maliciosos com atividade proeminente, as campanhas cibernéticas mais significativas e as vulnerabilidades críticas detectadas nesse período. Também identifica padrões recorrentes e descreve possíveis cenários futuros que podem influenciar estratégias de gestão de riscos e mitigação.

2.2. Escopo geográfico e temporal do relatório

A análise apresentada adota uma perspectiva global, permitindo-nos entender como as ameaças evoluem de forma interconectada em diferentes contextos geográficos. Essa visão ampla facilita a identificação de dinâmicas comuns e particularidades regionais que enriquecem a compreensão do ambiente cibernético atual.

Estamos em um ambiente marcado por mudanças relevantes no comportamento de ameaças e por eventos que tiveram um impacto significativo no ecossistema digital. Esse intervalo de tempo, que vai de julho a dezembro de 2025, é fundamental para antecipar possíveis movimentos futuros e fortalecer as capacidades de resposta em um ambiente cada vez mais complexo.

3. Visão Global de ameaças

Durante a segunda metade de 2025, o cenário global de ameaças evoluiu para um ambiente mais volátil e fragmentado, marcado pela convergência de tensões geopolíticas, interrupções tecnológicas e dinâmicas econômicas adversas. Essa combinação tem aumentado de forma constante a área de exposição para governos, empresas e cidadãos, especialmente em setores críticos e ecossistemas digitais interconectados.

Os riscos digitais não se manifestam mais isoladamente, mas interagem e se reforçam, gerando impactos sistêmicos que afetam simultaneamente múltiplos setores estratégicos (World Economic Forum, 2025). Nesse contexto, o ciberespaço se estabeleceu como um vetor transversal que amplifica conflitos pré-existentes e acelera dinâmicas mais amplas de confronto.

A crescente dependência de infraestrutura digital crítica, aliada à fragmentação geoeconômica e regulatória, tem complicado a cooperação internacional em cibersegurança. A coexistência de diferentes estruturas regulatórias, modelos tecnológicos e abordagens de governança aumenta a complexidade operacional e dificulta a resposta coordenada a incidentes transfronteiriços.

Esta seção identifica os fatores estruturais do ambiente global que, devido à sua natureza sistêmica, influenciam diretamente a evolução do risco cibernético e a estabilidade dos ecossistemas digitais.

3.1 Geopolítica e Cibersegurança

Durante a segunda metade de 2025, a relação entre geopolítica e cibersegurança se intensificou a ponto de consolidar o ciberespaço como um domínio central da competição estratégica entre Estados. Rivalidades tecnológicas, tensões econômicas e a luta pelo controle de recursos críticos não se limitam mais ao nível diplomático ou comercial, mas são projetados sistematicamente em infraestruturas digitais, cadeias de suprimentos e ecossistemas tecnológicos globais.

Esse período se desenvolveu em um contexto de multipolaridade desequilibrada, caracterizada pela ausência de uma ordem internacional estável e pela coexistência de múltiplos centros de poder com capacidade suficiente para corroer ou desestabilizar o sistema sem impor regras comuns (Aznar Fernández-Montesinos, 2025). Nesse cenário, Estados Unidos, China e Rússia continuam a definir o ritmo do confronto estratégico, com efeitos diretos sobre a estabilidade do ciberespaço.

A competição geopolítica é cada vez mais articulada por meio de instrumentos geoeconômicos, sanções, controles tecnológicos, friendshoring e pressão regulatória, que atuam como catalisadores indiretos para operações cibernéticas contra setores estratégicos. Essa dinâmica contribui para redirecionar ameaças para áreas como energia, transporte, manufatura avançada e serviços financeiros, aumentando o impacto potencial de incidentes cibernéticos.

Um elemento-chave dessa evolução é a consolidação dos modelos de Internet soberana. Iniciativas como a RuNet da Rússia refletem uma abordagem de controle estatal do tráfego, serviços e governança digital, apoiada por infraestruturas autônomas e estruturas regulatórias proprietárias. Esses modelos, potencialmente replicáveis em outros contextos, têm implicações diretas para atribuição, visibilidade de incidentes e resposta coordenada, reforçando a fragmentação do ciberespaço global (Hernández, 2025).

Paralelamente, a inteligência artificial se estabeleceu como um multiplicador estratégico. Sua integração em operações de ciberespionagem, desinformação e automação ofensiva reduz barreiras de entrada, acelera ciclos de ataque e amplifica o alcance das campanhas híbridas, tanto por estados quanto por atores criminosos avançados

Nesse contexto, o ciberespaço é consolidado como o ambiente preferido para confronto abaixo do limiar de conflito armado, permitindo que pressão, perturbação e sinalização estratégica sejam exercidos com risco político e militar limitado.

Friendshoring é uma estratégia para reorganizar cadeias de suprimentos através da qual estados ou empresas transferem produção, suprimentos ou serviços críticos para países considerados aliados, parceiros estratégicos ou países politicamente com ideias semelhantes, com o objetivo de reduzir riscos geopolíticos, econômicos e de segurança.

3.2 Geopolítica e principais atores

Durante a segunda metade de 2025, os principais conflitos internacionais não passaram por transformações abruptas, mas passaram por um aprofundamento de suas dimensões híbridas, nas quais o ciberespaço é estruturalmente integrado com pressões econômicas, manobras diplomáticas e narrativas informacionais.

- Rússia – Ucrânia: aprofundando a dimensão híbrida do conflito

A guerra entre Rússia e Ucrânia continuou sem grandes avanços territoriais, mas com uma intensificação sustentada de sua dimensão híbrida. Durante esse período, a Rússia reforçou o uso do ciberespaço como complemento à pressão política, econômica e diplomática, expandindo operações não apenas contra alvos ucranianos, mas também contra instituições e empresas europeias que apoiam Kiev.

A primeira metade do ano foi marcada por um aumento nas campanhas de negação de serviço, tentativas de interromper serviços essenciais e influenciar operações voltadas a manipular a percepção pública na União Europeia, visando órgãos públicos e infraestruturas digitais de países da UE e da OTAN alinhados à Ucrânia. Ao mesmo tempo, há uma maior convergência entre atores estatais e coletivos pró-russos de hacktivismo, com uma integração mais próxima entre desinformação, exploração de vulnerabilidades e ataques direcionados a setores críticos cujo principal objetivo dessas campanhas não é a destruição de sistemas, mas a interrupção operacional e o impacto midiático.

Um elemento relevante do período foi a tendência para atribuições públicas mais explícitas por parte dos governos ocidentais. Essa mudança reflete uma mudança de uma atitude predominantemente cautelosa para uma estratégia mais orientada para a dissuasão, que busca aumentar o custo político das operações maliciosas, fortalecer a atribuição coletiva e estabelecer precedentes regulatórios, embora com o risco de escaladas controladas no nível digital.

- Oriente Médio: o ciberespaço como cenário de confronto indireto

A segunda metade de 2025 foi marcada por uma intensificação das tensões entre Irã e Israel, onde o ciberespaço funciona como palco para confrontos diretos, porém contidos. As operações observadas combinam intrusões, vazamentos, sabotagem direcionada e campanhas de manipulação de informações com o objetivo de degradar capacidades críticas sem desencadear uma escalada militar aberta.

Um risco particularmente relevante nesse contexto é o transbordamento regional. A alta interdependência tecnológica entre infraestruturas de energia, financeira e logística aumenta a probabilidade de impactos colaterais em países terceiros e atores privados. Diferente dos militares, onde cessar-fogos podem marcar pontos de virada claros, no ciberespaço a dinâmica do confronto tende a permanecer ativa de forma autônoma, mesmo quando a violência física é reduzida.

- China – Ocidente: competição sistêmica e pressão tecnológica

A rivalidade entre China e potências ocidentais não levou a conflitos abertos, mas passou por uma intensificação notável na esfera digital. Durante este semestre, os atores associados a Pequim intensificaram suas campanhas de ciberespionagem contra setores estratégicos como semicondutores, telecomunicações, energia renovável, manufatura avançada e serviços financeiros, alinhadas com objetivos industriais e tecnológicos de longo prazo.

Uma característica marcante do período foi a redução do tempo entre a divulgação de vulnerabilidades críticas e sua exploração operacional, refletindo uma estrutura de inteligência técnica altamente eficiente. Essa dinâmica aumenta a pressão sobre as empresas ocidentais e reforça o uso do ciberespaço como ferramenta para condicionar decisões estratégicas, especialmente no contexto do Indo-Pacífico e das tensões em torno de Taiwan.

Derramamento regional: propagação indireta do impacto de um conflito para terceiros ou regiões interconectadas.

- Coreia do Norte e África: Persistência e Ambientes de Oportunidade

A Coreia do Norte mantém uma atividade sustentada focada na obtenção de recursos financeiros e espionagem estratégica, com sinais crescentes de cooperação operacional com atores russos. Essa convergência amplia o escopo potencial das suas operações e adiciona complexidade aos processos de atribuição.

Paralelamente, regiões como o Sahel continuam a oferecer ambientes propícios à proliferação de atores híbridos. A combinação de fraqueza institucional, fragmentação política e presença de infraestruturas críticas facilita atividades oportunistas de sabotagem digital, espionagem e desinformação, aumentando a exposição de empresas europeias com presença na região.

No geral, o segundo semestre de 2025 confirma que geopolítica, tecnologia e cibersegurança formam um sistema interdependente, no qual tensões estratégicas são transferidas para o ciberespaço com rapidez e efeitos transversais. Essas dinâmicas, embora nem sempre se materializem em conflitos abertos, estão redefinindo o equilíbrio digital global e condicionando diretamente a segurança dos Estados, setores estratégicos e organizações privadas.

3.3 Impacto setorial específico dos ciberataques

Para concluir com a análise do cenário de ameaças para o segundo semestre de 2025, o Departamento de Inteligência de Ameaças Cibernéticas da NTT DATA é essencial para examinar a evolução dos ciberataques pelos setores e países mais afetados. Os dados registrados entre julho e dezembro mostram que, apesar da persistência de padrões consolidados nos semestres anteriores, variações relevantes são observadas associadas à intensificação das tensões geopolíticas e ao aumento do número de atores com capacidade disruptiva.

Em comparação com o primeiro semestre de 2025 (H1 2025), a distribuição setorial mostra mudanças significativas na priorização dos objetivos, bem como uma consolidação dos ataques contra setores estruturais para a administração pública e o funcionamento econômico global.

A distribuição setorial dos ataques mais uma vez destaca a clara preferência de atores maliciosos, tanto estatais quanto não estatais, por setores estratégicos que concentram informações sensíveis, dependências operacionais críticas e um alto impacto potencial em caso de interrupção. Diferentemente do semestre anterior, no qual os ataques se concentraram em um número menor de setores, esse período viu um aumento geral no volume de ataques, especialmente no setor público, educação e serviços financeiros.

- Administração Pública e Governos:

O setor da Administração Pública continua ocupando a primeira posição em número de incidentes, acumulando um total de 3.343 ataques nos últimos seis meses. Esse número representa um aumento significativo em comparação com o primeiro semestre do ano e consolida a tendência observada desde o final de 2024, marcada por campanhas direcionadas a órgãos públicos de todos os níveis. A exposição constante dos sistemas administrativos, juntamente com a criticidade de suas operações, os torna um alvo prioritário para grupos que buscam obter informações estratégicas, comprometer serviços essenciais ou executar ações de pressão política por meio de vandalismo e vazamentos de dados.

O aumento das intrusões associadas a atores politicamente motivados, como as campanhas atribuídas a grupos ligados ao México durante esse período, mostra que as agências governamentais continuam sendo um dos principais vetores de impacto em um contexto de crescente cibertensão internacional.

Quanto ao Governo e ao Setor Público, 590 ataques confirmados foram registrados nos últimos seis meses, um número significativamente menor do que o observado na Administração Pública como um todo, mas que confirma que essa área continua sendo um alvo recorrente dentro do ecossistema de ameaças. Esses incidentes estão concentrados principalmente em organizações com alta visibilidade institucional e em entidades responsáveis pela prestação de serviços aos cidadãos, onde o impacto reputacional e operacional continua sendo um fator chave para os atacantes.

O termo Setor Público abrange todas as entidades controladas pelo Estado, enquanto Administração Pública refere-se especificamente aos órgãos e estruturas administrativas que executam políticas públicas.

- Educação:

Com 1.460 ataques cibernéticos, o setor educacional continua sendo um dos mais afetados. Embora o número seja um pouco menor do que o registrado no primeiro semestre, as instituições educacionais permanecem particularmente vulneráveis devido à heterogeneidade de seus sistemas, à gestão descentralizada de ativos e à presença de dados pessoais, acadêmicos e de pesquisa de alto valor.

Neste semestre, observou-se uma mudança no tipo predominante de ataque: junto com o roubo de credenciais e o comprometimento de redes internas, a presença de campanhas de extorsão baseadas em vazamentos de dados aumenta, aproveitando a baixa capacidade de resposta de muitas instituições regionais e privadas. As universidades continuam se destacando como um dos principais focos dessas ameaças.

- Serviços Financeiros:

O setor financeiro registrou 957 ataques nesse período, permanecendo entre os três mais afetados globalmente. Os incidentes continuam focados em ataques de ransomware, acessos não autorizados e roubo de informações sensíveis. A crescente sofisticação das técnicas empregadas por grupos criminosos, juntamente com a presença de atores estatais interessados em espionagem econômica, explica a persistência desse setor como um alvo de alto valor.

Também há um aumento do interesse em empresas fintech e plataformas de pagamento digital, cujo crescimento no último ano ampliou a área de exposição e atraiu campanhas oportunistas baseadas na exploração de vulnerabilidades críticas.

- Tecnologia da Informação e Telecomunicações:

Os setores de Serviços de TI (ataques 802) e Telecomunicações (614 ataques) têm sido novamente alguns dos mais pressionados digitalmente. A maioria dos incidentes registrados neste semestre está relacionada à exploração de vulnerabilidades em sistemas de terceiros, ataques direcionados contra provedores de serviços gerenciados e compromissos na cadeia de suprimentos.

A natureza interconectada dessas indústrias transforma qualquer intrusão em uma ameaça potencial multiplicada, já que os atacantes podem escalar lateralmente para clientes e parceiros tecnologicamente dependentes. Esse padrão foi consolidado especialmente nos meses de setembro e novembro, coincidindo com picos globais de atividade maliciosa.

- Transporte, Logística e Comércio Eletrônico:

Com 592 ataques em Transporte e Logística e 532 em Comércio Eletrônico, esses setores continuam sob alta pressão. A interrupção da cadeia de suprimentos, campanhas de fraude digital e manipulação de dados de clientes continuam sendo vetores comuns entre julho e dezembro.

No caso específico do comércio eletrônico, a recuperação da atividade coincide com a campanha comercial do último trimestre (com eventos como Black Friday, Cyber Monday ou a temporada de Natal), período em que os atacantes buscam maximizar o impacto por meio de carding, operações de skimming e compromissos em plataformas de vendas.

- Saúde e Serviços de Saúde:

O setor de saúde acumulou 526 incidentes, um número que, embora menor do que em semestres anteriores, continua a colocá-lo entre os alvos mais críticos. Os ataques de ransomware continuam sendo a principal ameaça, dado seu potencial para interromper serviços clínicos, comprometer dados médicos e causar impactos diretos no cuidado dos pacientes.

Este semestre destaca a concentração de incidentes em entidades de médio porte e provedores privados, indicando que os atacantes estão buscando alvos com menor capacidade de investimento em segurança, mas igualmente relevantes operacionalmente.

Em comparação com o primeiro semestre do ano, houve uma mudança significativa na composição dos setores mais afetados. Embora a maioria dos setores mantenha uma posição semelhante, a saída do setor manufatureiro se destaca, que até o semestre anterior estava entre os dez mais atacados.

Em seu lugar, durante a segunda metade do ano, o setor da Construção Urbana irrompeu (445 ataques), adquirindo peso suficiente para estar entre as áreas com maior volume de incidentes. Essa mudança mostra um realinhamento nas prioridades dos atores maliciosos, com maior ênfase em setores de alta lucratividade econômica.

Setores mais afetados por ciberataques no S2 de 2025 e comparação com o S1 de 2025

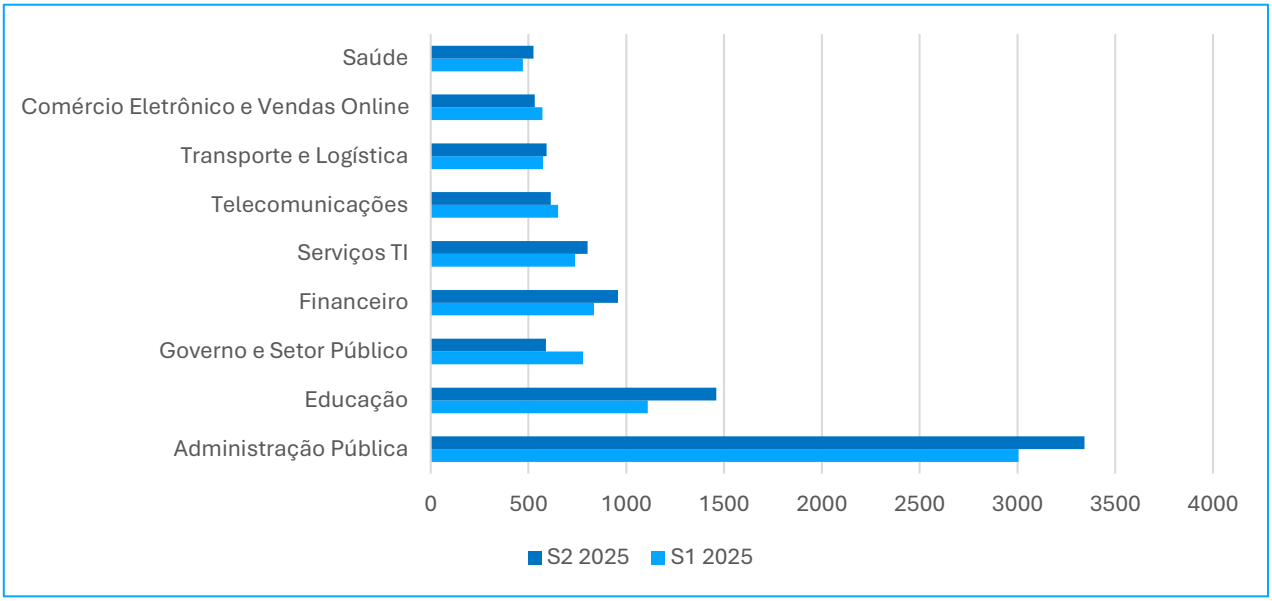


Figura 1 | Setores mais afetados por ataques cibernéticos no segundo semestre de 2025.

Os dados do segundo semestre de 2025 confirmam um padrão de continuidade no impacto geográfico, com ataques cibernéticos concentrados em países altamente digitalizados e com peso geopolítico, em estreita relação ao contexto político internacional.

- Os Estados Unidos são novamente o país mais afetado, acumulando 3.963 ataques em si. Embora haja uma leve redução em comparação ao semestre anterior, os Estados Unidos mantêm o maior volume de ataques globalmente. Este volume reflete tanto a liderança econômica do país quanto seu papel central em conflitos tecnológicos e geoestratégicos, especialmente sua rivalidade com a China e seu envolvimento na guerra na Ucrânia.

- A Tailândia, com 1.341 ataques, está entre os cinco países mais afetados pela primeira vez no período recente. O aumento do volume de ataques cibernéticos está relacionado à expansão das infraestruturas de pagamento digital, ao crescimento do comércio eletrônico e à maior exposição do país a campanhas de phishing e ransomware em larga escala implantadas no Sudeste Asiático.

- Na Índia, que registrou 1.244 ataques, há uma continuidade nas atividades maliciosas ligadas tanto às tensões regionais quanto à digitalização do país. A Índia continua sendo um alvo prioritário para atores criminosos e estatais devido ao seu tamanho populacional, ao crescimento de seu setor tecnológico e ao seu papel estratégico no Indo-Pacífico.

- Israel está em quarto lugar, com 1.233 ataques, um volume consistente com a persistência da tensão regional, apesar de registrar uma redução em relação ao semestre anterior. A atividade cibernética direcionada a Israel combina operações ofensivas ligadas a grupos estatais adversários com campanhas de hacktivismo motivadas pela situação no Oriente Médio.

- Finalmente, a Alemanha registra 856 ataques, permanecendo um dos principais alvos europeus. A atividade maliciosa tem se concentrado nos setores industriais, serviços governamentais e instituições financeiras, em um contexto marcado pelo impacto econômico da guerra na Ucrânia e seu papel como principal potência tecnológica da União Europeia.

Distribuição de ataques cibernéticos por país no S2 de 2025

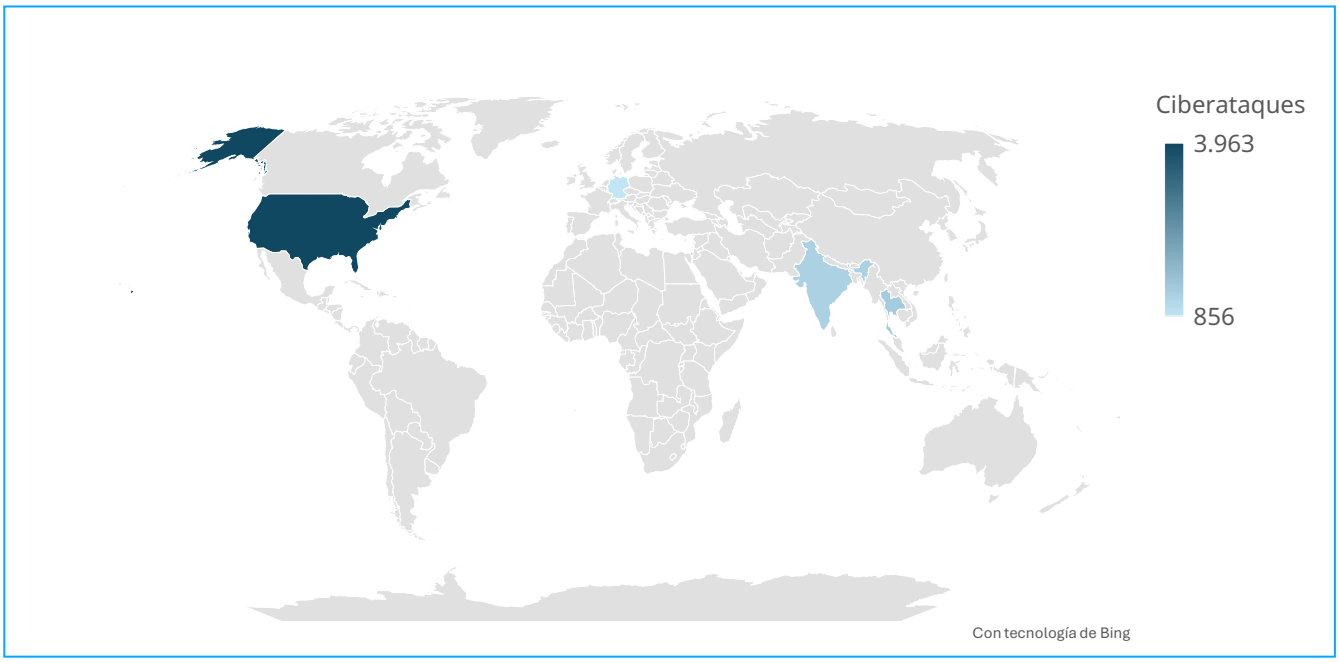


Figura 2 | Distribuição geográfica do impacto dos ciberataques no segundo semestre de 2025.

4. Grandes ameaças globais

Durante a segunda metade de 2025, o cenário global de ameaças tem sido marcado por alta intensidade operacional, com campanhas mais coordenadas, maior profissionalização dos atores e um impacto crescente em infraestrutura crítica, grandes organizações e cadeias de suprimentos.

A convergência entre ransomware, espionagem e sabotagem digital foi consolidada, com atores reutilizando técnicas e capacidades de diferentes ecossistemas criminosos e estatais. O período confirmou uma evolução para ataques mais persistentes, seletivos e difíceis de atribuir, reforçando a natureza estrutural da ameaça cibernética em nível global.

4.1. Incidentes cibernéticos notáveis e grandes campanhas

Os incidentes cibernéticos mais relevantes do semestre refletiram uma escalada em escopo e sofisticação, com campanhas de alto impacto direcionadas a setores estratégicos, serviços essenciais e grandes corporações. Operações prolongadas predominam, apoiadas por credenciais comprometidas, infraestruturas legítimas e técnicas Living-off-the-Land (LotL), que dificultam a detecção precoce. As grandes campanhas observadas mostram uma clara orientação para exfiltração massiva de dados, extorsão múltipla e interrupção operacional, consolidando modelos de ataque mais agressivos e eficazes.

O Departamento de Inteligência de Ameaças Cibernéticas da NTT DATA documentou alguns dos incidentes cibernéticos mais relevantes na segunda metade de 2025, selecionando-os por seu valor representativo das principais ameaças observadas neste período.

Vítimas	Setor	Atacante	País/região afetada	Origem do atacante	Data do Incidente	URL
SonicWall	Cibersegurança	Akira Ransomware Group	Global	Desconhecido	22/07/2025	Fonte
Salesforce / Salesloft	Cloud	UNC6395	Global	Desconhecido	09/08/2025	Fonte
Jaguar Land Rover (JLR)	Automotivo / Manufatura	Scattered Lapsus$ Hunters	Global	Desconhecido	01/09/2025	Fonte
Stellantis	Automotivo	ShinyHunters	América do Norte	Desconhecido	21/09/2025	Fonte
Claro Colombia	Telecomunicações	Crimson Collective	Colombia	Desconhecido	25/09/2025	Fonte
Asahi Group Holdings	Bebidas e produtos alimentícios	Qilin	Japão	Desconhecido	29/09/2025	Fonte
Red Hat	*Software*	Crimson Collective	Global	Desconhecido	01/10/2025	Fonte
Muji / Askul	Varejo	Desconhecido	Japão	Desconhecido	19/10/2025	Fonte
Knownsec	Cibersegurança	Desconhecido	Global	Desconhecido	02/11/2025	Fonte
Anthropic	Inteligência artificial	Desconhecido	Global	China	13/11/2025	Fonte
Logitech	Eletrônica	Cl0p	Global	Desconhecido	14/11/2025	Fonte
Pornhub	Entretenimento	ShinyHunters	Global	Desconhecido	16/12/2025	Fonte
Ministério do Interior francês	Governo/Segurança Pública	Desconhecido	França	Desconhecido	17/12/2025	Fonte
Agência Espacial Europeia(ESA)	Espacial	888	Europa	Desconhecido	31/12/2025	Fonte

Tabla 1 | Grandes incidentes de cibersegurança no segundo semestre de 2025.

Por outro lado, como previsto no relatório anterior, o segundo semestre de 2025 mostrou um ecossistema de ameaças mais automatizado, discreto e mais especializado setorialmente, impulsionado pela convergência de IA generativa, cadeias de suprimentos comprometidas e operações com forte componente geopolítico.

Campanhas de ciberataque no segundo semestre de 2025 agrupadas por alvo

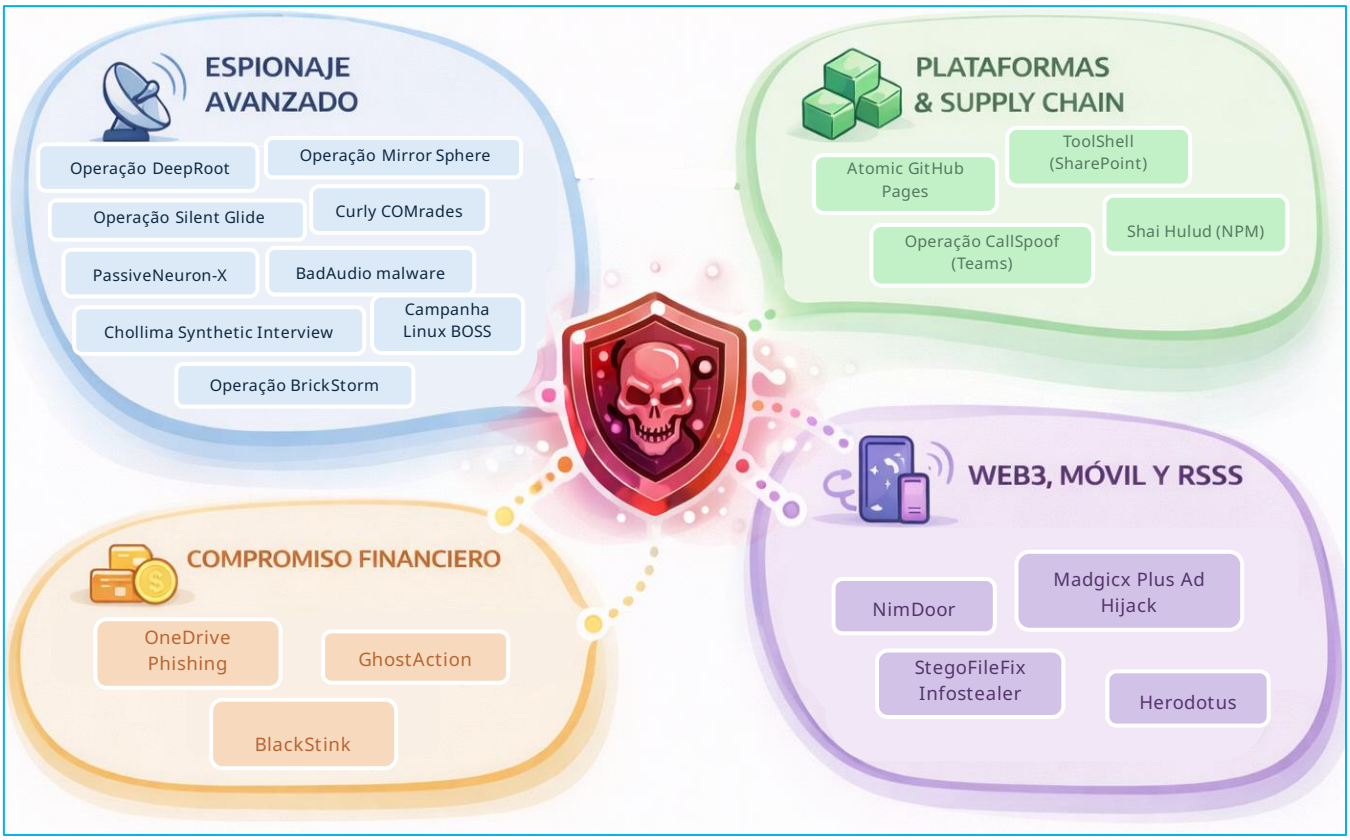


Figura 3 | Campanhas principais detectadas no segundo semestre de 2025.

4.2 Tendências Emergentes de Ataque

No segundo semestre de 2025, tendências se consolidaram que apontam para uma mudança estrutural nos modelos de ataque, com maior automação, modularidade das ferramentas e acesso inicial discreto, confirmando um cenário que já se esperava ser dinâmico, onde persistência, evasão e impacto econômico prevalecerão.

Nesse contexto, destacam-se as seguintes tendências técnicas e operacionais que marcam a atividade no ciberespaço durante a segunda metade do ano:

4.2.1 Ataques de baixo ruído e livres de malware, suportados por infraestruturas legítimas

O uso de técnicas Living-off-the-Land e um maior abuso de serviços legítimos, especialmente nuvem e SaaS, para persistir e se mover lateralmente com quase nenhum artefato, reduzindo a pegada forense, foram consolidados. O uso de serviços OneDrive, Google Drive, Slack, GitHub, Discord ou OAuth tem sido observado como canais secretos de comando e controle; abuso de autenticações válidas e tokens legítimos em vez de malware persistente; e a substituição de binários maliciosos por scripts nativos, tarefas agendadas e abuso de utilitários do sistema (LOLBins).

4.2.2 Inteligência artificial como multiplicador operacional

Mais uma vez, a IA tem sido observada como uma tendência contínua; durante esse período, seu uso predomina para acelerar fases específicas do ciclo operacional: automação de reconhecimento, geração de phishing convincente, desenvolvimento de cargas polimórficas e automação de campanhas (ransomware, fraude, identidade sintética), tudo adaptado dinamicamente ao perfil da vítima.

4.2.3. Engajamento em expansão da cadeia de suprimentos em software e plataformas de desenvolvimento

Os ataques observados neste semestre demonstraram um interesse crescente em comprometer ferramentas e processos de desenvolvimento: injeção de código malicioso em pacotes NPM, repositórios PyPI e GitHub (exemplo do caso Shai-Hulud 2.0 ou Glassworm em extensões VS Code); manipulação de pipelines CI/CD com cascata para múltiplas aplicações; e a publicação de dependências clonadas ou backdoor com propagação sem intervenção uma vez integradas.

4.2.4 Consolidação de cloud e do SaaS como superfície de ataque primária

O aumento sustentado de intrusões em ambientes de nuvem e SaaS refletiu a mudança dos ataques dos endpoints clássicos para ecossistemas interconectados na nuvem. Os agentes de ameaça priorizaram a exploração de configurações inseguras em ambientes multi-inquilino, o uso de aplicações de autorização aberta (OAuth) para obter acesso persistente sem a necessidade de credenciais, e o movimento lateral baseado em sincronização entre serviços SaaS, aproveitando conexões entre aplicações com excesso de permissões.

4.2.5 Espionagem avançada com forte componente geopolítico

A espionagem observada neste semestre apresentou características técnicas recorrentes, como maior persistência distribuída, onde atacantes utilizam vários mecanismos redundantes sem concentrar os riscos em um único ponto; o uso de C2 fragmentado e encoberto dentro do tráfego legítimo; técnicas de beaconing irregulares, evitando padrões detectáveis e ajustando a frequência de acordo com a atividade do usuário.

4.2.6 *Kits modulares reutilizáveis*

A adoção de arquiteturas modulares permitiu que os agentes ameaçadores mudassem seu propósito sem redesenhar a operação.

Essa prática marca a profissionalização dos grupos como uma evolução natural do mercado clandestino, como foi visto no início do ano. Estruturas que combinam roubo financeiro, espionagem corporativa e exfiltração seletiva, o reaproveitamento de implantações leves com ativação seletiva e o surgimento de ecossistemas persistentes de acesso como serviço, onde a infraestrutura é fornecida aos APTs, têm predominado.

4.3 Estatísticas globais sobre incidentes de segurança, tipos de ataques e atores ameaçadores envolvidos

Durante a segunda metade de 2025, o cenário global de cibersegurança foi marcado pela consolidação de ameaças maduras, especialmente ransomware, e pela aceleração de vetores habilitadores como engenharia social avançada e o uso de inteligência artificial. Longe de haver uma redução na atividade maliciosa após o pico no início do ano, os dados indicam uma estabilização em níveis elevados, acompanhada por maior sofisticação técnica e organizacional dos atores de ameaça.

4.3.1 Incidentes de segurança

O ransomware tem permanecido como principal gerador de incidentes de alto impacto. Durante o terceiro trimestre de 2025, 1.592 vítimas foram publicadas em sites de violação de dados, o que representa uma média aproximada de 535 vítimas por mês. Embora esse número seja menor do que o pico observado no primeiro trimestre de 2025 (2.289 vítimas), ele confirma que a segunda metade do ano foi caracterizada por atividade sustentada em valores historicamente altos, excluindo um cenário de contenção real da ameaça(Check Point Research, 2025).

Em nível agregado, foi observado que o ransomware está envolvido em aproximadamente 44% das violações de segurança registradas em 2025, em comparação com cerca de 32% em 2024, consolidando-se como o principal vetor de impacto operacional e econômico.

4.3.2 Tipos e vetores de ataque predominantes

No final do ransomware, estavam ataques à cadeia de suprimentos presentes em 30% dos incidentes em 2025, consolidando-se como o principal amplificador do risco; Ataques por malwares não relacionados a ransomware (Trojans, spyware, infostealer, etc.) representam cerca de 17%. Esse tipo de malware é usado principalmente como mecanismo de preparação e persistência do ambiente; e ataques DDoS com presença

mais limitada que 5%, mantendo um papel tático e complementar.

Em termos de vetores de entrada, o phishing continuou sendo o mais frequente, presente em cerca de 16% das violações, respondendo ao baixo custo e adaptabilidade das técnicas de engenharia social; No entanto, o compromisso de terceiros como ponto de acesso (15%) foi observado quase no mesmo nível, confirmando o deslocamento dos vetores iniciais para o perímetro organizacional além da própria infraestrutura; Por fim, o comprometimento das credenciais (10%) evidenciou o abuso de identidades legítimas, confirmando o padrão observado ao longo do relatório.

Do ponto de vista da evolução tecnológica, cerca de 16% dos incidentes já incorporaram algum uso de inteligência artificial por parte de atacantes, principalmente para geração de conteúdo de phishing, roubo de identidade e automação de campanhas (Khalil, 2025). Embora o uso da IA ainda não substitua as técnicas tradicionais, ele aumenta sua escala, credibilidade e eficácia, atuando como um multiplicador de risco.

4.3.3 Atores de Ameaça e Dinâmica de Ecossistemas

O ecossistema criminoso no segundo semestre de 2025 mostrou uma fragmentação sem precedentes, especialmente no campo de ransomware. Pelo menos 85 grupos ativos de ransomware foram identificados no terceiro trimestre, o maior número registrado até hoje (Check Point Research, 2025). Esse aumento não implica necessariamente mais capacidade global, mas uma maior atomização do modelo Ransomware-as-a-Service (RaaS), com proliferação de marcas, afiliados e campanhas de menor escala. Essa dinâmica dificulta a atribuição, reduz o efeito de interrupções pontuais e aumenta a volatilidade do ecossistema.

Da mesma forma, uma rotação constante de ferramentas e serviços criminosos tem sido observada.

A queda de 86% na atividade do Lumma Stealer na segunda metade em comparação com o primeiro semestre (ESET Research, 2025) não indica uma redução no roubo de credenciais, mas sim a rápida substituição de ferramentas após ações de desmantelamento contra infraestruturas MaaS. Esse padrão confirma que as operações policiais geram impacto, mas também aceleram a migração para novas famílias de malware.

No geral, as estatísticas do segundo semestre de 2025 refletem um ecossistema criminoso mais maduro, resiliente e adaptável, capaz de absorver interrupções e se reorganizar rapidamente.

Estatísticas globais por tipo de ataque em 2025

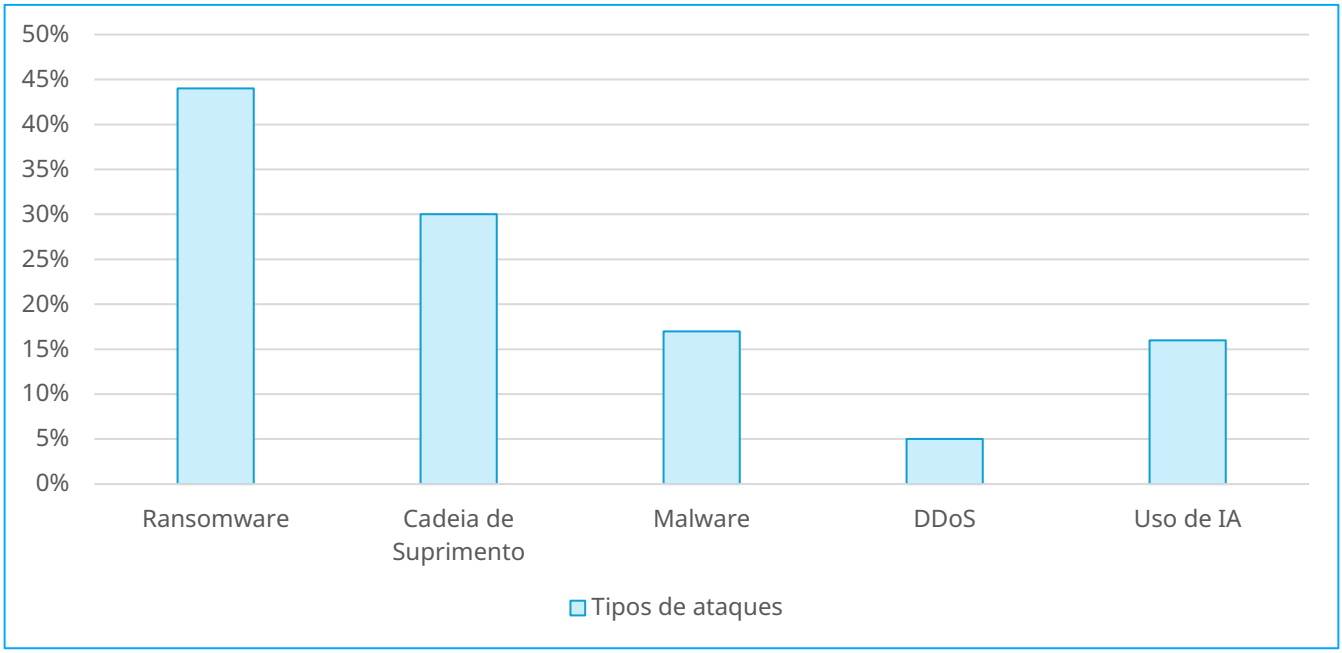


Figura 4 | Frequência de ataque por tipo durante 2025.

4.4 Custos dos ataques cibernéticos para empresas

Até 2025, o impacto econômico estimado do cibercrime foi de cerca de USD 10,5 bilhões por ano, confirmando sua natureza como um risco sistêmico para as organizações.

No nível operacional, o incidente mais frequente tem sido ransomware e, embora a demanda média de resgate tenha sido em torno de 115.000 USD, 64% das organizações optam por não pagar, o que transfere o peso econômico para custos indiretos, como interrupção operacional, recuperação técnica e consequências legais e reputacionais. com um custo total por incidente médio de US$ 5,08 milhões, além dos períodos de interrupção e recuperação.

Globalmente, o custo médio de uma violação de dados atingiu USD 4,44 milhões, 9% abaixo da média de 2024. No caso específico dos Estados Unidos, o número subiu para USD 10 milhões em setores regulados, como saúde, finanças ou infraestrutura crítica. O Oriente Médio tem um custo médio por violação de aproximadamente 7,3 milhões de dólares, embora uma redução de 18% em relação a 2024, atribuída ao aumento dos investimentos em cibersegurança e ao uso de defesas baseadas em IA. Em contraste, a Europa tem um custo médio de cerca de USD 4 milhões, influenciado por marcos regulatórios de proteção de dados mais consolidados e maior padronização dos processos de resposta.

No nível estrutural, em 2025 foram identificados alguns fatores-chave que atuam como multiplicadores do impacto econômico. Incidentes envolvendo terceiros são os maiores aumentos de custo, com um custo médio de 227.000 dólares.

Em seguida, vêm arquiteturas de segurança excessivamente complexas ($207.000+) e o uso de TI sombra ($200.000+), que dificultam a detecção e resposta. Além disso, o uso malicioso de IA ou a ausência de uma governança adequada dessa tecnologia adicionam cerca de US$ 193.000 ao custo médio de uma violação. De destaque especial é o fenômeno da IA Sombra, cujo uso não supervisionado pode aumentar o impacto econômico em aproximadamente US$ 670.000 por incidente.

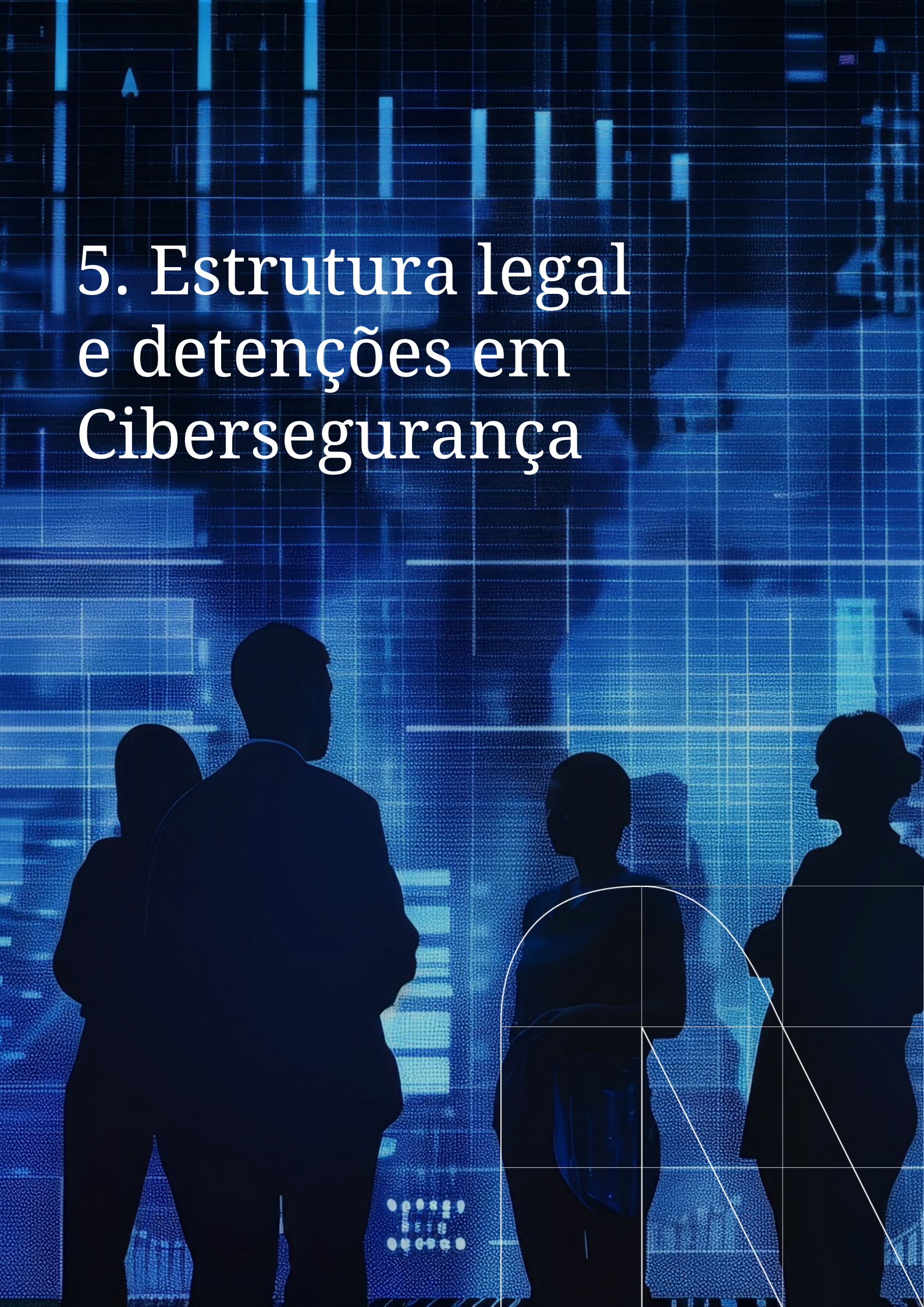
Pelo contrário, organizações que aplicam medidas de segurança integradas por design conseguiram reduzir significativamente o impacto econômico. Adotar o DevSecOps reduz o custo médio em US$ 227.000, o uso de análises de segurança baseadas em IA/ML em US$223.000, programas robustos de inteligência de ameaças em US$ 211.000 e a criptografia extensiva de dados em US$ 208.000. Juntos, o uso de IA e automação na defesa permite uma redução média de custo de 34%, destacando uma lacuna crescente entre organizações com alta maturidade em cibersegurança e aquelas com abordagens mais reativas (Khalil, 2025).

Estimativas de mercado publicadas em 2025 indicam que os gastos globais em segurança da informação e gestão de riscos são de cerca de USD 213.000 milhões, o que representaria um crescimento anual próximo a 14% (Stamford, 2025).

Esse número reflete uma realidade-chave da segunda metade do ano: o aumento sustentado dos investimentos em segurança em resposta à crescente complexidade do ambiente de ameaças, sem que isso ainda se traduza em uma redução proporcional no impacto econômico dos incidentes.

Embora este relatório foque nas tendências observadas durante o segundo semestre de 2025, as estatísticas utilizadas correspondem a dados agregados para todo o ano. Esses números são usados como referência para contextualizar as dinâmicas consolidadas ao longo de 2025 e para facilitar sua interpretação ao final do ano.

5. Estrutura legal e detenções em Cibersegurança



O Departamento de Inteligência de Ameaças Cibernéticas da NTT DATA considera essencial analisar as medidas de segurança implementadas, as leis aprovadas na área de cibersegurança e as prisões feitas por agências de aplicação da lei globalmente no segundo semestre de 2025.

Esta análise avalia o compromisso dos países com a regulação e controle das tecnologias atuais e emergentes, bem como sua aplicação responsável. Além disso, reflete o esforço conjunto dos órgãos legislativos, judiciais e de defesa para enfrentar violações de segurança corporativas e combater atividades ilícitas no ciberespaço.

5.1 Principais leis na área de cibersegurança

No segundo semestre de 2025, o arcabouço legal e regulatório sobre cibersegurança passou por uma evolução significativa em escala global, impulsionada pela necessidade de fortalecer a resiliência digital, melhorar a governança tecnológica e harmonizar as obrigações regulatórias entre setores e jurisdições. Durante esse período, diferentes organizações nacionais e internacionais publicaram ou implementaram novas leis, estratégias nacionais e padrões técnicos que consolidam a transição de uma abordagem puramente preventiva para uma de conformidade verificável e supervisão ativa.

Entre os avanços mais relevantes estão a aplicação completa do Regulamento DORA na União Europeia, reformas legislativas na Itália, Singapura e Brasil, e a atualização de marcos internacionais de referência como ISO/IEC 27001 e as diretrizes do NIST, que estabelecem as bases para a convergência regulatória global em cibersegurança.

Continente	Regulamentos	Instituição	Referencias
América del Norte	NIST SP 800-53 – Release 5.2.0 (27-ago-2025)	NIST / CSRC	Aviso e Resumo das Mudanças da Versão 5.2.0.
	NIST SP 800-88 Rev.2 – Sanitização da mídia (IPD 21 de julho de 2025; Publicação Final Set 2025) Obsoleta	NIST / CSRC	NIST Computer Security Resource Center
	NIST SP 800-18 Rev.2 – Planos de Sistema/Privacidade/SCRM (IPD, junho-jul 2025)	NIST / CSRC	NIST Computer Security Resource Center
América del Sur (Brasil)	Decreto nº 12.573/2025 – E-Ciber (Estratégia Nacional de Cibersegurança) (4 de agosto de 2025)	Presidência do Brasil (Planalto)	Diário Oficial em Planalto
Asia	Cybersecurity (Amendment) Act 2024 – Commencement Notification 2025 (Entra em vigor em 31 de outubro de 2025 em várias seções)	Gov. de Singapura (AGC / Estatutos Online)	Notificação S 677/2025 com detalhes das seções e data sso.agc.gov.sg
	Pacote de Cibercrime e Assistência Mútua (terceira leitura adotada; com destino à Convenção de Budapeste)	Governo da Nova Zelândia	Nota oficial (Beehive) 24-Jul-2025; contexto em Min. Justicia
Europa	DORA – RTS TIC Subcontratação (Regl. Delegado (UE) 2025/532, 2-jul-2025)	Comissão Europeia / EUR-Lex	Texto no DOUE
	DORA – Guia Crítico de Supervisão de Provedores de TIC (CTPPs) (15-jul-2025)	ESAs (EBA/EIOPA/ESMA)	Orientação conjunta publicada pelos ESAs
	DORA – Roteiro para a designação dos CTPPs(jul-2025)	ESAs (EBA/EIOPA/ESMA)	Nota/roadmap oficial
	RED/EN 18031 (serie) – Normas Harmonizadas de Cibersegurança (aplicáveis a partir de 1º de agosto de 2025)	Comissão Europeia / EUR-Lex	Decisão de Implementação (UE) 2025/138 citando a EN 18031-1/-2/-3 com restrições
	Lei 132/2025 – IA (deepfakes, fatores agravantes em cibercrime, governança) (em vigor em 10-out-2025)	República Italiana (Diário Oficial)	Publicação oficial (GU n.º 223, 25-sep-2025)
Internacional	ISO/IEC 27001:2022 – Fim da transição(31-oct-2025)	IAF/BSI (Acreditação e Certificação)	Linha do tempo (BSI) e critérios de transição (IAF MD26)
	ISO/IEC 19790:2025 (módulos criptográficos) & ISO/IEC 24759:2025 (testes)	ISO/IEC	Arquivo oficial ISO 19790:2025 Arquivo oficial ISO 24759:2025

Tabla 2 | Leis aprovadas ou aplicadas na segunda metade de 2025.

Esses padrões legais e técnicos, tanto nacional quanto internacionalmente, refletem avanços significativos rumo à consolidação de um arcabouço regulatório global em cibersegurança, focado na resiliência operacional, na proteção de infraestruturas críticas e na gestão de riscos tecnológicos.

5.2 Principais prisões na área de cibersegurança

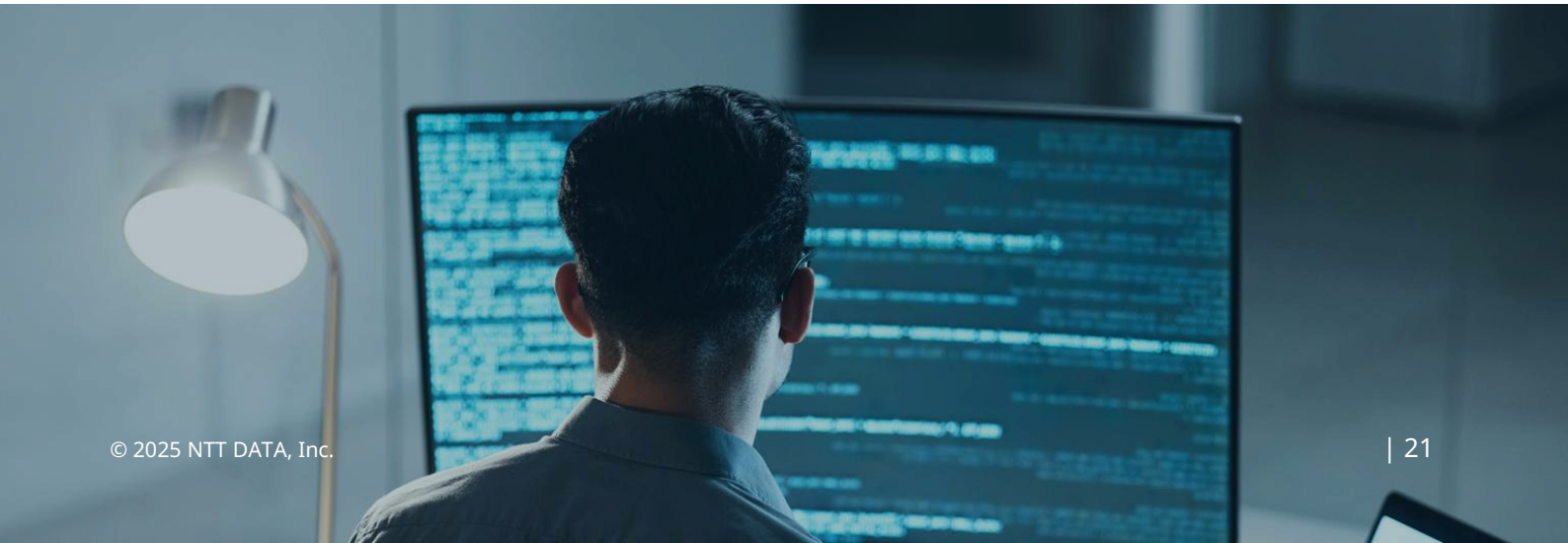
Durante o segundo semestre de 2025, foi mantido um alto nível de atividade em termos de cooperação policial e judicial internacional contra o cibercrime. Nesse período, múltiplas operações foram realizadas com o objetivo de neutralizar atores maliciosos e desmantelar infraestruturas criminosas associadas a ransomware, crime como serviço, hacktivismo e fraude financeira.

Essas ações, coordenadas entre Europol, INTERPOL, Eurojust, o Departamento de Justiça dos EUA e várias agências nacionais de aplicação da lei, refletem uma tendência consolidada em direção ao modelo colaborativo de disrupção, onde a inteligência técnica e a cooperação transfronteiriça são decisivas para impactar as capacidades operacionais dos grupos criminosos.

Abaixo está uma tabela resumida com as principais operações realizadas na segunda metade de 2025, destacando seus resultados e o papel das diferentes agências envolvidas:

Operação	Grupo do Setor de Ameaça	Forças de Segurança	Resultados	Referencias
Eastwood	*Hacktivismo pró-Rússia* (NoName057(16))	Europol, Eurojust, autoridades da Alemanha, França, Espanha, Suécia, Suíça e EUA.	Desmantelamiento >100 sistemas de infra; parte del "core" fuera de línea; 6 órdenes de arresto (DE).	Europol – Eastwood
Prisão admin XSS.is	Ecossistema subterrâneo / acesso e vendas de malware	Polícia Nacional Francesa, Ministoria Pública de Paris, SBU (Ucrânia), Europol	Arresto del presunto admin; plataforma con >50k usuarios; ganancias >€7M.	Europol – Press Release
Checkmate (BlackSuit/Royal)	Raas/Extorsão	Departamento de Justiça dos EUA (DOJ), FBI, Parceiros Internacionais	4 servidores y 9 dominios incautados; ≈$1M intervenido.	DOJ Press Release
Zeppelin Case	*Ransomware/Lavagem de Dinheiro em Criptomoedas*	DOJ (EUA), FBI	Incautación >USD 2,8M en cripto, USD 70k en efectivo y un vehículo; imputación a Ianis A. Antropenko.	DOJ – Indictment Zeppelin
Contender 3.0	Fraude Online / BEC / Phishing em Massa	INTERPOL + 25 países africanos	260 arrestos, 81 infra desmanteladas; 1.463 víctimas; pérdidas ≈USD 2,8M.	INTERPOL Press Release

Tabla 3 | Grandes operações de desmantelamento de gangues cibercriminosas realizadas no segundo semestre de 2025.



Operación	Grupo do Setor de Ameaça	Forças de Segurança	Resultados	Referencias
Serengeti 2.0	Cibercrime transnacional (ransomware, fraude, BEC)	INTERPOL + 18 países africanos e o Reino Unido	1.209 prisões, 11.432 infra-maliciosas desmanteladas; USD 97,4 milhões recuperados.	INTERPOL Press Release
SIMCARTEL Takedown	*Crime-as-a-Service (SIM-box / bypass OTP / fraude em telecomunicações)*	Europol, Eurojust, polícia letã, Áustria, Estônia, Finlândia	7 prisões, 1.200 caixas SIM, 40.000 SIMs, 5 servidores; perdas ≈€4,5M (AT) e €420k (LV); Dois sites intervieram.	Europol SIMCARTEL
Prisão no caso Collins Aerospace / Aeroportos da UE	Intrusão / Interrupção em infraestrutura crítica	NCA (Reino Unido), colaboração com forças europeias	1 prisão no Reino Unido; investigação em andamento; incidente relatado em 19 de setembro.	NCA Press Release
Eurojust–Europol Fraude Cripto	Fraude de investimentos/Lavagem de dinheiro	Eurojust, Europol, autoridades da França, Bélgica, Chipre, Alemanha e Espanha	9 presos; uma rede que fraudou > 600 milhões de euros por meio de plataformas de investimento falsas.	Eurojust Case Release
Endgame – fase nov-2025	*Malware/Crime-as-a-Service (ecosistema Rhadamanthys infostealer, VenomRAT RAT, botnet Elysium)*	Europol, Eurojust e LEAs de 10 países (incluindo EUA, REINO UNIDO, DE, FR, CA, AU, NL, GR)	1.025 servidores desmontados/interrompidos; 20 domínios confiscados; Principal suspeito de VenomRAT preso na Grécia (03-Nov-2025)	Europol (oficial) BleepingComputer The Hacker News
Prisão em Phuket (Tailandia)	APT/Patrocinado pelo Estado (espionagem) – supostos vínculos com Void Blizzard/ColdRiver (imprensa)	Bureau de Investigação de Crimes Cibernéticos (Tailândia) em coordenação com o FBI (EUA)	1 preso (06-Nov-2025); dispositivos apreendidos; início do processo de extradição para os EUA.	AP (NPR/AP syndication)
US DOJ – **Account Takeover Fraud**	Fraude financeira	Departamento de Justiça dos EUA (DOJ), FBI	Apreensão de bens e infraestrutura; banco de dados com credenciais roubadas; prejuízos estimados ≈USD 14,6 milhões; mais de 5.100 vítimas.	DOJ Press Release
Sentinel	Fraude Online/BEC/Ransomware	INTERPOL + 19 países africanos	574 prisões; ≈USD 3 milhões recuperados; desmantelar redes criminosas transnacionais e fechar infraestruturas maliciosas.	INTERPOL Press Release

Tabla 3 | Grandes operações de desmantelamento de gangues cibercriminosas realizadas no segundo semestre de 2025.

Destaque do Caso: Operação Eastwood — Desmantelando a Rede de Hacktivistas pró-Rússia NoName057(16)

Durante o mês de julho de 2025, a Europol, em colaboração com a Eurojust e as autoridades policiais da Alemanha, França, Espanha, Suécia, Suíça e Estados Unidos, executou a "Operação Eastwood", com o alvo da rede NoName057(16), uma das organizações de hacktivismo pró-Rússia mais ativas desde o início da guerra na Ucrânia(EUROPOL, 2025).

O grupo foi responsável por milhares de ataques coordenados DDoS contra infraestrutura crítica, entidades governamentais e mídia europeia, principalmente em países que apoiam a Ucrânia.

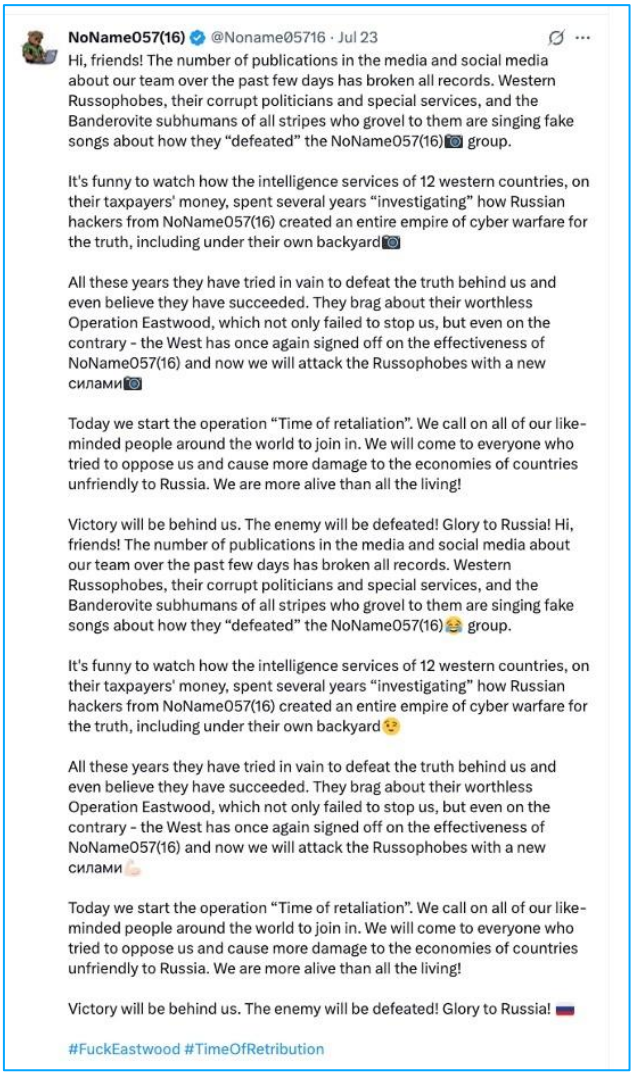
A operação possibilitou o desmantelamento de uma infraestrutura distribuída composta por mais de cem servidores usados para coordenar ataques e gerenciar a plataforma DDoSIA, usada pelo grupo para automatizar campanhas de negação de serviço por meio de um modelo de "voluntariado gamificado".

Além disso, sete mandados internacionais de prisão foram emitidos (seis deles na Alemanha) contra indivíduos identificados como membros-chave do grupo, e duas prisões foram feitas em território europeu (França e Espanha).

As investigações também possibilitaram identificar mais de mil usuários ativos nos canais de recrutamento do Telegram, muitos dos quais receberam incentivos econômicos em criptomoedas por participarem das ofensivas.

A relevância da Operação Eastwood transcende o nível técnico. Representa um marco na cooperação internacional contra o hacktivismo coordenado, pois é a primeira operação multinacional a neutralizar uma rede desse tipo por meio da combinação de capacidades judiciais, policiais e de inteligência cibernética.

A abordagem das agências participantes reflete maturidade operacional: foi dada prioridade à neutralização da infraestrutura, à acusação dos responsáveis e ao desmantelamento do modelo digital de financiamento e recrutamento que sustentava a campanha.



NoName057(16) @Noname05716 · Jul 23

Hi, friends! The number of publications in the media and social media about our team over the past few days has broken all records. Western Russophobes, their corrupt politicians and special services, and the Banderovite subhumans of all stripes who grovel to them are singing fake songs about how they “defeated” the NoName057(16)📷 group.

It's funny to watch how the intelligence services of 12 western countries, on their taxpayers' money, spent several years “investigating” how Russian hackers from NoName057(16) created an entire empire of cyber warfare for the truth, including under their own backyard📷

All these years they have tried in vain to defeat the truth behind us and even believe they have succeeded. They brag about their worthless Operation Eastwood, which not only failed to stop us, but even on the contrary - the West has once again signed off on the effectiveness of NoName057(16) and now we will attack the Russophobes with a new силами📷

Today we start the operation “Time of retaliation”. We call on all of our like-minded people around the world to join in. We will come to everyone who tried to oppose us and cause more damage to the economies of countries unfriendly to Russia. We are more alive than all the living!

Victory will be behind us. The enemy will be defeated! Glory to Russia! Hi, friends! The number of publications in the media and social media about our team over the past few days has broken all records. Western Russophobes, their corrupt politicians and special services, and the Banderovite subhumans of all stripes who grovel to them are singing fake songs about how they “defeated” the NoName057(16)😂 group.

It's funny to watch how the intelligence services of 12 western countries, on their taxpayers' money, spent several years “investigating” how Russian hackers from NoName057(16) created an entire empire of cyber warfare for the truth, including under their own backyard😉

All these years they have tried in vain to defeat the truth behind us and even believe they have succeeded. They brag about their worthless Operation Eastwood, which not only failed to stop us, but even on the contrary - the West has once again signed off on the effectiveness of NoName057(16) and now we will attack the Russophobes with a new силами

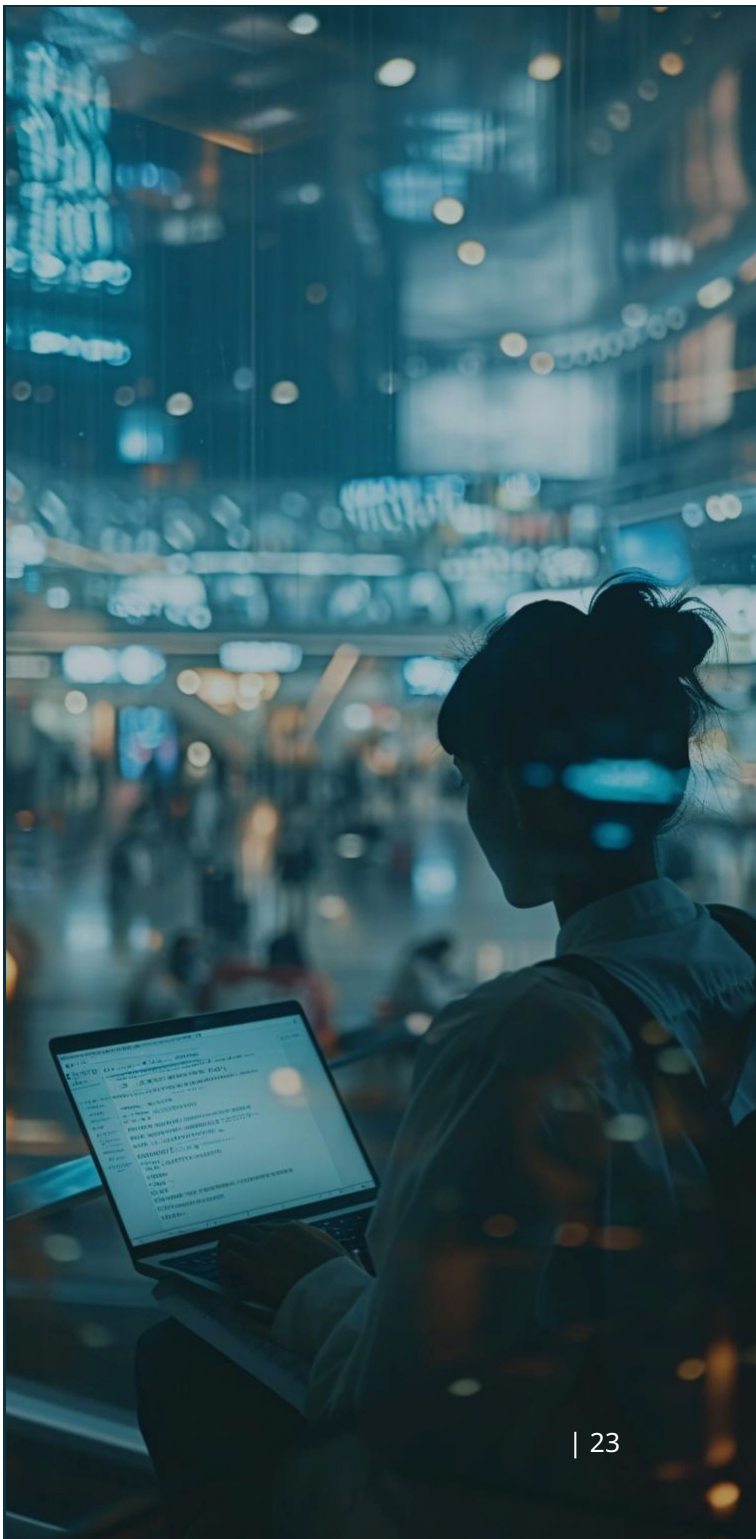
Today we start the operation “Time of retaliation”. We call on all of our like-minded people around the world to join in. We will come to everyone who tried to oppose us and cause more damage to the economies of countries unfriendly to Russia. We are more alive than all the living!

Victory will be behind us. The enemy will be defeated! Glory to Russia! 🇷🇺

#FuckEastwood #TimeOfRetribution

Ilustración 1 | NoName057(16) Declaração Pública de Intenção e Apelo à Ação Contra a Operação Eastwood.

Em termos estratégicos, a Operação Eastwood demonstra a evolução da abordagem europeia ao hacktivismo motivado por geopolíticas, mostrando como o uso de táticas híbridas e a instrumentalização de "voluntários digitais" já são considerados uma ameaça estruturada transnacional.
Este caso reforça a tendência para uma colaboração mais próxima entre as forças de segurança, agências policiais e parceiros do setor privado para responder de forma integrada a ameaças complexas que combinam motivações políticas, técnicas e financeiras.



6. Insights sobre a Dark Web

Durante o segundo semestre de 2025, o ecossistema de fóruns subterrâneos passou por uma reconfiguração significativa, impulsionada pela pressão contínua das forças de segurança, pelo desmantelamento de infraestrutura crítica usada por atores de destaque e pela fragmentação de comunidades históricas.

Enquanto grandes centros tradicionais continuam perdendo força, novas plataformas estão surgindo e absorvem parte do fluxo da atividade criminosa, enquanto outras estão desaparecendo ou sendo transformadas por prisões, apreensões ou conflitos internos.

Esse período é caracterizado por três dinâmicas principais:

- Interrupção contínua dos fóruns consolidados, causando migrações massivas e perda de confiança entre os atores.
- O surgimento de espaços alternativos ou o ressurgimento de comunidades pré-existentes, que se posicionam como novos centros de atividade.
- Aumento no uso de canais paralelos (Telegram, Tox, painéis privados) diante da crescente percepção de risco em fóruns públicos e semiprivados.

Esse contexto obriga o monitoramento de IST a ser adaptado a um ambiente mais distribuído e opaco, no qual prestígio e reputação digital se tornaram fatores críticos para o acesso a inteligência útil para tomada de decisões.

6.1 A Queda dos DarkForums: O Último Gigante a Cair

O DarkForums, herdeiro natural do BreachForums e um dos centros nervosos do cibercrime em 2025, entrou em colapso durante o segundo semestre do ano em um processo tão acelerado quanto revelador.

O que havia nascido como um refúgio para atores expulsos de outros fóruns acabou afundando sob seu próprio peso: crescente pressão policial, conflitos internos e uma deterioração técnica impossível de esconder.

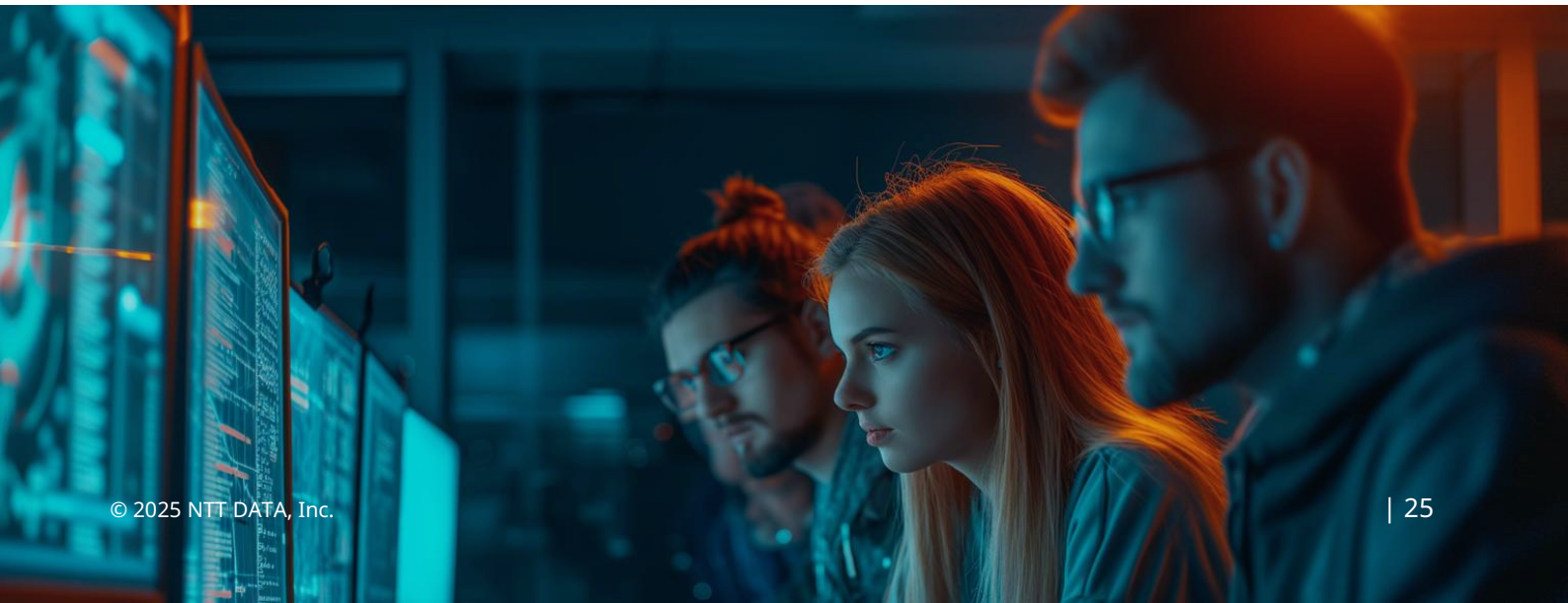
Primeiro vieram os rumores de infiltração. Depois, as falhas nos sistemas de acesso, os cortes constantes e as acusações entre moderadores. Em setembro, os membros mais veteranos já recomendavam publicamente deixar a plataforma. Em novembro, a migração para Telegram, Tox e outros canais privados foi massiva. O DarkForums passou em questão de semanas de ser "o novo BreachForums" para se tornar um espaço fantasma, sem atividade ou credibilidade.

A queda do DarkForums não apenas marca o fim do último grande fórum centralizado, mas simboliza uma mudança estrutural no ecossistema criminoso. Atores de ameaça, tradicionalmente ativos em fóruns da deep e dark web, apresentam perda de confiança mesmo nessas infraestruturas relativamente estáveis e optam por ambientes mais fragmentados, efêmeros e compartimentados, como canais privados, mercados temporários ou plataformas criptografadas, que são muito mais opacos e difíceis de monitorar.

6.2 Fóruns subterrâneos ativos

Durante a segunda metade de 2025, o ecossistema de fóruns underground permanece ativo apesar da queda dos DarkForums e da constante pressão policial sobre as comunidades de língua russa e inglesa. A atividade é redistribuída para plataformas mais fragmentadas, nichos técnicos e enclaves privados que servem como pontos de encontro para atores criminosos de diferentes níveis de sofisticação.

Os fóruns mais relevantes e operacionais desse período são destacados abaixo.



- Exploit.in: Com mais de 15 anos de atividade, Exploit.in continua sendo o epicentro do cibercrime técnico de língua russa. É um dos poucos fóruns com continuidade real após múltiplas falhas em outros espaços, e mantém uma comunidade altamente experiente onde 0-days, exploits de RCE, kits de intrusão e acessos iniciais de alto valor circulam.
- Dread: Dread recuperou sua atividade após meses de instabilidade devido a ataques DDoS e voltou a ser o grande centro social da darknet. Ele funciona como um "Reddit subterrâneo" onde são discutidos quedas de mercado, reputação de fornecedores, análise de operações policiais e alertas de golpes.
- Cracked.io: Após um forte retorno após a Operation Talent, Cracked.io continua sendo um dos fóruns mais movimentados do ecossistema de língua inglesa. Seu conteúdo é dominado por credenciais expostas, configurações para ladrões, ferramentas automatizadas, vazamentos e tutoriais de intrusão de baixo e médio nível.
- Nulled.to: Historicamente considerado um dos maiores fóruns de cracking e vazamento, Nulled.to mantém uma base sólida de usuários dedicada a compartilhar bancos de dados vazados, manuais técnicos, scripts maliciosos e ferramentas de ataque facilmente adotáveis.
- Sinister.ly: combina a estética da cultura hacker com conteúdo técnico voltado para phishing, carding, automação ofensiva e desenvolvimento em Python. Essa mistura a torna popular entre jovens que estão começando a entrar no ecossistema, servindo como uma "academia informal" onde técnicas acessíveis, porém eficazes, são compartilhadas.
- RAMP (Ransomware Affiliate Market Place): Embora não seja um fórum tradicional, o RAMP ainda é um hotspot para a comunidade de ransomware e de programas RaaS. Durante 2025, hospeda anúncios para recrutamento de afiliados, testes de painel e venda de acessos usados para intrusões associadas a grupos de ransomware.
- Ecossistema pós-XSS: subfóruns fragmentados e clãs russos: Após a queda do XSS.is, surgiram vários fóruns fragmentados e comunidades sucessoras que tentam ocupar o espaço deixado pelo que já foi um dos maiores fóruns criminosos de língua russa.
- RuTor / Ru.Tor: não é um fórum criminal no sentido estrito, mas sua comunidade semi-clandestina funciona como um ambiente onde malwares leves, ferramentas de cartão, serviços antifraude, métodos de cashout e scripts para automação criminal circulam.
- KernelForum / Kern3l: Um fórum técnico avançado focado em desenvolvimento de malware, reversão, loaders, crypters e OPSEC ofensivo. Embora seu tamanho seja pequeno, a qualidade técnica de seus usuários faz dele um espaço onde novas técnicas frequentemente surgem antes de serem usadas em campanhas reais.
- Comunidades especializadas em botnets e stealers (R0 Crew, etc.): existem pequenos fóruns dedicados especificamente a quebrar painéis de stealers, trocar configurações por botnets populares (RedLine, Lumma, Raccoon, etc.) e vender logs. Embora modestos em volume, eles são muito úteis para identificar novas variantes, padrões de distribuição e evoluções no ecossistema de malware comercializado.
- KickAss Forum: Um fórum emergente que ganhou destaque entre desenvolvedores de malware por seu foco em loaders, criptografadores, painéis personalizados e malwares privados. Cada vez mais usado por atores que buscam ferramentas mais "premium" sem se expor em fóruns enormes.

Durante o segundo semestre de 2025, observa-se uma mudança na atividade da dark web, marcada pelo aumento da venda de logs e acessos comprometidos, impulsionados por infecções por malware infostealer e pela crescente demanda por credenciais roubadas.

Principais Posts da Dark Web no S2 de 2025

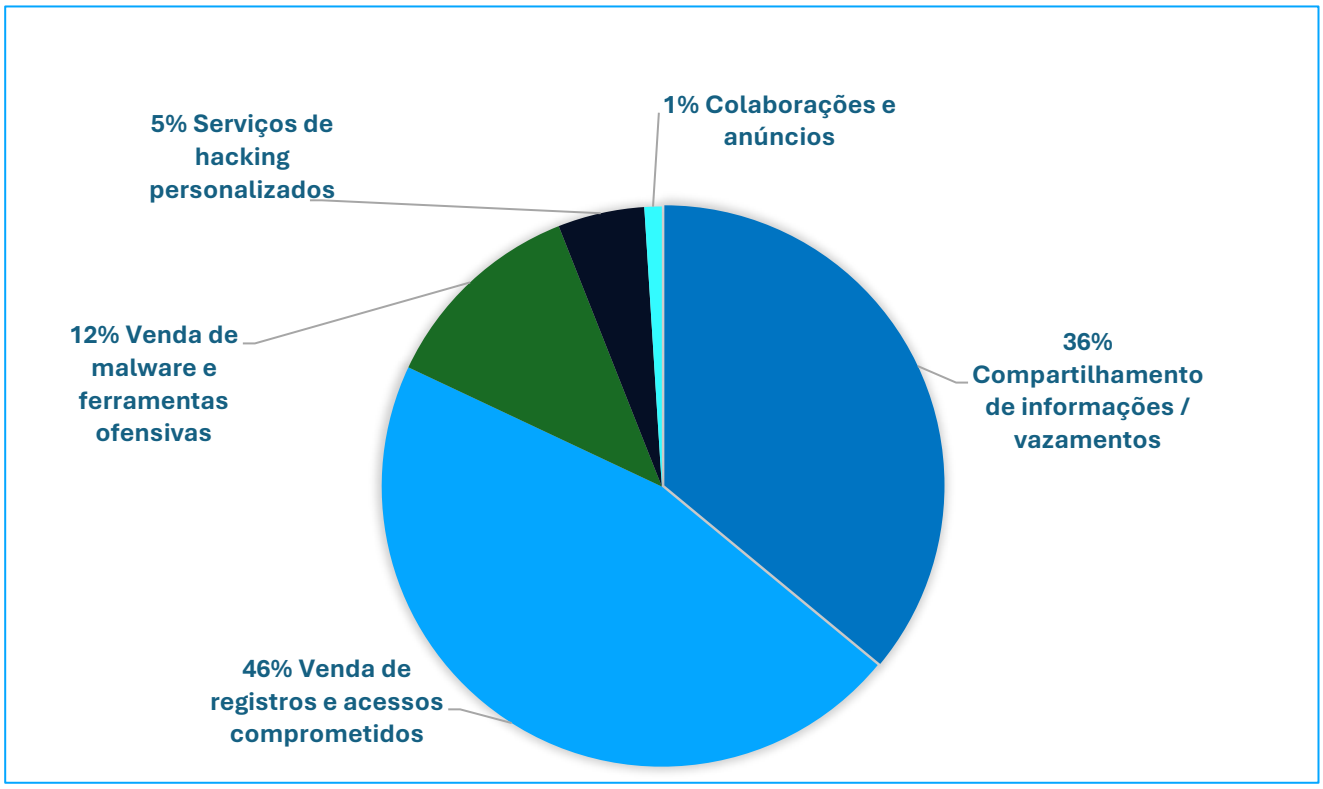


Figura 5 | Principais categorias de posts na dark web no segundo semestre de 2025.

Os dados estimados mostram um ecossistema criminoso cada vez mais orientado para a monetização do acesso e exploração de credenciais, enquanto vazamentos públicos perdem peso devido à fragmentação dos fóruns tradicionais. Por sua vez, a atividade em malware e ferramentas ofensivas continua a crescer, consolidando essas categorias como elementos-chave da segunda metade de 2025.

6.3 Mercados subterrâneos ativos

Durante a segunda metade de 2025, o ecossistema do mercado subterrâneo continuou a apresentar atividade sustentada, embora com mudanças estruturais relevantes em comparação com períodos anteriores. As disrupções dos mercados generalistas não levaram a uma redução do volume criminal, mas sim a uma reconfiguração do ecossistema, caracterizada por maior fragmentação, especialização funcional e uma dependência crescente de mercados orientados para dados, acesso e serviços associados à intrusão.

Os registros do Infostealer continuam sendo um dos ativos mais procurados no submundo. Famílias como Lumma, RisePro e RedLine continuam recorrentes nesse ecossistema, com grandes volumes de credenciais em circulação e uma clara prioridade para atualizações frequentes de estoque. Esse modelo reforça o papel dos marketplaces como provedores diretos de acesso inicial, estreitamente ligados a campanhas de ransomware e fraude.

Mercados consolidados

- Russian Market: continua sendo um dos principais centros de credenciais roubadas e *stealer logs*. Seu modelo em constante atualização e alta rotatividade de estoque fazem dele um ator-chave na cadeia de suprimentos do crime, especialmente para *Initial Access Brokers* (IABs) e operadores de ransomware.
- Brian's Club: continua sendo um marco histórico no carding, com um volume significativo de cards comprometidos. Embora o card perca peso relativo em comparação com a venda de acesso e credenciais, ainda é um mercado estrutural dentro do ecossistema de fraudes financeiras.
- Exodus Market: ganha relevância como um mercado orientado para a venda de acessos privilegiados, exploits e serviços associados à intrusão, com foco especial em ambientes corporativos. Se destaca por sua implementação

de mecanismos mais rigorosos de reputação e verificação, indicativos de uma profissionalização crescente.

Mercados em queda

- Abacus Market: Após sua proeminência durante o primeiro semestre de 2025, o mercado sofreu interrupções críticas em julho, terminando com sua queda. Os sinais observados apontam para um provável golpe de saída, reforçando a tendência de instabilidade dos DNMs generalistas e a perda de confiança em plataformas centralizadas.
- Plataformas generalistas de curta duração: durante o período analisado, múltiplos mercados de curta duração foram observados, com ciclos de vida curtos e baixo volume, que não se consolidam como players relevantes dentro do ecossistema.

Mercados emergentes e espaços alternativos

- Exploit.in: estabeleceu-se como um dos principais fóruns voltados para a venda de acessos iniciais (RDP, VPN, credenciais corporativas e acesso persistente). Durante a segunda metade de 2025, houve um aumento nas ofertas relacionadas a ambientes de negócios, reforçando seu papel como espaço de referência para a IAB.
- 2easy Market: marketplace especializado em logs de infostealers e credenciais roubadas, com forte presença de acessos corporativos reutilizáveis. Seu modelo operacional, focado na disponibilidade e busca por credenciais recentes, aumenta seu valor para atores que operam em estágios iniciais de intrusão.
- Styx Market: um mercado para ferramentas e serviços para campanhas de phishing, kits e suporte operacional para distribuição de malware. Durante esse período, mantém uma atividade relevante como plataforma de apoio para operações de intrusão.
- B1ack's Stash: Identificado como um mercado emergente de carding, voltado para a venda de cartões roubados e dumps recentes. Sua aparência reflete a atomização da fraude financeira, com plataformas de curta duração, alta agressividade comercial e monetização rápida.
- Mercado TorZon: Um DNM generalista que absorveu parte do tráfego residual após a queda de outros mercados, embora sem alcançar uma posição dominante. Sua atividade reflete a parcial mudança do tráfego para alternativas menos consolidadas.
- Outros Mercados e Espaços Fragmentados: Inclui fóruns IAB de baixo perfil, serviços privados de busca de logs, revendas de conjuntos de dados derivados (incluindo modelos legados de marketplaces desativados) e canais fechados e acessíveis por convite. Essa categoria reflete o alto grau de fragmentação e descentralização observado na segunda metade do ano.

Evolução do ecossistema de mercado subterrâneo

Durante este semestre, uma redistribuição significativa da atividade foi observada em comparação com o primeiro semestre de 2025, marcada principalmente pela queda dos marketplaces generalistas e pelo aumento do peso relativo das plataformas voltadas para acesso, credenciais e serviços de intrusão.

O desaparecimento anterior de players como Abacus Market e Breach Forums não levou a uma redução no volume criminal, mas sim a uma mudança de atividade para mercados especializados, fóruns centrados na IAB e canais privados, além de ambientes menos visíveis e mais difíceis de monitorar. Nesse contexto, plataformas como o Russian Market, Exploit.in e mercados especializados como o Exodus Market aumentaram sua relevância operacional.

Da mesma forma, observa-se uma maior fragmentação do ecossistema, com o surgimento de múltiplos nichos de mercado, especialmente no carding e venda de acessos iniciais, caracterizados por ciclos de vida mais curtos, menor visibilidade pública e rápida rotatividade de estoque.

Durante a segunda metade de 2025, vários desses atores estiveram frequentemente associados a campanhas de intrusão e ransomware, atuando como provedores de acesso inicial, credenciais roubadas e dados reutilizáveis. Esse modelo reforça o papel dos mercados subterrâneos como infraestrutura crítica dentro da cadeia de valor do cibercrime, além de sua função tradicional como simples plataformas de negociação.

Em termos de comunicação operacional, embora o Telegram continue sendo uma plataforma de referência, foi identificado um aumento sustentado no uso de canais privados e aplicações criptografadas de ponta a ponta (como Signal, TOX e soluções descentralizadas). Essa tendência responde a uma maior percepção de risco por parte dos atores criminosos e à busca por menor exposição a infiltrações, apreensões de infraestrutura e monitoramento OSINT.

Abaixo está a distribuição estimada das principais plataformas de vendas subterrâneas ativas durante o segundo semestre de 2025, com base no volume de atividade observado e em sua relevância dentro do ecossistema cibercriminoso.

Plataformas de venta *underground* en S2 2025

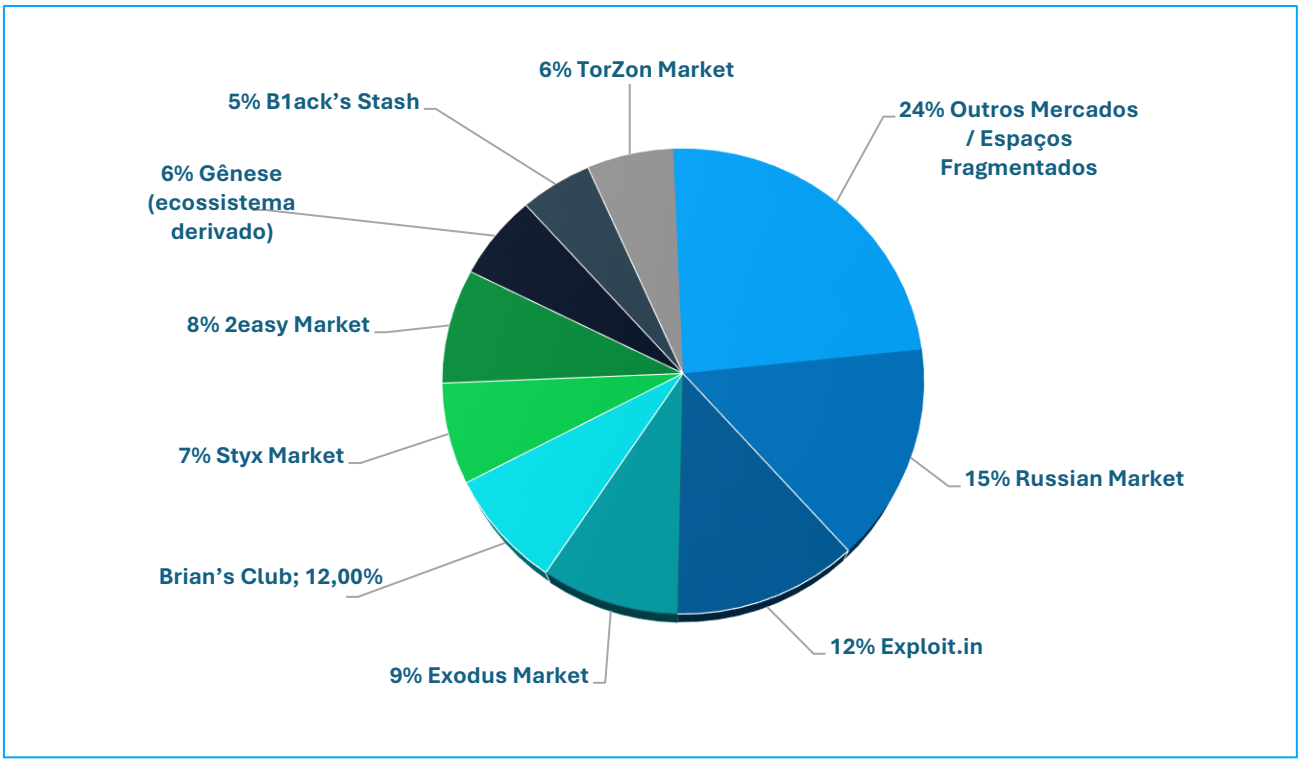


Figura 6 | Principais plataformas de vendas subterrâneas identificadas no segundo semestre de 2025.

7. Atores de ameaça *(Threat Actors)*

O semestre confirmou um ecossistema mais híbrido e difícil de atribuir, onde cibercrime, espionagem e hacktivismo convergem em técnicas, infraestrutura e objetivos.

Com predominância de exfiltração seletiva, engenharia social avançada e abuso de serviços legítimos, enquanto pequenos grupos ágeis e alianças temporárias proliferaram que compartilham TTPs e amplificam o impacto de suas operações.

7.1 Novos atores identificados

O relatório do semestre passado antecipou um aumento na colaboração entre grupos criminosos, bem como uma convergência progressiva entre cibercrime e ciberespionagem. Os novos atores identificados nesse período confirmaram plenamente essa evolução: pequenos coletivos altamente dinâmicos com estruturas flexíveis que combinam técnicas de extorsão, intrusões silenciosas e exploração do acesso legítimo. Sua atividade traçou um quadro mais fragmentado, no qual a separação entre motivações financeiras e operacionais foi borrada e a exfiltração seletiva de dados foi consolidada como o vetor dominante.

FulcrumSec

Detectada em setembro de 2025, a FulcrumSec se destaca por focar exclusivamente na extorsão por meio de exfiltração de dados, sem implantar ransomware, para posteriormente publicá-los em seu site de vazamentos (clearnet e dark web) ou canal do Telegram, com a intenção de vender a base para um único comprador e maximizar o lucro. Seu principal alvo são empresas de alto perfil, até o momento duas vítimas relevantes no setor de tecnologia foram confirmadas publicamente, dedicadas à distribuição global de componentes e soluções, embora em seu "muro da fama" confirme ter obtido acesso a dados altamente sensíveis (PII) e segredos corporativos de pelo menos uma dúzia de corporações globais multimilionárias, Por meio de backends expostos publicamente. No entanto, seu canal no Telegram e seu site na dark web estão inativos, aparentemente desde o início de novembro, sem confirmação de seu desaparecimento completo ou paralisação temporária para a preparação de novos ataques (Shenouda, 2025).

NetMedved

Esse ator foi identificado em meados de outubro de 2025 como responsável por uma campanha voltada principalmente contra empresas na Rússia. Sua tática inclui phishing com e-mails contendo arquivos ZIP com acesso enganoso (arquivo LNK disfarçado de fatura ou solicitação comercial), para implantar malware NetSupportRAT para espionagem ou movimentos subsequentes dentro da rede. Essa combinação de engenharia social, abuso de ferramentas legítimas como scripts PowerShell, múltiplos domínios de entrega e persistência sugere uma evolução tática mais refinada, possivelmente herdada de campanhas anteriores (Shenouda, 2025) (AlienVault, 2025).

Zestix

A Zestix é um player emergente em dezembro de 2025, focado na exfiltração e venda direta de dados, sem o uso de ransomware. Sua operação mais proeminente é o acesso às informações jurídicas e de clientes da Mercedes-Benz USA em toda a cadeia de suprimentos, comprometendo terceiros que gerenciavam documentação sensível. O grupo demonstra reconhecimento prévio, seleção de arquivos de alto valor (estratégias legais, reivindicações, dados corporativos) e monetização rápida por meio de fóruns clandestinos. Ele também foi creditado por duas vendas de bancos de dados com informações de projetos de uma empresa turca de robótica e de uma empresa industrial mecânica e de gás no Peru. Sua atividade reflete uma tendência crescente: novos players com estrutura frouxa que combinam técnicas clássicas de intrusão com uma orientação quase corporativa de inteligência, priorizando o acesso indireto e dados estratégicos em detrimento de volumes massivos(Shenouda, 2025).

7.2 *Ransomware*

O ransomware evoluiu para modelos de extorsão baseados em dados, maior autonomia dos afiliados e expansão global sustentada. Alianças entre grupos fortaleceram a coordenação, o compartilhamento de recursos e o aumento das campanhas de pressão pública, consolidando um ecossistema mais profissionalizado, voltado para maximizar visibilidade e monetização.

7.2.1 Novos grupos

A distribuição temporal mostrou um ecossistema em expansão, porém altamente volátil(DarkFeed, 2025). Julho e agosto concentraram o maior volume de novos grupos, refletindo uma fase de entrada de atores oportunistas e consolidação de modelos de extorsão baseados em dados, com o SLH como um marco que acelera a

Cooperação entre grupos. Setembro introduziu uma camada de especialização, com grupos orientados a nichos (cripto, vazamentos seletivos, branding agressivo), um sinal de maturidade e segmentação do mercado criminoso. A partir de outubro, o ruído operacional aumentou com rebrandings e grupos efêmeros, enquanto em

Em novembro, o número diminuiu, mas a definição técnica dos novos atores cresceu. No geral, o padrão confirmou um semestre marcado por proliferação inicial/média, diversificação no ponto central e especialização no final do período.

Novos grupos de ransomware no S2 2025

Figura 7 | Grupos de ransomware detectados no segundo semestre de 2025.

Este semestre destacou o coletivo Scattered LAPSUS$ Hunters (SLH), que representa uma fusão operacional entre três dos grupos criminosos mais notórios: Scattered Spider, LAPSUS$ e ShinyHunters. Ele surgiu em agosto de 2025 como um modelo federado de extorsão e exfiltração de dados. Sob esse guarda-chuva, eles compartilharam canais no Telegram para coordenar operações, recrutar afiliados e amplificar campanhas de pressão pública, refletindo uma estrutura híbrida entre cibercrime e estratégia de marca no underground. O SLH opera principalmente com extorsão como serviço (EaaS), convocando associados para exigir pagamento em troca do uso de sua reputação estabelecida, e utilizou técnicas clássicas de engenharia social, spear-phishing, troca de SIM e comprometimento de plataformas como a Salesforce para obter acesso inicial e exfiltrar dados sensíveis. Essa aliança ilustrou uma tendência preocupante de colaboração mais próxima entre coletivos anteriormente independentes, com o compartilhamento de táticas e recursos que dificulta a atribuição e aumenta o impacto das campanhas globais de extorsão (Lakshmanan, 2025).

7.2.2 Grupos mais ativos

A atividade de ransomware na segunda metade do ano manteve um nível alto e estável, mas com uma característica mais marcante do que nos semestres anteriores: fragmentação operacional e mobilidade dos afiliados, refletindo um mercado RaaS mais maduro, descentralizado e competitivo.

- Qilin: se estabeleceu como o principal polo de atração para afiliados no semestre. Seu crescimento não foi tanto impulsionado por inovação técnica disruptiva, mas sim por sua capacidade de capitalizar a desestabilização de outros RaaS, oferecendo continuidade operacional, infraestrutura estável e monetização confiável. Ele representa um modelo de ransomware industrializado e escalável, mais próximo de uma plataforma do que de um grupo tradicional.
- Akira: manteve uma presença consistente no topo sem picos abruptos, sugerindo um núcleo de afiliados estável e campanhas bem integradas no mercado de RaaS. Sua persistência reforça a tendência para operações sustentadas de baixo risco, priorizando continuidade e lucratividade em detrimento da visibilidade ou expansão agressiva.
- INC Ransomware: destacou-se como um exemplo de crescimento acelerado durante o semestre, com uma clara orientação para objetivos de alto impacto operacional. Sua evolução aponta para uma estratégia de posicionamento rápido por meio de campanhas mais seletivas, o que o torna um ator relevante para explicar a mudança de foco para setores e ambientes críticos com maior pressão de tempo para negociação.

- Play: reforçou seu papel como um player de volume constante, alinhado com campanhas menos sofisticadas, mas sustentadas, ao longo do tempo. Seu comportamento se encaixa em um ecossistema em que a lucratividade vem da repetição e padronização, e não da inovação técnica ou especialização setorial.
- Safepay: apresentou uma evolução irregular, com redução progressiva de sua atividade até novembro, seguida por uma recuperação abrupta em dezembro. Esse padrão sugere uma estratégia seletiva de reativação, consistente com crescimento controlado e redução da exposição operacional, focada em organizações de médio porte e na exploração de superfícies de ataque menos saturadas por grandes operadores de RaaS.

Top grupos de *ransomware* del S2 2025

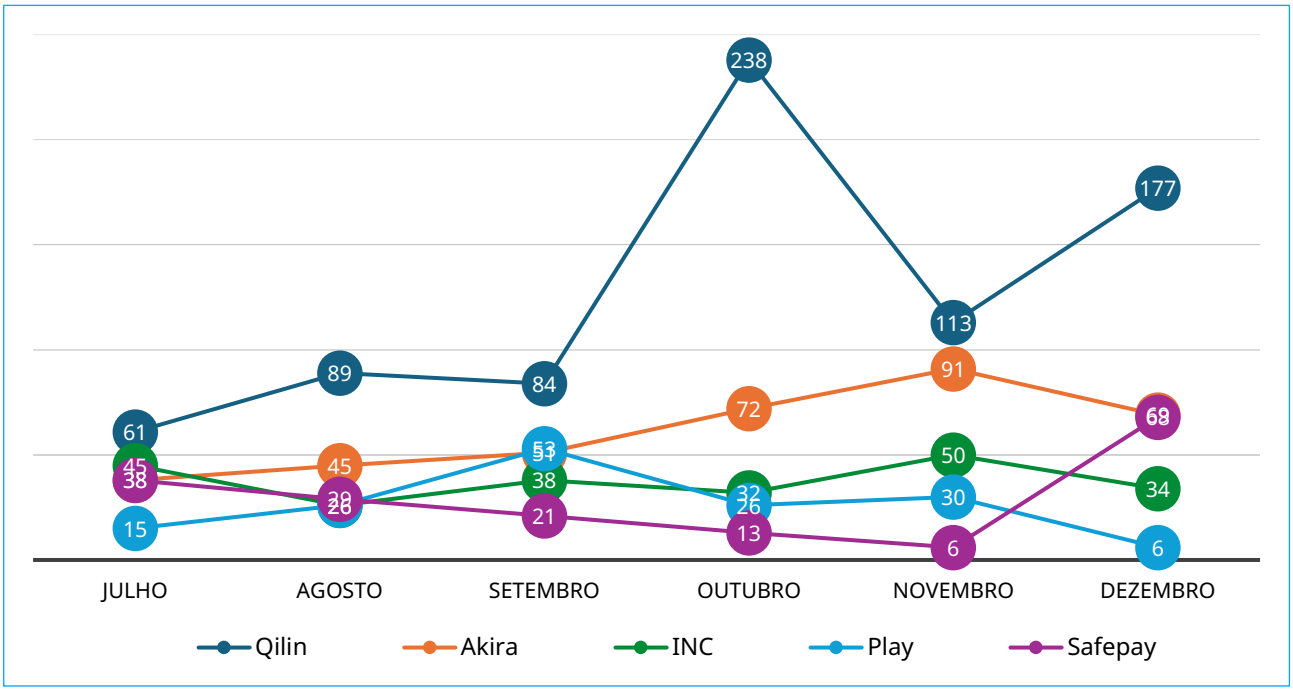


Figura 8 | Atividade dos grupos de ransomware mais ativos no segundo semestre de 2025.

7.2.3 Impacto global

O mercado. A distribuição geográfica das vítimas confirma que os grupos de ransomware continuaram a concentrar suas atividades em economias desenvolvidas, com um epicentro claro nos Estados Unidos e uma expansão progressiva para a Europa, Ásia-Pacífico e, em menor grau, o Oriente Médio. Nos dados de julho a dezembro, os Estados Unidos permaneceram consistentemente como o primeiro alvo (de 280 para 461 incidentes por mês) (DarkFeed, 2025), consolidando-o como a "Capital Mundial do Ransomware" pelo valor dos ativos, maturidade digital e capacidade de pagamento, em vez de por população ou tamanho

No segundo escalão estavam um bloco de países ocidentais com alta exposição: Reino Unido, Alemanha, França, Canadá, Espanha e Itália apresentaram números sustentados e, em alguns casos, crescimento notável no trimestre (por exemplo, Canadá e França triplicaram seus números em outubro). Esse padrão se encaixa em uma vitimização concentrada na América do Norte e Europa, onde cadeias de suprimentos complexas, alta dependência de serviços digitais e estruturas regulatórias que exigem o relato de incidentes são combinadas, aumentando a visibilidade estatística.

A partir de setembro, houve também uma diversificação para a Ásia-Pacífico e outras regiões: Coreia do Sul, Índia, Tailândia, Japão e Austrália apareceram com mais peso, enquanto em outubro também houve atividade significativa registrada nos Emirados Árabes Unidos, sinalizando uma extensão das campanhas para o Oriente Médio.

Nessas regiões, o modelo RaaS e a fragmentação do ecossistema facilitaram campanhas simultâneas em múltiplas geografias.

No geral, a tendência no segundo semestre do ano aponta para um duplo eixo: concentração do volume total nos Estados Unidos e países ocidentais, como discutido no relatório anterior, mas com um foco cada vez mais globalizado nas operações, nas quais afiliados rotacionam infraestruturas e listas de vítimas entre regiões para maximizar a pressão, Evite saturar as defesas locais e aproveitar janelas regulatórias ou de maturidade cibernética desiguais entre países.

Países mais afetados pelo ransomware no S2 2025

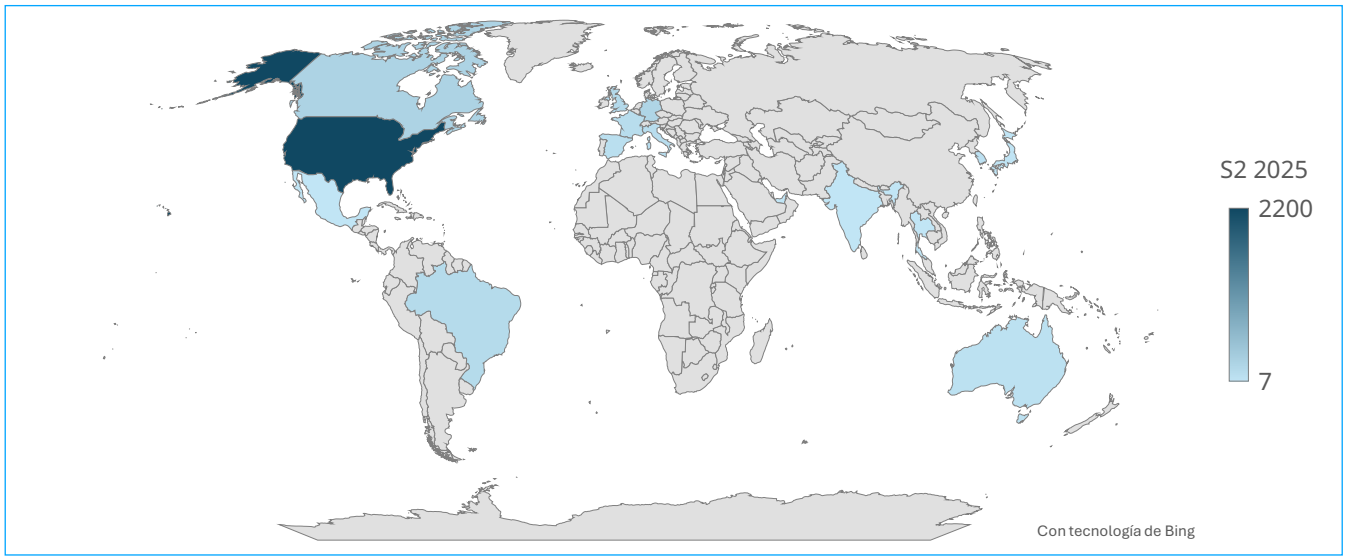
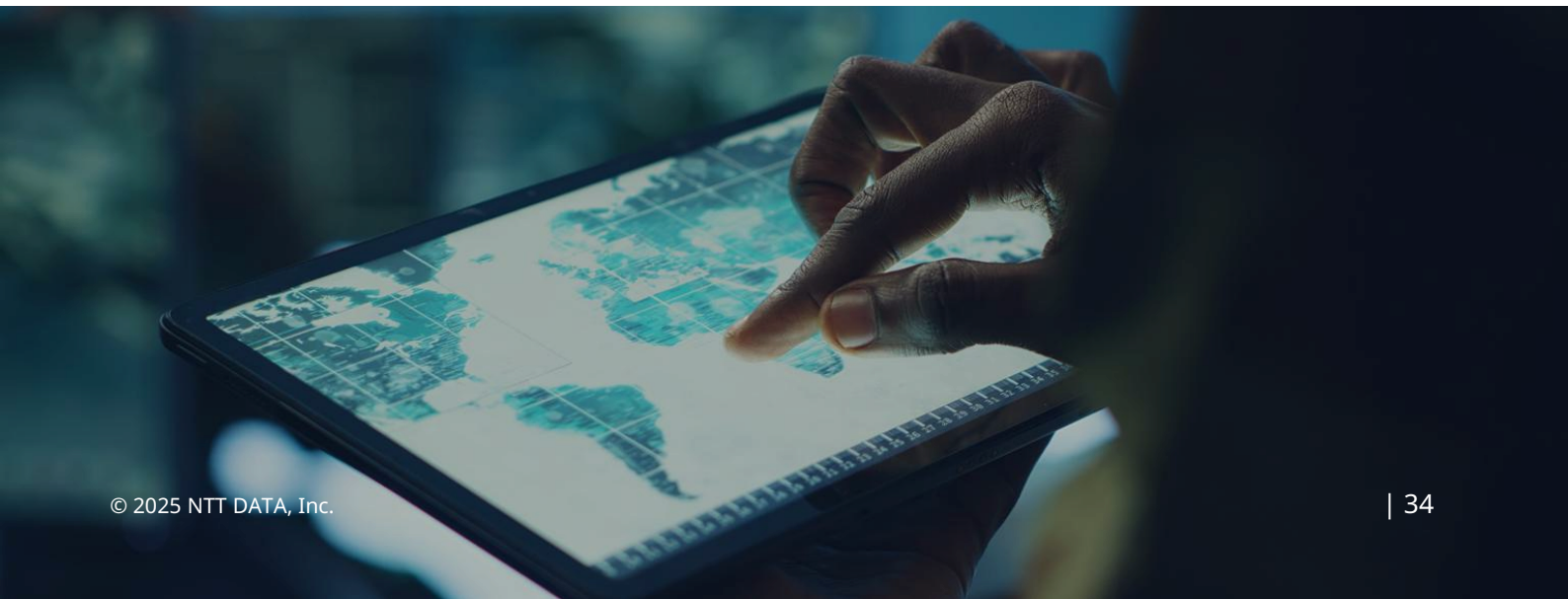


Figura 9 | Países mais afetados por ransomware na segunda metade de 2025.



Por outro lado, a análise setorial do segundo semestre de 2025 confirmou uma concentração sustentada do impacto do ransomware em setores com alta dependência operacional e baixa tolerância a interrupções, em vez daqueles simplesmente mais digitalizados. Consultoria (serviços profissionais + jurídico) tem sido o principal setor agregado do semestre, com crescimento claro a partir de outubro. A manufatura manteve uma pressão constante e transversal, impulsionada pela exposição a ambientes híbridos de TI/OT, pela criticidade dos sistemas industriais e pelo alto custo associado às paralisações de produção. O varejo e o consumo discricionário foram adicionados a esse núcleo, sendo particularmente sensíveis à sazonalidade da segunda metade do ano, e serviços de TI e profissionais, cuja atratividade reside na capacidade de gerar impacto em cadeia em múltiplas organizações.

Do ponto de vista estrutural, o semestre demonstrou uma maturidade estratégica do ecossistema de ransomware: os atores priorizam setores onde o tempo, a pressão regulatória ou reputacional acelera a tomada de decisões da vítima. Saúde, administração pública e educação mantiveram uma afetação constante, não por volume, mas por seu valor coercitivo, enquanto o peso persistente do setor reforça a tendência de ataques voltados ao impacto operacional, e não à mera exploração em massa. A contribuição diferencial em comparação com semestres anteriores não é uma mudança nos setores-alvo, mas sim uma otimização do segmento, com campanhas melhor alinhadas aos ciclos econômicos e pressão mais sustentada, antecipando a continuidade desse padrão de risco para 2026.

Ataques de ransomware por setor no segundo semestre de 2025

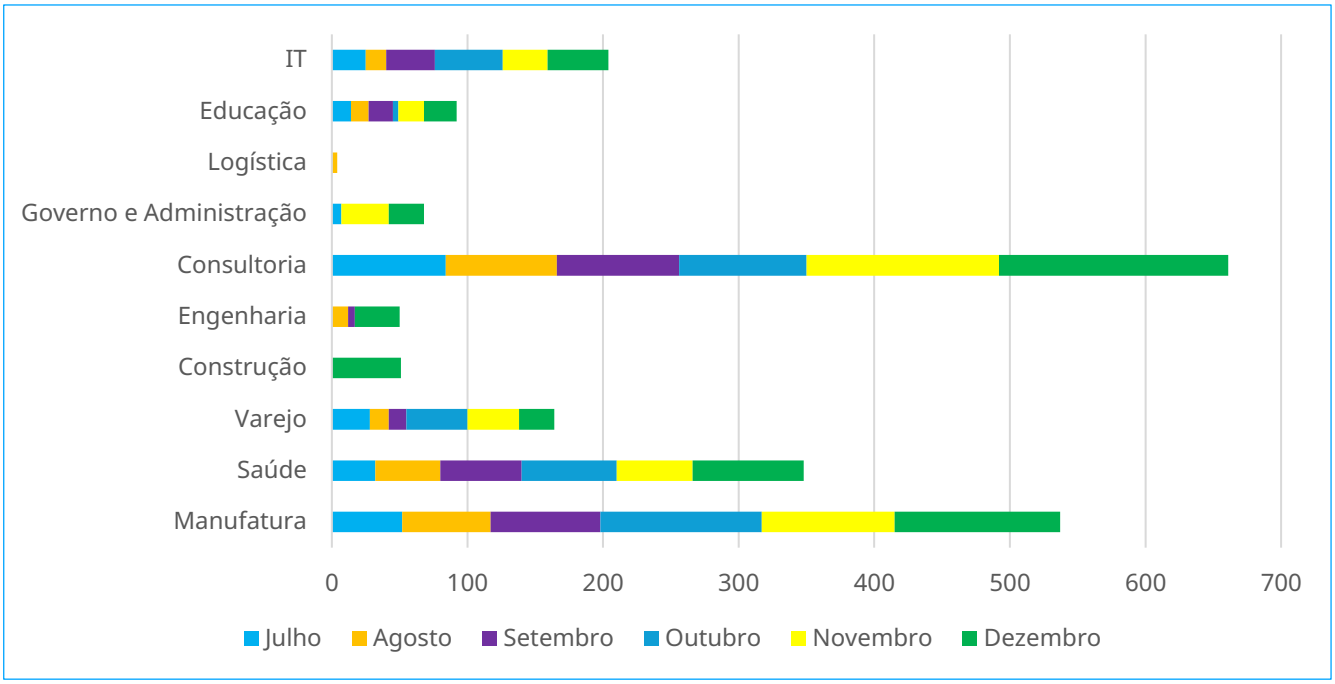


Figura 10 | Setores mais afetados pelo ransomware no segundo semestre de 2025.

7.3 *Hacktivismo*

Durante o segundo semestre do ano, observou-se uma clara intensificação do fenômeno hacktivista, caracterizada não tanto pelo surgimento de novos atores, mas pela consolidação de modelos de coordenação entre grupos e maior alinhamento com agendas geopolíticas definidas (FalconFeeds.io, 2025).

O ecossistema foi articulado em torno de blocos regionais e afinidades ideológicas, destacando, por um lado, o ambiente pró-Rússia, estruturado em coletivos como NoName057(16) e Anonymous Russia, que atuaram como nós de coordenação e agregação de capacidades. Esses grupos atuaram como espinha dorsal para campanhas distribuídas, voltadas principalmente contra infraestrutura, instituições e entidades associadas aos países da OTAN e à Ucrânia.

Paralelamente, um segundo bloco foi consolidado no ambiente Ásia-Pacífico, especialmente ativo no Sudeste Asiático e articulado em torno do BD Anonymous, Nullsec Philippines e Cyber Team Indonesia, onde múltiplos coletivos operaram sob uma lógica federada, compartilhando recursos, narrativas e objetivos, e permitindo a execução de campanhas regionais de maior escopo e persistência. compensando capacidades técnicas limitadas por meio de volume, continuidade e coordenação em janelas de tempo específicas.

Um terceiro eixo tem sido composto por atores alinhados à causa palestina e a outras correntes ideológicas relacionadas de natureza antiocidental e político-religiosa, como A Al-Mujahideen Force 313, Red Eye of Palestine y Cyber Islamic Resistance aumentaram progressivamente seu nível de cooperação trans-regional. Esses grupos demonstraram maior interconexão com outros grupos geográficos, ampliando sua visibilidade e impacto, especialmente em tempos de alta tensão geopolítica.

A análise realizada também nos permite identificar vários grupos conectores que atuaram como nós de alta qualidade e facilitaram a disseminação de TTPs e infraestrutura entre ecossistemas: BD Anonymous é o ator mais repetido nas alianças do período; NoName057(16) e Dark Storm Team com seu papel como centro para o meio ambiente pró-Rússia; Keymous+ e Clobelsec são um elo estável entre grupos de Bangladesh, Oriente Médio, Europa e Rússia; enquanto Hezi Rash, Hider_Nex ou LunarisSec reforçam a estrutura técnica na parte final do semestre.

A atividade observada confirmou um perfil orientado para a perturbação e pressão simbólica, em vez de espionagem profunda, com ataques DDoS, desfigurações, vazamentos seletivos e ações de amplificação de propaganda, com forte reutilização de infraestruturas, ferramentas conhecidas e reivindicações cruzadas entre grupos para maximizar a visibilidade.

No geral, a segunda metade do ano confirmou a evolução do hacktivismo em direção a um modelo mais organizado, coordenado e persistente, baseado em alianças flexíveis entre grupos fortemente reativos ao contexto geopolítico, com capacidade para sustentar campanhas prolongadas e ataques diretos contra alvos de alto valor simbólico e operacional. Esse padrão reforça o risco de ações sincronizadas e de maior impacto contra infraestrutura crítica e entidades estratégicas em múltiplas regiões.

Supernós de grupos hacktivistas

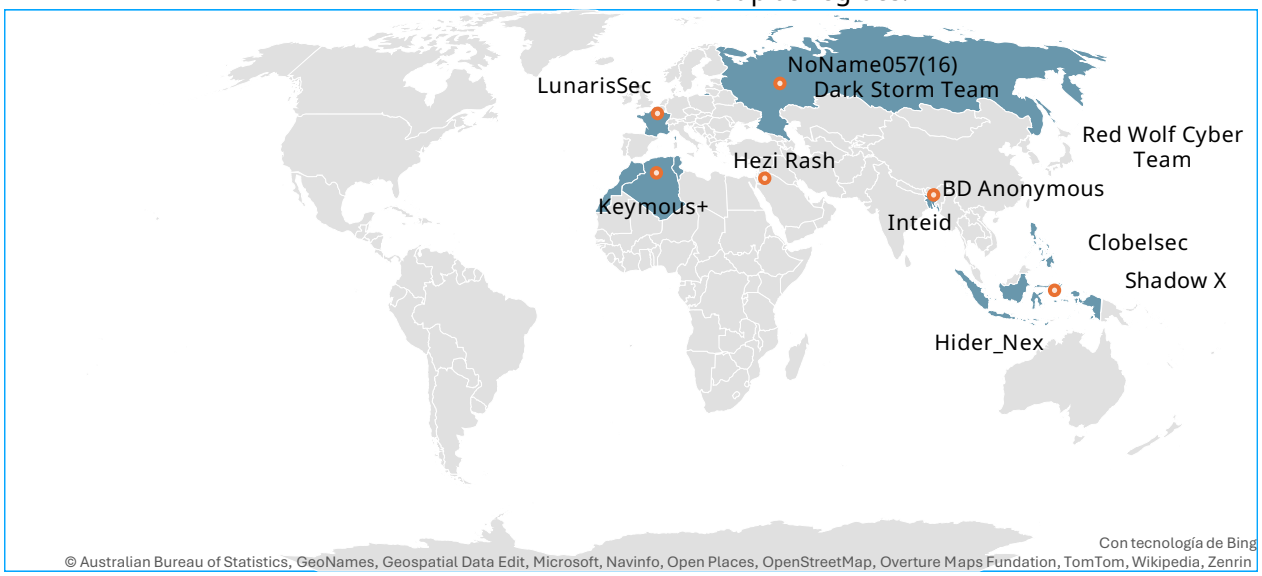


Figura 11 | Grupos de Conectores Hacktivistas por Geolocalização.

7.4 APT

Entre julho e dezembro de 2025, um padrão muito claro foi consolidado: maior sofisticação técnica, expansão geográfica das campanhas e uma ênfase crescente em compromissos de longo prazo que proporcionam vantagens estratégicas, tanto geopolíticas quanto econômicas (ESET Research, 2025).

- APT russos

O segundo semestre refletiu uma transição da agressividade aberta da primeira metade para uma estratégia de infiltração prolongada, com campanhas ativas focadas principalmente na Ucrânia e nos estados europeus. Entre os principais players, a RomCom explorou uma vulnerabilidade 0-day no WinRAR (CVE-2025-8088) para distribuir malware e estabelecer acesso persistente, enquanto a Gamaredon permaneceu um dos grupos com maior volume de atividade, caracterizada por campanhas massivas de spear-phishing, uso intensivo de malware personalizado e alta rotação de infraestruturas, voltadas para espionagem tática e coleta de inteligência contra entidades governamentais ucranianas, e União Europeia. A Sandworm manteve seu perfil de operações destrutivas e disruptivas ao implantar limpadores de para-brisas como ZEROLOT e Sting contra entidades governamentais, de energia e logísticas. A atividade do cluster InedibleOchotense, focado em spear-phishing com cargas que combinam ferramentas legítimas e seus próprios backdoors, também foi identificada. Por fim, o ecossistema hacktivista mostrou menos convergência operacional do que na primeira metade do ano: campanhas DDoS e vazamentos de informações continuaram frequentes, mas uma redução nas operações coordenadas em nível técnico e uma maior fragmentação na execução das ações foram observadas.

- APT chineses

As campanhas identificadas durante o segundo semestre do ano mostraram uma diversificação de objetivos, principalmente transporte, governos, manufatura e educação. A persistência aumentou, mais do que a variedade de novas capacidades: operações políticas e estratégicas de inteligência com longos ciclos operacionais foram priorizadas. Atividade intensa foi observada em grupos como Mustang Panda, Flax Typhoon, Speccom e FamousSparrow, este último especialmente ativo na América Latina, com intrusões em múltiplos governos. Ele destacou o aumento no uso de técnicas adversário-in-the-middle (AitM) para acesso inicial e movimento lateral, bem como a exploração de roteadores, atualizações e outros vetores de confiança para implantar backdoors, observada em grupos como SinisterEye e PlushDaemon. Comparado ao primeiro semestre do ano, nenhum equivalente a grandes blocos de malware (como o NanoSlate) foi detectado, mas sim uma otimização incremental do arsenal existente.

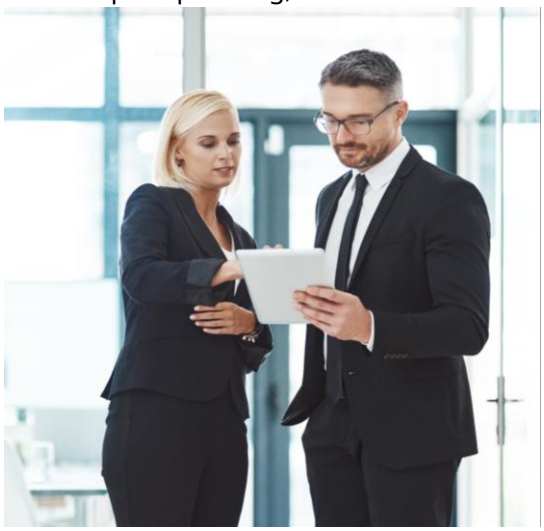
- APT Iranianos

O foco do Irã mudou para infiltração e engenharia social com técnicas mais credíveis e difíceis de detectar, reforçando a tendência global de persistência encoberta. A MuddyWater se destacou por intensificar suas campanhas globais de spear-phishing ao usar caixas de correio internas comprometidas para enviar e-mails maliciosos, uma técnica já identificada no primeiro semestre do ano. Outros players como BladedFeline (parte da OilRig) e GalaxyGato evoluíram seu arsenal, incorporando sequestro de DLL por ordem de busca e novas versões de backdoors como o C5, projetados para roubo de credenciais, persistência e evasão. Os principais alvos continuaram sendo agências governamentais e setores estratégicos no Oriente Médio, embora com a expansão para a Europa e Ásia Central, tenha consolidado uma presença mais ampla e técnica no campo da espionagem.

- APT Coreanos do Norte

Grupos ligados à Coreia do Norte mantiveram alta atividade, combinando espionagem e operações voltadas para gerar renda para o Estado, consolidando um modelo híbrido APT-crime. Players como Lazarus, Kimsuky, DeceptiveDevelopment e Konni mantêm campanhas diversificadas, focadas em governos, diplomacia, tecnologia e, especialmente, no setor de criptomoedas.

Este semestre viu uma colaboração sem precedentes entre Kimsuky e Lazarus, que combinam capacidades de espionagem e exploração técnica em campanhas globais coordenadas. Kimsuky, especializado em reconhecimento de inteligência e exfiltração via sofisticado spear-phishing,



inicia intrusões com e-mails direcionados (por exemplo, convites acadêmicos com malware FPSpy e keylogger) para mapear redes e coletar credenciais. Uma vez comprometido o ambiente, a Lazarus explora vulnerabilidades zero-day e distribui pacotes maliciosos que ganham privilégios de SISTEMA e implantam a backdoor InvisibleFerret, projetada para evasão e exfiltração de EDR de ativos de alto valor (incluindo criptomoedas).

Ambos os grupos utilizam uma infraestrutura compartilhada para coordenação, execução e limpeza de impressões digitais, e têm como alvo setores críticos como defesa, finanças, energia e blockchain. Essa aliança reforçou a tendência para operações APT mais integradas, onde a combinação de técnicas de espionagem e crimes financeiros cibernéticos aumenta a eficácia das campanhas (De Jong, 2025).

De acordo com as estatísticas observadas (NSFOCUS, 2025), as tendências que marcaram o período são:

Principais tendências observadas nos grupos de APT no segundo semestre de 2025

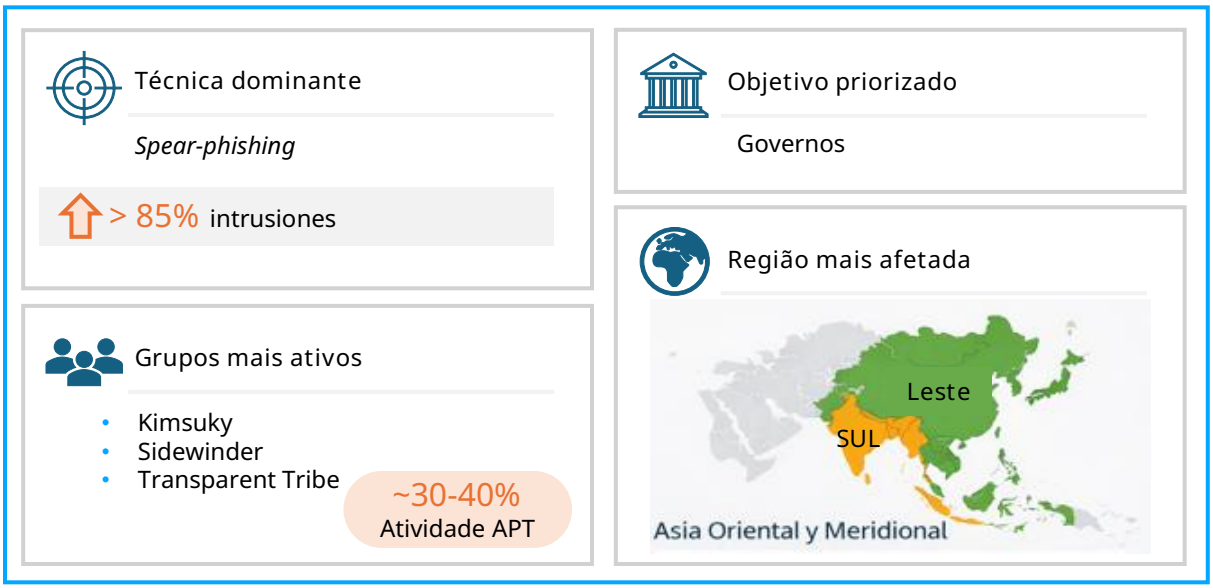
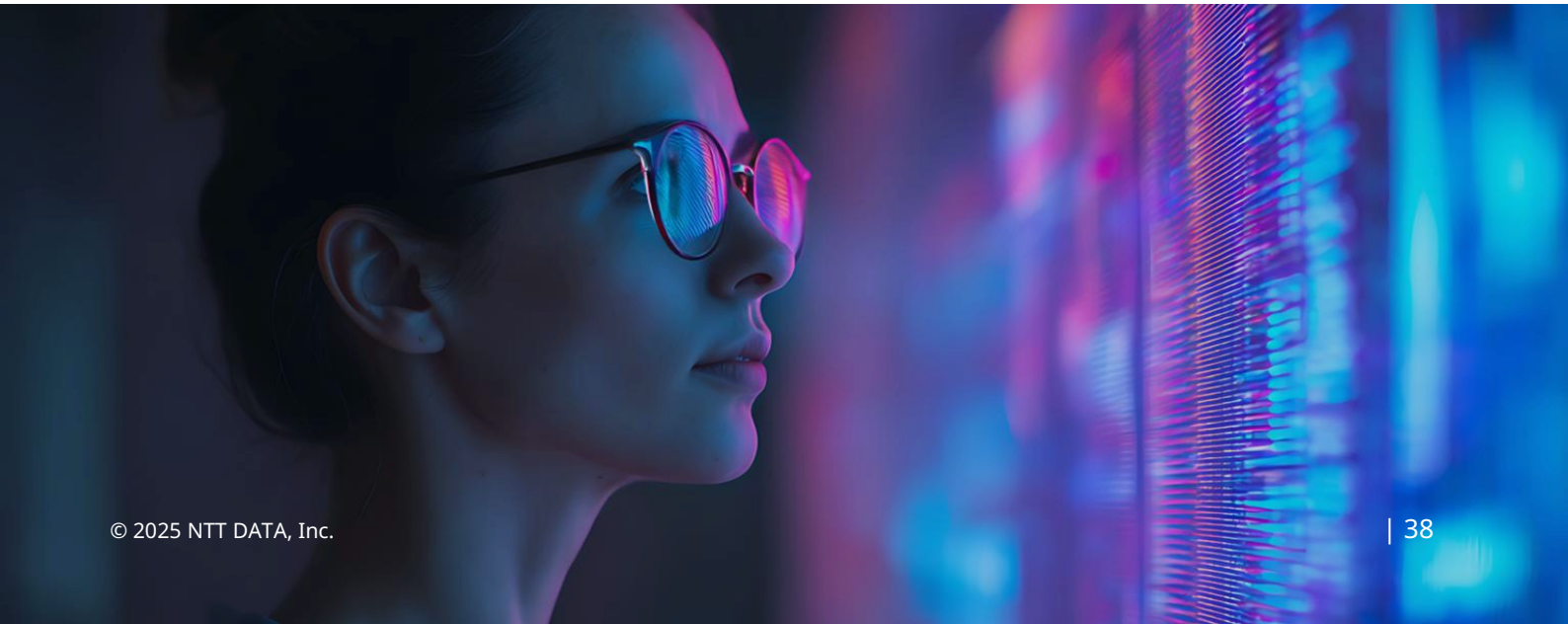


Figura 12 | Tendências principais do grupo APT durante o segundo semestre de 2025.

A análise do segundo semestre de 2025 confirmou a predominância de campanhas persistentes de espionagem por APTs alinhados com grupos da China, Coreia do Norte e Sul da Ásia, em comparação com um componente disruptivo e destrutivo maior em atores ligados à Rússia e, em menor grau, ao Irã. Essa diferenciação operacional, condicionada pelo contexto geopolítico, possibilita identificar padrões claros por região e antecipar uma evolução rumo a intrusões mais longas e furtivas, visando obter vantagens estratégicas no médio e longo prazo.



8. Táticas, Técnicas e Procedimentos (TTPs)

Durante o segundo semestre de 2025, a equipe de Inteligência de Ameaças Cibernéticas da NTT DATA analisou a evolução das táticas, técnicas e procedimentos (TTPs) empregados por grupos cibercriminosos e atores motivados geopoliticamente. A análise confirma uma tendência clara: os atacantes não dependem principalmente de técnicas radicalmente novas, mas da combinação de TTPs conhecidos executados com maior velocidade, escala e automação, cada vez mais suportados por ferramentas baseadas em inteligência artificial.

Dados coletados em relatórios de referência do setor mostram que o cibercrime motivado economicamente continua dominando o cenário global, respondendo por mais de 70% das intrusões interativas observadas no último ano (CrowdStrike, 2025). Nesse contexto, *ransomware*, extorsão múltipla, abuso de identidade e exploração de infraestrutura exposta continuam sendo os pilares operacionais da maioria das campanhas.

8.1 Descrição dos TTPs mais comuns usados por cibercriminosos

Comparado ao primeiro semestre de 2025, os TTPs observados durante o segundo semestre de 2025 não introduzem novas técnicas dentro do quadro MITRE ATT&CK, mas mostram uma mudança em seu uso e combinação. Observa-se um maior peso de técnicas voltadas para persistência, acesso a credenciais e evasão de defesas, em comparação com abordagens mais diretas e ruidosas do semestre anterior. Da mesma forma, a relevância do abuso de identidades válidas e serviços remotos aumenta, especialmente em ambientes de nuvem, e a exfiltração de dados é consolidada como um passo preliminar para o ransomware, reforçando esquemas de extorsão dupla. No geral, o segundo semestre do ano reflete maior maturidade operacional dos atacantes, mais focados em manter o acesso e maximizar o impacto do que em implantar técnicas inovadoras.

Tática	MITRE ATT&CK ID	Descrição
Persistência (TA0003)	T1098 – Manipulação de contas	Atacantes modificam contas existentes (usuários locais, contas *cloud* ou de serviço) para manter o acesso persistente e dificultar a detecção.
	T1136.001 – Criar Conta: Conta Local	Criação de contas locais adicionais para garantir persistência após o acesso inicial.
	T1547.001 – Execute no Início: Chaves do Registro / Pasta de Inicialização	Configuração de persistência usando chaves de início automático em sistemas Windows.
	T1133 – Serviços Remotos Externos	Uso de serviços expostos (RDP, VPN, aplicações web) para acessar ou persistir no ambiente comprometido.
	T1098.004 – Manipulação de Conta: Chaves de Nuvem Adicionais	Adicione chaves, tokens ou credenciais em ambientes *cloud* para manter o acesso persistente.
Escalada de privilégios (TA0004)	T1134 – Manipulação de *tokens* de acesso	Uso indevido de tokens para executar ações em um contexto de maior privilégio.
	T1548 – Abuso dos Mecanismos de Elevação de Privilégio	Aproveitamento de configurações fracas ou controles inadequados para elevar privilégios.

Tabela 4 | TTPs mais comuns durante o segundo semestre de 2025.

Táticas	MITRE ATT&CK ID	Descrição
Evasão das defesas (TA0005)	T1562.001 – Desativar ou modificar ferramentas de segurança	Desativar antivírus, EDR ou mecanismos de proteção para evitar a detecção.
	T1562.004 – Modificar ou desativar o *firewall* do sistema	Alteração de regras de *firewall* para facilitar a comunicação com atacantes.
	T1070.001 – Eliminação de Indicadores: Excluindo Registros	Excluindo *logs* do sistema para esconder vestígios de invasão.
	T1564.008 – Ocultar Artefatos: Regras de ocultação de e-mails	Uso de regras de e-mail para ocultar comunicações maliciosas ou exfiltração de dados.
Acesso a credenciais (TA0006)	T1003 – Despejo de credenciais do OS	Extração de credenciais armazenadas na memória ou nos arquivos do sistema.
	T1552 – Credenciais não protegidas	Obtenção de credenciais armazenadas em texto claro, *scripts* ou configurações.
	T1528 – Roubo de *token* de acesso a aplicativos	Roubo de tokens válidos para acessar aplicativos e serviços remotos.
Descoberta (TA0007)	T1046 – Descoberta de Serviços de Rede	Enumeração de serviços e portas para identificar alvos adicionais.
	T1082 – Descoberta de Informações do Sistema	Obtenção de detalhes sobre sistema operacional e *hardware*.
	T1016 – Descoberta de Configuração de Rede	Identificação de topologia e conexões de rede usando comandos nativos.
	T1057 – Descoberta de processos	Enumeração de processos ativos para identificar *softwares* de segurança ou alvos críticos.
	T1087.001 – Descoberta de Conta: Conta Local	Enumeração de contas de usuários locais para facilitar movimentos subsequentes.
Movimento lateral (TA0008)	T1021 – Serviços Remotos	Uso de RDP, SMB ou outros serviços para se mover lateralmente dentro da rede.
Exfiltração (TA0010)	T1041 – Exfiltração sobre o canal de comando e controle	Exfiltração de dados por canais já estabelecidos com o atacante.
Impacto (TA0040)	T1486 – Criptografia de dados para impacto	Criptografia de sistemas e arquivos como parte de campanhas de *ransomware*.
	T1490 – Inibição da Recuperação do Sistema	Deletar ou desativar backups para evitar recuperação.

Tabela 4 | TTPs mais comuns durante o segundo semestre de2025.

8.2 Vetores de entrada mais comuns

Durante o segundo semestre de 2025, os vetores de entrada usados por cibercriminosos mantêm uma continuidade clara com os observados no primeiro semestre de 2025. No entanto, a análise realizada pela equipe de Inteligência de Ameaças Cibernéticas da NTT DATA confirma que a relevância desses vetores não está em sua novidade técnica, mas em sua consolidação como mecanismos de acesso inicial silenciosos, persistentes e de baixa visibilidade.

Diferentemente de períodos anteriores, o acesso inicial depende cada vez menos da exploração direta de vulnerabilidades visíveis e mais de identidades, credenciais legítimas, confiança organizacional e serviços devidamente configurados, porém abusados. Essa mudança dificulta a detecção precoce e reduz a capacidade de diferenciar entre atividades legítimas e maliciosas desde os estágios iniciais da intrusão

Identidade como vetor de acesso	Engenharia social orientada à identidade	Ambientes de *cloud* e APIs
O abuso de identidades válidas é consolidado como um dos principais mecanismos de acesso inicial. Atacantes usam credenciais roubadas, *cookies* de sessão e *tokens* de acesso para operar sem implantar *malware*, reduzindo significativamente a visibilidade e aumentando o tempo de detecção. Esse vetor favorece intrusões prolongadas e facilita o movimento lateral desde os estágios iniciais.	Uso de técnicas de engenharia social com o objetivo de obter credenciais ou consentimento do usuário, incluindo *vishing*, personificação de suporte técnico, campanhas BEC e abuso de fluxos comuns de autenticação. Esse vetor explora a confiança nos processos cotidianos e permite o acesso inicial sem a necessidade de exploração técnica direta.	Aumento no acesso inicial devido a erros de configuração em ambientes *cloud*, permissões excessivas, chaves de API expostas e abuso de relações de confiança entre serviços. Esse vetor é especialmente relevante em arquiteturas híbridas e *multicloud*, onde visibilidade e controle são mais limitados.
Infostealers avançados	*Software* não autorizado / *shadow* IT	Abuso de serviços remotos legítimos
Evolução do uso de *infostealers* como fase prévia estrutural para ataques de *ransomware*, fraudes e acessos não autorizados. O roubo automatizado de credenciais, *cookies* e dados do navegador posiciona esse vetor como um dos mais eficazes do semestre, tanto por sua escalabilidade quanto pelo baixo custo operacional.	Uso de ferramentas e *softwares* profissionais baixados fora dos canais oficiais como porta de entrada inicial. Esse vetor aproveita a pressão operacional e a confiança em aplicações aparentemente legítimas, introduzindo acesso persistente e reduzindo a capacidade de detectar e atualizar a segurança.	Uso de RDP, VPN e ferramentas de administração remota com credenciais válidas como mecanismo inicial de acesso. Esse vetor permite que atacantes operem usando serviços legítimos, minimizando a pegada técnica do acesso e complicando a detecção precoce por equipes defensivas.

Tabela 5 | Vetores de entrada mais comuns usados no segundo semestre de 2025.

No geral, durante o segundo semestre de 2025, o acesso inicial não é mais baseado principalmente em falhas técnicas óbvias e está cada vez mais orientado para identidades, confiança e uso legítimo dos serviços. Essa abordagem aumenta a dificuldade da detecção precoce e o impacto potencial dos ataques, permitindo que os adversários estabeleçam acesso inicial que não gera alertas imediatos ou comportamentos claramente anômalos.

Essa evolução reforça a necessidade de abordar a segurança de acesso inicial a partir de uma perspectiva que combine controles técnicos, gestão de identidades, visibilidade sobre ambientes em *cloud* e monitoramento de processos humanos, lançando as bases para entender a evolução operacional que está ocorrendo na área de inovação em ataques.

8.3 Inovação em ataques: novas técnicas e táticas

Durante o segundo semestre de 2025, a inovação em campanhas de ciberataque não se manifestou no surgimento de técnicas radicalmente novas dentro do quadro MITRE ATT&CK, mas sim em uma mudança estrutural na lógica operacional do atacante. Ao contrário das abordagens mais diretas e oportunistas observadas na primeira metade do ano, a segunda metade consolida um modelo baseado na persistência, automação e exploração sistemática da confiança, onde o objetivo não é apenas comprometer sistemas, mas integrar ao longo de um longo período de tempo aos processos normais da organização.

Essa mudança não é expressa na fase inicial de acesso, descrita na seção de vetores de entrada, mas na forma como os atacantes operam uma vez dentro do ambiente comprometido, gerenciando o tempo, reduzindo sinais de detecção e maximizando o impacto final.

De ataques barulhentos a operações prolongadas e de baixo perfil

Uma das principais diferenças em relação ao primeiro semestre do ano é a redução deliberada do ruído técnico.

Os atacantes estão priorizando cada vez mais técnicas *hands-on-keyboard*, o uso de ferramentas legítimas do sistema e execução manual assistida, em detrimento da implantação massiva de *malware* persistente. Relatórios de *threat hunting* confirmam que uma proporção crescente de intrusões interativas é desenvolvida sem implantar malware tradicional, dificultando a detecção precoce e prolongando significativamente o tempo gasto em ambientes comprometidos (CrowdStrike, 2025).

Nesse contexto, o tempo torna-se um ativo estratégico do atacante. O tempo de permanência prolongado permite que você entenda o ambiente, identifique ativos críticos, observe padrões operacionais e se prepare para o impacto final com mais precisão. Essa abordagem marca uma transição clara de campanhas oportunistas para operações seletivas, onde o valor não está na velocidade inicial, mas na capacidade de permanecer indetectado e fragmentar sinais defensivos em múltiplos domínios (identidade, *endpoint* e *cloud*).

Industrialização do *ransomware* e consolidação da extorsão múltipla

Durante o segundo semestre do ano, o *ransomware* deixou de ser uma técnica de impacto pontual e foi consolidado como um processo de negócios altamente estruturado. Dados disponíveis indicam que as receitas globais associadas aos pagamentos de *ransomware* ultrapassam US$ 2 bilhões, demonstrando a maturidade econômica e organizacional do modelo (Financial Crimes Enforcement Network [FinCEN], 2025).

A inovação não está na criptografia em si, mas na orquestração de ponta a ponta da campanha. Atacantes automatizam a classificação de informações roubadas, priorizam os dados mais sensíveis e utilizam vazamentos parciais e em níveis como mecanismo de negociação. Esse modelo reforça esquemas de extorsão dupla e tripla e reduz a dependência da criptografia como único meio de pressão, permitindo que lucros sejam obtidos mesmo sem interromper completamente a operação da vítima.

Inteligência artificial como acelerador tático, não como substituto

Diferentemente do primeiro semestre de 2025, quando a inteligência artificial apareceu principalmente como uma tendência emergente, durante o segundo semestre de 2025 observa-se sua integração prática e sistemática em diferentes fases do ataque. A IA é utilizada para acelerar tarefas específicas: geração de conteúdo de engenharia social, adaptação linguística e cultural, análise de informações anteriores sobre a vítima ou suporte ao desenvolvimento e modificação de ferramentas maliciosas (IBM Security, 2025).

No campo de *malware*, casos de ferramentas desenvolvidas ou ajustadas com suporte à IA para reduzir erros de código, melhorar a ofuscação ou adaptar cargas úteis a diferentes ambientes operacionais foram documentados (ESET, 2025; Garaschenko, 2025). No entanto, esses desenvolvimentos ainda exigem supervisão humana, confirmando que a IA não substitui o operador, mas sim reduz o custo cognitivo e operacional do ataque, permitindo que as campanhas sejam escaladas com menos esforço e mais rapidamente.

Exploração dos processos de confiança e organizacionais como vetor operacional

Um elemento claramente diferenciador da segunda metade do ano é a instrumentalização dos processos organizacionais legítimos como parte central da tática de ataque. Além do acesso inicial, os atacantes utilizam processos como contratação, colaboração técnica, trabalho remoto ou o uso diário de ferramentas profissionais para normalizar sua presença dentro da organização.

Foram identificadas campanhas em que atores maliciosos usam identidades sintéticas e assistência baseada em IA para passar em entrevistas técnicas, integrar-se às equipes de trabalho e manter acesso prolongado a sistemas internos. Esses tipos de táticas mudam o foco da infraestrutura tecnológica para a confiança operacional e cultural, expandindo significativamente a superfície de ataque e borrando a fronteira entre ameaças externas e internas(CrowdStrike, 2025).

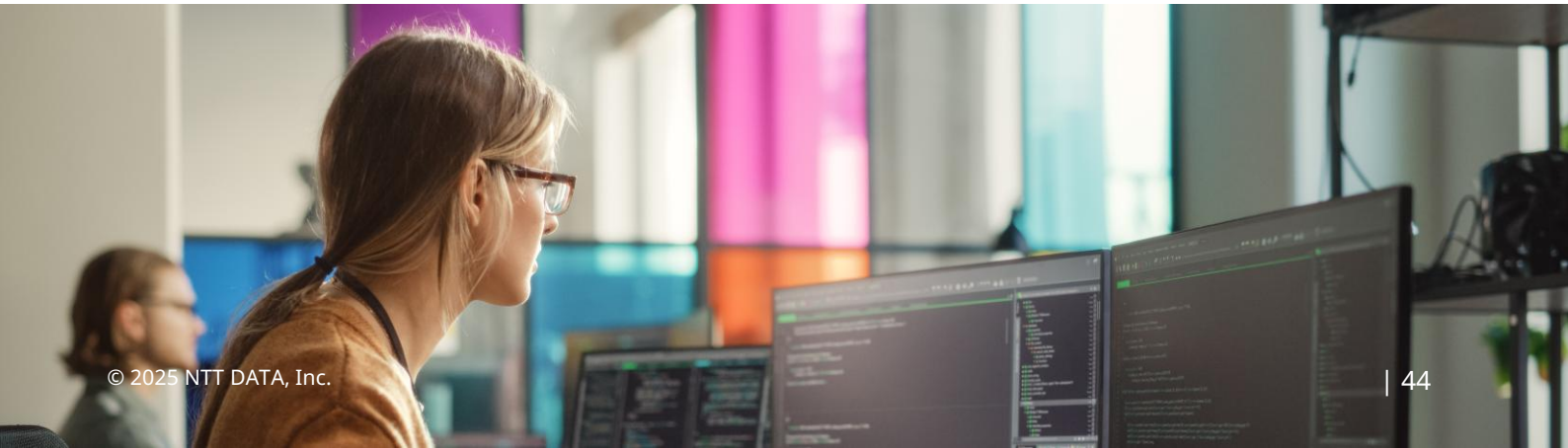
Velocidade de exploração e pressão de tempo na defesa

O segundo semestre do ano também consolida uma redução drástica na margem para reação defensiva. Vulnerabilidades críticas estão sendo exploradas cada vez mais rapidamente após a divulgação pública, sendo integradas quase imediatamente em campanhas automatizadas. Esse comportamento aumenta a pressão sobre as equipes defensivas e penaliza especialmente as organizações com ciclos lentos de patch, visibilidade limitada ou dependência de processos manuais (Arctic Wolf, 2025; Wright, 2025)

A combinação de automação, inteligência artificial e especialização criminal transforma a divulgação pública de uma vulnerabilidade em uma corrida assimétrica, onde atacantes podem reagir mais rápido do que muitas organizações defensivas.

No geral, o segundo semestre de 2025 marca uma evolução qualitativa em comparação com a primeira: menos foco no acesso inicial e mais ênfase em como operar dentro da organização sem ser detectado. A inovação não se expressa em novas técnicas isoladas, mas sim na combinação de persistência, automação, inteligência artificial e abuso de confiança para executar ataques mais direcionados, duradouros e lucrativos.

Essa dinâmica reforça a necessidade de abordar a cibersegurança não apenas pela tecnologia, mas de uma perspectiva abrangente que inclui processos, cultura organizacional e capacidades de detecção contextual, capazes de interpretar sinais fracos e operações distribuídas em múltiplos domínios.



9. Vulnerabilidades

O segundo semestre de 2025 consolidou vulnerabilidades críticas como um dos principais vetores de compromisso inicial, com um padrão claro de exploração rápida, campanhas direcionadas e uso recorrente de *0-days*. A atividade observada reflete uma redução sustentada no tempo entre a divulgação, e até mesmo antes dela, e a exploração ativa, evidenciando uma alta maturidade operacional dos atores ameaçadores.

Durante esse período, a exploração não se limitava a ataques oportunistas, mas era integrada em campanhas estruturadas, combinando acesso inicial, movimento lateral e persistência.

Abaixo está uma análise mensal das vulnerabilidades mais proeminentes do período, como base para orquestrar as grandes campanhas detectadas.

- Julho:

A vulnerabilidade conhecida como SharePoint ToolShell Exploitation refere-se a uma campanha de exploit direcionada a servidores Microsoft SharePoint em ambientes locais que não foram devidamente corrigidos. Essa campanha foi baseada na exploração de falhas críticas de segurança que permitiam a um atacante executar código remotamente e realizar técnicas de personificação, comprometendo completamente o sistema afetado.

Inicialmente, a exploração estava associada a vulnerabilidades identificadas como CVE-2025-49706 e CVE-2025-49704, que depois foram ampliadas e correlacionadas com os identificadores CVE-2025-53770 e CVE-2025-53771. Essas vulnerabilidades afetavam especificamente as instalações *on-premises* do SharePoint, aumentando o risco em organizações que não aplicavam atualizações de segurança em tempo hábil.

A campanha foi atribuída a vários atores de ameaça avançados. Entre eles estão o Storm-2603, um ator de *ransomware* ligado à China, assim como o Threat Group-3390 e o ZIRCONIUM, este último principalmente associado a atividades de ciberespionagem. A diversidade dos atores envolvidos mostra o alto valor estratégico dessas vulnerabilidades e seu uso tanto para fins econômicos quanto de inteligência.

As informações e atribuições dessa campanha são documentadas pela MITRE ATT&CK, onde são coletadas como uma campanha específica de exploração sob o identificador correspondente, servindo como referência para a análise e mitigação desse tipo de ameaça (MITRE, 2025).

- Agosto:

A vulnerabilidade de Travessia de Diretórios no WinRAR corresponde a uma falha crítica de segurança identificada na versão para Windows deste *software* de compressão. Essa fraqueza permitia que um atacante manipulasse os caminhos internos dos arquivos comprimidos para escrever ou executar arquivos fora do diretório pretendido, o que abria a porta para a execução arbitrária de código no sistema da vítima.

A vulnerabilidade foi registrada como CVE-2025-8088 e explorada usando arquivos especialmente elaborados. Quando abertos pelo usuário, esses arquivos permitiam a instalação silenciosa de código malicioso sem a necessidade de privilégios elevados ou interação adicional, comprometendo diretamente a integridade do sistema afetado.

Essa falha foi ativamente explorada globalmente, destacando seu uso pelo grupo de ameaça RomCom, um ator alinhado com interesses russos. A RomCom aproveitou essa vulnerabilidade como um vetor de acesso inicial para implantar *malware* do tipo backdoor, facilitando o controle remoto, a persistência em sistemas comprometidos e a execução subsequente de atividades maliciosas.

As informações técnicas e o monitoramento dessa vulnerabilidade foram documentados por várias fontes de inteligência de ameaças, que alertaram sobre sua exploração ativa e a necessidade de atualizar o WinRAR para mitigar o risco associado a esse vetor de ataque (Strobes, 2025).

- Setembro:

A vulnerabilidade arbitrária na execução de código no Windows refere-se a uma falha crítica de segurança que permitiu a um atacante executar código malicioso em sistemas afetados por meio da interação do usuário. Comprometendo diretamente a confidencialidade, integridade e disponibilidade de sistemas Windows vulneráveis.

Essa vulnerabilidade pode ser usada como vetor de acesso inicial, resultando na execução de código e comprometimento do endpoint afetado, sem necessariamente exigir privilégios elevados.

Identificada como CVE-2025-9491, a vulnerabilidade foi ativamente explorada antes do lançamento de um patch oficial. Seus abusos afetaram a confidencialidade, integridade e disponibilidade dos sistemas comprometidos.

A exploração dessa vulnerabilidade foi atribuída ao ator ameaçador UNC6384, um grupo afiliado à China. Esse ator mirou alvos de alto valor, nomeadamente sistemas pertencentes a diplomatas europeus localizados na Bélgica, Hungria e outros Estados-membros da União Europeia, indicando uma clara motivação de ciberespionagem.

Informações sobre essa vulnerabilidade e sua exploração foram registradas, servindo como referência para monitorar a ameaça e implementar medidas de segurança voltadas a prevenir esse tipo de ataque em ambientes Windows (Girnus, 2025).

- Outubro:

A vulnerabilidade CVE-2025-41244 afetou certos componentes da VMware, incluindo VMware Tools / VMware Aria Operations, e tem sido associada principalmente a cenários locais de elevação de privilégios em sistemas vulneráveis. Diversos avisos de segurança indicaram sinais de exploração em ambientes reais, reforçando a necessidade de implementar urgentemente as atualizações e mitigações publicadas pelo fabricante.

Embora a vulnerabilidade não permita a execução remota de código ou movimentação lateral, sua exploração pode facilitar o fortalecimento da posição do atacante após o acesso inicial prévio, aumentando o impacto de uma intrusão contínua nas infraestruturas corporativas.

Em campanhas reais observadas durante o período, uma vez que o acesso inicial foi obtido por outros vetores, os atacantes usaram ferramentas de acesso remoto como o ScreenConnect para operação interativa e persistência, bem como para movimentos laterais dentro da rede corporativa. Essas técnicas devem ser entendidas como TTPs pós-compromisso, e não como mecanismos inerentes à exploração direta da vulnerabilidade CVE-2025-41244.

A atividade maliciosa relacionada a essas cadeias de ataques tem sido atribuída ao grupo de ameaça UNC5174, um ator com capacidades avançadas e experiência em ambientes empresariais complexos. Este caso destaca o risco de explorar falhas em plataformas de virtualização amplamente implantadas e a importância de manter uma estratégia adequada de gerenciamento de vulnerabilidades e detecção pós-exploração em ambientes Vmware (SOCRadar, 2025; SOCRadar Extended Threat Intelligence, 2025).

- Novembro:

Uma falha crítica de desserialização no Microsoft Windows Server Update Services (WSUS) foi identificada e ativamente explorada em novembro de 2025. Essa vulnerabilidade afetava servidores WSUS expostos e permitia que um atacante executasse código remotamente com privilégios do sistema, comprometendo completamente o servidor afetado.

A vulnerabilidade foi registrada como CVE-2025-59287 e foi um *0-day* durante o período inicial de exploração, até que a Microsoft publicou o patch de segurança correspondente. Os atacantes exploraram essa falha como um vetor de acesso inicial, permitindo que assumissem o controle do serviço WSUS e o usassem como ponto de entrada para a infraestrutura interna das organizações.

Após a exploração, os agentes ameaçadores implantaram a *backdoor* modular ShadowPad, uma ferramenta avançada que oferece controle remoto persistente, capacidades de espionagem e execução de comandos. O uso do ShadowPad é especialmente relevante, já que esse *malware* é rotineiramente associado a grupos de ciberespionagem patrocinados pelo Estado chinês, sugerindo uma motivação estratégica por trás dos ataques.

Informações sobre essa vulnerabilidade e sua exploração foram documentadas em relatórios de inteligência de ameaças que alertaram sobre a gravidade do impacto e a necessidade urgente de aplicar as atualizações de segurança correspondentes para mitigar o risco associado ao CVE-2025-59287 (Lakshmanan, 2025).

- Dezembro:

Em dezembro de 2025, uma falha crítica no React Server Components, conhecida como React2Shell, foi identificada e ativamente explorada, afetando aplicações web expostas usando certas versões do *framework* React no lado do servidor. Essa vulnerabilidade permitiu que um atacante executasse código remotamente no servidor alvo, comprometendo a aplicação e o ambiente subjacente sem a necessidade de autenticação prévia.

A vulnerabilidade foi registrada como CVE-2025-55182 e recebeu uma pontuação CVSS de 10,0 devido ao seu impacto crítico. A falha residia no manuseio inseguro do processo de desserialização dos dados enviados do navegador para o servidor por meio do protocolo React Flight. Ao enviar uma única requisição HTTP especialmente manipulada, um atacante poderia interferir na lógica interna da aplicação e realizar execução arbitrária de código JavaScript com os mesmos privilégios da aplicação afetada. Essa fraqueza impactou diretamente *frameworks* baseados em React Server Components, como Next.js, expandindo significativamente a superfície de ataque.

Após a exploração inicial, múltiplas atividades pós-exploração foram observadas em sistemas comprometidos, incluindo o download e execução de *loaders* maliciosos, a instalação secreta de Node.js, a criação de mecanismos de persistência usando systemd, cron e rc.local, bem como comunicações com infraestruturas de comando e controle hospedadas em serviços públicos de *cloud*. Tarefas de reconhecimento de rede, exfiltração básica de informações e o uso de *webhooks* e Canarytokens também foram detectados para confirmar o sucesso da intrusão.

Diversas investigações atribuíram a exploração dessa vulnerabilidade a atores de ameaça avançada, principalmente ligados à China, incluindo infraestruturas associadas a grupos como Earth Lumia e Jackpot Panda. No entanto, a publicação de código de prova de conceito aumentou rapidamente o risco de exploração por atores oportunistas, ampliando o escopo do impacto além da espionagem estatal. Relatórios de inteligência de ameaças destacaram a necessidade urgente de aplicar patches de segurança publicados e revisar a exposição de aplicativos React acessíveis pela internet para mitigar o risco associado ao CVE-2025-55182 (Westman y Sophos, 2025).

Tendências de exploração dessas vulnerabilidades

O segundo semestre de 2025 confirma e reforça as tendências já observadas durante o primeiro semestre do ano, nas quais uma exploração cada vez mais precoce e sistemática de vulnerabilidades críticas como principal vetor de acesso inicial foi antecipada. Longe de estabilizar, a taxa de abuso de bugs de alto impacto se intensificou na S2, consolidando um cenário marcado pela redução das janelas de exposição entre a divulgação e a exploração ativa.

Como previsto no primeiro semestre de 2025, os atacantes priorizaram vulnerabilidades em tecnologias corporativas amplamente adotadas, incluindo plataformas Microsoft, infraestruturas de virtualização, *softwares* de uso em massa e componentes web modernos.

A exploração observada em S2 não se deveu apenas a dinâmicas oportunistas, mas também foi recorrentemente integrada em campanhas estruturadas, tanto em operações de ciberespionagem quanto em atividades motivadas economicamente.

A análise mensal do período também confirma outra das previsões para o primeiro semestre do ano: a exposição de serviços críticos, ambientes híbridos e aplicações acessíveis pela Internet continua a amplificar o impacto dessas vulnerabilidades.

Fraquezas persistentes no gerenciamento de patches e a falta de priorização baseada na exploração real continuam sendo fatores-chave, reforçando a necessidade de abordagens proativas e contínuas de gestão de vulnerabilidades para reduzir o risco operacional em ambientes do mundo real.

10. Perspectivas futuras

O que nos espera em 2026?

Olhando para 2026, o cenário das ameaças cibernéticas aponta para uma consolidação e aprofundamento das dinâmicas observadas durante 2025, em vez de uma disrupção radical do modelo de ataque. O cibercrime continuará a evoluir para estruturas altamente especializadas e persistentes, voltadas para maximizar o impacto operacional e reputacional, apoiadas por uma economia subterrânea cada vez mais fragmentada, porém resiliente.

A profissionalização progressiva do *ransomware*, combinada com a reutilização de infraestruturas, afiliados e ferramentas de grupos desmontados ou enfraquecidos, favorecerá um ecossistema mais distribuído, menos dependente de marcas específicas. Paralelamente, atores estatais e grupos ideologicamente alinhados continuarão a borrar a linha entre espionagem, sabotagem e crime econômico, usando o ciberespaço como um domínio estratégico de pressão prolongada, em vez de um vetor para ataques isolados.

Durante 2026, espera-se um aumento sustentado nas campanhas baseadas em persistência silenciosa, abuso de identidades e exploração de relações de confiança, tanto humanas quanto técnicas. O uso ofensivo da inteligência artificial continuará a se expandir, não tanto por meio de técnicas disruptivas, mas como acelerador de processos existentes: Automação de reconhecimento, personalização avançada de engenharia social, geração de conteúdo sintético e otimização de seleção de alvos. Essa evolução reduzirá ainda mais as barreiras de entrada para o cibercrime e ampliará a base de atores capazes de executar ataques complexos.

Ao mesmo tempo, a crescente fragmentação geopolítica e a desglobalização digital reforçarão a regionalização das ameaças, com campanhas alinhadas a conflitos ativos, interesses estratégicos nacionais e tensões econômicas. Setores críticos, administrações públicas, infraestruturas tecnológicas e cadeias de suprimentos continuarão concentrando grande parte do risco, atuando como amplificadores do impacto sistêmico dos incidentes.

Nesse contexto, 2026 se perfila como um ano marcado por menos ataques visíveis, mas por intrusões mais prolongadas, onde o valor estará não apenas na exploração imediata, mas na capacidade dos atores de permanecer em ambientes comprometidos, influenciar decisões, condicionar operações e monetizar o acesso de forma flexível ao longo do tempo.

11. Referências

- AlienVault (2025, 26 de noviembre). *The 'Bear' attacks: what we learned about the phishing campaign targeting Russian organizations*. AlientVault. https://otx.alienvault.com/pulse/6926cae8043aabe58197d11e
- Arctic Wolf (2025). *2025 Arctic Wolf Threat Report*. Arctic Wolf. https://arcticwolf.com/resource/aw/arctic-wolf-threat-report-2025?lb-mode=overlay
- Aznar Fernández-Montesinos, F. (2025). *El gran reto geopolítico del siglo XXI: La multipolaridad desequilibrada (Documento de Análisis IEEE 06/2025)*. Instituto Español de Estudios Estratégicos – Ministerio de Defensa de España. https://www.ieee.es/Galerias/fichero/docs_analisis/2025/DIEEEA06_2025_FAFM_Multipolaridad.pdf
- Check Point Research (2025). *Threat Intelligence Reports*. Check Point. https://research.checkpoint.com/intelligence-reports/
- Check Point Research (2025, 14 de enero). *5 KEY CYBER SECURITY TRENDS FOR 2025*. Check Point. https://blog.checkpoint.com/research/5-key-cyber-security-trends-for-2025
- CrowdStrike (2025). *CrowdStrike 2025 Threat Hunting Report*. CrowdStrike. https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/
- DarkFeed (2025). *RANSOMWARE GROUPS: 2025 ACTIVITY*. [Publicaciones de X]. X. https://x.com/ido_cohen2/
- De Jong, L. (2025, 22 de noviembre). *Kimsuky and Lazarus join forces in coordinated attacks*. CYBERWARZONE. https://cyberwarzone.com/2025/11/22/kimsuky-and-lazarus-join-forces-in-coordinated-attacks/
- ESET (2025, 2 de septiembre). *ESET descubre el primer ransomware basado en IA*. ESET. https://www.eset.com/pa/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/eset-descubre-el-primer-ransomware-basado-en-ia/
- ESET Research (2025, 6 de noviembre). *ESET APT ACTIVITY REPORT Q2 2025–Q3 2025*. ESET. https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2025-q3-2025.pdf
- ESET Research (2025, 16 de diciembre). *ESET Threat Report H2 2025*. ESET. https://web-assets.eset.com/fileadmin/ESET/IT_2/Agenzia_Davide/H2-2025_Threat-Report.pdf
- EUROPOL (2025, 16 de julio). *Global operation targets NoName057(16) pro-Russian cybercrime network*. EUROPOL. https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network
- FALCONFEEDS.IO (2025). *ALERT: NEW HACKTIVIST ALLIANCE*. [Publicaciones de X]. X. https://x.com/FalconFeedsio
- Financial Crimes Enforcement Network [FinCEN] (2025, 4 de diciembre). FinCEN Issues Financial Trend Analysis on Ransomware. FinCEN. https://www.fincen.gov/news/news-releases/fincen-issues-financial-trend-analysis-ransomware
- Garaschenko, V. (2025, 14 de noviembre). *AI Malware and LLM Abuse: The Next Wave of Cyber Threats*. SOC Prime. https://socprime.com/blog/latest-threats/ai-malware-and-llm-abuse/

- Girnus, P. (2025, 18 de marzo). *(0Day) Microsoft Windows LNK File UI Misrepresentation Remote Code Execution Vulnerability*. Trend Micro Zero Day Initiative. https://www.zerodayinitiative.com/advisories/ZDI-CAN-25373/
- Hernández, A. (2025, 20 de noviembre). *Internet en la agenda de seguridad nacional rusa: RuNet y la soberanía digital*. UCM. https://doi.org/10.5209/geop.95098
- IBM Security (2025). *IBM X-Force 2025 Threat Intelligence Index*. IBM. https://www.ibm.com/reports/threat-intelligence
- Khalil, M. (2025, 29 de noviembre). *Cybersecurity Statistics 2025: Breach Costs, Ransomware & AI Threats*. DeepStrike. https://deepstrike.io/blog/cybersecurity-statistics-2025-threats-trends-challenges
- Lakshmanan, R. (2025, 4 de noviembre). *A CYBERCRIME MERGER LIKE NO OTHER — SCATTERED SPIDER, LAPSUS$, AND SHINYHUNTERS JOIN FORCES*. The Hacker News. https://thehackernews.com/2025/11/a-cybercrime-merger-like-no-other.html
- Lakshmanan, R. (2025, 24 de noviembre). *ShadowPad Malware Actively Exploits WSUS Vulnerability for Full System Access*. The Hacker News. https://thehackernews.com/2025/11/shadowpad-malware-actively-exploits.html
- Macías, E. (2025, 15 de octubre). *Mango sufre un ciberataque a través de su cadena de suministro*. COMPUTERWORLD. https://www.computerworld.es/article/4072830/mango-sufre-un-ciberataque-a-traves-de-su-cadena-de-suministro.html
- MITRE (2025, 15 de octubre). *SharePoint ToolShell Exploitation*. MITRE. https://attack.mitre.org/campaigns/C0058/
- NSFOCUS (2025, 25 de agosto). *NSFOCUS MONTHLY APT INSIGHTS – JULY 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-july-2025/
- NSFOCUS (2025, 18 de septiembre). *NSFOCUS MONTHLY APT INSIGHTS – AUGUST 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-august-2025/
- NSFOCUS (2025, 12 de noviembre). *NSFOCUS MONTHLY APT INSIGHTS – SEPTEMBER 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-september-2025/
- NSFOCUS (2025, 28 de noviembre). *NSFOCUS MONTHLY APT INSIGHTS – OCTOBER 2025*. NSFOCUS. https://nsfocusglobal.com/nsfocus-monthly-apt-insights-october-2025/
- Pico, R. (2025, 28 de Agosto). Elche es el último ayuntamiento bloqueado por un ataque informático. COMPUTERWORLD. https://www.computerworld.es/article/4047504/elche-es-el-ultimo-ayuntamiento-bloqueado-por-un-ataque-informatico.html
- SHENOUDA, J. (2025, 29 de octubre). *NEW THREAT ACTOR: FULCRUMSEC*. SHENOUDA.NL. https://www.shenouda.nl/new-threat-actor-fulcrumsec/
- SHENOUDA, J. (2025, 29 de noviembre). *NEW THREAT ACTOR: NETMEDVED*. SHENOUDA.NL. https://www.shenouda.nl/new-threat-actor-netmedved/

- SHENOUDA, J. (2025, 2 DE DICIEMBRE). *NEW THREAT ACTOR: ZESTIX*. SHENOUDA.NL. HTTPS://WWW.SHENOUDA.NL/NEW-THREAT-ACTOR-ZESTIX/
- SOCRADAR (2025, 1 DE OCTUBRE). *VMWARE CVE-2025-41244 EXPLOITED: WHAT YOU NEED TO KNOW ABOUT THE LATEST FLAWS*. SOCRADAR. HTTPS://SOCRADAR.IO/BLOG/VMWARE-CVE-2025-41244-EXPLOITED/
- SOCRADAR EXTENDED THREAT INTELLIGENCE (2025, OCTUBRE). *VMWARE CVE-2025-41244 EXPLOITED BY UNC5174 APT GROUP*. LINKEDIN. HTTPS://WWW.LINKEDIN.COM/POSTS/SOCRADAR_VMWARE-CVE-2025-41244-EXPLOITED-WHAT-YOU-ACTIVITY-7379088943851536385-ZS75/
- STAMFORD, C. (2025, 29 DE JULIO). *GARTNER FORECASTS WORLDWIDE END-USER SPENDING ON INFORMATION SECURITY TO TOTAL $213 BILLION IN 2025*. GARTNER. HTTPS://WWW.GARTNER.COM/EN/NEWSROOM/PRESS-RELEASES/2025-07-29-GARTNER-FORECASTS-WORLDWIDE-END-USER-SPENDING-ON-INFORMATION-SECURITY-TO-TOTAL-213-BILLION-US-DOLLARS-IN-2025
- STROBES (2025, AGOSTO). *CVE-2025-8088*. HTTPS://VI.STROBES.CO/CVE/CVE-2025-8088
- VALDEOLMILLOS, C. (2025, 20 DE OCTUBRE). *ESPAÑA ES EL QUINTO PAÍS QUE MÁS CIBERATAQUES HA SUFRIDO EN LA PRIMERA MITAD DE 2025, SEGÚN MICROSOFT*. MCPRO. HTTPS://WWW.MUYCOMPUTERPRO.COM/2025/10/20/ESPANA-QUINTO-PAIS-CIBERATAQUES-PRIMERA-MITAD-2025-MICROSOFT
- WORLD ECONOMIC FORUM. (2025, 13 DE ENERO). *GLOBAL CYBERSECURITY OUTLOOK 2025*. WORLD ECONOMIC FORUM. HTTPS://WWW.WEFORUM.ORG/REPORTS/GLOBAL-CYBERSECURITY-OUTLOOK-2025
- WESTMAN, R. Y SOPHOS COUNTER THREAT UNIT RESEARCH TEAM (2025, 11 DE DICIEMBRE). *REACT2SHELL FLAW (CVE-2025-55182) EXPLOITED FOR REMOTE CODE EXECUTION*. SOPHOS. HTTPS://WWW.SOPHOS.COM/EN-US/BLOG/REACT2SHELL-FLAW-CVE-2025-55182-EXPLOITED-FOR-REMOTE-CODE-EXECUTION
- WRIGHT, R. (2025, 31 DE MARZO). CISA WARNS NEW MALWARE TARGETING IVANTI ZERO-DAY VULNERABILITY. CYBERSECURITY DIVE. HTTPS://WWW.CYBERSECURITYDIVE.COM/NEWS/CISA-WARNS-MALWARE-TARGETING-IVANTI-ZERO-DAY/743967/


NTT DATA