Tendências de CTI

Inteligência contra ameaças cibernéticas

1º semestre de 2025

Índice

Índice

Introdução

1.1. Escopo do relatório

Este relatório apresenta uma visão geral detalhada das tendências e dos desenvolvimentos mais relevantes no campo da inteligência contra ameaças cibernéticas (em inglês: Cyber Threat Intelligence - CTI) durante o primeiro semestre de 2025. O relatório analisa as ameaças emergentes que estão redefinindo o cenário da cibersegurança, os agentes com maior atividade, as campanhas cibernéticas de maior relevância e as vulnerabilidades críticas detectadas nesse período. Além disso, são identificados padrões recorrentes e projetados possíveis cenários futuros que podem influenciar as estratégias de gestão e mitigação de riscos.

1.2. Escopo geográfico e período de cobertura do relatório

A análise apresentada adota uma perspectiva global, permitindo compreender 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.

Trata-se de um cenário marcado por mudanças relevantes no comportamento das ameaças e por eventos que tiveram impacto significativo no ecossistema digital. Esse intervalo de tempo é fundamental para antecipar possíveis movimentos futuros e fortalecer as capacidades de resposta diante de um contexto cada vez mais complexo.

Panorama global de ameaças

2. Panorama global de ameaças

Em 2025, o mundo enfrenta um ambiente de riscos cada vez mais complexo e interconectado, em que ameaças físicas e digitais não apenas coexistem, mas se reforçam mutuamente, ampliando seu impacto. Os conflitos armados, os fenômenos meteorológicos extremos e os ciberataques a infraestruturas críticas estão entre os cinco riscos mais críticos do ano (World Economic Forum, 2025), criando um cenário cada vez mais incerto.

Essa combinação de ameaças reflete uma tendência clara: os riscos não se manifestam mais de forma isolada, mas de forma interligada, em um contexto de crescente fragmentação geopolítica, polarização social e aceleração tecnológica. Nesse cenário, a colaboração internacional e a resiliência organizacional tornaram-se pilares fundamentais para enfrentar um panorama de ameaças que evolui rapidamente e exige respostas coordenadas, adaptativas e baseadas em inteligência contra ameaças.

2.1 Geopolítica e cibersegurança

No cenário atual, os riscos geopolíticos e tecnológicos destacam-se como os fatores de maior preocupação no curto prazo. De um lado, a digitalização massiva, somada à expansão da IA, ampliou a superfície de ataque e facilitou o surgimento de novas formas de crime cibernético, espionagem e desinformação. Por outro lado, o aumento das tensões geopolíticas, impulsionado pela desglobalização crescente, obriga Estados e organizações a operarem em um ambiente cada vez mais hostil, caracterizado por ataques descentralizados e pela dificuldade em impor normas regulatórias ou diretrizes eficazes para conter essas ameaças, o que torna as estratégias de cibersegurança ainda mais complexas.

Entre janeiro e junho de 2025, foram observadas as seguintes tendências que intensificam a relação entre cibersegurança e o cenário geopolítico global (Group-IB, 2025; CrowdStrike, 2025):

- **Ascensão dos agentes estatais e da ciberespionagem geopolítica**

Observou-se um aumento da atividade atribuída a agentes patrocinados por Estados, com destaque para operações associadas à República Popular da China, que intensificou a ciberespionagem em setores estratégicos como finanças, manufatura e mídia. A **Coreia do Norte** e o **Irã** também intensificaram suas operações, combinando espionagem, geração de receitas ilícitas e campanhas de desinformação com fins políticos. Além disso, as ameaças persistentes avançadas (em inglês: Advanced Persistent Threat - APT) tornaram-se mais especializadas e difíceis de rastrear, operando com maior segurança operacional (em inglês: Operational Security - OPSEC) e compartilhando ferramentas entre grupos.

- **Uso de IA Generativa em campanhas de desinformação e espionagem**

Conforme destacamos no relatório do semestre anterior, a IA Generativa estabeleceu-se como uma ferramenta fundamental para os adversários. A tecnologia permite orquestrar campanhas de engenharia social mais sofisticadas, criar perfis falsos, produzir deepfakes e disseminar desinformação eleitoral em grande escala, o que tem levado governos a estabelecer unidades especializadas de detecção (Federal Ministry of the Interior, 2025). Essa tecnologia reduziu as barreiras de entrada para agentes de ameaças, facilitando a automatização de ataques e o desenvolvimento de scripts maliciosos com maior rapidez e eficiência, principalmente para explorar vulnerabilidades e automatizar campanhas de phishing.

- **Ransomware como ferramenta de pressão geopolítica**

Tanto o modelo de Ransomware-as-a-Service (RaaS) quanto o número de ataques de ransomware divulgados em sites de vazamento continuam em crescimento. Alguns ataques tiveram impacto geopolítico direto sobre infraestruturas críticas, especialmente em redes governamentais e indústrias de manufatura, evidenciando seu potencial desestabilizador. O surgimento de novos grupos de ransomware em 2025 também revela uma tendência à profissionalização dos crimes cibernéticos, com algumas iniciativas de autopromoção que imitam estratégias de marketing empresarial.

- **Fragmentação digital e barreiras normativas**

La desglobalización digital y el aumento de tensiones políticas dificultan la cooperación internacional en materia de ciberseguridad. As barreiras jurisdicionais e a ausência de marcos regulatórios comuns dificultam a perseguição de agentes transnacionais, situação que vem sendo explorada por grupos criminosos e estatais para operar a partir de regiões com baixa cooperação legal.

Assim, a cibersegurança consolidou-se como um instrumento estratégico no contexto geopolítico global, essencial para antecipar ameaças tecnológicas que vão além do ambiente digital e se projetam sobre o mundo físico.

2.2 Geopolítica e principais agentes

A evolução do cenário de cibersegurança durante o primeiro semestre de 2025 foi profundamente influenciada pelos conflitos armados, pelas tensões diplomáticas e pelas rivalidades estratégicas entre potências. Nesse contexto, os agentes de ameaças vinculados a Estados-nação intensificaram suas operações, utilizando ferramentas digitais para espionagem, sabotagem e desinformação.

Esta seção analisa os principais focos de conflito geopolítico e os grupos cibernéticos mais ativos, destacando como suas ações impactaram a estabilidade regional e global por meio de campanhas direcionadas e persistentes.

- **Ciberguerra nas sombras: Rússia e Ucrânia no front digital**

No conflito entre Rússia e Ucrânia, as operações digitais desempenharam papel central nas **estratégias de desgaste e controle da informação**, estendendo-se também a países com interesse geopolítico, especialmente na União Europeia.

As campanhas atribuídas a agentes russos evidenciaram uma dupla dimensão: por um lado, o ciberespionagem e a desinformação como instrumentos de pressão diplomática e manipulação narrativa; por outro, as operações de interrupção e sabotagem digital direcionadas a infraestruturas críticas, especialmente contra a Ucrânia.

Essa tática híbrida combina persistência técnica com objetivos políticos, ampliando o alcance do conflito para além das fronteiras físicas. Uma análise técnica mais detalhada dessas operações, assim como dos agentes responsáveis, é apresentada na seção “6.4. APT”, dedicada a esse tipo de ameaça, onde são exploradas a evolução de campanhas específicas, as ferramentas utilizadas e seu impacto regional.

- **Oriente Médio: escalada regional e ameaças transnacionais**

Durante o primeiro semestre de 2025, o Oriente Médio experimentou uma intensificação das tensões geopolíticas, com consequências diretas no ambiente digital. Em 13 de junho, Israel lançou uma importante ofensiva aérea contra o Irã, e os ciberataques contra Israel aumentaram em 700% nos dois dias seguintes. O número de grupos iranianos ou alinhados ao Irã parece ser muito maior. Embora a cultura ativista continue forte nos países ocidentais, a cena hacktivista é amplamente dominada por agentes do hemisfério oriental, onde o Irã conta com maior apoio.

Fontes distintas identificaram 65 grupos pró-Irã, 11 anti-Irã e 6 pró-Israel, totalizando 82 grupos. Espera-se que esse número aumente com a continuidade do conflito.

Os agentes alinhados ao Irã permaneceram altamente ativos, com destaque para o grupo MuddyWater, que recorrentemente utilizou ferramentas de gerenciamento remoto (em inglês: Remote Monitoring and Management - RMM) em ataques de phishing. O grupo BladedFeline voltou a atacar uma vítima anterior, uma empresa de telecomunicações no Uzbequistão, coincidindo com o avanço diplomático do Irã. Outros grupos, como o Cyber Toufan, realizaram operações destrutivas, executando ataques de exclusão de dados contra múltiplas organizações em Israel.

- **Estados Unidos contra a China: batalha digital entre superpotências**

O conflito geopolítico entre Estados Unidos e China em 2025 transcendeu o plano diplomático e econômico para se consolidar como uma ciberguerra de alta intensidade pelo domínio tecnológico, pela soberania informacional e pelo controle do comércio e das infraestruturas críticas, resultando em uma crescente fragmentação das cadeias de suprimentos globais.

Por um lado, Volt Typhoon, um grupo APT vinculado ao governo chinês, protagonizou campanhas de espionagem cibernética em redes dos Estados Unidos e de Taiwan, especialmente nos setores de telecomunicações, energia e defesa. O grupo adota uma abordagem baseada no sigilo e na persistência, utilizando técnicas Living off the Land (LotL) para evitar a detecção. As manobras militares e os ciberataques em torno de Taiwan também se intensificaram recentemente.

Por outro lado, o Equation Group e o TAO, ambos associados à Agência de Segurança Nacional (em inglês: National Security Agency - NSA) representam a resposta cibernética dos Estados Unidos, com capacidades ofensivas altamente sofisticadas. Esses grupos foram acusados de conduzir operações de espionagem e sabotagem digital em infraestrutura estrangeira, incluindo alvos chineses.

- **Conflito na península coreana: uma guerra sem disparos**

Os agentes alinhados à Coreia do Norte estiveram particularmente ativos em campanhas com fins financeiros.

O grupo **DeceptiveDevelopment** ampliou significativamente seus alvos, utilizando falsas ofertas de emprego, principalmente nos setores de criptomoedas, blockchain e finanças. Foram aplicadas técnicas de engenharia social como ataques **ClickFix** e publicações falsas para disseminação do malware multiplataforma **WeaselStore**.

O roubo de criptomoedas da Bybit, atribuído pelo FBI ao grupo TraderTraitor, envolveu a exploração de uma vulnerabilidade da cadeia de suprimentos da Safe, resultando em perdas de aproximadamente US$ 1,5 bilhão.

Enquanto isso, outros grupos alinhados à Coreia do Norte apresentaram oscilações em seu ritmo operacional. No início de 2025, **Kimsuky e Konni** retomaram seus níveis habituais de atividade após uma queda significativa no final de 2024, direcionando seus ataques sobretudo a entidades e diplomatas sul-coreanos.
O grupo **Andariel** ressurgiu, após um ano de inatividade, com um ataque sofisticado contra uma empresa sul-coreana de software industrial.

- **Outros focos na região do Indo-Pacífico**

A situação atual em Mianmar favoreceu um ambiente onde a **ciberespionagem interna e a repressão digital** promovida pelo regime militar convergem com operações criminosas transnacionais de fraude **cibernética em larga escala.** Com o uso de deepfakes, IA Generativa (GenAI) e tecnologias blockchain, golpes como o pig butchering, as apostas ilegais e as fraudes com criptomoedas alcançaram novos níveis de anonimato, eficiência e sofisticação operacional para os grupos criminosos.

Paralelamente, em 22 de abril, a tensão entre Índia e Paquistão se intensificou após um ataque terrorista na região de Jammu e Caxemira, que aumentou a tensão política entre os dois países, provocando uma série de confrontos militares até o cessar-fogo mediado pelos Estados Unidos em 10 de maio. Esses eventos resultaram em uma intensa campanha de desinformação nas redes sociais e na mídia digital, marcada por **vídeos manipulados, narrativas fabricadas e pela propagação de conteúdos polarizadores** utilizando redes de contas falsas. Além disso, os serviços governamentais da Índia sofreram diversos ciberataques atribuídos a grupos como **AnonSec, Sylhet Gang (SG) e DieNet**, parte de uma guerra de informação que mobiliza agentes estatais e não estatais em meio a um conflito cibernético cada vez mais intenso.

O ano de 2025 marca a consolidação da ciberespionagem como elemento-chave na competição geopolítica global. O spear phishing permanece como a técnica preferida das APTs em várias regiões, enquanto as operações disruptivas — especialmente oriundas do Oriente Médio — e as campanhas de desinformação ganham importância crescente, definindo o rumo do conflito digital contemporâneo.

2.3 Impacto dos ciberataques em setores específicos

Para encerrar a seção sobre ameaças globais, o **Departamento de Cyber Threat Intelligence da NTT DATA** considera relevante apresentar a evolução dos ciberataques nos setores e países mais afetados no primeiro semestre de 2025, com pequenas variações estruturais em relação à disposição do segundo semestre de 2024.

A distribuição dos ataques reflete novamente a forte influência das tensões geopolíticas, com foco principal em setores estratégicos e países de grande relevância econômica ou envolvidos em conflitos. O impacto desses ataques apresentou variações, ainda que as diferenças entre setores tenham diminuído de forma significativa. Em comparação com o segundo semestre de 2024, a variabilidade do grau de impacto setorial diminuiu cerca de 8%.

- **Administração pública e governos**

Este setor continua liderando em número de ciberataques no primeiro semestre de 2025, com **3.005 incidentes direcionados** a administrações públicas e **779 ao governo e ao setor público**, somando 3.784 ataques — **um crescimento de 41,30%** em comparação ao relatório anterior. As tensões constantes entre nações continuam motivando novas ameaças contra essas entidades, visando à obtenção de informações sensíveis com potencial de gerar vantagens estratégicas ou realizar ações de hacktivismo.

- **Educação:**

O número de ciberataques registrados contra instituições educacionais **reduziu cerca de 23%** em relação ao ano anterior, totalizando **1.110 ataques**. Mesmo com a redução no número de ataques neste setor, as instituições de ensino — especialmente as universidades — continuam sendo alvos estratégicos devido à propriedade intelectual, aos dados pessoais e às suas vulnerabilidades operacionais.

- **Serviços financeiros:**

O setor financeiro apresentou um crescimento de **26,9% no número de ciberataques em comparação a 2024, totalizando 835 incidentes** e permanecendo entre os três setores mais atacados. Observa-se uma tendência de redistribuição dos ataques em função do contexto geopolítico, com os agentes de ameaça priorizando alvos governamentais e, em seguida, ampliando o foco para objetivos financeiros.

- **Tecnologia da informação e telecomunicações:**

Com 739 e 652 ciberataques registrados, respectivamente, os recursos tecnológicos permanecem como um dos principais focos de exploração cibernética. Entre os tipos de ataque mais recorrentes destacam-se o roubo de dados e o comprometimento de sistemas, com finalidades que variam de ganhos financeiros à interrupção de serviços e operações ou, em casos isolados, à geração de danos físicos.

O ransomware continua sendo o principal vetor de ataque. Embora a tendência tenha diminuído no último trimestre (abril a junho de 2025), os maiores picos de atividade foram registrados entre janeiro e fevereiro. Nos últimos três meses, os setores mais impactados foram o da construção civil e o industrial, que juntos concentram 12% do total de ataques. Geograficamente, os países mais atingidos foram os Estados Unidos (664), o Canadá (77) e a Alemanha (69).

Esse vetor de ataque é detalhado na seção “6.2. Grupos de ransomware”.

Setores mais afetados por ciberataques: comparação entre S2 2024 e S1 2025

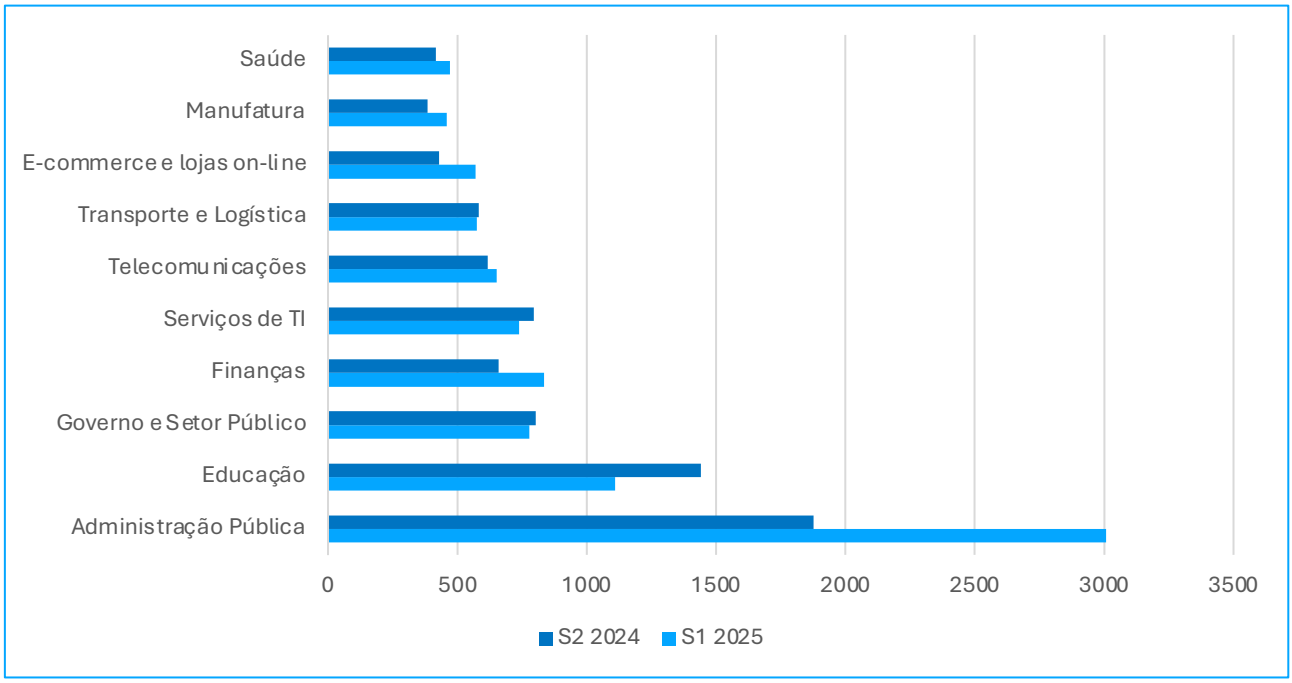


Figura 1 | Setores mais afetados por ciberataques no primeiro semestre de 2025.

Além disso, a distribuição temporal dos ciberataques registrados apresentou um aumento contante durante o último trimestre de 2024, mantendo-se relativamente estável ao longo do primeiro trimestre de 2025 e caindo quase pela metade em abril deste ano. A tendência segue estável desde maio, porém projeta-se um novo aumento dos valores ao longo do ano.

Distribuição temporal dos ciberataques

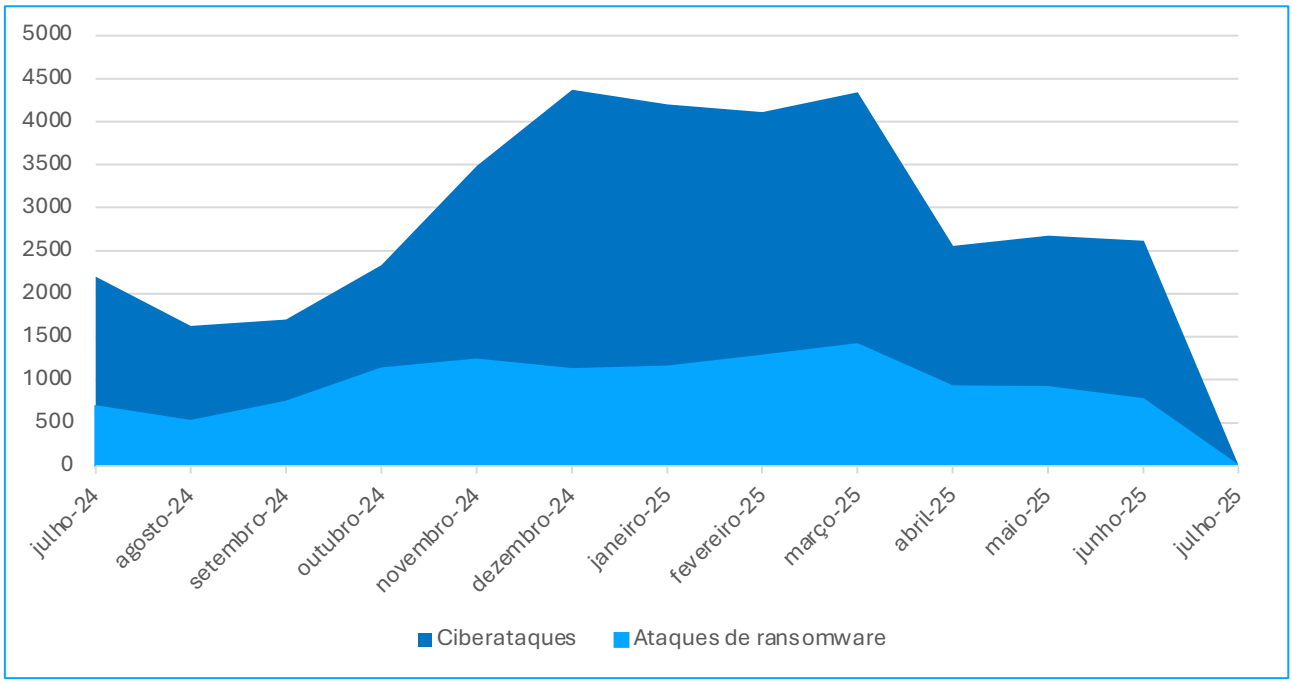


Figura 2 | Distribuição temporal dos ciberataques registrados de S2 2024 a 2025.

Com relação à distribuição do impacto, observa-se não apenas uma variação significativa entre setores, mas também uma tendência relevante em determinados países que sofreram volumes mais altos de ciberataques neste primeiro semestre do ano:

- **Estados Unidos:** Com **4.046 ataques**, lidera a lista dos países mais afetados, refletindo sua relevância estratégica e econômica. **Houve um aumento de 35,6% em relação a 2024.**
- **Índia:** Envolvida em conflitos armados e, recentemente, alvo de diversos agentes de ameaça, registrou **1.644 ataques**, uma queda de quase 21% em comparação com o semestre anterior.
- **Israel:**A guerra com a Palestina levou o país a enfrentar a oposição de várias potências e, com 1.637 ciberataques registrados em 2025, Israel ocupa a terceira posição entre os países mais afetados do mundo.
- **França: Com 921 ataques (4% da distribuição global)**, o país intensifica sua preparação para a ciberguerra realizando exercícios de defesa baseados em simulações de ataques reais inspirados no conflito Rússia-Ucrânia.
- **Ucrânia:** Registrando **768 ataques**, o país continua enfrentando ameaças associadas aos conflitos regionais, como espionagem cibernética e sabotagem de infraestruturas críticas. No entanto, as estratégias de defesa e contra-ataque parecem estar surtindo efeito, pois o número atual de ataques registra uma **queda de 36% em relação ao semestre anterior**.

Distribuição de ciberataques por país de janeiro a junho de 2025

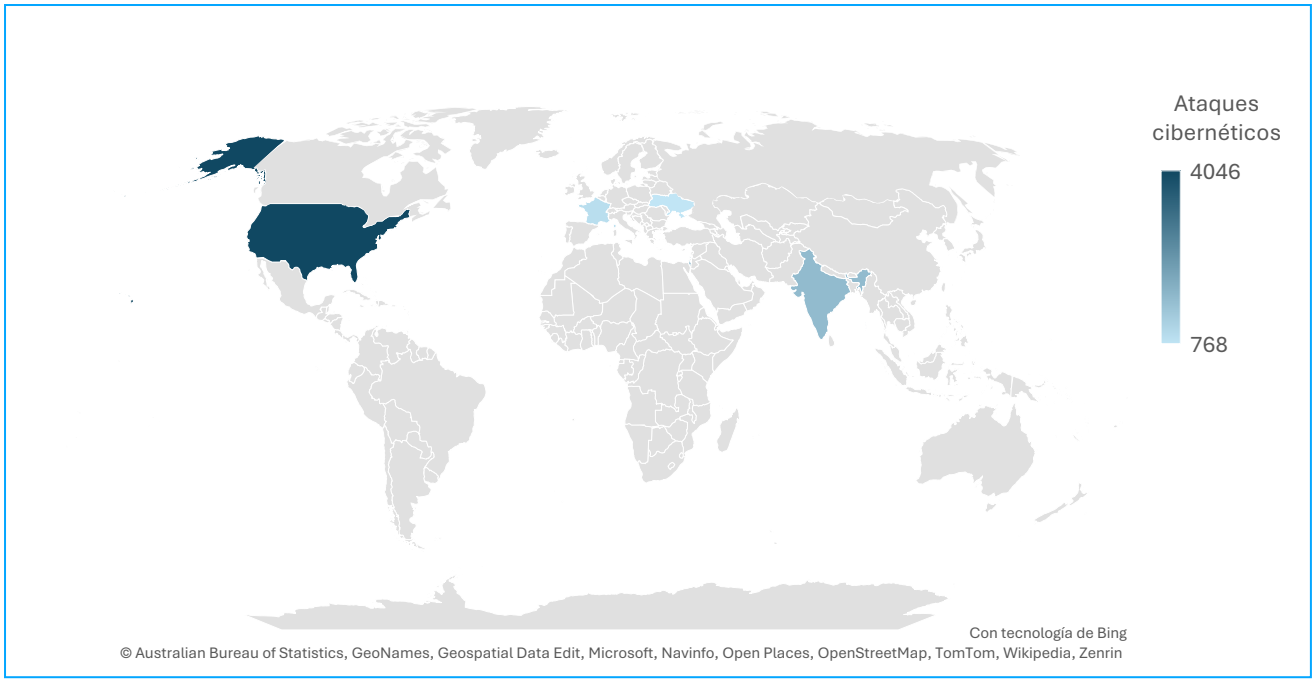


Figura 3 | Distribuição geográfica do impacto dos ciberataques no primeiro semestre de 2025.

A distribuição geográfica dos ciberataques evidencia os Estados Unidos como principal alvo, resultado do conflito com a China em meio à guerra comercial, tecnológica e territorial, e da rivalidade histórica com a Rússia, conhecida por abrigar grupos APT altamente sofisticados. Da mesma forma, as demais potências afetadas continuarão sob ameaça enquanto os conflitos atuais persistirem, já que a distribuição geográfica dos ataques está diretamente ligada à expansão do cenário geopolítico para o ciberespaço.

Principais ameaças globais

3. Principais ameaças globais

O primeiro semestre de 2025 registrou um cenário de ciberameaças em evolução contínua, definido por um nível avançado de sofisticação e pela intensificação da exploração de vulnerabilidades críticas. Embora muitas das táticas observadas em 2024 ainda estejam em uso, observa-se uma especialização cada vez maior por parte dos agentes de ameaças.

Os ciberincidentes com impacto global, o surgimento de novas técnicas de acesso e persistência e a profissionalização de modelos como o RaaS refletem uma ameaça que não apenas persiste, mas também se adapta rapidamente. Ao mesmo tempo, o mercado underground continua operando, embora com menos exposição pública, resultado da migração para canais mais restritos e menos visíveis.

3.1 Grandes ciberincidentes e campanhas

Nos primeiros seis meses de 2025, o mundo presenciou uma série de ciberincidentes em larga escala que comprometeram infraestruturas críticas, serviços essenciais e a privacidade de milhões de pessoas. Esses eventos não apenas expuseram vulnerabilidades técnicas, como também evidenciaram deficiências na gestão de riscos, na resposta a incidentes e na preparação frente a ameaças complexas.

O **Departamento de Cyber Threat Intelligence da NTT DATA** documentou alguns dos ciberincidentes mais relevantes do primeiro semestre de 2025, selecionados por seu valor representativo das principais ameaças observadas nesse período. A lista inclui casos confirmados de ransomware, violação de dados, campanhas de phishing, ataques DDoS, malware e ataques cibernéticos destrutivos, demonstrando a variedade dos setores impactados e o avanço das táticas adotadas pelos agentes de ameaças.

Vítimas	Tecnologia/Setor	Autor do ataque	País afetado	País do autor do ataque	Data do incidente	URL
United Health	Saúde/Dados pessoais	Desconhecido	EUA	Desconhecido	01/01/2025	Fonte
Plataforma e-commerce	Infraestrutura Web	Desconhecido	Japão	Desconhecido	01/01/2025	Fonte
Cloudflare	Rede/Infraestrutura	Desconhecido	Global	Desconhecido	02/02/2025	Fonte
Insight Partners	Serviços financeiros	Desconhecido	EUA	Desconhecido	19/02/2025	Fonte
Marks & spencer	Varejo	Scattered Spider	Reino Unido	Desconhecido	27/04/2025	Fonte
Synnovis	Saúde pública	Qilin	Reino Unido	Desconhecido	20/05/2025	Fonte
Condado de Cobb	Governo local	Qilin	EUA	Desconhecido	20/05/2025	Fonte
Várias plataformas	Serviços on-line/senhas	Malware/Infostealer	Global	Desconhecido	28/05/2025	Fonte
GLS (Phishing)	Logística	Desconhecido	Espanha	Desconhecido	31/05/2025	Fonte
Victoria's Secret	Varejo/E-commerce	Desconhecido	EUA	Desconhecido	02/06/2025	Fonte
Coinbase	Tecnologia/BPO	Insider/Ameaça interna	Índia	Desconhecido	02/06/2025	Fonte
Telefónica	Telecomunicações	Dedale	Peru	Desconhecido	03/06/2025	Fonte
SVT/Bank-ID	Televisão/Sistemas de identificação	Desconhecido	Suécia	Desconhecido	11/06/2025	Fonte

Tabela 1 | Principais ciberincidentes de segurança no primeiro semestre de 2025.

3.2 Tendências emergentes de ataques

No primeiro semestre de 2025, o cenário de ameaças cibernéticas se intensificou de forma significativa, com avanços rápidos na sofisticação e frequência dos ataques. A maturidade operacional dos grupos de ransomware, o avanço da IA ofensiva, a industrialização dos acessos iniciais e a exploração coordenada de vulnerabilidades impulsionaram a criação de um ecossistema mais ágil, furtivo e imprevisível.

Nesse contexto, destacam-se as seguintes tendências técnicas e operacionais que marcaram a atividade no ciberespaço ao longo deste primeiro semestre:

3.2.1 Uso massivo de brokers de acesso e IA ofensiva

Os Initial Access Brokers (IABs) consolidaram seu papel como facilitadores-chave para operações de ransomware e exfiltração de dados. Seus catálogos cresceram 15%, com destaque para acessos a tecnologias como Ivanti Connect Secure, Fortinet FortiOS e equipamentos da Palo Alto (Group-IB, 2025).

Esses acessos são vendidos por valores que variam de US$ 300 a US$ 5.000. Paralelamente, ferramentas de IA estão sendo utilizadas para o reconhecimento automatizado de superfícies de ataque expostas, fornecendo a corretores e APTs informações atualizadas sobre ativos vulneráveis.

3.2.2 Profissionalização do ransomware: alianças, reagrupamentos e especializações

O modelo RaaS atingiu um nível inédito de maturidade operacional. Grupos como Cl0p, Akira, Qilin e RansomHub lideraram a maioria das campanhas, somando mais de 1.200 ataques no semestre. Destaca-se a prática recorrente por parte dos criminosos ao utilizar ferramentas legítimas previamente à etapa de criptografia — técnica conhecida como Living off the Land (LotL) — em que se prioriza-se o uso de softwares já instalados no ambiente da vítima para garantir persistência e dificultar a detecção por soluções de antivírus convencionais.

Além disso, observa-se um fenômeno inédito no ecossistema de ransomwares: a incorporação de afiliados e o reaproveitamento de infraestruturas por grupos emergentes, que utilizam componentes técnicos e operacionais remanescentes de grupos dissolvidos como LockBit ou Alphv.

Esse reaproveitamento é possível graças a informações estratégicas coletadas em fóruns e canais do Telegram comprometidos, onde são expostos dados operacionais de grupos dissolvidos.

Paralelamente, consolidam-se colaborações entre grupos de especialidades distintas, inclusive procedentes de regiões geopoliticamente opostas. Esses acordos possibilitam a divisão de lucros, a terceirização de etapas dos ataques e a otimização de recursos, funcionando de maneira semelhante a estruturas empresariais.

Registram-se também casos de confrontos entre grupos, como o encerramento das operações do Black Basta em abril de 2025 após vazamentos internos, enquanto em plataformas como o X foram identificadas disputas públicas entre agentes maliciosos pela apropriação de vítimas de vazamentos de informações, demonstrando um ecossistema cada vez mais competitivo e fragmentado (Group-IB, 2025).

3.2.3 Automação de fraude com IA: falsificações e ataques direcionados

No primeiro semestre de 2025, consolidou-se o uso da IA em campanhas de fraude, falsificação e engenharia social, impulsionando ataques mais personalizados, convincentes e automatizados. A IA vem sendo empregada na criação de identidades falsas, vozes sintéticas e e-mails de spear phishing baseados em dados vazados ou perfis públicos, além de automatizar etapas completas de ataques contra os setores financeiro e governamental (Hitachi Cyber, 2025; KrakenLabs, 2025).

Paralelamente, observa-se o surgimento de um ecossistema de ferramentas ofensivas baseadas em IA que tornam o cibercrime mais acessível e menos complexo. Entre essas ferramentas destacam-se: geradores de texto como FraudGPT e WormGPT (para criação de comunicações fraudulentas); ferramentas de clonagem de voz (ElevenLabs, Voicemy.ai) e vídeo (DeepFaceLab, Faceswap) usadas para burlar verificações de identidade; kits como EvilProxy e Robin Banks, que automatizam páginas de phishing com recursos Adversary-in-the-Middle (AiTM) para roubo de credenciais com MFA. Além disso, identificou-se o uso de bots sociais com IA no Telegram e em outras plataformas, projetados para simular interações de suporte técnico e capturar informações sensíveis.

Essas capacidades estão reduzindo drasticamente a barreira técnica de entrada no cibercrime, permitindo que agentes sem experiência executem campanhas sofisticadas e direcionadas — agravando o risco para empresas e governos.

3.2.4 Malware as a Service: ascensão de infostealers como Lumma e RedLine

O mercado Malware-as-a-Service (MaaS) teve como principais protagonistas o Lumma Stealer e o RedLine, com registros de mais de 3 milhões de credenciais roubadas por dia (MTI, MDC & MSE, 2025). O Lumma tem sido vinculado a diversas campanhas de roubo massivo de dados, incluindo cookies de sessão, carteiras digitais (e-wallets), senhas armazenadas em navegadores e configurações de VPN.

Mesmo após a infraestrutura ter sido desativada em maio pela Europol e pela Microsoft, ocorreu um ressurgimento quase imediato mediante forks e rebranding de seu C2. Além disso, os cibercriminosos passaram a distribuir o malware por canais privados como Discord e Telegram, dificultando sua detecção e rastreamento.

3.2.5 Seleção de alvos e exploração setorial

Os agentes de ameaças estão refinando suas campanhas conforme o setor-alvo. Indústrias como a financeira, educacional e administração pública concentraram a maioria dos ataques devido ao baixo nível de segurança, alta dependência digital e potencial impacto reputacional (CERT-EU, 2025). Essa segmentação não apenas melhora as taxas de sucesso, mas também permite maximizar a pressão extorsiva ao adaptar a linguagem, os documentos roubados e as técnicas de comunicação.

3.3 Estatísticas globais sobre incidentes de segurança, tipos de ataques e agentes de ameaça envolvidos

O Departamento de Cyber Threat Intelligence da NTT DATA identificou que, durante o primeiro semestre de 2025, os ciberataques não apenas mantiveram um ritmo consistente, mas também evoluíram em termos de foco, complexidade técnica e segmentação setorial.

A seguir, são apresentadas as principais estatísticas e tendências observadas nesse período:

- **Ransomware:** Continua sendo a principal ameaça global. O número de ataques **aumentou cerca de 32% em relação ao semestre anterior.** Mais de 1.200 incidentes foram atribuídos a grupos como Akira, Cl0p e RansomHub, com destaque para a segmentação por setor e o uso sistemático de técnicas de dupla extorsão e ferramentas legítimas antes do processo de criptografia (CrowdStrike, 2025; KrakenLabs, 2025).
- **Phishing e vishing:** Observou-se um crescimento significativo do vishing assistido por IA, com aumento dos ataques desde o final de 2024. As campanhas tornaram-se mais realistas ao utilizar tecnologias de clonagem de voz e perfis sintéticos para realizar fraudes direcionadas, especialmente em ambientes financeiros e de recursos humanos (Group-IB, 2025; Hitachi Cyber, 2025).
- **Violações de dados:** Mais de 1.000 incidentes relevantes foram registrados no período, muitos com impacto em organizações dos setores financeiro, varejista e administração pública. Mantém-se a tendência de crescimento registrada em 2024, com agentes de ameaças empregando ferramentas mais avançadas para a exfiltração e monetização de dados (World Economic Forum, 2025; CyberArk, 2025).
- **Ataques DDoS:** Embora o volume global tenha apresentado uma ligeira queda, os ataques tornaram-se mais sofisticados e passaram a ser combinados com táticas de extorsão. As campanhas direcionadas contra infraestruturas críticas e plataformas de pagamento consolidaram-se como uma ferramenta recorrente de pressão (CERT-EU, 2025).
- **Ataques impulsionados por IA:** O uso ofensivo de inteligência artificial consolidou-se como uma tática transversal. Aplica-se a múltiplas fases do ataque — da automação do reconhecimento à geração de e-mails maliciosos ou identidades falsas. Como resultado, campanhas de phishing, falsificação e ataques multivetoriais tornaram-se mais sofisticados, convincentes e executados em maior escala (KrakenLabs, 2025; CrowdStrike, 2025).

Aumento percentual estimado de ataques por categoria (S1 2025)

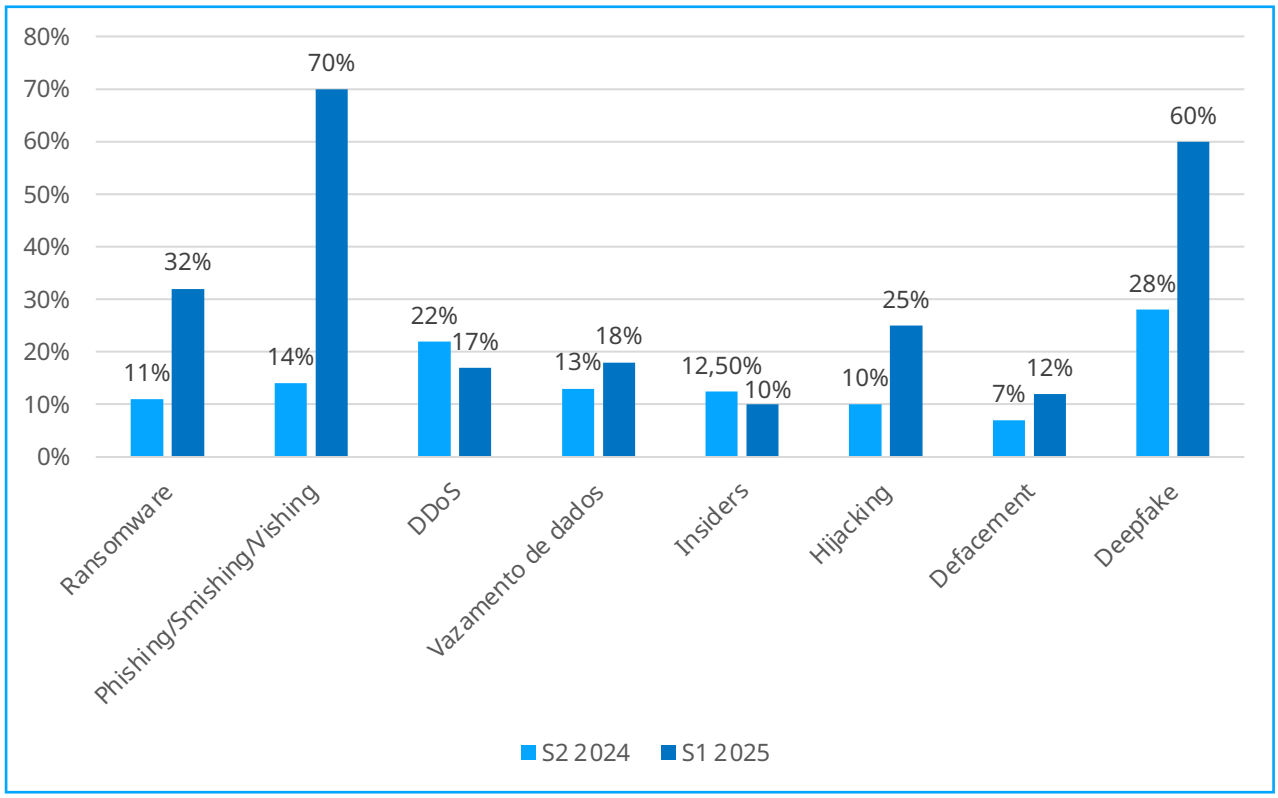


Figura 4 | Percentual do número de ataques por categoria em comparação com o segundo semestre de 2024.

Embora categorias como phishing, smishing e deepfakes apresentem um aumento percentual maior em relação ao semestre anterior, isso não significa que tenham superado, em volume absoluto, ameaças consolidadas como o ransomware.

Esses dados evidenciam a rápida transformação do cenário de ameaças, com o crescimento acelerado de técnicas emergentes. Apesar disso, **o ransomware segue na liderança em termos de impacto operacional, alcance global e rentabilidade para os cibercriminosos**.

3.4 Custos dos ciberataques para as empresas

Durante o primeiro semestre de 2025, os custos decorrentes dos ciberataques mantiveram uma trajetória crescente, impulsionados tanto pela frequência e sofisticação dos incidentes quanto pelo impacto direto nas operações das empresas. As estimativas mais recentes indicam que o **custo global do cibercrime atingiu o valor recorde de US$ 10,5 trilhões por ano**, com uma projeção de crescimento contínuo que **pode chegar a valores entre US$ 12 e US$ 15 trilhões até o final do ano**, caso os níveis atuais de atividade maliciosa se mantenham (Cybersecurity Ventures, 2025).

As despesas mais relevantes para as organizações durante este semestre foram:

- **Interrupções de negócio:** Lideram o impacto econômico, com **média estimada de US$ 13,2 trilhões**, devido à interrupção de cadeias de suprimentos, plataformas de pagamento e serviços críticos.
- **Custos de"reforço em cibersegurança":** Incluem investimentos em detecção, resposta e capacitação, totalizando **US$ 10,8 trilhões**, impulsionados pela adoção acelerada de tecnologias baseadas em IA e ambientes multicloud.
- **Pagamentos de resgate** a grupos de ransomware: Os resgastes alcançaram o valor de **US$ 6,3 trilhões**, com um aumento expressivo nas exigências superiores a US$ 5 milhões por incidente, especialmente nos setores de saúde, manufatura e transporte.

- **Sanções econômicas e legais:** Resultantes de incidentes e violações de dados, superaram **US$ 7,14 trilhões**, impulsionadas por regulamentações mais rígidas em regiões como União Europeia, Reino Unido e Ásia-Pacífico (Gov.UK, 2025; Stamford, 2024).

Em comparação com o final de 2024, verifica-se um **aumento estimado de 15% nos custos globais com cibersegurança, especialmente concentrado em setores que dependem de infraestruturas críticas ou operam com processos altamente interconectados.**

As campanhas direcionadas em datas estratégicas também contribuíram para o aumento desses custos, resultando em picos de até 40% adicionais nos custos de contenção, especialmente em empresas impactadas nos meses de dezembro e janeiro (Stamford, 2024; Tamzid, 2025).

Evolução custos estimados de cibersegurança por ano no período de 2020 a 2025

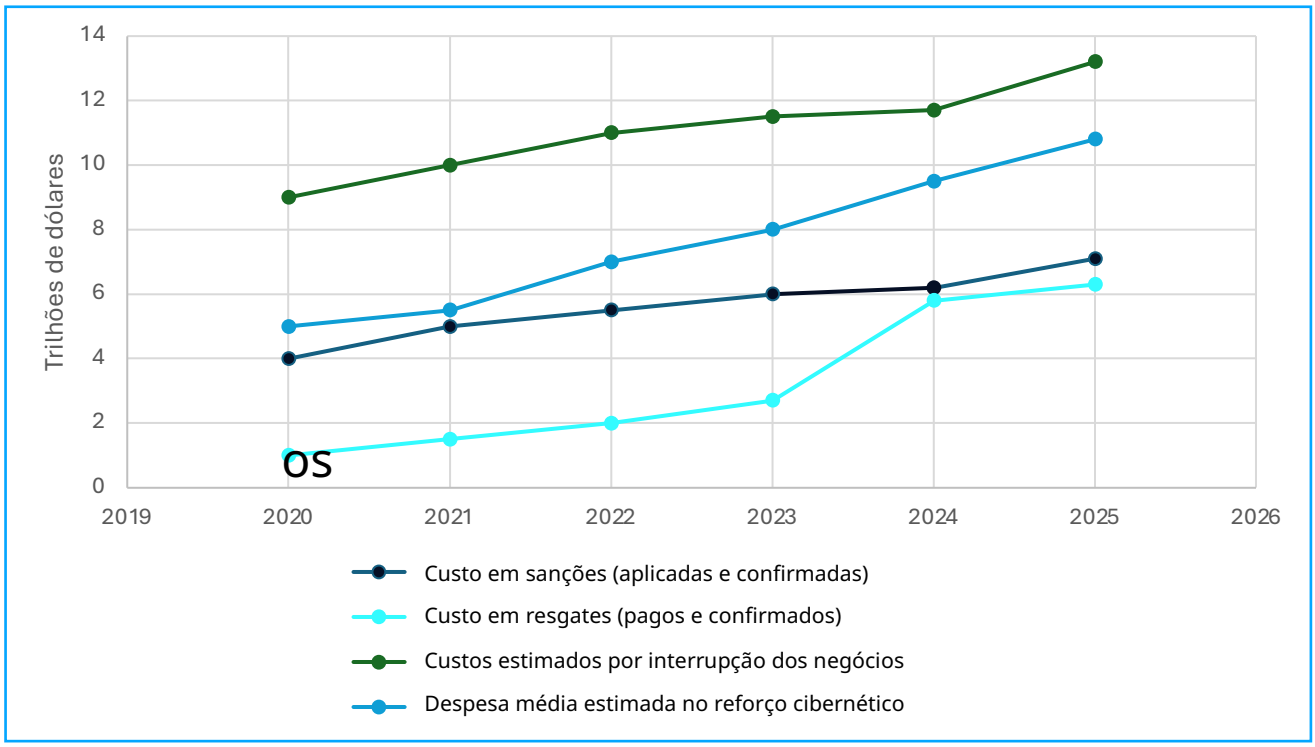


Figura 5 | Evolução anual comparativa dos custos estimados de cibersegurança (2020-2025), detalhados em sanções, resgates, interrupções de negócios e reforço cibernético.

A ilustração foi atualizada para refletir os dados consolidados do segundo semestre de 2024 e do primeiro semestre de 2025, com base em fontes oficiais e relatórios de fornecedores internacionais. No relatório anterior, as estatísticas de 2024 foram apresentadas como estimativas, uma vez que o ano estava parcialmente encerrado e as informações permaneciam sujeitas a validação. Com a publicação em 2025 de métricas padronizadas e confiáveis sobre os impactos econômicos do crime cibernético, as divergências foram corrigidas, oferecendo agora um retrato mais preciso da realidade.

Marco regulatório e detenções em cibersegurança

4. Marco regulatório e detenções em cibersegurança

Para o **Departamento de Cyber Threat Intelligence** da **NTT DATA**, é essencial analisar as medidas de segurança adotadas, as leis aprovadas no âmbito da cibersegurança e as detenções realizadas pelas forças de segurança em escala global durante o primeiro semestre de 2025.

Essa análise permite avaliar o comprometimento dos países com a regulamentação e o controle de tecnologias atuais e emergentes, bem como com sua aplicação responsável. Além disso, demonstra o esforço integrado dos poderes Legislativo e Judiciário e das forças de defesa para mitigar vulnerabilidades de segurança corporativa e conter atividades ilícitas no espaço cibernético.

4.1 Panorama das principais legislações em cibersegurança

No primeiro semestre de 2025, o conjunto de leis e regulamentações sobre cibersegurança continuou evoluindo nos âmbitos global e nacional. Embora alguns documentos ainda estejam em fase de implementação ou revisão, já é possível observar avanços importantes na harmonização legislativa no ciberespaço. Entre os principais destaques estão :

Continente	Legislação	Instituição	Referências
África	The Cyber Security Act, 2025 The Cyber Crime Act, 2025	Parlamento da Zâmbia	Assembleia Nacional da Zâmbia
América do Norte	Insure Cybersecurity Act of 2025	U.S. National Telecommunications and Information Administration	U.S. Government
	HIPAA Privacy Rule (Atualizações 2025)	U.S. Department of Health & Human Services	Access Partnership
América do Sul	Lei Marco de Cibersegurança Nº 21.663	Ministério do Interior e Segurança Pública do Chile	Biblioteca do Congresso Nacional do Chile
	Plano Federal de Prevenção a Crimes Cibernéticos e Gestão Estratégica da Cibersegurança (2025–2027)	Ministério de Segurança da Argentina	Boletim Oficial da República Argentina
Ásia	Regulamento sobre a Gestão da Segurança dos Dados em Rede (Novo projeto de emendas)	Conselho de Estado da República Popular da China	China Briefing
	Lei de Tecnologia Digital (DTI Law – Aprovada em junho)	Ministério da Ciência e Tecnologia do Vietnã	Vietnam Briefing
	Projeto de Lei de Proteção a Infraestruturas Críticas (Sistemas de Informação)	Conselho Legislativo de Hong Kong	Conselho Legislativo de Hong Kong
	Projeto de Lei de Prevenção a Fraudes	Parlamento de Singapura	Governo de Singapura
	Lei de Defesa Cibernética Ativa (ACD - aprovada em maio)	Parlamento Nacional do Japão	The House of Representatives, Japan
Europa	Regulamento sobre resiliência cibernética (Cyber Resilience Act (CRA))	Comissão Europeia	Comissão Europeia
	Regulamento da Inteligência Artificial	União Europeia	Conselho Europeu
	Regulamento (UE) 2025/37	União Europeia	União Europeia
	Regulamento de Cibersolidariedade (Cyber Solidarity Act)	União Europeia	União Europeia
	NIS2 Directive	União Europeia	NIS2 Directive
	Digital Operational Resilience Act (DORA)	Comissão Europeia/ Autoridades Financeiras UE	Field Fisher
	EU Cybersecurity Act (em revisão com novos padrões de certificação)	Agência de Cibersegurança da UE (ENISA)	Field Fisher
	Lei de Coordenação e Governança da Cibersegurança	Governo da Espanha/INCIBE Espanha	Ministério do Interior
Oceania	Cyber Security (Ransomware Payment Reporting) Rules 2025	Governo da Austrália	Federal Register of Legislation

Tabela 2 | Leis aprovadas ou em vigor no primeiro semestre de 2025.

Essas normas e leis, tanto no âmbito nacional quanto europeu, buscam aumentar a proteção contra riscos digitais, fortalecer a segurança de dados e de infraestruturas críticas e estabelecer processos mais robustos para avaliação de riscos. Especialmente, a Diretiva NIS2 e o regulamento DORA, representam avanços importantes na padronização das normas de segurança digital entre os países membros da União Europeia.

4.2 Principais operações de detenção no setor de cibersegurança

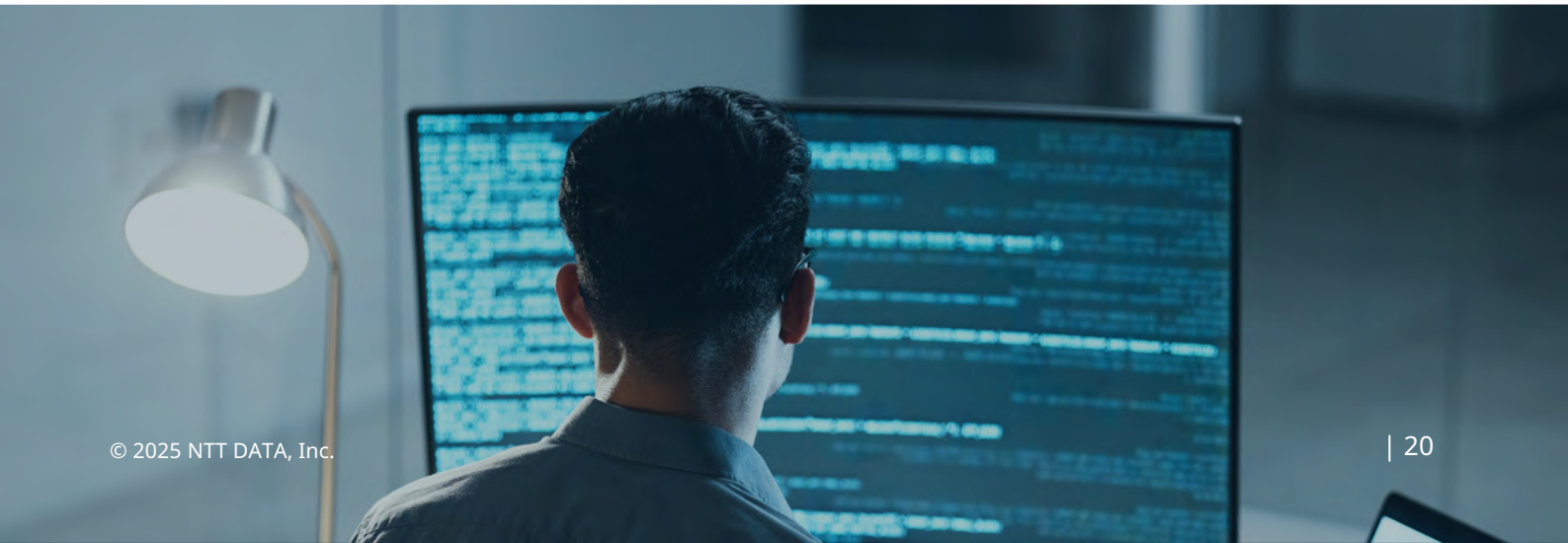
Durante o primeiro semestre de 2025, foram realizadas diversas operações internacionais voltadas para a desarticulação de redes cibercriminosas e a neutralização de grupos de ransomware, agentes de desinformação e APTs.

Essas ações, muitas vezes impulsionadas por colaborações entre forças de segurança, agências governamentais e entidades privadas, permitiram interromper as atividades de agentes altamente organizados e com atuação transnacional.

A seguir, apresentamos um resumo das principais operações realizadas no primeiro semestre de 2025:

Operação	Grupo de agentes de ameaças	Forças e órgãos de segurança	Referências
Operação contra Lumma Stealer	Vários domínios	Departamento de Justiça dos EUA Europol Microsoft's Digital Crimes Unit (DCU)	Justice Government
Phobos	Phobos Ransomware	Europol Interpol Orgãos locais de vários países	United States Attorney's Office
Phobos Aetor	8Base Ransomware	Europol Tenente-General da Polícia Trairong Phiwphan Orgãos de segurança locais	Dark Web Informer
Sindoor	AnonSec e agentes ligados à desinformação e terrorismo	Governo da Índia Inteligência militar	Clarion India
Raptour	Vendedores da dark web	Europol Orgãos de segurança da Áustria, Brasil, Alemanha e outros países	Europol
Operation secure	Infraestruturas maliciosas com infostealers	Interpol Orgãos locais de vários países	Interpol
Operation Deep sentinel	Archetyp Market	Orgão de segurança da Alemanha Europol Eurojust	Europol
Operação contra BreachForums	Liderança do BreachForums	Brigada de Cibercrime (BL2C) (Paris) FBI	USA Attorney's Office Le Parisien

Tabela 3 | Principais operações de desarticulação de grupos cibercriminosos realizadas em 2025.



Além dessas operações conduzidas por autoridades de segurança reconhecidas globalmente, observou-se também uma intensificação das **campanhas de violação de dados internas e exposições** de grupos conhecidos de ransomware por outros grupos de reputação suspeita. Um dos exemplos mais relevantes desse fenômeno foi o surgimento do canal "**GangExposed**" no Telegram, operado pelo grupo **CactusPulse**, conhecido pela coleta, validação e divulgação de inteligência operacional sobre membros de grupos cibercriminosos altamente destrutivos, como **Conti, Trickbot e Black Basta**.

Nos meses de abril e maio, o GangExposed tornou públicas imagens e perfis de 15 integrantes do grupo Conti, incluindo o suposto negociador-chefe Arkady Valentinovich Bondarenko. Além disso, foi revelada a identidade de um agente conhecido como "8G", considerado um dos principais coordenadores do Black Basta, responsável pelas operações de implantação, evasão de antivírus, seleção de alvos e pagamentos em criptomoedas.

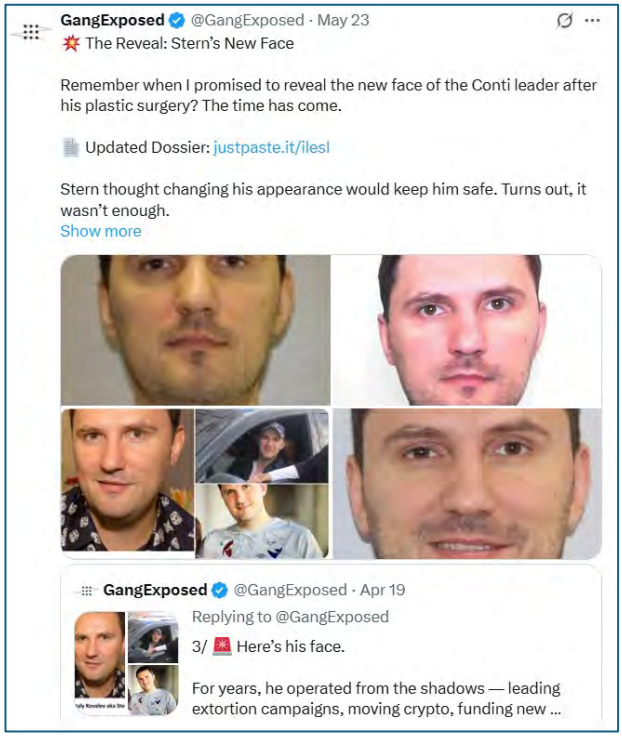
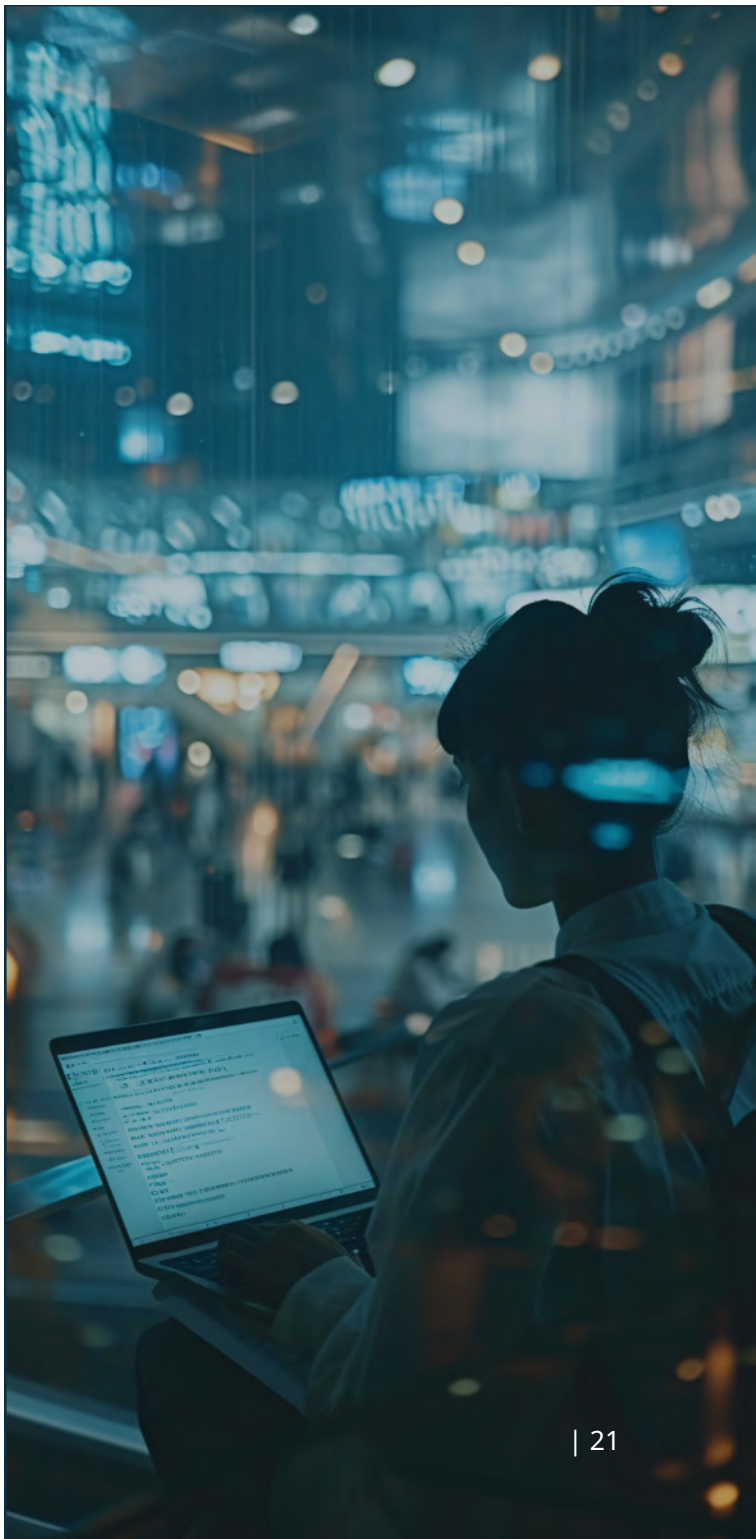


Ilustração 1 | Exposição na plataforma X realizada pelo grupo GangExposed.

As publicações do canal incluíram conversas internas vazadas, evidências de pagamentos, estratégias de engenharia social usadas para abordar vítimas e manuais operacionais para atividades maliciosas. Essa atividade representa um tipo de guerra de inteligência nunca antes visto no cenário atual.

Trata-se de uma prática crescente no ambiente cibercriminoso, em que certos grupos ou indivíduos, motivados por represálias, incentivos governamentais ou conflitos internos, escolhem divulgar dados confidenciais e estruturas hierárquicas de antigos aliados.

Esse fenômeno está ajudando as autoridades a identificar e rastrear lideranças do cibercrime organizado, ao mesmo tempo em que desestabiliza estruturas criminosas que antes se julgavam protegidas pelo anonimato e pela descentralização.



Dark Web Insights

5. Dark Web Insights

No primeiro semestre de 2025, a dark web continuou operando como um dos principais ecossistemas da atividade cibercriminosa, especialmente no que diz respeito à compra e venda de dados roubados, acessos ilícitos a sistemas, credenciais, ferramentas de malware e serviços de hacking baseados no modelo Crime-as-a-Service (CaaS). Esse período foi marcado por uma profunda reconfiguração tanto nos mercados quanto nos fóruns underground, principalmente após a perda do Breach Forums.

5.1 A queda do BreachForums: impacto e consequências

O encerramento do BreachForums em abril de 2025, seguido pela tentativa de venda do fórum por um de seus administradores em junho e pela prisão dos principais administradores como IntelBroker, representou um ponto crucial.

O fórum era uma das principais plataformas para a troca de bases de dados roubadas, acessos comprometidos, logs de infostealers e ferramentas ofensivas. Seu desaparecimento gerou um vácuo logístico e simbólico no ecossistema do cibercrime. Esse colapso forçou uma **migração de usuários** para fóruns privados, canais criptografados e marketplaces já consolidados. Como consequência direta, observou-se uma maior descentralização das atividades maliciosas e o crescimento de plataformas especializadas.

5.2 Fóruns underground ativos em 2025

- Na ausência do BreachForums, outros fóruns passaram a ganhar protagonismo:
- **Dread:** Fórum semelhante ao Reddit na dark web, usado para doxing, violações de dados e discussões técnicas.
- **XSS.is:** Considerado o principal fórum da dark web, frequentado por cibercriminosos de língua russa. Alguns de seus membros foram associados a ataques contra infraestruturas críticas no Leste Europeu.
- **Dark Forums:** Contava com **mais de 12.767 usuários registrados em abril de 2025**, atraído a maioria dos usuários após o fim do BreachForums. Possui uma comunidade muito ativa em malware, infostealers e cracking de contas. É um dos poucos fóruns que oferece uma seção com conteúdo técnico, incluindo tutoriais aprofundados sobre programação de scripts utilizados em ataques cibernéticos.
- **Exploit.in:** Com mais de 15 anos de atividade contínua, é considerado o fórum mais antigo ainda em funcionamento na dark web. Frequentemente, vulnerabilidades são divulgadas antes mesmo de aparecer no CVE. **Em fevereiro de 2025, uma vulnerabilidade de zero dia contra a Palo Alto Networks** foi revelada nesse fórum.
- **Nulled:** Especializado no compartilhamento de credenciais, ferramentas de cracking e vazamentos de dados massivos.
- **Sinister.ly:** Combina conteúdo técnico com fóruns sociais e de cultura hacker, o que o torna atraente para públicos mais jovens. É uma das plataformas com maior volume de discussões sobre ferramentas em Python, utilizado para a automação de phishing.
- **Cracked.io:** Portal híbrido entre fórum e marketplace, especializado na comercialização de contas de serviços on-line.
- **KickAss:** Apesar de mais recente, ganhou popularidade por reunir desenvolvedores de malware modular. Também oferece serviços personalizados para grupos APT.

Esses fóruns facilitam o intercâmbio de ferramentas, tutoriais, vulnerabilidades, dumps de bases de dados, assim como a disponibilização da contratação de serviços.

Principais publicações na dark web

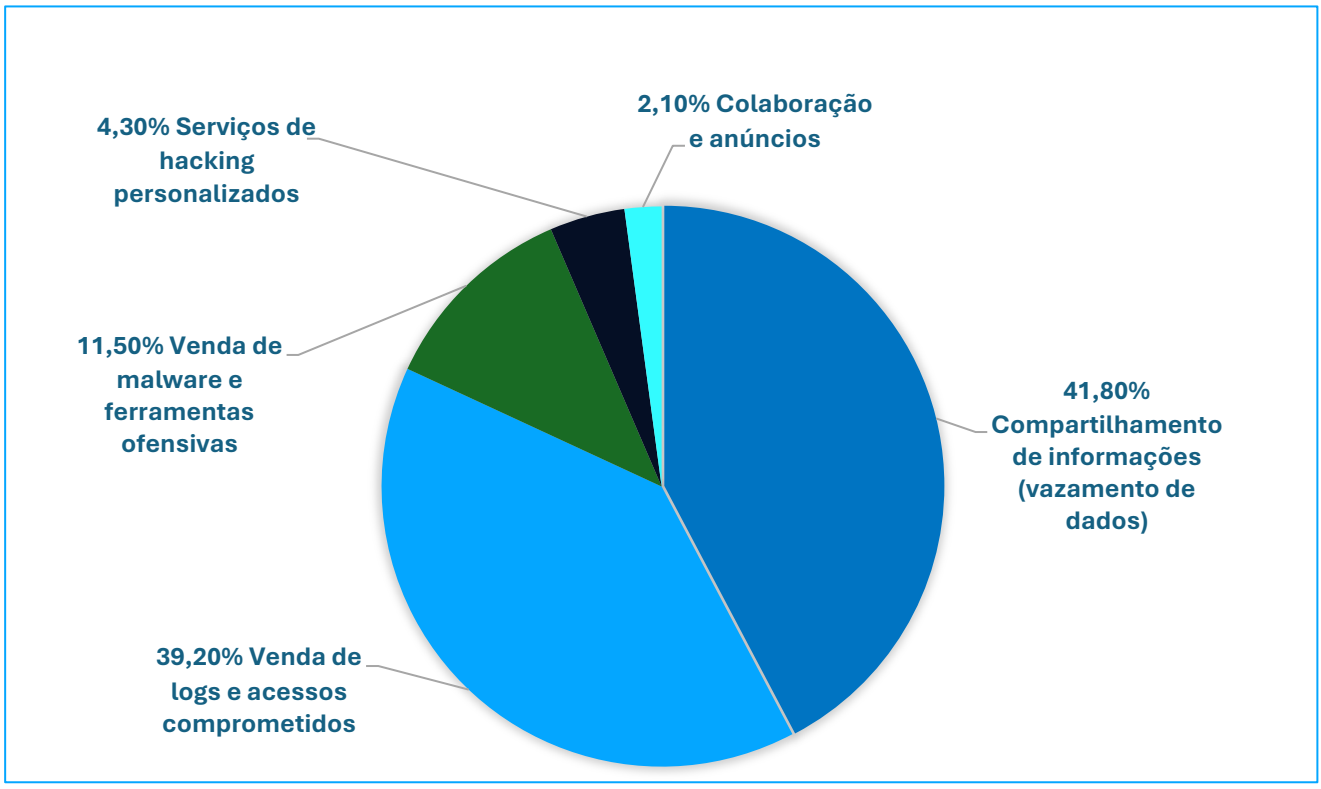


Figura 6 | Principais categorias de publicações na dark web no primeiro semestre de 2025.

Os logs provenientes de infostealers como **Lumma**, **RisePro** e **RedLine** dominaram o cenário, totalizando mais de **7,7 milhões de conjuntos de credenciais listados** nos primeiros cinco meses de 2025. Por sua vez, os dumps de cartões comprometidos chegaram a **14,4 milhões, sendo 80% de cartões dos Estados Unidos**, vendidos por valores entre US$ 5 e US$ 30.

5.3 Mercados underground ativos em 2025

- **Abacus Market:** Com uma interface simples, é conhecido pela venda de chips SIM anônimos e kits de roubo de identidade. Ganhou relevância em 2025 com o aumento de vendedores especializados em deepfakes personalizados. No entanto, no final de junho, foram observadas **diversas interrupções no serviço**, o que pode indicar uma possível desativação do mercado após a publicação deste relatório.
- **Russian Market:** Aceita diversas criptomoedas e disponibiliza diariamente **mais de 150 mil credenciais roubadas**. Seu diferencial é o serviço de atualização automatizada de logs a cada 24 horas, o que garante que os dados ofertados estejam sempre recentes e utilizáveis.
- **Brian's Club:** Após ter sido hackeado em 2019, ressurgiu e, em 2025, voltou a figurar **entre os três maiores em volume de cartões de crédito**. Estima-se que gerencie mais de 10 milhões de registros ativos.
- **Exodus Market:** Seu ponto forte está nos exploits de dia zero e no acesso privilegiado a servidores corporativos em regiões como América Latina e Ásia-Pacífico. Possui um sistema de reputação com três etapas de verificação para os vendedores.
- **Styx Market:** Especializado em ferramentas para ataques de phishing multicanal. Em março de 2025, foi vinculado a várias campanhas de distribuição de Lumma e RisePro por meio de macros maliciosas em arquivos Excel.
- **BidenCash:** Tornou-se conhecido por publicar gratuitamente mais de 2 milhões de cartões roubados em campanhas de marketing cibercriminoso em 2022, mantendo sua atividade com vendas de credenciais até ser desativado na Operação RapTor.

A seguir, apresentamos uma **estimativa da distribuição** das principais plataformas de venda underground que estiveram ativas no primeiro semestre de 2025, considerando seu nível de atividade e importância estratégica dentro do ecossistema cibercriminoso:

Plataformas de venda underground

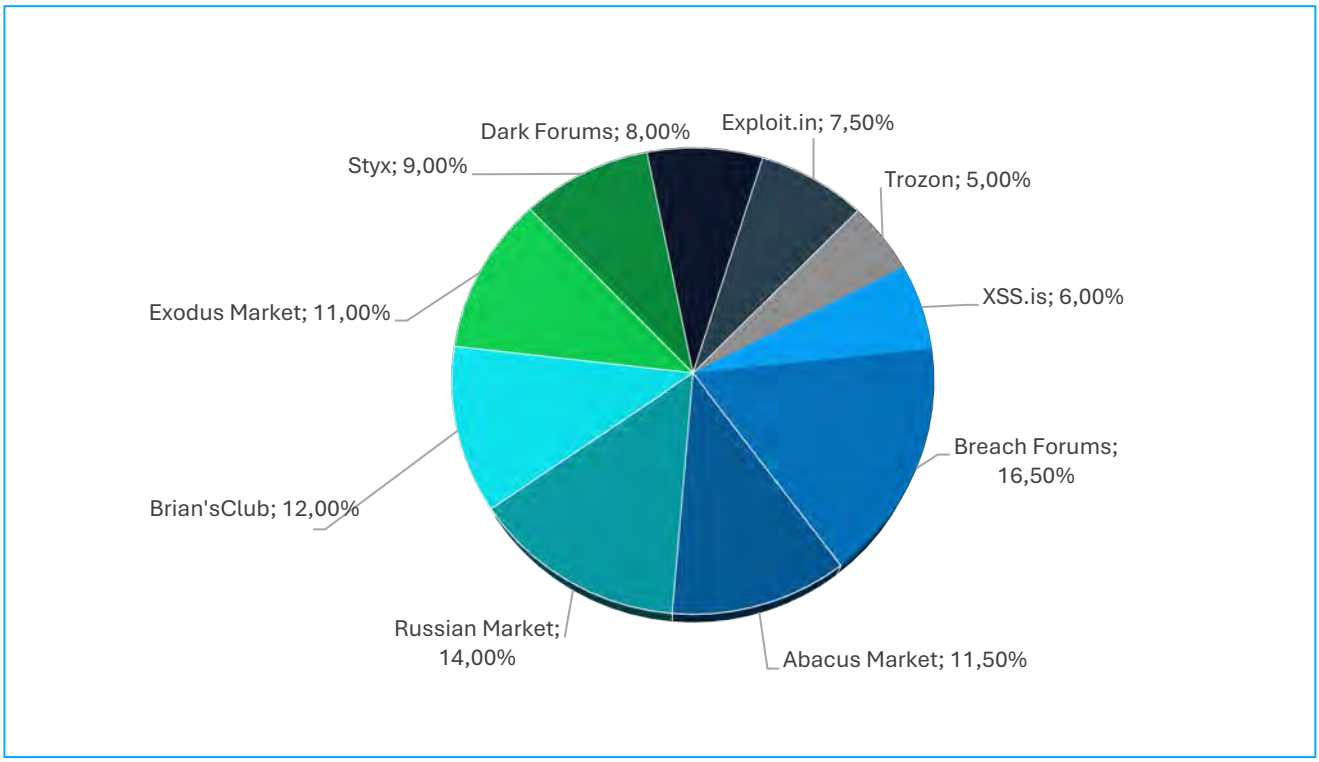


Figura 7 | Principais plataformas de venda underground identificadas no primeiro semestre de 2025.

Durante este período, destacou-se a atividade do grupo **RansomHub**, que não apenas absorveu antigos afiliados de outros grupos, como também diversificou suas operações em fóruns e markets como **Styx** e **Brian's Club**. Também foi identificado um crescimento operacional de **grupos como Storm-0953** e de afiliados associados a ferramentas de infostealing. Entre os **15 agentes mais ativos e influentes no segundo semestre de 2024 e no primeiro semestre de 2025**, **nove tiveram algum tipo de ligação com o BreachForums**.

Esses grupos estiveram por trás de alguns dos ciberataques mais relevantes em 2025, incluindo a violação de dados de usuários e ataques contra grandes instituições do setor financeiro na Ásia (SOCRadar, 2025). Em relação à comunicação operacional, embora o Telegram continue sendo uma das plataformas de referência, observou-se um aumento significativo no uso de **TOX, SimpleX e Signal** — todas aplicações Essas plataformas estão ganhando adesão por oferecerem maior privacidade, menor vigilância e menos exposição a ataques de infiltração das forças de segurança ou invasão de servidores.

Agentes de ameaças (Threat Actors)

6. Agentes de ameaças (Threat Actors)

Durante o primeiro semestre de 2025, o cenário de ameaças cibernéticas continuou em constante evolução, impulsionado pelo surgimento de novos agentes de ameaças, pela expansão e sofisticação dos grupos de ransomware, pela crescente coordenação entre hacktivistas e pelo aparecimento de novas tendências e padrões de atuação dos grupos APT.

6.1 Novos agentes identificados

A diversificação dos agentes de ameaças durante a primeira metade de 2025 não decorre apenas do surgimento de novos grupos cibercriminosos, mas também da consolidação de agentes emergentes. Esse movimento reforça, como já apontado anteriormente, o avanço da profissionalização no ecossistema de ameaças.

Sector 16/S16

Grupo ativo desde janeiro de 2025, com possível atribuição à Rússia. Associado a outros agentes de ameaças, como a aliança **Z-Pentest** e o grupo hacktivista **OverFlame**, consolidando ataques contra infraestruturas críticas, particularmente no setor de petróleo e gás e em sistemas de tratamento de água. Com o uso de **técnicas de acesso inicial não autorizado a sistemas de controle industrial e manipulação de parâmetros operacionais**, foram realizados ataques contra organizações em diferentes partes do mundo: o sistema SCADA de bombas de petróleo e tanques de armazenamento no Texas (EUA), uma empresa italiana de bombas de água industriais e duas empresas espanholas — uma de tratamento de águas e um sistema APCS de uma planta de dióxido de carbono (Orange Cyberdefense, 2025).

LazurGroup

Grupo de origem francesa, surgiu em janeiro de 2025, com foco na Europa Ocidental, especialmente França e Bélgica. Suas operações combinam técnicas avançadas de spear phishing, uso de ferramentas de acesso remoto como o Cobalt Strike e malware personalizado. Além disso, utilizam canais no Telegram para distribuição e coordenação interna. O nível de organização e sofisticação fez com que especialistas o classificassem como uma potencial ameaça híbrida, combinando motivações criminais e ideológicas.

BianLian

Ativo desde 2022, este grupo de ransomware migrou para um **modelo de extorsão sem criptografia**, baseado exclusivamente no vazamento de dados. Em 2025, a CISA e o FBI emitiram alertas sobre campanhas fraudulentas em que agentes independentes se fazem passar pelo BianLian para extorquir executivos por e-mail. Essas técnicas de falsificação dificultam a atribuição com precisão, mas confirmam o papel central do grupo no atual cenário de ameaças (CISA, 2025; FBI, 2025).

Rhysida

Identificado em 2023, este RaaS aumentou significativamente sua atividade em 2025. A CISA, o FBI e o MS-ISAC atualizaram seus indicadores de comprometimento e técnicas, táticas e procedimentos (TTPs) após diversos ataques contra instituições educacionais, de saúde e governamentais. Sua estrutura descentralizada e abordagem multivetorial representam um desafio para os mecanismos de defesa (CISA, 2025).

Void Blizzard

Também conhecido como Laundry Bear, é um grupo com afiliação russa, ativo desde abril de 2024, cujas atividades anteriores foram atribuídas em maio de 2025. Utiliza principalmente técnicas de spear phishing, exfiltração de dados e roubo de credenciais, tendo direcionado ataques a infraestruturas críticas da Ucrânia e de seus aliados (membros da OTAN), assim como a governos e forças especiais da Europa e dos Estados Unidos, motivado por interesses geopolíticos (Microsoft Threat Intelligence, 2025; Bleeping Computer, 2025).

Observa-se uma tendência crescente à **diversificação tática**, com maior uso de **ferramentas Living off the Land (LotL)**. Ao longo do ano, espera-se um aumento da **colaboração entre grupos** e uma maior convergência entre cibercrime e ciberespionagem, fundindo objetivos econômicos e estratégicos que dificultam ainda mais a atribuição dos ataques.

6.2 Grupos de ransomware

Em 2025, o cenário das ciberameaças foi marcado pelo surgimento de novos grupos de ransomware que demonstraram alta capacidade de adaptação e crescente agressividade em suas táticas. Paralelamente, os grupos já consolidados elevaram seu nível de sofisticação, aperfeiçoando técnicas de evasão, criptografia e extorsão. Essa evolução intensificou a pressão sobre organizações de todos os setores, consolidando o ransomware como uma das ameaças mais persistentes e disruptivas do ecossistema digital atual.

6.2.1 Novos grupos

Nos primeiros meses do ano, especialmente em janeiro e fevereiro, registrou-se um volume elevado de atividades atribuídas a campanhas de ransomware, muitas delas associadas a agentes já conhecidos.

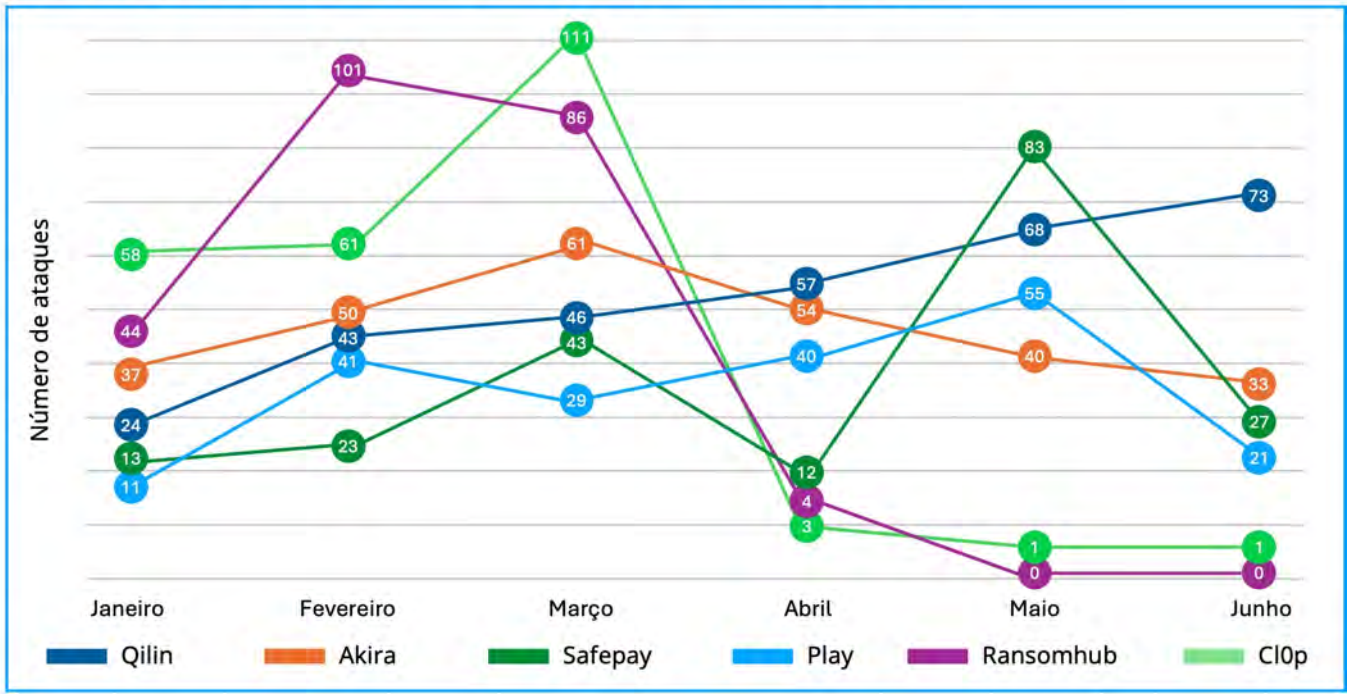
Consequentemente, desde março e abril, verificou-se um crescimento na detecção de novos grupos, alguns surgidos como dissidências de grupos anteriormente desarticulados; um processo contínuo de renovação do ecossistema criminoso, no qual a fragmentação e a reconfiguração de agentes têm papel central na resiliência do modelo de ransomware como serviço (RaaS) (DarkFeed, 2025).

Figura 8 | Grupos de ransomware identificados no primeiro semestre de 2025.

6.2.2 Grupos com maior atividade

A atividade criminosa nesse segmento continuou se adaptando às evoluções tecnológicas, às medidas de defesa e às oportunidades oferecidas pelo modelo RaaS. Esse movimento resultou em um ambiente altamente dinâmico e instável, no qual a inovação técnica, a exploração de novos alvos e a descentralização das operações se tornaram fatores cruciais para compreender a complexidade das ameaças atuais.

A seguir, apresenta-se um gráfico que mostra os grupos de ransomware mais ativos ao longo do primeiro semestre de 2025, ilustrando sua distribuição e evolução nesse período (DarkFeed, 2025).



- **RansomHub e Cl0p:** Ambos apresentaram distribuição de ataques semelhantes. O grupo Cl0p, recentemente incluído nos rankings de ransomware, registrou o maior número de ataques em março (111) de 2025. Por outro lado, o RansomHub, que se consolidou como um dos grupos mais ativos de 2024, sofreu uma queda brusca em abril e desapareceu completamente em maio e junho.
- **Qilin e Akira:** Aparece no topo da lista em volume de ataques. O Qilin destacou-se como um dos grupos dominantes de 2025, com crescimento acelerado atribuindo-se, em parte, à migração de afiliados do RansomHub e à sua infraestrutura técnica robusta, que permite operações eficientes, escaláveis e profissionais. O Akira manteve presença constante e alto nível de sofisticação, consolidando-se como um grupo persistente com infraestrutura madura.
- **Play e Safepay:** O grupo Play continua figurando entre as ameaças mais ativas deste semestre. Sem liderar em volume de ataques, tem evoluído para operações mais especializadas e técnicas, demonstrando maior profissionalização em suas campanhas. Já o Safepay concentrou suas campanhas em pequenas e médias empresas e setores menos protegidos, explorando vulnerabilidades comuns. Seu crescimento gradual aponta para uma possível ascensão no segundo semestre de 2025, devendo ganhar mais notoriedade ao longo do ano.

6.2.3 Impacto global

A atividade dos grupos de ransomware em 2025 tem causado impactos em escala global, atingindo organizações de diferentes portes e setores em diversas regiões do mundo. Embora a distribuição geográfica dos ataques apresente variações conforme o grupo e seus objetivos estratégicos, observa-se uma clara concentração em países com alta digitalização, com destaque para os Estados Unidos, e em setores críticos como saúde, educação, manufatura e serviços financeiros.

A análise dos setores mais afetados por ataques de ransomware nos últimos seis meses, apresentada neste relatório, indica que o setor de manufatura continua liderando como principal alvo dos cibercriminosos em escala global.

Essa tendência, observada de forma consistente nos últimos anos, reflete uma combinação de fatores estruturais que tornam o setor um dos alvos mais atraentes para os cibercriminosos. A forte dependência de sistemas operacionais industriais, aliada à crescente integração entre ambientes OT e redes IT, somada à pressão constante por garantir a continuidade das cadeias globais de suprimentos, torna o setor de manufatura especialmente vulnerável — onde até mesmo interrupções de curto prazo podem resultar em perdas financeiras significativas.

Em 2025, os cibercriminosos aperfeiçoaram suas técnicas, direcionando ataques a sistemas SCADA, hipervisores e ambientes de produção virtualizados, aumentando o nível de sofisticação e impacto das ofensivas. O gráfico a seguir destaca os setores que mais sofreram ataques de ransomware nos primeiros seis meses de 2025, evidenciando a posição de liderança mantida pelo setor de manufatura ao longo do período:

Ataques de ransomware por setor (S1 2025)

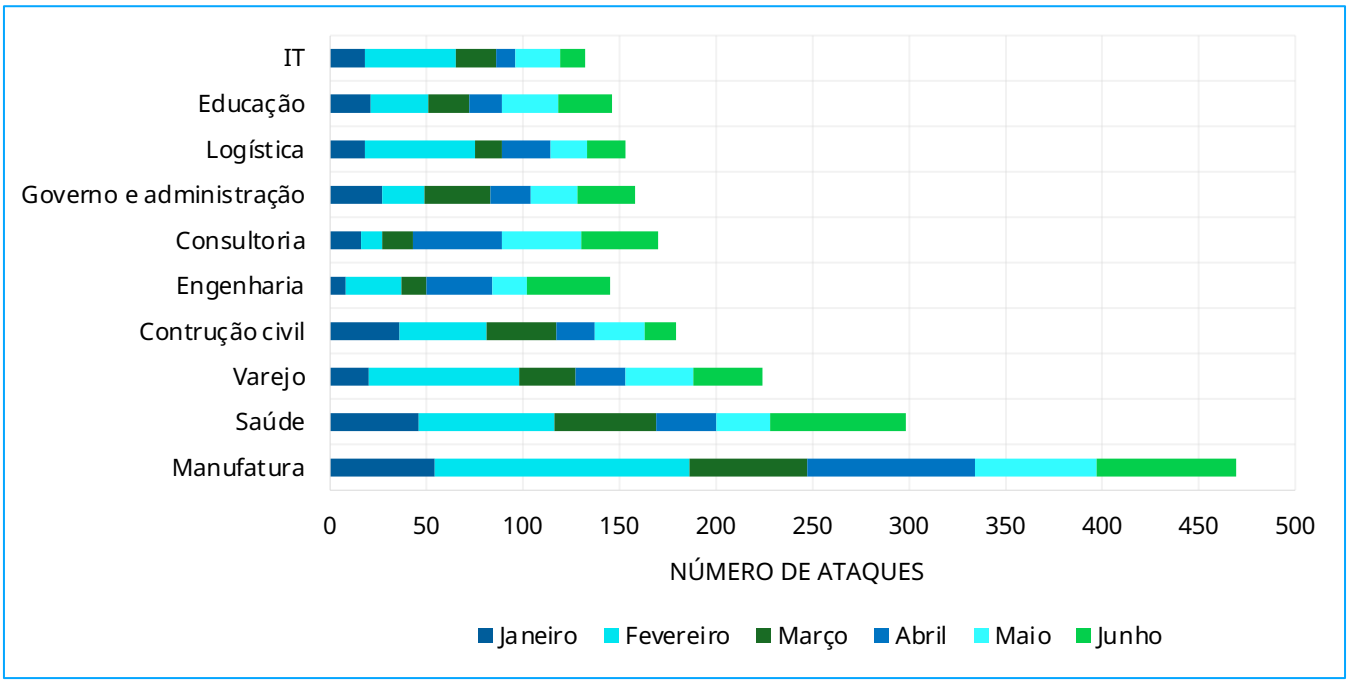


Figura 10 | Setores mais afetados por *ransomware* no primeiro semestre de 2025.

O gráfico a seguir apresenta a distribuição geográfica dos países mais impactados por esse tipo de ataque no mesmo período:

Países mais afetados por ransomware de janeiro a junho de 2025

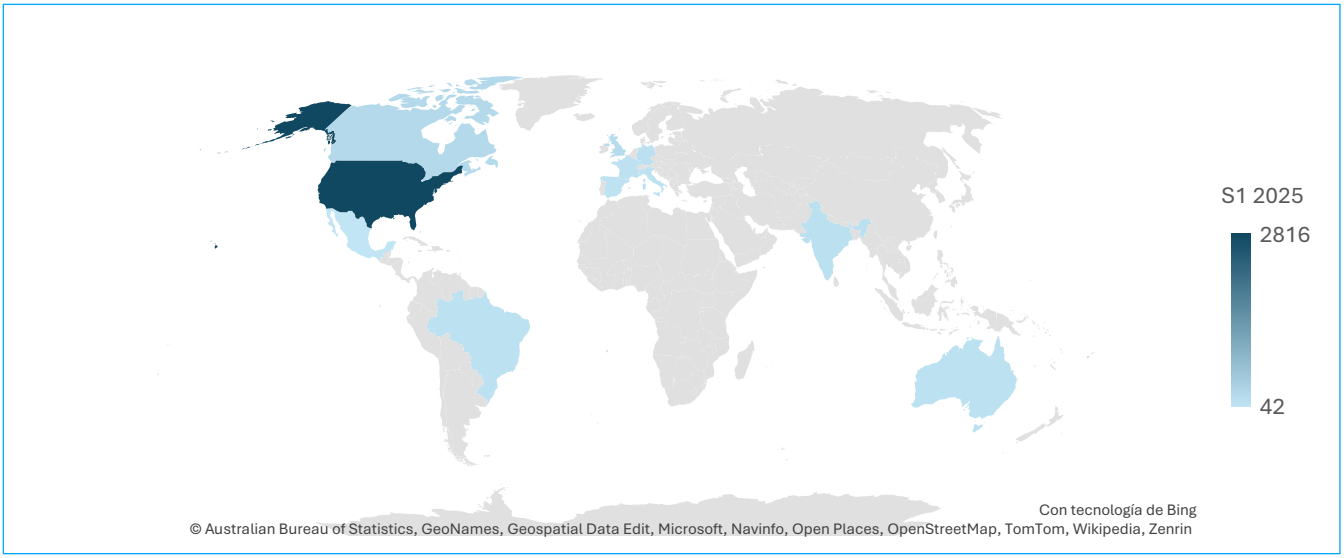


Figura 11 | Países mais afetados por ransomware no primeiro semestre de 2025.

Como já destacado nesta seção, os **Estados Unidos** lideram o ranking como o país mais atacado, com foco especial em infraestruturas críticas, sistemas financeiros e redes governamentais. Em seguida, figuram países como a **Índia**, com alta exposição geopolítica, além do **Reino Unido** e da **Alemanha**, cujos setores industriais e financeiros, altamente digitalizados, ampliam suas vulnerabilidades.

Por outro lado, o **aumento dos ataques à América do Sul** pode refletir uma tendência de expansão para economias emergentes, onde os níveis de digitalização avançam mais rapidamente do que as capacidades de ciberdefesa. Nesse cenário, o Brasil se destaca como um dos países mais afetados da região, concentrando uma parcela significativa dos ataques, especialmente contra setores-chave como educação, saúde, logística e até mesmo serviços digitais.

Paralelamente, na América Central, o México tem registrado uma atividade crescente de grupos como Cl0p, LockBit e Akira. Com motivações predominantemente financeiras, essas operações têm causado impactos relevantes em setores como o financeiro, a administração pública e a manufatura, consolidando o país como um dos principais alvos de campanhas de ransomware cada vez mais sofisticadas e persistentes que nos demais países da região.

Essa distribuição geográfica evidencia uma tendência consolidada: os cibercriminosos estão direcionando suas operações para países com alta dependência de tecnologia, infraestruturas críticas fortemente interconectadas e que, frequentemente, apresentam deficiências significativas em suas capacidades de resposta e resiliência cibernética.

6.3 Hacktivistas

Em 2025, o hacktivismo registrou um expressivo crescimento, impulsionado tanto por conflitos geopolíticos quanto por causas sociais de alcance global.

O fenômeno evoluiu para além das ações individuais ou grupos menores, dando origem a alianças transnacionais de grupos hacktivistas que atuam com um nível inédito de coordenação. Em muitos casos, esses grupos recebem apoio velado de determinados Estados, que os veem como uma ferramenta útil para exercer pressão política sem recorrer a confrontos militares diretos.

O cenário global do hacktivismo tem se intensificado com a formação de alianças entre grupos que operam em contextos de conflito geopolítico. O grupo **AnonSec**, tradicionalmente associado a campanhas de vazamento de dados, tem coordenado ataques descentralizados contra infraestruturas críticas e disseminado campanhas de desinformação. Estabeleceu alianças com grupos pró-Palestina como **Mr. Hamza, Ghosts of Gaza, Handala Hack, Sylhet Gang-SG e Moses Staff** — todos com forte orientação antiocidental, com foco principal nos Estados Unidos, Israel e, mais recentemente, na Índia. Este país, por sua vez, tem atuado por meio do grupo nacionalista **Indian Cyber Force**, direcionando suas operações contra países como Paquistão e China.

Outros grupos como **DieNet e DragonForce** Malaysia também ampliaram suas atividades contra interesses norte-americanos, alinhando-se a causas islâmicas e anti-imperialistas. No eixo pró-Rússia, o grupo **NoName057(16)** se destacou como o mais ativo, liderando campanhas DDoS contra a Ucrânia e seus aliados. Atuou em colaboração com os grupos **Killnet e Anonymous Sudan**, tendo como alvos principais sites governamentais, financeiros e de transporte na Europa.

A crescente cooperação entre esses grupos reflete uma tendência à profissionalização do hacktivismo, com estruturas mais organizadas e objetivos estratégicos bem definidos.

Ataques de ransomware por setor (S1 2025)

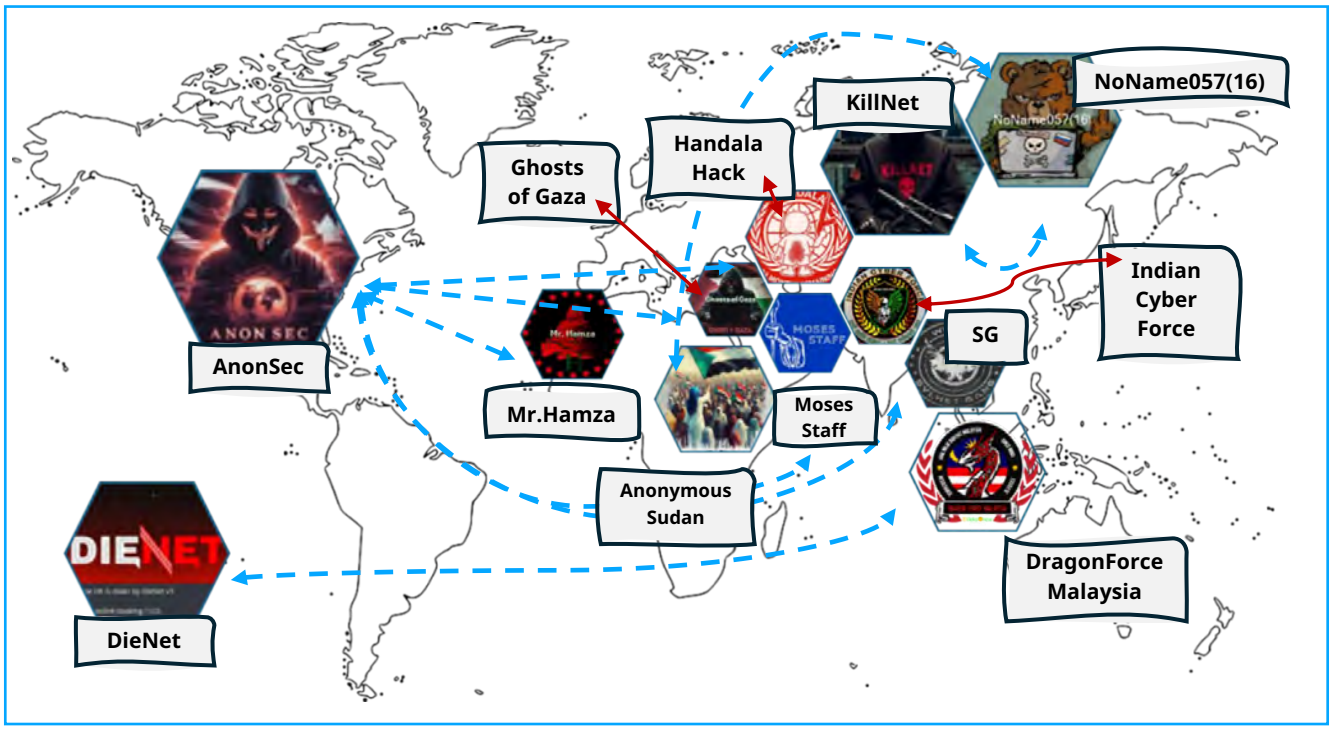
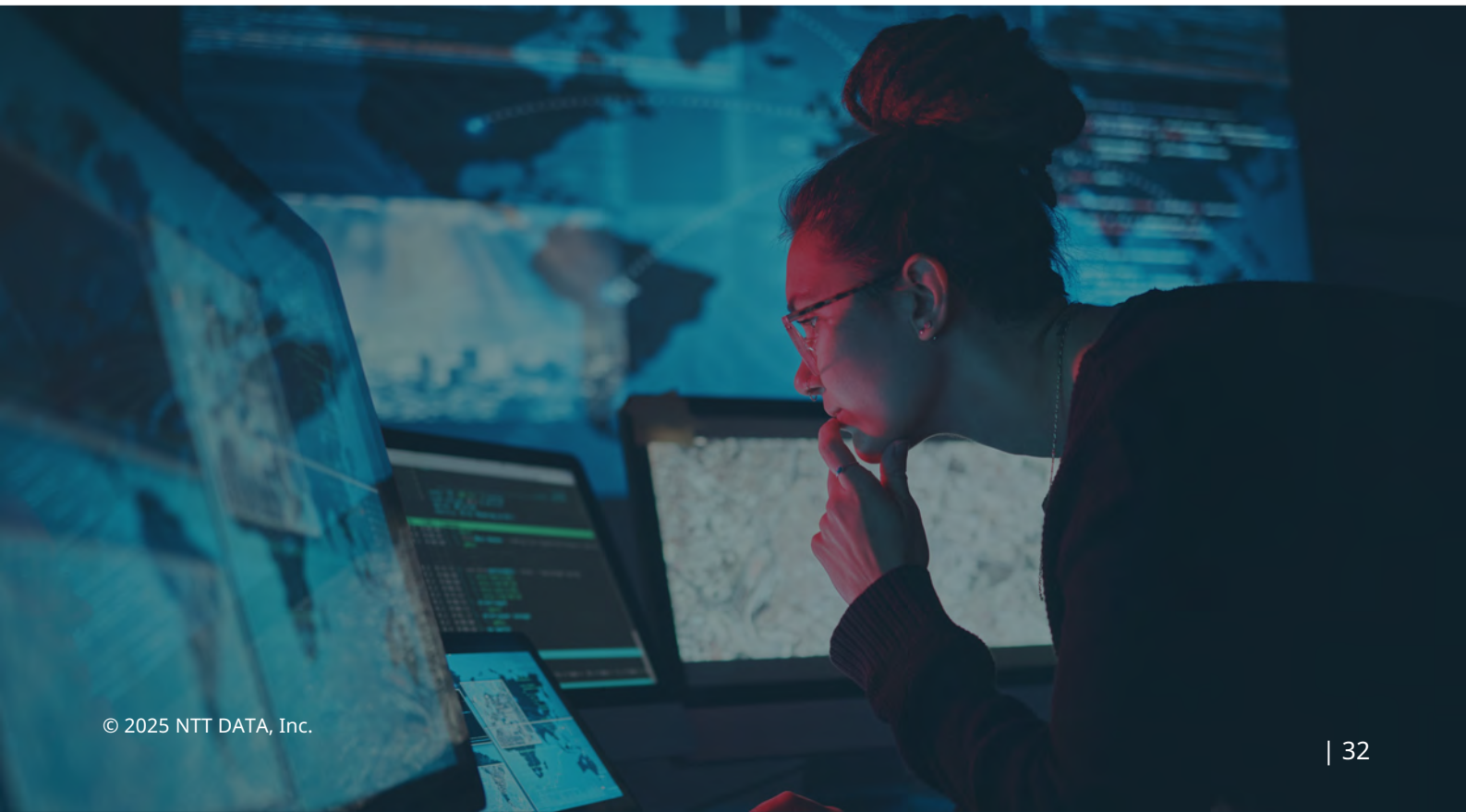


Figura 12 | Alianças de grupos hacktivistas por principais conflitos geopolíticos.

O hacktivismo, que inicialmente se limitava a manifestações simbólicas ou protestos digitais de baixo impacto, evoluiu para uma ferramenta estratégica no cenário geopolítico atual. No entanto, atualmente evoluiu para uma **ferramenta estratégica no âmbito geopolítico**, com operações meticulosamente orquestradas e objetivos alinhados a interesses estatais ou ideológicos. Essa evolução torna mais complexo o cenário da cibersegurança global, ao eliminar as fronteiras separam o ativismo digital, as operações de inteligência e os conflitos cibernéticos com envolvimento dos Estados.



6.4 APT

Durante o primeiro semestre de 2025, os grupos APT intensificaram suas atividades, aprimorando suas campanhas tanto do ponto de vista técnico quanto em termos de persistência. A seguir, veja as principais tendências por região e por agentes estatais:

- **APTs russas:** como adiantamos no início deste relatório, mantiveram uma estratégia agressiva focada em três frentes: ciberespionagem diplomática, interrupção de serviços críticos e desinformação.

  - O **Sandworm** atuou na Ucrânia com o novo wiper "ZEROLOT", cujo objetivo é interromper operações de empresas do setor energético, disseminado por meio de políticas de grupo no Active Directory e ferramentas RMM.

  - Outros, como o **Sednit (APT28)**, ampliaram a já conhecida **Operação RoundPress** (inicialmente direcionada ao Roundcube) para também afetar plataformas de e-mail como Horde, Zimbra e MDaemon, explorando vulnerabilidades XSS e dia zero. Um dos casos mais relevantes foi a exploração da **CVE-2024-11182** contra alvos ucranianos. Adicionalmente, observou-se a exploração de falhas de dia zero, incluindo a **CVE-2024-9680** no Mozilla Firefox e a **CVE-2024-49039** no Microsoft Windows, o que reforça o caráter ofensivo de seu perfil.

  - **Gamaredon**, focado exclusivamente na Ucrânia, manteve uma alta frequência de ataques, com atualizações constantes em seus implantes e técnicas de ofuscação. Infiltrou o PteroBox, um ladrão de arquivos que utiliza o Dropbox como canal não convencional de exfiltração de dados.

  Grupos hacktivistas pró-Rússia como **NoName057(16)**, **Cyber Army of Russia Reborn** e **Solntsepyok** seguiram com campanhas DDoS e vazamento de dados contra mídia e governos europeus. Em alguns casos, foi identificada uma convergência operacional com campanhas APT, reutilizando vulnerabilidades como as mencionadas anteriormente para obter acesso inicial — o que reflete uma crescente profissionalização no ecossistema hacktivista.

- **APT chinesas:** intensificaram seus ataques a infraestruturas críticas e redes governamentais, principalmente na Europa e Ásia. Observou-se a consolidação do uso de ferramentas compartilhadas entre grupos estatais, com integração de novas backdoors e técnicas evasivas.

  - **APT41** e **Earth Baku** seguiram com campanhas direcionadas a sistemas OT e dispositivos de rede, fazendo uso do ShadowPad e de novas variantes como a"VELVETSHELL".

  - **DigitalRecyclers** utilizou a backdoor HydroRShell junto com técnicas de tunneling com KMA VPN para comprometer instituições europeias.

  - **PerplexGoblin** implantou o malware avançado NanoSlate em C++ contra órgãos governamentais da Europa Central.

  Esses grupos se destacaram pelo uso coordenado de exploits contra roteadores, switches Cisco Nexus e proxies corporativos para estabelecer uma persistência invisível.

- **APT iranianas:** mostraram uma dualidade clara entre operações de ciberespionagem e campanhas direcionadas contra Israel.

  - **MuddyWater** e **Lyceum** adotaram softwares legítimos de administração remota para obter acesso inicial em campanhas de spear phishing voltadas a setores industriais e de infraestrutura em Israel.

  - Em uma ação coordenada, observou-se **BledEdFeline** colaborando com MuddyWater no compartilhamento de componentes de persistência.

  - O grupo emergente **Cyber Toufan**, com vínculos hacktivistas, combinou vazamento de dados, destruição de sistemas e manipulação de informações.

- **APT norte-coreanas:** continuam focadas em operações de espionagem diplomática e roubo de criptomoedas para financiamento do regime.
  - O grupo **DeceptiveDevelopment** ampliou o uso de job lures relacionadas a empregos e plataformas como a WeaselStore, visando desenvolvedores blockchain e profissionais de TI.
  - O grupo **TraderTraitor** foi vinculado ao ataque à carteira Safe{Wallet}, comprometendo sua cadeia de fornecimento e resultando em um roubo de mais de US$ 1,5 bilhão em ativos digitais.
  - **Kimsuky** e **Andariel** retornaram com campanhas contra alvos sul-coreanos e diplomatas da região da Ásia-Pacífico.

O **Departamento de Cyber Threat Intelligence da NTT DATA** elaborou uma estimativa, com base em fontes públicas e dados de inteligência aberta, para classificar as campanhas APT do semestre de acordo com sua motivação predominante.

Atividade APT classificada pela motivação por região (S1 2025)

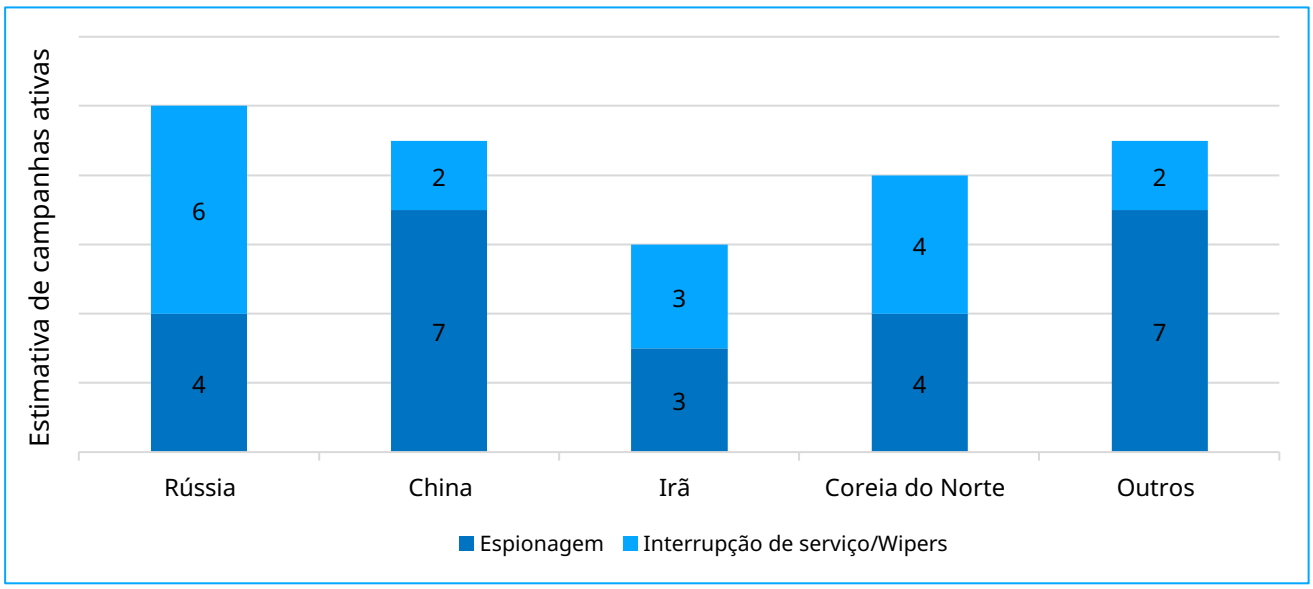


Figura 13 | Atividade dos grupos APT por região, classificada por motivação, durante o primeiro semestre de 2025.

A análise mostra uma postura mais destrutiva em agentes como Rússia e Irã, enquanto China, Coreia do Norte e grupos do Sul da Ásia mantêm foco principal em operações de espionagem. Essa segmentação permite identificar padrões operacionais distintos por região e antecipar prováveis evoluções táticas conforme o contexto geopolítico.

Táticas, Técnicas e Procedimentos (TTPs)

7. Táticas, Técnicas e Procedimentos

As Táticas, Técnicas e Procedimentos (TTPs) constituem uma abordagem fundamental para compreender as estratégias adotadas por agentes de ameaças no cenário cibernético. Identificar esses padrões não apenas permite fortalecer a postura defensiva das organizações, mas também antecipar e mitigar possíveis riscos de maneira proativa.

7.1 Descrição das TTPs mais comuns utilizadas por cibercriminosos

Durante o primeiro semestre de 2025, o phishing foi a principal técnica de acesso inicial, com hackers utilizando vishing, links e anexos maliciosos, além de ataques BEC (Business Email Compromise). Também foi observado um uso ampliado de ferramentas comerciais e de código aberto de acesso remoto, como **SplashTop, Atera, TeamViewer, AnyDesk, LogMeIn, ScreenConnect, QuickAssist, TightVNC** e a plataforma **RMM da Level**.

A tabela a seguir apresenta as técnicas do MITRE ATT&CK mais observadas no primeiro semestre de 2025:

Tática	MITRE ATT&CK ID	Descrição
Reconhecimento (TA0043)	T1590 – Coleta de informações sobre a rede da vítima	Os hackers podem coletar informações sobre as redes das vítimas que podem ser utilizadas para realizar ataques. Essas informações podem incluir diversos detalhes, como dados administrativos, bem como detalhes sobre sua topologia e operações.
	T1595.002 – Varredura ativa: Varredura de vulnerabilidades	Os hackers podem executar varreduras de vulnerabilidades na infraestrutura pública de uma organização para identificar possíveis vulnerabilidades que possam ser exploradas.
Acesso inicial aos sistemas (TA0001)	T1598.004 – Phishing de informações: Spear phishing por voz	Em uma campanha observada, os usuários receberam chamadas de hackers se passando por suporte de TI e foi solicitado que iniciassem uma sessão de QuickAssist.
	T1598.003 – Phishing de informações: Link de spear phishing	Os hackers podem enviar mensagens de spear phishing com um link malicioso para obter informações confidenciais que possam ser utilizadas durante o ataque.
	T1598 – Phishing de informações: Anexo de spearphishing	Os hackers podem enviar mensagens de spear phishing com um anexo malicioso para obter informações confidenciais que possam ser utilizadas em ataques direcionados.
	T1190 – Exploração de uma aplicação pública	Os hackers podem explorar uma vulnerabilidade para acessar o sistema alvo.
	T1078 – Contas válidas	Os hackers podem utilizar credenciais comprometidas para acessar contas válidas durante o ataque.
Execução (TA0002)	T1059.001 – Interpretador de comandos e scripts: PowerShell	Os hackers podem utilizar o PowerShell para executar comandos ou scripts durante o ataque.
	T1047 – Ferramenta de administração do Windows	Os hackers podem utilizar a WMI (Instrumentação de Gerenciamento do Windows) para executar comandos maliciosos durante o ataque.
	T1053 – Tarefa/trabalho agendado	Os hackers podem utilizar a programação de tarefas para facilitar a execução inicial ou recorrente de código malicioso.

Tática	MITRE ATT&CK ID	Descrição
Persistência (TA0003)	T1098 – Manipulação de contas	Os hackers podem manipular contas para manter ou aumentar o acesso aos sistemas das vítimas.
	T1136.001 – Criação de conta: Conta local	Os hackers podem criar uma conta local para manter o acesso aos sistemas das vítimas.
	T1547.001 – Execução automática ao iniciar sessão ou sistema: Chaves de execução no Registro/pasta de inicialização	Os hackers estabeleceram persistência por meio da inserção de endereços IP na chave de registro do TitanPlus.
	T1133 – Serviços remotos externos	Os hackers podem explorar serviços remotos externos para obter acesso inicial ou manter persistência em uma rede.
	T1546.008 – Execução ativada por eventos: Funções de acessibilidade	Os hackers podem estabelecer persistência ou escalar privilégios por meio da execução de conteúdo malicioso ativado por funções de acessibilidade.
Escalada de privilégios (TA0002)	T1134 – Manipulação de tokens de acesso	Os hackers podem modificar tokens de acesso para operar sob o contexto de segurança de outro usuário ou do sistema, realizando ações e contornando controles de acesso.
Evasão de defesas (TA0005)	T1562.001 – Enfraquecimento de defesas: Desativação ou modificação de ferramentas	Os hackers podem desativar ou desinstalar ferramentas de segurança para evitar serem detectados.
	T1562.004 – Enfraquecimento de defesas: Desativação ou modificação do firewall do sistema	Os hackers podem desativar ou modificar os firewalls do sistema para contornar os controles que limitam o uso da rede.
	T1564.008 – Ocultação de itens maliciosos: regras de ocultação de e-mails	Os hackers podem usar regras de e-mail para ocultar mensagens de entrada ou de saída na caixa de correio de um usuário comprometido.
	T1070.001 – Eliminação de indicadores: Exclusão de logs de eventos do Windows	Os hackers podem apagar os registros de eventos do Windows para ocultar seus rastros e dificultar a análise forense.
	T1112 – Modificação do Registro	O hacker pode realizar algumas modificações no registro para obter escalada de privilégios.
Acesso a credenciais (TA0006)	T1003 – Extração de credenciais do sistema operacional	Os hackers podem extrair credenciais de diversas fontes para facilitar o movimento lateral.
	T1528 – Roubo de *tokens* de acesso a aplicativos	Os hackers podem roubar tokens de acesso a aplicativos para obter credenciais e acessar sistemas e recursos remotos.
Descoberta (TA0007)	T1046 – Descoberta de serviços de rede	Os hackers podem usar ferramentas como scanners de portas avançados para escanear a rede.
	T1057 – Descoberta de processos	Os hackers podem tentar obter informações sobre os processos em execução em um sistema.
	T1018 – Descoberta de sistemas remotos	Os hackers podem tentar descobrir informações sobre sistemas remotos com comandos como "net view".
	T1082 – Descoberta de informações do sistema	Um hacker pode tentar obter informações detalhadas sobre o sistema operacional e o hardware.
	T1016 – Descoberta da configuração de rede do sistema	Os hackers podem usar comandos como "ifconfig" e "net use" para identificar conexões de rede.
	T1087.001 – Descoberta de contas: Conta local	Listar as contas de usuário no sistema.

Tática	MITRE ATT&CK ID	Descrição
Movimento lateral (TA0008)	T1021.001 – Serviços remotos: Protocolo de Área de Trabalho Remota	Os hackers podem abusar de contas válidas por meio do RDP para se movimentarem lateralmente em um ambiente alvo.
	T1021.006 – Serviços remotos: Administração Remota do Windows	Os hackers podem usar contas válidas para interagir com sistemas remotos por meio da Administração Remota do Windows (WinRM).
Comando e controle (TA0011)	T1219 – Software de acesso remoto	Um hacker pode usar software legítimo de suporte de desktop e acesso remoto para estabelecer um canal interativo de comando e controle para os sistemas alvo dentro das redes.
	T1105 – Transferência de ferramentas de entrada	Os hackers podem transferir ferramentas de um sistema externo para um sistema comprometido.
	T1572 – Tunneling de protocolos	Os hackers podem realizar o tunneling de comunicações de rede de e para um sistema vítima por meio de um protocolo alternativo, como SMB, para evitar a detecção ou permitir o acesso.
Exfiltração (TA0010)	T1048 – Exfiltração por meio de um protocolo alternativo	Os hackers podem roubar dados extraindo-os por meio de um protocolo diferente daquele utilizado no canal de comando e controle existente, como o WinSCP.
Impacto (TA0040)	T1486 – Criptografia de dados para impacto	Os hackers podem usar ransomware para criptografar dados em um sistema alvo.
	T1490 – Inibir a recuperação do sistema	Os hackers podem desabilitar funções de recuperação do sistema, como snapshots de volume.
	T1489 – Interrupção de serviço	Os hackers podem interromper ou desativar serviços em um sistema para que não estejam disponíveis para usuários legítimos.

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

Com base na evolução dessas TTPs e nas tendências atuais, **para o segundo semestre de 2025**, espera-se um aumento na **utilização de ferramentas legítimas**, maior **sofisticação nas técnicas de evasão**, crescimento no uso de **scripts automatizados e baseados em IA**, e **maior persistência em ambientes híbridos**, onde há mais pontos de entrada expostos.

A relação com o framework MITRE ATT&CK não apenas permite compreender essas ameaças, mas também proporciona uma abordagem prática para mitigá-las.

7.2 Vetores de entrada mais utilizados

Neste contexto, e considerando que o ransomware continua sendo uma das ameaças mais persistentes e lucrativas, as tendências atuais de vetores de entrada podem ser resumidas da seguinte forma (Check Point Research, 2025):

Dispositivos edge	Infostealers	Ambientes cloud
O aumento no uso de dispositivos IoT, wearables e hardware para trabalho remoto facilita a entrada de novos ataques, por serem alvos menos protegidos e mais suscetíveis à vigilância e exploração.	Esse tipo de malware, voltado ao roubo de informações confidenciais, está em alta, sendo uma das ameaças mais ativas da atualidade. Sua **facilidade de acesso**, impulsionada pela popularização do **Malware-as-a-Service (MaaS)**, e sua **distribuição criativa**, ampliaram seu uso na fase inicial de ataques subsequentes de ransomware ou APTs. (Lumma Stealer – PupkinStealer – FormBook)	A adoção crescente de soluções baseadas em infraestruturas de **cloud híbrida e multicloud** enfrenta desafios como o **gerenciamento de configurações** e a **segurança de APIs** — fatores que tornam esses ambientes vetores de entrada de fácil exploração.
Business Email Compromise (BEC)	**Negação de serviço (DDoS)**	**Man-in-the-Middle (MitM)**
Crescimento de ataques BEC impulsionados por IA Generativa. Com motivações financeiras, trata-se de uma das ameaças emergentes com maior impacto econômico. As táticas estão em constante evolução, com foco ampliado em setores críticos. (Cartier, 2025)	Padrões de **ataques automatizados e adaptados** em tempo real para evadir defesas. Coordenação mais eficiente de **botnets IoT**. Uso de ataques DoS/DDoS como **tática de distração** para encobrir outras ações maliciosas. Aumento de ataques contra **infraestruturas críticas**. Maior acessibilidade com a ascensão do modelo **DDoS-as-a-Service**. (Cloudflare – X)	**Exploração de vulnerabilidades em redes de nova geração,** com interceptação de tráfego criptografado em redes 5G e WiFi 6E. Aumento de ataques **a sistemas SCADA e dispositivos IoT industriais.** Crescimento de ataques MitM por meio de **aplicativos móveis.** Técnicas cada vez mais sofisticadas, muitas vezes combinadas com outros vetores e vinculadas a campanhas **APT**.

Tabela 5 | Vetores de entrada mais comuns utilizados no primeiro semestre de 2025.

Em resumo, mesmo com o avanço contínuo de novas técnicas de intrusão, os vetores de entrada tradicionais seguem sendo alarmantemente eficazes. O **phishing** permanece como o método mais recorrente para enganar usuários e obter acesso inicial, enquanto os **ataques remotos**, o uso de **credenciais comprometidas** e a **exploração de vulnerabilidades** — inclusive do tipo dia zero — seguem como portas de entrada predominantes, continuamente adaptadas e aprimoradas pelos invasores.

7.3 Inovação em ataques: novas técnicas e táticas desconhecidas

A seguir, são descritas algumas das técnicas mais disruptivas observadas, analisando seus mecanismos, campanhas associadas e o motivo pelo qual representam uma novidade em relação a táticas anteriores.

Instaladores de ferramentas de IA como vetor de distribuição de malware

Essa técnica baseia-se em camuflar malware dentro de instaladores falsos de ferramentas de IA. Os executáveis maliciosos simulam esses softwares populares, incluindo assistentes de produtividade e geradores de texto ou imagem, explorando assim o crescimento da IA Generativa.

- Foram observados em campanhas reais distribuindo ransomware (CyberLock), malware de controle remoto (Lucky_Gh0st) e a **nova ameaça identificada como Numero** (Cisco Talos Intelligence, 2025).
- A inovação dessa tática está no aproveitamento do interesse massivo por IA, combinando engenharia social com técnicas avançadas de empacotamento.
- Diferentemente de campanhas anteriores que utilizavam anexos ou scripts, essas amostras incorporam interfaces falsas de instalação para conferir legitimidade ao download.

Bypass de MFA por meio de proxies reversos e manipulação do protocolo OAuth

Essa técnica permite que hackers interceptem tokens de autenticação e assumam o controle de sessões protegidas por autenticação multifator (MFA). Baseia-se na criação de sites falsos que replicam o fluxo de login legítimo, redirecionando o tráfego via proxies reversos como o Evilginx2 (Google Cloud, 2025).

- Utilizada em campanhas reais pelo grupo de APT ColdRiver, direcionadas a ONGs, jornalistas e entidades governamentais do ociedente.
- O que torna essa tática especialmente perigosa é a sua **capacidade de falsificar completamente o fluxo de autenticação sem a necessidade de malware local**, além de extrair, em tempo real, tanto credenciais quanto tokens válidos.
- Diferentemente de ataques anteriores que dependiam de infecções no endpoint, essa técnica opera de forma 100% remota, apresenta maior dificuldade de rastreamento e mostra-se altamente efetiva com MFA.

Extensões de navegador com dupla funcionalidade: útil e maliciosa

Essas extensões oferecem funcionalidades legítimas (como edição de documentos ou análise de sites), mas realizam atividades ocultas, como exfiltração de cookies, keylogging ou conexão com servidores de comando remoto.

- A DomainTools identificou mais de 30 extensões ativamente utilizadas em campanhas reais na Chrome Web Store (DomainTools, 2025).
- Essa técnica é inovadora por utilizar ferramentas legítimas como cavalo de Troia, criando uma sensação real de confiança no usuário. Além disso, por estarem disponíveis em lojas oficiais, conseguem driblar controles de segurança comuns.
- Diferentemente de extensões maliciosas clássicas, essas funcionam perfeitamente, o que prolonga seu tempo de permanência e reduz a taxa de desinstalação.

"Crime-as-a-Service"

- Plataformas clandestinas passaram a oferecer hacking sob demanda e bomber services (SOCRadar, 2025), permitindo a execução de campanhas de DDoS, flooding de SMS ou spam em larga escala apenas com um registro, contando com dashboards no modelo SaaS, suporte técnico e segmentação por país.
- Detectadas em mercados de língua russa em maio, essas plataformas destacam-se pela facilidade de uso e implantação imediata, oferecendo até tutoriais para hackeers inexperientes (SOCRadar, 2025).
- A novidade está no nível de maturidade operacional: esses serviços permitem que agentes de baixo nível conduzam operações antes reservadas a APTs ou grupos com infraestrutura.
- Em comparação com fóruns como Genesis Market, essa nova geração oferece automação total, sem a necessidade de contato direto entre as partes.

Chaos RAT

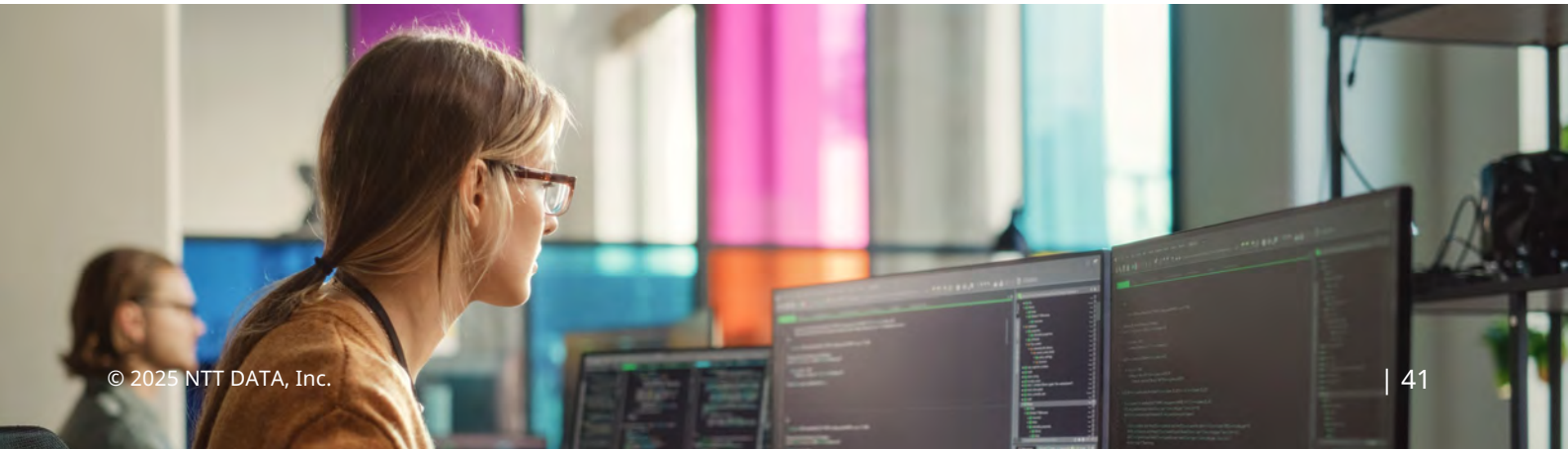
A nova versão do trojan Chaos RAT apresenta arquitetura modular, canal C2 com criptografia personalizada, instalação sigilosa e persistência em ambientes Windows, Linux e até dispositivos IoT (Acronis, 2025).

- Observado em maio em campanhas ainda não atribuídas, seu design permite operar como uma plataforma ofensiva completa, com distribuição sob demanda de payloads e execução remota de comandos em redes comprometidas.
- Destaca-se pela capacidade de operar sem detecção por semanas e por sua resistência a técnicas comuns de contenção, como listas de processos confiáveis.
- Em contraste com RATs tradicionais como njRAT ou Quasar, o Chaos funciona como um framework ofensivo com controle total do ambiente-alvo.

Além de todas as técnicas descritas nesta seção, o **Departamento de Cyber Threat Intelligence** observou uma tendência emergente no uso de malware multicomponente — uma tática que, embora não seja nova, vem **ganhando relevância em campanhas recentes**. Esse tipo de malware caracteriza-se por ser dividido em múltiplos fragmentos, entregues de forma sequencial por meio de canais de comunicação criptografados. Cada fragmento, isoladamente, é inofensivo, mas ao ser montado no dispositivo da vítima, forma a carga maliciosa completa.

Seu ressurgimento está ligado ao uso de canais alternativos de distribuição, como os serviços de mensagens criptografadas Telegram e Signal. O principal risco reside em sua capacidade de evasão e persistência furtiva, o que exige melhorias em sistemas de detecção baseados em comportamento e análise contextual.

A evolução técnica observada evidencia a importância de ajustar de forma contínua as capacidades defensivas para lidar com TTPs cada vez mais segmentadas, modulares e complexas de correlacionar em tempo real.



Vulnerabilidades

8. Vulnerabilidades

O primeiro semestre de 2025 confirmou a continuidade de uma ameaça persistente e sofisticada em torno das vulnerabilidades críticas, que continuam sendo uma das principais portas de entrada para ataques cibernéticos em escala global.

Ao longo desses seis meses, foi registrada uma alta atividade relacionada à identificação e exploração ativa de falhas críticas, com uma tendência significativa voltada a ambientes corporativos, infraestruturas industriais e dispositivos móveis.

Entre janeiro e junho, o **Departamento de Cyber Threat Intelligence da NTT DATA** monitorou cerca de 7.664 vulnerabilidades com CVE publicado, das quais 285 foram classificadas como críticas e ao menos 105 foram exploradas ativamente em ambientes reais *(in the wild)*. Esse número evidencia a agilidade dos hackers em explorar vulnerabilidades recém-divulgadas e reforça a urgência de aprimorar os prazos de aplicação de patches e a supervisão contínua dos ambientes.

A seguir, é possível ver uma análise mensal das vulnerabilidades críticas **mais relevantes do período**, considerando seu impacto técnico, exploração em cenários reais e efeito sobre setores críticos.

• Janeiro:

Em janeiro de 2025, foram identificadas **517 vulnerabilidades**, das quais **22 foram classificadas como críticas** e **20 foram exploradas ativamente**. Essas vulnerabilidades marcaram um início de ano com foco em plataformas de rede e ambientes Linux, notáveis por sua facilidade de exploração e pela rápida integração em ferramentas de ataque automatizadas.

Vulnerabilidades-chave identificadas:

- **CVE-2024-12084 (rsync):** Heap overflow amplamente explorável em ambientes Linux.
- **CVE-2025-0060/0061 (SAP BusinessObjects):** Execução remota de código (RCE) em plataformas corporativas de BI.
- **CVE-2024-40891/40890 (Zyxel):** Injeção em dispositivos de rede, utilizadas por botnets.

Principais impactos:

- Comprometimento de infraestruturas de rede.
- Roubo de dados e acesso não autorizado a sistemas corporativos estratégicos.
- O predomínio de ataques automatizados e a velocidade com que essas vulnerabilidades foram incorporadas a kits de exploração reforçam a necessidade de segmentação de rede e monitoramento contínuo.

• Fevereiro:

Em fevereiro de 2025, foram identificadas **1.558 vulnerabilidades**, das quais **33 foram** classificadas como **críticas** e **16 foram exploradas ativamente** — um aumento significativo em relação ao mês anterior. Essas vulnerabilidades afetaram principalmente infraestruturas de rede e ambientes cloud-native, refletindo uma mudança para alvos mais dinâmicos e difíceis de proteger.

Vulnerabilidades-chave identificadas:

- **CVE-2024-11218 (containers/Red Hat):** Vazamento de contêiner com exploração ativa confirmada.
- **CVE-2025-0890 (Zyxel):** Nova falha crítica em roteadores amplamente distribuídos.
- CVE-2025-21198 **(Microsoft Exchange):** Falha crítica em serviços de e-mail corporativo com exploração ativa.
- **CVE-2024-45569 (Qualcomm):** Vulnerabilidade em *chipsets* Exynos, explorada em dispositivos móveis.

Principais impactos:

- Acesso remoto a sistemas corporativos, controle de dispositivos IoT, vazamento de informações confidenciais em ambientes de usuário final.
- A exploração ativa de múltiplas falhas em infraestruturas amplamente implementadas evidencia o desafio contínuo de manter uma postura de segurança robusta e consistente.

• Março:

Em março de 2025, foram identificadas **1.032 vulnerabilidades**, das quais **43 foram** classificadas como **críticas** e **24 exploradas ativamente**. O mês marcou um aumento na exploração de falhas em produtos amplamente utilizados por empresas, incluindo sistemas de transferência de arquivos e ferramentas de desenvolvimento Web, com divulgação quase imediata de provas de conceito (em inglês: Proof of Concept - PoC), elevando o risco de exploração.

Vulnerabilidades-chave identificadas:

- **CVE-2023-13124 (SAP NetWeaver Visual Composer):** Vulnerabilidade que permite a carga não autorizada de binários maliciosos em ambientes SAP via componente Metadata Uploader. Sua exploração foi documentada em campanhas direcionadas a organizações altamente dependentes dessa plataforma, comprometendo a integridade e a disponibilidade.
- **CVE-2023-3161 (CrushFTP):** Bypass de autenticação em versões <11.3.1, explorado ativamente. Permite acesso não autenticado por falha na validação de HMAC, facilitando o controle total do sistema.
  Foi associado a campanhas de ransomware contra instituições financeiras e serviços gerenciados.
- **CVE-2025-0603 (Aviatrix Controller):** Execução remota de comandos via manipulação de parâmetros da API (*cloud_type*). Sua exploração ativa representa um risco elevado em ambientes multicloud e plataformas híbridas utilizadas em operações críticas.

Principais impactos:

- Comprometimento de servidores expostos.
- Persistência nos sistemas e escalada de privilégios.

• Abril:

Em abril foram identificadas **1.381 vulnerabilidades**, sendo **57 classificadas como críticas** e 13 exploradas ativamente. O mês se destacou pela diversidade de produtos afetados e pela exploração focada em dispositivos de edge e ambientes de microsserviços.

Vulnerabilidades-chave identificadas:

- **CVE-2025-22457 (Ivanti EPMM):** Acesso remoto não autenticado em plataformas móveis.
- **CVE-2025-30215 (NATS.io):** Execução remota de código (RCE) em *middleware* de microsserviços.
- **CVE-2024-51138/51139 (DrayTek):** Vulnerabilidade em roteadores amplamente utilizados.

- ## Maio:

Em maio de 2025, foram identificadas **1.549 vulnerabilidades**, das quais **44 foram classificadas como críticas** e **17 foram exploradas ativamente.** As vulnerabilidades mais relevantes envolveram produtos essenciais de segurança e plataformas móveis, reforçando a tendência de ataques altamente direcionados e persistentes.

Vulnerabilidades-chave identificadas:

- **CVE-2025-40595 (SonicWall):** *Exploit* ativo contra *firewalls* e dispositivos edge.
- **CVE-2025-22252 (Fortinet):** Execução remota de código (RCE) sem autenticação em soluções amplamente implantadas.
- **CVE-2025-31219 (Apple): Dia zero** em sistemas Apple**.**
- **CVE-2025-0203 (Ivanti Connect Secure/Policy Secure):** Buffer overflow em *gateways* ZTA amplamente implementados, permitindo execução de código arbitrário sem autenticação. Sua exploração tem sido associada a grupos de ransomware com alvos nos setores governamentais e de telecomunicações, devido ao caráter crítico do acesso que proporciona.

Principais impactos:

- Acesso inicial aos sistemas.
- Persistência em redes corporativas.
- Exposição de dados de usuários móveis.

- ## Junho:

Foram identificadas **1.426 vulnerabilidades, das quais 81 são críticas e pelo menos 17 foram exploradas ativamente**.
Junho apresentou uma atividade significativa em dispositivos VoIP, servidores Linux e dispositivos móveis, indicando uma continuidade na preferência dos ataques por ambientes críticos e com alta superfície de exposição.

Vulnerabilidades-chave identificadas:

- **CVE-2025-30507 (CyberData SIP):** Execução remota de código (RCE) em dispositivos VoIP industriais.
- **CVE-2025-49087 (Red Hat/Perl-FCGI):** RCE em ambientes *Web baseados* em Linux**.**
- **CVE-2025-23107 (Samsung Exynos):** Exploradas em ataques direcionados a dispositivos móveis.

Principais impactos:

- Ameaças à infraestrutura crítica de voz, servidores *Web* e ecossistemas Android/iOS. Reflete-se a necessidade de visibilidade total sobre os dispositivos conectados, considerando que a maioria dos usuários desconhece a existência dessas vulnerabilidades e os riscos potenciais associados.

Tendências de exploração de vulnerabilidade (S2 2024 - S1 2025)

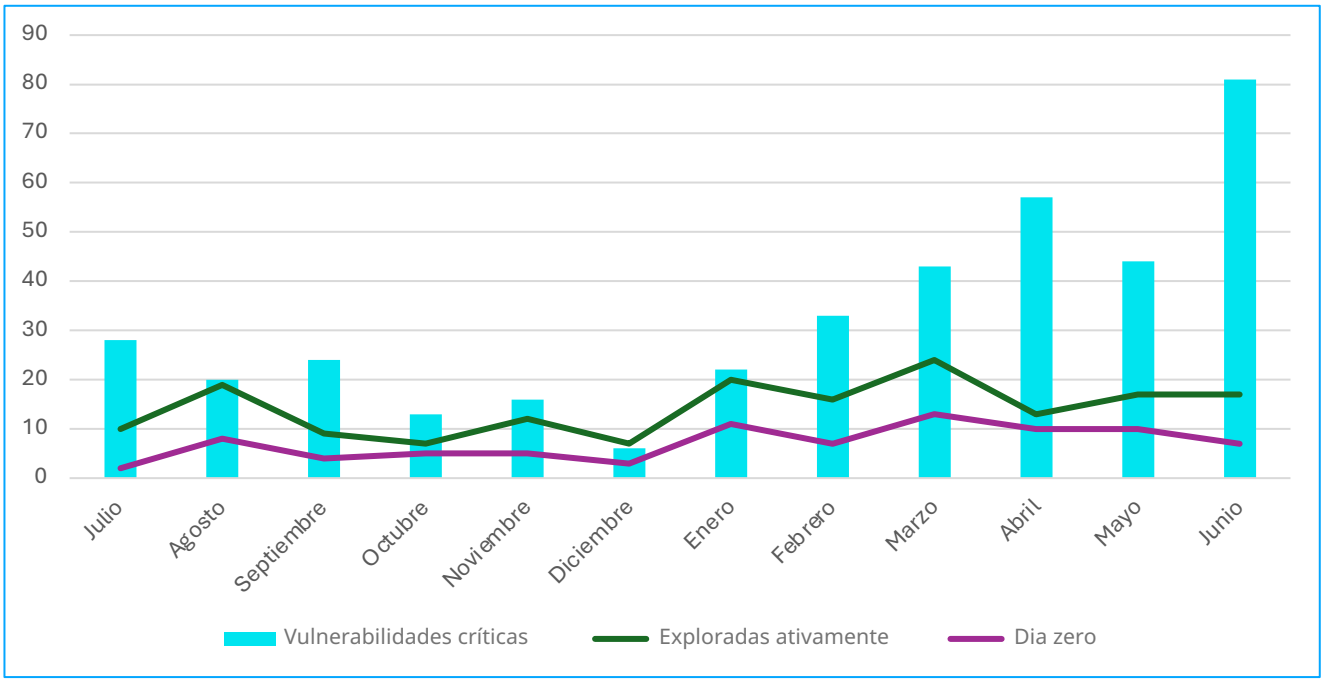


Figura 14 | Comparação entre a exploração e a presença de vulnerabilidades críticas no segundo semestre de 2024 em relação ao primeiro semestre de 2025.

Tendências de exploração dessas vulnerabilidades:

- Durante o primeiro semestre de 2025, consolidou-se uma **estratégia por parte dos agentes de ameaças** baseada na **exploração imediata de vulnerabilidades críticas após sua divulgação**, especialmente aquelas com PoCs públicas. Em contraste com o segundo semestre de 2024, observou-se um aumento considerável na taxa de exploração ativa em relação ao número total de falhas críticas divulgadas.

A preferência operacional dos cibercriminosos concentrou-se em:

- Sistemas expostos à rede e **dispositivos perimetrais**, como roteadores, firewalls e soluções de acesso remoto.
- **Ambientes OT e dispositivos industriais**, nos quais as falhas causam impactos mais disruptivos e críticos para a continuidade das operações.
- **Infraestruturas cloud-native e contêineres**, explorando a complexidade de gestão para escalar privilégios e manter a persistência.
- **Plataformas móveis e chipsets** populares, como Exynos e Apple SoC, cada vez mais visados pela função que desempenham na gestão de identidades e no acesso a dados.

Além disso, reforça-se a hipótese de uma **maior sofisticação por parte dos grupos de ransomware e APTs**, que estão alinhando suas campanhas com os calendários de divulgação de vulnerabilidades, reduzindo o tempo de preparação técnica com o uso de ferramentas automatizadas de exploração.

Essa mudança tática evidencia uma necessidade crítica de reduzir o tempo médio de aplicação de patches, implementar medidas rápidas de mitigação (como listas de controle de acesso ou segmentação de rede) e reforçar a inteligência proativa sobre ameaças — especialmente nos setores industrial, de telecomunicações e de serviços críticos.

Perspectiva para o futuro

9. O que esperar do segundo semestre de 2025?

O segundo semestre de 2025 projeta-se como uma continuação lógica — e possivelmente intensificada — das atividades observadas na primeira metade do ano. Durante o primeiro semestre, o ecossistema de ameaças caracterizou-se por um alto volume de vulnerabilidades (incluindo várias de dia zero) e por sua exploração ativa por agentes de ameaças em campanhas reais, o que evidencia a redução do intervalo entre o período de divulgação e o uso ofensivo dessas falhas.

No cenário dos agentes de ameaça, o semestre foi caracterizado por alta atividade dos grupos **RansomHub** e **Cl0p**, líderes incontestáveis de ransomware em 2025 até o momento. Embora alguns grupos como o **LockBit** tenham reduzido sua visibilidade, outros, como **Akira** e **Qilin**, mantiveram-se firmemente entre os cinco principais em número de campanhas registradas, consolidando um modelo de negócio altamente profissionalizado. A expectativa é de que esses grupos — ou novas dissidências originadas deles — permaneçam ativos e **aumentem seu volume operacional à medida que se aproximam períodos de maior pressão fiscal e orçamentária no ambiente corporativo**.

Paralelamente, o primeiro semestre também foi marcado por um fenômeno emergente: **a fragmentação do ecossistema cibercriminoso**. Novas coalizões entre grupos hacktivistas surgiram, muitas vezes formadas de forma oportunista ou ideológica, no contexto da crescente polarização geopolítica — **especialmente em torno do conflito entre Israel e Gaza**.

Essa polarização vem transformando organismos governamentais ocidentais, infraestruturas críticas de países da OTAN e entidades ligadas a interesses israelenses em **alvos prioritários**.
A tendência é que esse cenário se mantenha — ou até se agrave — no segundo semestre.

Por outro lado, o mundo underground também passa por uma transformação significativa.

As recentes detenções, **a desativação do BreachForums** e **o colapso do maior mercado de drogas da dark web, o Archetype**, resultaram em um cenário de instabilidade que vem redefinindo o equilíbrio de poder entre agentes e plataformas. Observa-se um **efeito rebote**, em que os **impactos nas camadas profundas do cibercrime começam a se refletir na superfície:** o surgimento de grupos dedicados a extorquir outros grupos, denunciar ex-parceiros ou interferir em campanhas rivais pode gerar um aumento nos vazamentos internos de informação, campanhas de doxing e disputas por visibilidade em fóruns undergrounds.

A isso se soma uma crescente profissionalização do crime cibernético. A disponibilidade de ferramentas acessíveis, ambientes de colaboração técnica e uma economia paralela que vê no crime digital uma forma de sustento estão impulsionando o surgimento de novos grupos operacionais a cada mês. Esse movimento, somado ao fato de que muitos desses agentes já atuam com lógicas empresariais, permite prever um **aumento no volume e no grau técnico dos ataques no segundo semestre**.

Diante desse cenário, torna-se essencial reforçar os mecanismos de detecção precoce de vulnerabilidades e aplicar modelos de priorização adaptativa, que reduzam o tempo entre a identificação da falha e sua mitigação efetiva. Também será fundamental monitorar o cenário de ameaças não apenas em sua expressão técnica (TTPs), mas também em sua dimensão social e geopolítica — para antecipar a evolução de campanhas impulsionadas por polarização ideológica ou por conflitos entre grupos criminosos.

O monitoramento constante do mundo underground e da evolução do seu ecossistema também será crucial: os eventos nessas camadas nos próximos meses podem ser o prenúncio de novas campanhas, ferramentas ou vazamentos massivos com impacto direto sobre o tecido empresarial e governamental global.

Referências

- Cartier, M. (3 de março de 2025). *Business Email Compromise Statistics 2025*. Hoxhunt. https://hoxhunt.com/blog/business-email-compromise-statistics
- CERT-EU. (2025). *Threat Landscape Q1 & Q2 2025 Reports*[RG1] [SS2] . https://cert.europa.eu/publications/threat-intelligence/2025
- Check Point Research. (14 de janeiro de 2025) *5 Key Cyber Security Trends for 2025*. Check Point. https://blog.checkpoint.com/research/5-key-cyber-security-trends-for-2025
- CISA. (20 de novembro de 2024). *#StopRansomware: BianLian Ransomware Group.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a
- CISA. (30 de abril de 2025). *#StopRansomware: Rhysida Ransomware*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
- Cloudforce One. (21 de maio de 2025). *Cloudflare participates in global operation to disrupt Lumma Stealer*. Cloudflare. https://www.cloudflare.com/es-es/threat-intelligence/research/report/cloudflare-participates-in-joint-operation-to-disrupt-lumma-stealer/
- CrowdStrike. (2025). *CrowdStrike Global Threat Report 2025*. https://www.crowdstrike.com/global-threat-report/
- Cyber News Centre Team. (4 de julho de 2025). *The State of APAC Cybersecurity: CNC Intelligence Overwatch Report - July 2025*. Cyber News Centre. https://www.cybernewscentre.com/the-state-of-apac-cybersecurity-cnc-intelligence-overwatch-report-july-2025/
- Cybersecurity Ventures. (2025). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybersecurity Ventures. https://cybersecurityventures.com/cyberwarfare-report-intrusion/[RG3]
- CYFIRMA. (9 de maio de 2025). *PupkinStealer : A .NET-Based Info-Stealer*. CYFIRMA. https://www.cyfirma.com/research/pupkinstealer-a-net-based-info-stealer/
- DarkFeed. (2025). *Here's a look at the most active ransomware groups of 2025* [Publicações de X]. X. https://x.com/ido_cohen2
- DarkFeed. (2025). *New Ransomware Group* [Publicações de X]. X. https://x.com/ido_cohen2
- Department for Science, Innovation and Technology, Home Office and Feryal Clark MP. (10 de abril de 2025). *Cyber Security Breaches Survey 2025*. Gov.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/
- Yoachimik, O. y Pacheco, J. (27 de abril de 2025). *Targeted by 20.5 million DDoS attacks, up 358% year-over-year: Cloudflare's 2025 Q1 DDoS Threat Report*. Cloudflare. https://blog.cloudflare.com/es-la/ddos-threat-report-for-2025-q1/

- FBI. (6 de março de 2025) *Mail Scam Targeting Corporate Executives Claims Ties to Ransomware.* Internet Crime Complaint Center. https://www.ic3.gov/psa/2025/psa250306-2#:~:text=March%206%2C%202025-,Mail%20Scam%20Targeting%20Corporate%20Executives%20Claims%20Ties%20to%20Ransomware,come%20from%20a%20ransomware%20group.
- Federal Ministry of the Interior. (2025). *Protecting the 2025 Bundestag elections from hybrid threats and disinformation*. Federal Ministry of the Interior. https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation-election/disinformation-election-artikel.html
- Fox, J. (23 de dezembro de 2024) *Top Cybersecurity Statistics 2025*. Cobalt. https://www.cobalt.io/blog/top-cybersecurity-statistics-2025/
- Franceschi-Bicchierai, L. (23 de maio de 2025). *Mysterious hacking group Careto was run by the Spanish government, sources say*. TechCrunch. https://techcrunch.com/2025/05/23/mysterious-hacking-group-careto-was-run-by-the-spanish-government-sources-say/
- Fry, C. (2025). *The Cost of a Cyber Attack in 2025 on SMEs*. Robinson https://www.robison.co.uk/cost-of-a-cyber-attack-2025/
- Gatlan, S. (27 de maio de 2025). *Russian Laundry Bear cyberspies linked to Dutch Police hack*. BleepingComputer. https://www.bleepingcomputer.com/news/security/russian-void-blizzard-cyberspies-linked-to-dutch-police-breach/
- Group-IB. (2025). *Hi-Tech Crime Trends Report 2025*. https://www.group-ib.com/landing/high-tech-crime-trends-2025/
- Hitachi Cyber. (17 de janeiro de 2025). *Cyber Threat Landscape in 2025: Trends and Challenges*. Hitachi. https://hitachicyber.com/cyber-threat-landscape-in-2025-trends-and-challenges/
- Identity Defined Security Alliance. (2025). *2025 Identity Security Landscape Report*. https://www.idsalliance.org
- KrakenLabs. (2025). *Threat Context Monthly Reports (January–May 2025)*. Outpost24. https://outpost24.com/blog
- Márquez, J. (24 de maio de 2025). *El misterioso grupo de hackers Careto se encontraba detrás de un agente inesperado: el Gobierno de España*. Xataka. https://www.xataka.com/seguridad/misterioso-grupo-hackers-careto-se-encontraba-agente-inesperado-gobierno-espana-techcrunch
- Zang, X. (22 de abril de 2025). Infostealer Malware FormBook Spread via Phishing Campaign – Part I. Fortinet. https://www.fortinet.com/blog/threat-research/infostealer-malware-formbook-spread-via-phishing-campaign-part-i

- Microsoft Threat Intelligence. (27 de maio de 2025). *New Russia-affiliated actor Void Blizzard targets critical sectors for espionage*. Microsoft. https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/
- Microsoft Threat Intelligence, Microsoft Digital Crimes Unit and Microsoft Security Experts [MTI, MDC & MSE]. (21 de maio de 2025). *Lumma Stealer: Breaking down the delivery techniques and capabilities of a prolific infostealer*. Microsoft. https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/
- Miliefsky, G. (13 de março de 2025). *The true cost of cybercrime: Why global damages could reach $1.2 to $1.5 trillion by end of 2025*. Cyber Defense Magazine. https://www.cyberdefensemagazine.com
- Newman, L.H. (11 de março de 2025). *What Really Happened With the DDoS Attacks That Took Down X*. Wired. https://www.wired.com/story/x-ddos-attack-march-2025/
- Orange Cyberdefense. (2025). *Sector 16 Group*. Orange. https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/Sector16/Sector16Group.pdf
- Stamford, C. (28 de agosto de 2024). *Gartner Forecasts Global Information Security Spending to Grow 15% in 2025*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025
- SOCRadar. (22 de maio de 2025). *Top 10 Deep Web and Dark Web Forums*. https://socradar.io/top-10-deep-web-and-dark-web-forums/
- Tamzid, A. (23 de maio de 2025). *Cybercrime statistics and financial impact*. Bright Defense. https://www.brightdefense.com/resources/cybercrime-statistics/
- Toulas, B. (1 de maio de 2025). *Pro-Russia hacktivists bombard Dutch public orgs with DDoS attacks.* BleepingComputer. https://www.bleepingcomputer.com/news/security/pro-russia-hacktivists-bombard-dutch-public-orgs-with-ddos-attacks/
- World Economic Forum. (13 de janeiro de 2025). *Global Cybersecurity Outlook 2025*. https://www.weforum.org/reports/global-cybersecurity-outlook-2025
- Yilmaz, E. y Yildirim, E. (10 de maio de 2025). *Cyber threats to cost $10.5T by 2025 as cybersecurity investments surge*. AA News. https://www.aa.com.tr/en/science-technology/cyber-threats-to-cost-105t-by-2025-as-cybersecurity-investments-surge/3563268


NTT DATA