Edição 114 | Maio de 2026

NTT DATA

Radar

A revista de cibersegurança

Além do algoritmo: a reinvenção da CTI diante da democratização dos ataques

Por Alexis Martín García

Como profissionais de inteligência, costumamos dizer que nosso trabalho consiste basicamente em reduzir a incerteza para facilitar a tomada de decisão. No entanto, no último ciclo, essa incerteza não apenas mudou, como também passou a evoluir em um ritmo acelerado que desafia nossos modelos tradicionais de defesa. Não estamos mais enfrentando apenas grupos estatais com recursos ilimitados ou o oportunismo do cibercrime convencional; estamos diante de uma democratização da capacidade ofensiva que redefiniu as regras de atuação que conhecíamos até poucos meses atrás.

Na prática, a barreira de entrada para o adversário desmoronou. A ascensão da automação ofensiva e o uso de modelos de linguagem aplicados ao desenvolvimento de *malware* transformaram a economia dos ataques: hoje, o custo de execução para o atacante é próximo de zero, enquanto o custo de defesa para as organizações continua sendo linear e crescente. Agora, qualquer agente com uma intenção clara pode gerar *payloads* polimórficos capazes de contornar soluções de *endpoint* baseadas em assinaturas ou desenvolver campanhas de engenharia social tão precisas que deixam o fator humano totalmente despreparado. Passamos da detecção manual de ataques para o gerenciamento de milhares de alertas automatizados. Esses alertas, impulsionados por algoritmos persistentes, buscam continuamente aquele único ativo esquecido na superfície de exposição ou uma vulnerabilidade de dia zero recém-divulgada.

Nesse cenário de saturação, os indicadores de comprometimento (IoCs) tradicionais — aqueles IPs, domínios e *hashes* que ontem eram nossa base operacional — tornaram-se ativos voláteis. Sua vida útil no ecossistema atual é tão curta que, quando chegam às nossas listas de bloqueio, o adversário já rotacionou sua infraestrutura de comando e controle (C2). Por isso, o foco da inteligência moderna precisa se deslocar inevitavelmente para a análise das **TTPs (Táticas, Técnicas e Procedimentos)**. Entender o modus operandi e os padrões de comportamento deixou de ser uma opção acadêmica e passou a ser a única forma real de antecipar um vetor de acesso antes que ele se transforme em um incidente de impacto sistêmico.

No entanto, essa corrida armamentista tecnológica não é unidirecional. Como defensores, também aumentamos nossa capacidade de resposta por meio da mesma tecnologia que nos desafia. Pela primeira vez, a integração da inteligência artificial e do machine learning ao fluxo de Inteligência de Ameaças Cibernéticas (CTI) está nos permitindo processar telemetria e fontes de dados abertas (OSINT) em uma escala que, até recentemente, era puramente teórica.

Estamos conseguindo conectar pontos dispersos entre um evento de rede aparentemente trivial e uma campanha direcionada que está apenas na fase de reconhecimento. A capacidade de filtrar o ruído e priorizar as ameaças com base no risco real é o que permite que nossas equipes de resposta não sejam vencidas pela fadiga de alertas.

É justamente nesse ponto, na detecção de padrões invisíveis e na orquestração de inteligência, que nossa disciplina se torna o ativo estratégico mais crítico. Nas páginas desta edição, faremos uma jornada por essa tridimensionalidade que define o CTI atual: desde o peso da realidade global e as tensões que ditam os objetivos estratégicos até a sofisticação técnica que possibilita o comprometimento inicial, encerrando com as tendências que estão redefinindo nosso roteiro operacional. Não se trata apenas de coletar dados, mas de transformá-los em conhecimento acionável que permita à organização estar sempre um passo à frente.

No fim das contas, embora a tecnologia forneça a velocidade e a força bruta necessárias para lidar com esse novo cenário, o **julgamento do analista,** aquela capacidade única de interpretar a intenção, o contexto geopolítico e a psicologia por trás dos dados, continua sendo nossa última e mais sólida linha de defesa. A IA pode automatizar a busca, mas só o analista humano pode dar sentido a ela.

Sejam bem-vindos a uma análise aprofundada do cenário atual, em que a inteligência se tornou, mais do que nunca, o fator que separa a resiliência do comprometimento.

Alexis Martín García
Gerente de Projetos do Cyber Threat Intelligence & Hacking Center

Quando a confiança se torna o perímetro: anatomia de um mês de ataques

Cibercrônica por Eduardo Gil Ciruelos

O período de meados de março a meados de abril de 2026 não trouxe um ataque histórico, mas sim algo mais incômodo: uma série de incidentes que, analisados em conjunto, retratam com precisão o cenário previsto no artigo anterior. A barreira de entrada do adversário desmoronou, a automação acelerou os ciclos e, ao mesmo tempo, as organizações descobriram que seus perímetros não estão mais onde pensavam. Esta é a crônica dessas semanas.

Tudo começou, ou pelo menos ficou evidente, no dia **11 de março**. Às cinco da manhã (UTC), colaboradores da **Stryker** em 79 países viram seus dispositivos desligarem ao mesmo tempo. Um **grupo ligado ao Irã** havia comprometido uma única conta administrativa do **Microsoft Intune**, criado um novo administrador global e usado a ferramenta legítima para apagar duzentos mil computadores. Não havia *malware*, não havia *ransomware*, não havia nenhum binário para analisar. O sistema não detectou um ataque porque, tecnicamente, não estava tendo um ataque: o que havia era um administrador fazendo o seu trabalho.

Poucos dias depois, as atenções se voltaram para o **Crunchyroll**, embora a origem do incidente estivesse muito mais distante. Um agente de suporte da **Telus International**, que estava trabalhando em um notebook na Índia, caiu em um e-mail de *phishing*. As credenciais capturadas permitiam acessar, por meio do SSO da Okta, o Zendesk, o Slack, o Workspace e o Jira. Em menos de 24 horas**, 100 GB de dados e quase sete milhões de endereços de e-mail foram exfiltrados**. Quando a equipe de segurança conseguiu revogar o acesso, a operação já havia terminado. O perímetro atacado não ficava em Tóquio nem na Califórnia, mas alocado em um contrato de terceirização.

Enquanto esses casos viravam notícias, outro caso veio à tona com atraso. Em março, a **Marquis Software Solutions,** que presta serviços a centenas de instituições financeiras nos Estados Unidos, divulgou um incidente ocorrido sete meses antes. Um *firewall da* **SonicWall** comprometido havia permitido a implantação de um *ransomware* que acabou afetando 700 mil pessoas e 74 bancos. Por mais de seis meses, as vítimas não sabiam que precisavam se proteger.

Quase ao mesmo tempo, a **Universidade Sapienza de Roma**, com seus 120 mil alunos, acordou sem serviços digitais. Provas, e-mails, trâmites administrativos. Tudo ficou paralisado por vários dias. Não houve reivindicações imediatas nem grandes exigências públicas; apenas a constatação de que bastava uma única porta comprometida para paralisar uma instituição inteira.

A primeira semana de abril trouxe uma reviravolta inesperada. No dia 7 de março, o plugin **Smart Slider 3 Pro,** presente em mais de 800 mil instalações do **WordPress**, lançou uma nova versão por meio do seu canal oficial. Na verdade, por seis horas, essa versão foi um backdoor completo, desenvolvido por um invasor que havia assumido o controle da infraestrutura de atualizações. Cada site que fez a atualização nesse período se transformou automaticamente em um ponto de acesso remoto.

Dois dias depois, a situação se repetiu com outra assinatura. No dia **9 de abril**, os links oficiais de download do **CPU-Z** e do **HWMonitor**, no site da CPUID, começaram a redirecionar para domínios maliciosos. A alteração durou cerca de 19 horas. Os binários assinados ainda eram legítimos, mas o site que os distribuía não era mais. Mesmo o usuário que fazia exatamente o que deveria, ou seja, atualização do site original, acabava sendo afetado.

Naqueles mesmos dias, o foco se voltou para o setor público latino-americano. No **México**, o vazamento no sistema **Safe Smart Port** da Secretaria da Marinha expôs quase 40 GB de informações sobre 640 mil trabalhadores portuários, incluindo dados biométricos, tipo sanguíneo e local de trabalho. A violação não comprometia apenas dados pessoais, mas também a rastreabilidade operacional de uma infraestrutura crítica de logística.

Na Argentina, o grupo **Chronus Team** havia anunciado dias antes, nas redes sociais, que iria atacar. E atacou. Ocorreram 28 vazamentos simultâneos contra órgãos governamentais nacionais e provinciais, órgãos de saúde, finanças e forças de segurança. Mesmo com o aviso prévio não houve nenhuma resposta coordenada visível.

O final do mês foi marcado por incidentes no setor privado. A **Adobe** confirmou a exposição de 13 milhões de tickets de suporte, 15 mil registros de colaboradores, documentos internos e envios completos do seu programa de recompensas por *bugs*. O risco não estava em cada peça isolada, mas no que podia ser reconstruído ao correlacioná-las.

Em **11 de abril**, o grupo **ShinyHunters** assumiu a responsabilidade por duas operações quase consecutivas: na Rockstar Games, o comprometimento de métricas de instâncias do Snowflake por meio da integração com o Anodot; e na Abrigo, a exfiltração de mais de 1,7 milhão de registros do Salesforce. Em nenhum dos dois casos o acesso partiu do alvo final, mas de um serviço conectado.

Considerando o mês como um todo, o que conecta todos esses incidentes não é um fator técnico. Nenhum deles exigiu habilidades extraordinárias. O que os une é a maneira como cada agente de ameaça encontrou uma relação de confiança, uma credencial, um provedor, uma atualização assinada ou uma integração SaaS que a organização havia deixado de questionar há muito tempo. Nenhum deles arrombou uma porta. Todos tinham a chave.

Eduardo Gil Ciruelos
Analista júnior de Inteligência de Ameaças Cibernéticas (CTI)

Quando o conflito não é declarado: o ciberespaço como ferramenta de poder geopolítico

Artigo por Sandra Somastre

O ciberespaço se consolidou como um espaço de competição geopolítica no qual os Estados projetam poder sem a necessidade de confronto direto. Nesse cenário, as ciberoperações não são eventos isolados, mas fazem parte de estratégias mais amplas voltadas à persistência, à influência e à obtenção de vantagem. Para entender as ameaças atuais, é preciso ir além dos dados técnicos e analisar o contexto estratégico em que elas se desenvolvem.

No contexto geopolítico atual, há uma competição constante entre Estados com interesses estratégicos cada vez mais bem definidos.

Diferentemente dos modelos tradicionais de confronto, os conflitos não se desenrolam mais apenas no âmbito físico, mas se estendem a outros espaços onde a pressão pode ser exercida de forma contínua e com menor risco de escalada.

Nesse contexto, o ciberespaço se consolidou como um vetor essencial para a projeção de poder. Não se trata de um ambiente autônomo, mas sim de um espaço onde muitas das dinâmicas geopolíticas atuais se definem: pressão econômica, rivalidade tecnológica, operações de influência e obtenção de inteligência.

O ciberespaço não acompanha mais o conflito: ele faz parte dele desde a sua concepção.

Um ambiente de competição persistente

O equilíbrio internacional evoluiu para um modelo mais fragmentado, no qual vários atores estatais competem entre si sem uma separação clara entre períodos de paz e de conflito.

Essa situação favorece uma atividade contínua, na qual as operações não buscam necessariamente um impacto imediato, mas sim se posicionar de forma estratégica. Essa lógica se aplica de forma ideal às atividades no ciberespaço, o que permite agir de forma contínua sem precisar recorrer a métodos tradicionais de confronto.

Conflitos como a guerra entre a Rússia e a Ucrânia, as tensões no Oriente Médio ou a competição tecnológica entre a China e o Ocidente refletem essa evolução. Em todos esses casos, o componente cibernético é parte estrutural do conflito, complementando outras formas de pressão.

Além disso, esse modelo apresenta uma característica fundamental**:** a **assincronia.**

Enquanto os conflitos tradicionais têm fases mais ou menos identificáveis, a atividade no ciberespaço não para. Mesmo em momentos de aparente estabilidade, as operações continuam, acumulando acesso, informações e capacidade de influência.

O ciberespaço como ferramenta de pressão estratégica

No contexto atual, o valor do ciberespaço se baseia na sua capacidade de operar no que é conhecido **como zonas cinzentas do conflito**. Em outras palavras, ele permite realizar ações que causam impacto sem ultrapassar limites que exijam uma resposta direta, o que o torna particularmente eficaz em um cenário geopolítico no qual a escalada aberta tem um custo elevado.

Essa lógica não fica apenas na teoria, mas se manifesta diretamente em cenários internacionais importantes, onde essa atividade acompanha, intensifica e até previne conflitos.

Nesse sentido, é possível identificar diferentes padrões de uso do ciberespaço de acordo com o contexto geopolítico:

- **Rússia – Ucrânia:** A atividade cibernética foi incorporada de forma estrutural ao conflito, combinando operações de influência, campanhas direcionadas a países terceiros e a interrupção de serviços. O ciberespaço permite ampliar o alcance do conflito sem a necessidade de uma escalada tradicional, causando impacto em aliados, cadeias de suprimentos e na opinião pública.
- **Oriente Médio (Israel e atores regionais):** Nesse cenário, o ciberespaço atua como um meio de confronto indireto. Campanhas de desinformação, vazamentos e ataques coordenados se combinam a operações de hacktivismo alinhadas ideologicamente. O objetivo não é apenas técnico, mas também influenciar a percepção pública e aumentar a pressão em momentos de tensão.

- **China – Ocidente:** As ações se concentram em campanhas de ciberespionagem direcionadas a setores críticos, como tecnologia, energia ou manufatura avançada. Essa abordagem reflete uma estratégia de longo prazo, na qual a obtenção de informações e o domínio tecnológico são prioridades em relação à uma disrupção imediata.

- **Estados Unidos:** Seu papel na economia digital e seu peso geopolítico. A forma como o ciberespaço é usado para influenciar diretamente áreas que determinam a vantagem global, desde a estabilidade econômica até a inovação, fica evidente pela concentração de atividades em setores estratégicos.

- **Irã e Coreia do Norte:** Esses atores combinam operações de influência, espionagem e atividades voltadas à obtenção de recursos. O ciberespaço se torna uma ferramenta para superar restrições estruturais, especialmente no setor econômico, e para expandir a capacidade além das fronteiras.

Em resumo, esses cenários mostram uma tendência clara: as operações cibernéticas não são eventos isolados, mas fazem parte de **estratégias contínuas destinadas a exercer influência, desgastar e colocar os atores em um ambiente de competição constante**. O impacto não é medido apenas em termos técnicos, mas também pela capacidade de se integrar a processos mais amplos e de produzir efeitos cumulativos ao longo do tempo.

A evolução técnica como reflexo do contexto

O aumento de técnicas baseadas na exploração de identidades, no uso de ferramentas legítimas ou na redução de *malwares* convencionais reflete não apenas uma evolução operacional, mas também uma adaptação ao cenário geopolítico. Em um contexto em que a atribuição tem efeitos estratégicos, a capacidade de operar de forma discreta se torna um fator diferenciador.

Isso explica por que muitas campanhas atuais priorizam o acesso silencioso em vez da exploração visível. O objetivo não é apenas entrar, mas permanecer.

Nesse sentido, a técnica deixa de ser um objetivo em si e passa a ser um meio a serviço de uma estratégia mais ampla. A escolha de ferramentas, vetores e objetivos se baseia em uma lógica que vai além do aspecto técnico.

Um ecossistema de atores cada vez mais complexo

O cenário atual também se caracteriza por uma crescente conexão entre atores estatais e não estatais.

A colaboração entre grupos de hacktivismo, cibercriminosos e estruturas associadas a Estados cria um ecossistema mais adaptável, no qual as capacidades são compartilhadas e as motivações se confundem. Esse modelo não apenas dificulta a atribuição, mas também permite que os Estados mantenham uma margem de ambiguidade quanto ao seu real envolvimento.

Além disso, a disseminação de ferramentas acessíveis, serviços criminosos e modelos "*as-a-service*" reduziu as barreiras de entrada, aumentando o número de atores que podem participar dessas operações.

Do ponto de vista criminológico, isso introduz dinâmicas típicas de ambientes organizados: especialização, terceirização de funções e adaptação constante com base no risco e no benefício.

O papel da ciberinteligência em um cenário de ambiguidade

Nesse contexto, o principal desafio para a inteligência cibernética de ameaças não é apenas detectar, **mas também interpretar a atividade.**

O volume de informações disponíveis está cada vez maior, mas o valor delas depende da capacidade de contextualizá-las. Para entender uma campanha, é preciso analisar não apenas como é executada, mas também **por que ocorre, em que momento e com que objetivo estratégico.**

Isso representa uma mudança na forma de abordar as análises. As investigações não podem mais se limitar à identificação de indicadores técnicos ou padrões conhecidos, mas precisam levar em conta variáveis externas, como o contexto geopolítico, a evolução dos conflitos ou os interesses dos atores envolvidos.

Nessa perspectiva, a inteligência de ameaças cibernéticas se aproxima cada vez mais de disciplinas que se concentram na análise do comportamento e do ambiente, onde a interpretação é tão relevante quanto as evidências de suporte. A capacidade de prever movimentos não depende mais apenas da detecção, mas também da **compreensão do cenário em que se atua**.

Dessa forma, o ciberespaço se consolidou como uma extensão direta da competição geopolítica. As operações não são mais incidentes isolados, mas fazem parte de estratégias contínuas em que a persistência, a ambiguidade e a pressão indireta ditam o ritmo do conflito.

Por isso, em um cenário em que o conflito nem sempre é declarado, a diferença não está em detectar mais, mas em interpretar melhor.

Sandra Somastre
Analista de Inteligência de Ameaças Cibernéticas (CTI)

Do acesso à intenção: a visão da CTI quando o atacante é um usuário

Artigo por Raquel Gálvez Huertas

Cada vez mais, os ciberataques começam com um acesso aparentemente legítimo, em vez de uma invasão visível. O atacante não precisa violar os sistemas: basta que o sistema confie nele. Essa mudança não é apenas operacional, é estrutural. A segurança tradicional foi desenvolvida para detectar acessos não autorizados. No entanto, cada vez mais ataques usam acessos válidos, o que torna a fronteira entre atividades legítimas e comportamentos mal-intencionados menos nítida. Nesse contexto, a inteligência de ameaças cibernéticas (CTI) enfrenta um desafio diferente: não basta mais identificar ameaças externas, mas também entender como os atacantes se comportam quando já se parecem com usuários.

A mudança de paradigma pode ser melhor explicada por meio das técnicas que ganharam destaque recentemente. Todas elas têm um elemento em comum: o atacante não "quebra" o sistema, ele usa em seu benefício.

Quando o acesso não é mais um sinal de legitimidade

Um dos destaques é o *phishing* do tipo ***Adversary-in-the-Middle*** **(AiTM)**, que se consolidou como um dos principais vetores em campanhas direcionadas. Ao contrário do *phishing* tradicional, essa abordagem permite interceptar as credenciais e as sessões do usuário em tempo real, mesmo em ambientes protegidos por autenticação multifator (MFA). O resultado não é apenas o roubo de senhas, mas também o roubo de sessões ativas totalmente válidas.

Esse modelo atingiu um nível significativo de industrialização. Em março de 2026, a Europol e a Microsoft desmantelaram a plataforma **Tycoon 2FA**, um serviço de *phishing-as-a-service* baseado em AiTM que permitia comprometer contas em cerca de 100 mil organizações, gerando campanhas em massa capazes de contornar a MFA e operar com acessos legítimos em grande escala.

Além disso, nota-se um aumento no **sequestro de sessão**, especialmente em ambientes de *cloud* e SaaS, onde os atacantes reutilizam *cookies* ou *tokens* de autenticação para acessar serviços sem precisar se autenticar novamente. Esse tipo de técnica foi observado em incidentes recentes em ambientes do Microsoft 365, nos quais agentes avançados, como o **Storm-2755**, acessaram contas institucionais usando *tokens* de autenticação válidos, sem credenciais nem novos processos de login. O acesso foi realizado por meio de sessões legítimas já iniciadas, o que dificultava a detecção, pois não havia irregularidades evidentes no processo de autenticação.

Persistência sem credenciais: o abuso de Oauth

Outra técnica emergente, especialmente relevante em ambientes corporativos, é a exploração de aplicações **OAuth**. Nesses casos, o atacante faz com que o usuário autorize o acesso a uma aplicação mal-intencionado com permissões para sua conta (e-mail, arquivos etc.). Depois disso, o acesso é mantido sem a necessidade de credenciais adicionais.

Em março de 2026, uma campanha ativa não atribuída que explorava fluxos legítimos de OAuth comprometeu mais de 340 organizações. Para isso, induziu os usuários a inserir códigos em páginas de autenticação legítimas. Sem que soubessem, eles autorizavam o acesso dos atacantes, gerando *tokens* válidos sem a necessidade de roubo de credenciais.

Essas práticas apresentam um novo desafio: a persistência não depende mais de credenciais comprometidas, mas de permissões concedidas.

Ataques sem *malware*: invisibilidade operacional

Por outro lado, consolida-se o uso de abordagens conhecidas como ***Living-off-the-Land*** **(LotL)**, nas quais os atacantes usam ferramentas legítimas do próprio ambiente (*scripts*, APIs, funcionalidades de *cloud*) para realizar suas ações.

Campanhas atuais de agentes de APT, como **APT29** e **APT28**, motivados pelo conflito geopolítico, refletem esses métodos. Nesses casos, os atacantes se infiltram nos sistemas de infraestrutura crítica do inimigo usando ferramentas nativas e permanecem sem serem detectados enquanto extraem informações para fins estratégicos.

Assim, quando a atividade se baseia em LotL, um dos principais indicadores tradicionais de comprometimento, o *malware* fica em segundo plano ou até mesmo desaparece.

O resultado é uma operação integrada, difícil de distinguir daquela de um usuário real, sem alertas evidentes nem comportamentos inesperados. Se o acesso não é mais uma barreira, o próximo ponto de controle passa a ser o próprio usuário.

O usuário como vetor de *bypass*

Outra tendência relevante é o uso de técnicas que exploram diretamente o usuário como mecanismo de evasão.

O **MFA *fatigue***, também conhecido como *push bombing*, consiste em "bombardear" o usuário com solicitações de autenticação até que, por engano ou por cansaço, ele aceite uma delas. Nesse momento, o atacante consegue acesso sem precisar violar nenhuma medida de segurança técnica.

Ao mesmo tempo, observou-se um aumento nos **ataques direcionados a serviços de suporte de TI ou *helpdesk***, nos quais os invasores se passam por outras pessoas para solicitar a redefinição de credenciais ou alterações nos fatores de autenticação. Nesse caso, o vetor não é tecnológico, mas sim processual.

Esses mecanismos refletem uma mudança clara: o foco do atacante está passando das vulnerabilidades nos sistemas para os processos e as pessoas.

Essa abordagem tem sido usada repetidamente por grupos como o **Scattered Spider**, que, em campanhas ativas em 2025/26, combinaram o envio em massa de notificações de MFA com engenharia social direcionada a serviços de suporte de TI para obter acesso legítimo em ambientes corporativos. Depois de conseguir acesso, o objetivo não é mais se esconder, mas agir sem levantar suspeitas.

Implicações para a CTI: quando a confiança gera incerteza

Embora sejam diferentes na forma como são

A integração desses fatores ao próprio ataque não apenas reduz a visibilidade técnica, mas também muda o tipo de problema que a segurança precisa enfrentar.

Quando não há *malware*, nenhuma exploração evidente e nenhum evento suspeito, os mecanismos tradicionais perdem a capacidade de interpretar o que está acontecendo.

Agora, o objetivo não é burlar os controles, mas sim se encaixar neles.

Assim, o valor das equipes de CTI não se limita à detecção de sinais evidentes, mas evolui para interpretar o que acontece dentro dessa aparente normalidade. Ao identificar padrões de uso que não se encaixam, correlacionar pequenas anomalias e entender as técnicas do invasor, é possível entender atividades que, isoladamente, parecem normais.

Em um ambiente onde o acesso deixa de ser um indicador confiável, a capacidade de interpretar o comportamento se torna o elemento-chave para reduzir a incerteza e apoiar a tomada de decisão.

Raquel Gálvez Huertas
Analista de Inteligência de Ameaças Cibernéticas (CTI)

A nova ordem das ameaças: as tendências que estão redefinindo nosso roteiro estratégico

Tendências por Alberto Herrera García

Os primeiros quatro meses de 2026 confirmaram o que já pressentíamos: as ameaças não apenas aumentaram em volume, mas também mudaram de natureza. A identidade substituiu o perímetro como principal campo de batalha, a cadeia de suprimentos se tornou uma vulnerabilidade estrutural e a IA deixou de ser uma vantagem exclusiva do defensor para se tornar uma aliada de campanha do adversário. Além de tudo isso, há uma geopolítica que define objetivos com mais precisão do que nunca e uma exigência crescente de que o analista pare de apenas informar e comece a tomar decisões.

A identidade como o novo perímetro de combate

A conclusão mais contundente que surge dos principais relatórios de inteligência publicados até agora neste ano é, ao mesmo tempo, a mais incômoda de aceitar: a identidade se tornou a principal porta de entrada para os ambientes empresariais modernos. À medida que as organizações se expandem para plataformas em *cloud*, ecossistemas SaaS e modelos de acesso remoto, as fronteiras tradicionais da rede se desvanecem. Agora, a identidade define o acesso, a exposição e o comprometimento. Por isso, os agentes de ameaças deixaram de forçar a entrada e explorar sistemas. Passaram a fazer login com credenciais válidas, obtidas em larga escala por meio de *malwares infostealers*, registros e mercados ilícitos. Isso já é conhecido na comunidade como *"log in, don't break in"*.

Ao longo de 2025, centenas de milhares de credenciais de plataformas de IA apareceram em mercados clandestinos, o que confirma que as ferramentas de produtividade corporativa se tornaram um dos principais vetores de exposição. Para o CTI operacional, essa nova tendência implicou redefinir quais ações constituem o monitoramento de exposição: desde o monitoramento da *dark web* até o rastreamento de *tokens*, chaves de API e sessões ativas.

Cadeia de suprimentos: de vetor de ataque a condição sistêmica

Já se foi o tempo em que os ataques à cadeia de suprimentos eram incidentes isolados realizados por agentes sofisticados. Nos últimos cinco anos, os comprometimentos de terceiros quadruplicaram e, o que antes era uma categoria de ataque isolada, tornou-se uma condição permanente do ecossistema. Os adversários não atacam mais o *endpoint* da organização-alvo, mas atacam diretamente os ambientes onde o software dela é desenvolvido e implantado.

A exploração de aplicações públicos é uma tendência claramente crescente, impulsionada pela fragilidade das cadeias de dependência. Um único repositório comprometido pode distribuir atualizações maliciosas para milhares de projetos relacionados antes que qualquer sistema de detecção gere o primeiro alerta. Para a CTI, isso exige ampliar o modelo de coleta de informações, incorporando visibilidade sobre a postura de segurança dos nossos fornecedores, suas dependências de código aberto e os acessos que eles têm à nossa infraestrutura. O mapa de riscos da cadeia de suprimentos, enriquecido com telemetria de ameaças, deixou de ser um diferencial de maturidade para se tornar o padrão mínimo exigido.

IA adversária, de ferramenta a aliada do adversário

O uso de inteligência artificial por adversários já não pertence ao futuro próximo. Famílias de *malware* como *Promptflux* e *Promptsteal* consultam ativamente modelos de linguagem durante sua própria execução para adaptar seu comportamento e evitar a detecção em tempo real.

Estamos diante de *malwares* capazes de raciocinar sobre o ambiente em que se encontram. Ao mesmo tempo, os chamados ataques de destilação (*distillation attacks)* ganharam relevância. Esses ataques permitem extrair a lógica proprietária de modelos de alto valor, transformando os ativos de inteligência artificial de uma organização em um alvo de exfiltração tão crítico quanto qualquer banco de dados.

O aumento dos ataques realizados por adversários com capacidades habilitadas por IA confirma que isso não é mais algo exclusivo de atores de elite.

Em particular, a engenharia social também passou por uma transformação qualitativa, com deepfakes gerados com precisão contextual, personificação de equipes de suporte técnico e campanhas de *phishing* em várias etapas capazes de neutralizar o fator humano antes que o alvo identifique a ameaça.

A geopolítica como variável da inteligência estratégica

Nenhuma análise do cenário de 2026 estaria completa sem reconhecer o peso da geopolítica como uma variável central. Conflitos ativos, disputas comerciais e a redefinição de alianças continuam a definir os objetivos e o ritmo dos agentes de ameaças de forma tão decisiva quanto qualquer vulnerabilidade técnica. Por esses motivos, a linha que separava o cibercrime com motivação financeira das operações de espionagem patrocinadas por Estados se tornou tão tênue que, na maioria dos casos, é praticamente impossível fazer uma atribuição clara. Por exemplo, os grupos de *ransomware* estão atuando simultaneamente como fontes de financiamento e como agentes de disrupção geopolítica.

Ao mesmo tempo, a convergência de ferramentas compartilhadas, programas de afiliados e infraestrutura oculta criou um ecossistema adversário dinâmico no qual os modelos de atribuição tradicionais (baseados em TTPs ou em agentes específicos) se mostram insuficientes. Do ponto de vista estratégico, essa situação exige que os analistas incorporem a geopolítica como uma camada permanente do ciclo de inteligência e como uma variável preditiva, buscando prever quem será o próximo alvo, quando e com que intensidade.

Inteligência como decisão, não como dado

Esta análise das principais tendências dos primeiros cinco meses do ano nos deixa com uma certeza que não precisa de dados adicionais para se sustentar: a complexidade do cenário atual não se resolve com mais ferramentas nem com mais *feeds*.

Isso deve ser resolvido com melhores análises, com estruturas que permitem que a inteligência se transforme em ação e com a capacidade de manter uma visão estratégica, justamente no momento em que o ruído operacional está no auge.

Quando as ameaças se movem à velocidade de uma máquina, uma defesa focada exclusivamente no ser humano não é mais suficiente. No entanto, a autonomia defensiva não significa que o analista seja irrelevante, mas sim que ele é valorizado. Alguém precisa desenvolver os modelos, calibrar os limites e interpretar as anomalias que nenhum sistema já viu antes. Essa função não pode ser delegada.

O que as tendências confirmam é que a inteligência concluiu sua transição de uma disciplina técnica especializada para uma função estratégica de primeiro nível. Passamos da coleta de indicadores para a modelagem de adversários, do monitoramento de ameaças para a gestão de exposições, e da geração de relatórios para a participação ativa no ciclo de tomada de decisões.

Trata-se de uma responsabilidade maior, mas também do reconhecimento de que, em um ambiente onde os adversários operam com velocidade algorítmica e eficiência industrial, a única resposta que temos é a inteligência: desenvolvida com rigor e aplicada com o discernimento que só o analista humano pode oferecer.

Alberto Herrera García
Analista júnior de Inteligência de Ameaças Cibernéticas (CTI)

Vulnerabilidades

Vulnerabilidade de bypass em produtos da Cisco

Data: 1º de abril de 2026
CVE: CVE-2026-20093

CVSS: 9,8

CRÍTICA

Descrição

Foi identificada uma vulnerabilidade crítica do tipo *bypass* contra a autenticação do Cisco Integrated Management Controller (IMC).

Essa vulnerabilidade está presente na função de alteração de senha do Cisco IMC, na qual um invasor pode enviar uma solicitação HTTP especialmente criada a um dispositivo vulnerável. Se essa vulnerabilidade for explorada com sucesso, o invasor poderá contornar o processo de autenticação, alterar as senhas de qualquer usuário existente e obter acesso ao sistema com a identidade desse usuário.

A Cisco lançou atualizações que corrigem essa vulnerabilidade; não há informações sobre a existência de outras soluções.

Solução

Recomenda-se:

- Instalar a atualização correspondente ao patch 2026-04-01 ou posterior, dependendo do produto afetado

Produtos afetados

Alguns dos produtos afetados são:

- Sistemas de computação de rede empresarial (ENCS) da série 5000 (CSCwq55648)
- Catalyst 8300 Series Edge uCPE (CSCwq68912)
- Servidores em rack UCS C-Series M5 e M6 em modo autônomo (CSCwq55659)
- Servidores UCS E-Series M3 (CSCwq55648)

Referências

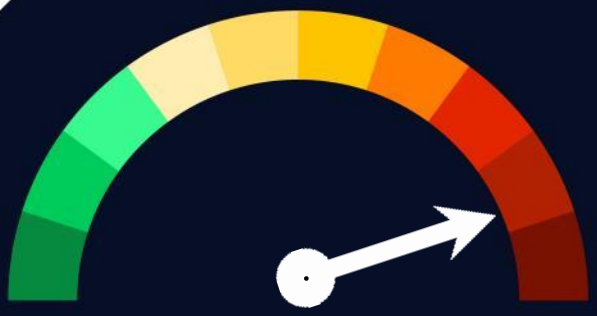
- sec.cloudapps.cisco.com
- socradar.io
- thehackernews.com

TLP:WHITE

Vulnerabilidades

Vulnerabilidade no Docker permite acesso não autorizado

Data: 30 de março de 2026
CVE: CVE-2026-34040



CVSS: 8,8

ALTA

Descrição

Foi descoberta uma vulnerabilidade de gravidade alta no Docker Engine que permite que invasores contornem os *plugins* de autorização (AuthZ) e obtenham acesso ao *host*.

A falha se deve a uma correção incompleta de uma vulnerabilidade anterior que permite o envio de solicitações de API manipuladas cujo conteúdo não é analisado pelos mecanismos de controle. Como consequência, é possível criar contêineres privilegiados com acesso ao sistema host, expondo credenciais e chaves SSH.

A vulnerabilidade já foi corrigida na versão 29.3.1, e recomenda-se fazer a atualização imediatamente ou aplicar medidas de mitigação, como restringir o acesso à API.

Solução

- A vulnerabilidade foi corrigida no Docker Engine versão 29.3.1
- Recomenda-se atualizar para esta versão o mais rápido possível

Produtos afetados

- Produtos que usam o Docker Engine em versões anteriores à 29.3.1 e que também utilizam plugins de autorização (AuthZ).
- Alguns exemplos: Docker Desktop (Windows/macOS), Docker CE (Community Edition), Docker EE / Mirantis Container Runtime, servidores Linux com o Docker Engine instalado manualmente etc.

Referências

- thehackernews.com
- cybersecuritynews.com

Atualização urgente devido a vulnerabilidade crítica no FortiClient EMS

Data: 5 de abril de 2026
CVE: CVE-2026-35616

Crítica

Descrição

A Fortinet lançou um patch de emergência para uma vulnerabilidade crítica no FortiClient EMS (CVE-2026-35616), que já está sendo explorada ativamente.

A falha se deve a um problema de controle de acesso que permite que invasores contornem a autenticação da API e executem código ou comandos por meio de solicitações manipuladas.

A vulnerabilidade afeta as versões 7.4.5 e 7.4.6, para as quais já foram lançados *hotfixes*, enquanto a correção definitiva será fornecida na versão 7.4.7.

Os pesquisadores detectaram a exploração da vulnerabilidade como um ataque de dia zero antes de ser divulgada e identificaram mais de 2.000 instâncias expostas na Internet.

Produtos afetados

- A vulnerabilidade afeta as versões 7.4.5 e 7.4.6 do FortiClient EMS
- Também será corrigida na futura versão 7.4.7
- A versão 7.2 não foi afetada

Solução

- Recomenda-se aplicar os patches imediatamente para evitar comprometimentos.
- Links para instalar os patches:
  - FortiClient 7.4.5
  - FortiClient 7.4.6

Referências

- bleepingcomputer.com
- thehackernews.com

Google corrige vulnerabilidade do tipo dia zero

Data: 1º de abril de 2026
CVE: CVE-2026-5281

Alta

Descrição

O Google lançou uma correção de segurança urgente para o Chrome para corrigir uma vulnerabilidade do tipo dia zero.

De acordo com a descrição oficial do fornecedor, trata-se de uma vulnerabilidade do tipo UAF (*use after free) na* implementação de código aberto do padrão WebGPU, que é usado nos navegadores Chromium.

Essa vulnerabilidade permitiria que um invasor remoto, após comprometer o processo de renderização usado nesses navegadores, executasse código arbitrário em uma página HTML previamente criada.

Essa vulnerabilidade foi relatada por meio de um programa de recompensas por descoberta de *bugs*, que já havia informado sobre outras duas vulnerabilidades corrigidas em outra atualização do Chrome em 23 de março.

Produtos afetados

Os produtos afetados por essa vulnerabilidade incluem todas as versões do Google Chrome anteriores à versão:

- 146.0.7680.177/178 para Windows/Mac
- v146.0.7680.177 para Linux

Solução

Recomenda-se:

- Atualizar para as versões mais recentes do software.

Referências

- helpnetsecurity.com/
- app.opencve.io

TLP:WHITE

Eventos

Conferência Internacional sobre Privacidade e Proteção de Dados – ICDPP
2 de maio

A ICDPP reúne pesquisadores, profissionais e responsáveis por conformidade para discutir os desafios atuais em privacidade e proteção de dados. Com foco especial no marco regulatório europeu, incluindo o RGPD, o congresso oferece uma visão abrangente que conecta a pesquisa acadêmica à sua aplicação em ambientes empresariais. Trata-se de um fórum essencial para analisar as tendências em governança de dados, ética digital e conformidade, em um cenário no qual a gestão responsável da informação se torna cada vez mais crucial.

Link

Cybersec Europe
20 a 21 de maio

A Cybersec Europe se consolida como um dos principais pontos de encontro da cibersegurança na Europa, reunindo especialistas, empresas de tecnologia e líderes empresariais para discutir os desafios mais atuais do setor. A edição de 2026 terá como foco áreas como segurança em cloud, gestão de identidades (IAM) e resiliência digital, combinando inovação tecnológica com uma orientação estratégica bem definida. Com uma forte presença de parceiros e líderes de mercado, o evento também se destaca por sua capacidade de gerar networking de alto nível e oportunidades de colaboração.

Link

CyberWiseCon Europe 2026
19 a 22 de maio

O GenAI Summit EU 2026 será realizado de 17 a 18 de abril de 2026 em Valência, Espanha, em um formato presencial de dois dias, destinado a profissionais de IA, dados e *machine learning*. O evento reunirá líderes de tecnologia, inovadores e equipes técnicas para explorar o potencial transformador da inteligência artificial generativa. A programação inclui palestras técnicas, painéis sobre ética, governança e segurança, além de espaços para *networking* e *workshops*.

Link

CYSAT Europe 2026
20 a 21 de maio

A CYSAT Europe é uma das propostas mais inovadoras do cenário atual, com foco na cibersegurança aplicada ao setor espacial e de satélites. Em um contexto em que as infraestruturas críticas vão além do ambiente terrestre, este evento aborda os riscos emergentes nas comunicações espaciais, nos satélites e nos sistemas associados. Com uma abordagem que combina indústria, defesa e tecnologia, o CYSAT destaca a necessidade de se antecipar a ameaças cada vez mais sofisticadas em um domínio estratégico em plena expansão.

Link

Recursos

➢ Monitoramento de ameaças cibernéticas e relatórios setoriais

Em abril de 2026, a Cyble publicou novos relatórios setoriais, incluindo o *Healthcare Threat Landscape Report 2026*, no qual analisa ameaças reais ativas em setores críticos. Esse tipo de relatório oferece informações diretamente acionáveis sobre *ransomware*, atividades na *dark web* e campanhas direcionadas. E são especialmente úteis para entender, quase em tempo real, como os agentes de ameaças estão adaptando suas táticas em cada setor.

Link

➢ Resumo semanal de vulnerabilidades – CVE Watchtower

Este briefing semanal é extremamente valioso para as equipes de segurança: em apenas uma semana, foram registradas mais de 1.300 novas vulnerabilidades, incluindo *zero-days* críticos que exigem ação imediata. O relatório filtra o ruído e prioriza o que é realmente explorável, ajudando as equipes de SOC e de gestão de vulnerabilidades a tomar uma decisão mais rápida e baseada em risco.

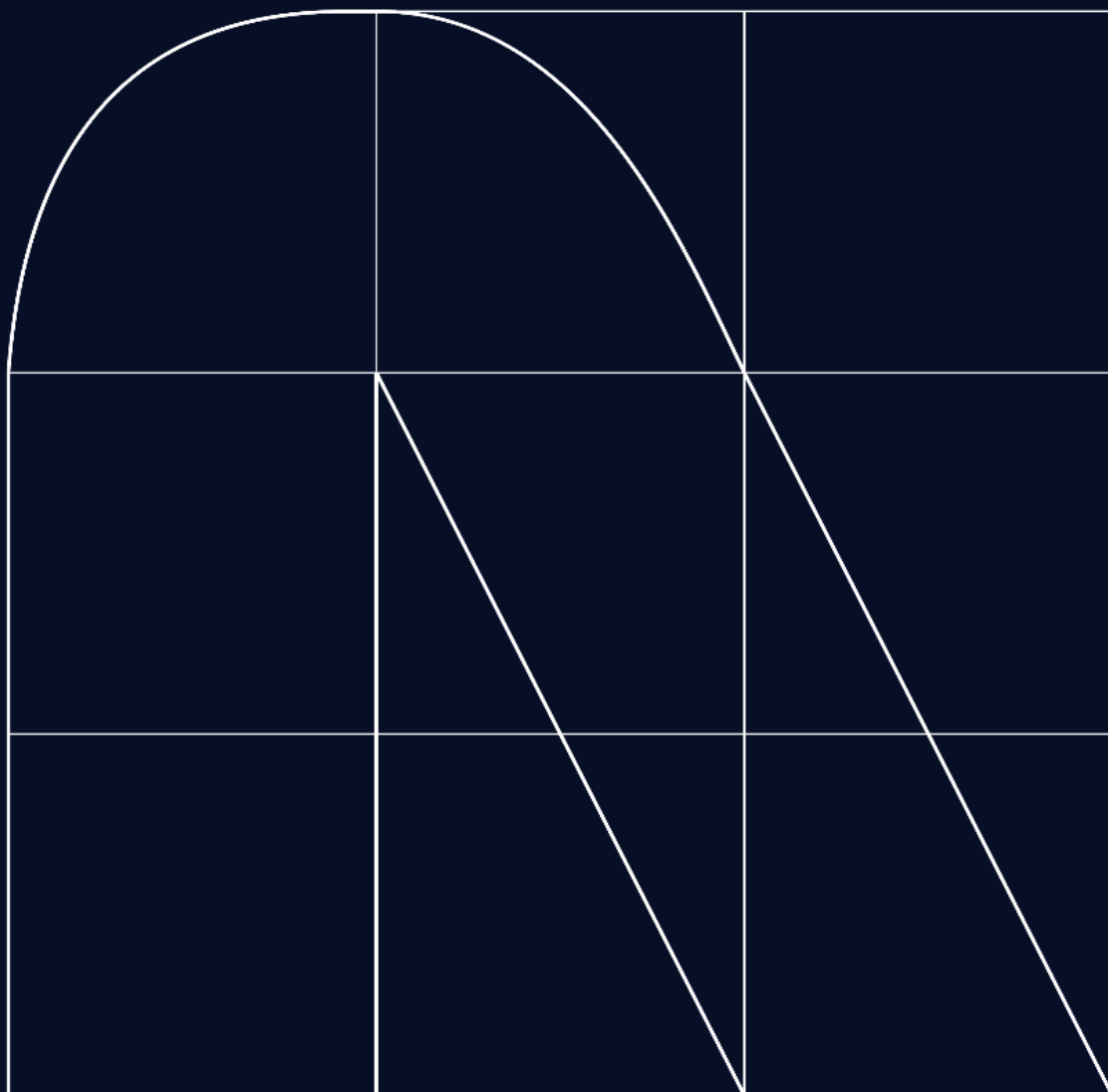
Link

➢ Estatísticas de vulnerabilidades de 2026

Um recurso extremamente atual: até abril de 2026, já haviam sido publicadas mais de 17.000 vulnerabilidades, o que representa um aumento de 26% em relação ao ano anterior. Este paidel, atualizado diariamente, permite entender a velocidade real do risco e dimensionar o desafio operacional que as equipes de cibersegurança enfrentam.

Link

Assine a RADAR
up.nttdata.com/suscribetearadar



Powered by the cybersecurity NTT DATA team

br.nttdata.com