TLP: CLEAR

Pesquisa de Cibersegurança
Cyber Threats

ATAQUES À CADEIA DE SUPRIMENTOS:
A Industrialização da Confiança como Superfície de Ataque

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse a inteligência que produzimos sobre as Táticas, Técnicas e Procedimentos de determinados *Threat Actors*, análises de *malwares* emergentes no cenário de cibersegurança, análises de vulnerabilidades críticas e outras informações no *blog* da ISH Tecnologia, clicando na imagem abaixo.

ISH

ALERTA HEIMDALL! HTTP2 RAPID RESET_IMPACTOS E DETECÇÃO DA CVE-2023-44487

Falhas de negação de serviço (DoS) não são apenas interrupções técnicas. Elas representam riscos reais à continuidade do negócio, à confiança dos clientes e à reputação da marca. Nisto temos a vulnerabilidade CVE-2023-44487, conhecida como HTTP/2 Rapid Reset.

BAIXAR

ISH

ALERTA HEIMDALL! BABUK2 EM 2025: RETORNO LEGÍTIMO OU COPYCAT ESTRATÉGICO

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e com surgimento de novos grupos. Nesse contexto, temos o ransomware Babuk2.

BAIXAR

ISH

ALERTA HEIMDALL! A ANATOMIA DO RANSOMWARE AKIRA E SUA EXPANSÃO MULTIPLATAFORMA

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e ganhando bastante popularidade. Nesse contexto, temos o ransomware Akira.

BAIXAR

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO EXECUTIVO:

Figura 1 - Representação da Interconexão

A arquitetura da segurança corporativa atravessa uma mudança estrutural. O modelo tradicional de defesa baseado em perímetro (centrado na proteção direta de ativos internos) vem se tornando insuficiente diante de um cenário em que a superfície de ataque das organizações passou a incluir todo o seu ecossistema digital. Cadeias de suprimentos tecnológicas modernas são compostas por uma rede complexa de provedores de software, integrações **SaaS**, bibliotecas de código aberto, **APIs** e prestadores de serviços gerenciados. Essa interdependência criou um ambiente no qual comprometer um único fornecedor pode gerar impactos em cascata sobre dezenas ou centenas de organizações.

Atores de ameaça, incluindo grupos de cibercrime organizado e operações patrocinadas por Estados-nação, adaptaram suas estratégias para explorar exatamente esse modelo de interdependência. Em vez de direcionar esforços para invadir diretamente cada organização, adversários passaram a comprometer componentes de alta confiança dentro da cadeia de suprimentos digital. Essa mudança representa uma forma de ***industrialização do comprometimento***, onde a escala e o alcance de um ataque são ampliados pela posição estratégica do fornecedor comprometido dentro do ecossistema tecnológico.

Os dados mais recentes demonstram que essa tendência já representa um vetor dominante de risco. Estima-se que **35,5%** das violações de dados tenham origem em comprometimentos de terceiros, um aumento significativo em relação ao ano anterior e provavelmente subestimado devido à dificuldade de rastrear dependências indiretas e fornecedores de quarta ou quinta parte. O impacto financeiro acompanha essa evolução: **o custo global anual associado a ataques à cadeia de suprimentos ultrapassa US$ 53 bilhões**, refletindo não apenas perdas diretas, mas também interrupções operacionais, custos de resposta a incidentes e danos reputacionais prolongados.

Sob a perspectiva técnica, os ataques à cadeia de suprimentos evoluíram para além da simples inserção de código malicioso em *softwares* distribuídos. Atualmente, os adversários exploram principalmente identidades, integrações e canais legítimos de comunicação entre sistemas. *Tokens* de acesso, concessões ***OAuth*** e credenciais comprometidas de fornecedores *upstream* permitem que atacantes acessem ambientes corporativos *downstream* sem disparar alertas

tradicionais, muitas vezes contornando controles robustos como autenticação multifator. Ao mesmo tempo, o envenenamento de ecossistemas de código aberto (incluindo repositórios amplamente utilizados como **npm** e **PyPI**) permite que código malicioso seja distribuído em escala global através de *pipelines* de desenvolvimento contínuo antes mesmo que mecanismos de detecção em tempo de execução sejam acionados.

A incorporação crescente de inteligência artificial nas operações adversárias atua como um multiplicador de força nesse contexto. Ferramentas automatizadas baseadas em **IA** estão reduzindo drasticamente o tempo entre o acesso inicial e a exfiltração de dados, com registros recentes indicando que operações de eCrime podem alcançar tempos de *breakout* de apenas alguns minutos. É fundamental distinguir que, enquanto o movimento lateral humano médio é de **29 minutos**, a automação ofensiva via *scripts* e **IA** em *pipelines* comprometidos pode reduzir essa janela para meros segundos, exigindo respostas automatizadas (**SOAR**) em vez de puramente manuais.

Para organizações e conselhos executivos, o risco associado a ataques à cadeia de suprimentos vai além da perda direta de dados. Incidentes envolvendo fornecedores frequentemente desencadeiam interrupções sistêmicas, incluindo paralisação de operações enquanto organizações avaliam o alcance da exposição, suspensão de integrações críticas e impactos financeiros decorrentes da indisponibilidade de serviços. Em setores altamente interconectados, como manufatura, saúde, logística e serviços financeiros, esse tipo de comprometimento pode resultar em efeitos cascata capazes de afetar cadeias produtivas inteiras.

Diante desse cenário, a resiliência organizacional passa a depender não apenas da robustez das defesas internas, mas da capacidade de governar e validar continuamente a segurança de todo o ecossistema digital ao qual a organização está conectada. Estratégias eficazes de mitigação exigem a adoção de arquiteturas ***Zero Trust***, visibilidade aprofundada sobre dependências de *software* por meio de ***Software Bills of Materials*** (**SBOM**) e mecanismos de governança capazes de identificar, monitorar e isolar rapidamente integrações de terceiros comprometidas.

Em um ambiente digital caracterizado por interdependência estrutural, a segurança deixou de ser apenas uma questão de proteção interna. A verdadeira medida de resiliência organizacional será a capacidade de verificar e controlar a confiança em cada elo da cadeia de suprimentos tecnológica.

INTELIGÊNCIA ESTRATÉGICA

A INDUSTRIALIZAÇÃO DO COMPROMETIMENTO

O cenário contemporâneo de ameaças cibernéticas reflete uma profunda transformação na lógica operacional dos adversários. O modelo tradicional de intrusões direcionadas a organizações individuais vem sendo gradualmente substituído por uma estratégia mais eficiente e escalável: o comprometimento de componentes críticos dentro da cadeia de suprimentos digital.

Esse modelo explora a interdependência estrutural das infraestruturas tecnológicas modernas. Sistemas corporativos dependem amplamente de provedores **SaaS**, bibliotecas de código aberto, serviços gerenciados, *pipelines* de integração contínua e plataformas de colaboração em nuvem. Cada um desses componentes introduz um elo adicional na cadeia de confiança digital e, consequentemente, um novo vetor potencial de comprometimento.

Ao comprometer um único fornecedor *upstream*, atores maliciosos podem obter acesso indireto a centenas ou até milhares de organizações *downstream*. Essa dinâmica cria um efeito multiplicador que transforma ataques isolados em incidentes sistêmicos. Em termos operacionais, trata-se de uma industrialização do comprometimento, na qual adversários maximizam escala, alcance e eficiência operacional.

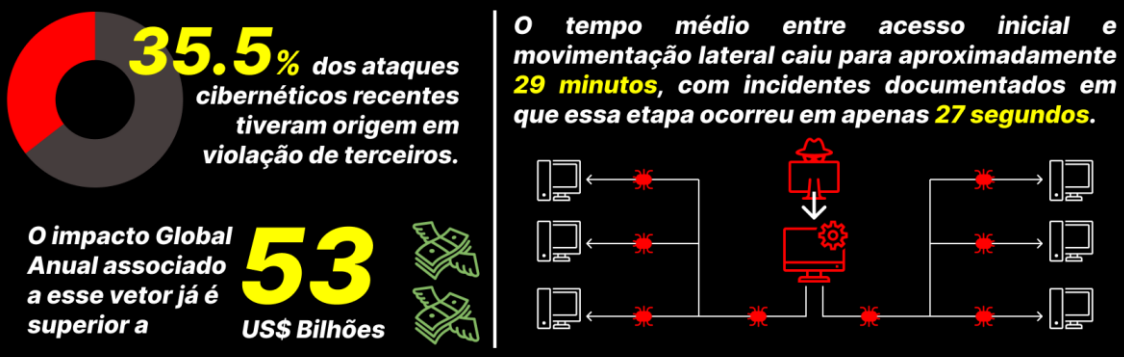


Figura 2 - Impactos do comprometimento de terceiros

Os dados recentes confirmam essa tendência. Estima-se que **35,5%** de todas as violações de dados atualmente tenham origem em comprometimentos de terceiros, um aumento significativo em relação ao ano anterior. O impacto econômico associado a esse vetor também é expressivo, com custos globais anuais superiores a **US$ 53 bilhões** atribuídos a ataques à cadeia de suprimentos.

A complexidade desse modelo é ampliada pela presença de dependências indiretas. **Aproximadamente 4,5% das violações já envolvem entidades de quarta parte**, nas quais uma organização é impactada não por seu fornecedor direto, mas por um parceiro do fornecedor: um cenário que frequentemente escapa aos mecanismos tradicionais de gestão de risco de terceiros.

Outro fator crítico é a aceleração operacional das campanhas adversárias. O tempo médio entre acesso inicial e movimentação lateral *(breakout time*) caiu para aproximadamente 29 minutos, com incidentes documentados em que essa etapa ocorreu em apenas 27 segundos. Em alguns casos, a exfiltração de dados foi iniciada menos de quatro minutos após o acesso inicial, reduzindo drasticamente a janela disponível para detecção e resposta.

O ransomware também passou a explorar intensivamente essa superfície de ataque. Atualmente, **41,4%** dos incidentes de extorsão digital começam com comprometimentos de terceiros, refletindo a capacidade desse vetor de amplificar impacto financeiro e reputacional. Grupos especializados têm explorado vulnerabilidades em softwares amplamente utilizados, como ferramentas de transferência de arquivos, para comprometer múltiplas organizações simultaneamente.

O ecossistema de desenvolvimento de software também se tornou um alvo prioritário. A análise recente de repositórios de código aberto identificou mais de **877 mil** pacotes maliciosos, muitos deles inseridos deliberadamente em bibliotecas populares utilizadas em pipelines de integração contínua (CI/CD). Quando essas dependências comprometidas são incorporadas ao ciclo de desenvolvimento de software corporativo, o código malicioso pode ser distribuído em escala global antes mesmo que mecanismos tradicionais de segurança sejam acionados.

Dependência Tecnológica Global e Concentração de Risco

A crescente digitalização da economia global criou uma dependência estrutural de fornecedores tecnológicos compartilhados. Plataformas de nuvem, softwares empresariais e frameworks de desenvolvimento tornaram-se componentes fundamentais da operação de praticamente todas as organizações modernas.

Paradoxalmente, essa dependência cria uma concentração significativa de risco sistêmico. Um único fornecedor amplamente adotado pode representar um ponto único de falha capaz de impactar simultaneamente milhares de empresas.

Estudos recentes identificam um fenômeno conhecido como “Efeito da Riqueza”: organizações e países com maior maturidade tecnológica tendem a registrar maiores taxas de ataques à cadeia de suprimentos. Isso ocorre porque suas defesas perimetrais e controles internos são mais robustos, incentivando adversários a buscar caminhos indiretos através de fornecedores e parceiros.

Esse padrão pode ser observado em diversos mercados desenvolvidos. **Em algumas economias altamente digitalizadas, como Singapura e Países Baixos, mais de 70% das violações possuem algum componente relacionado a terceiros.**

Grande parte desse risco está associado à dependência de software de terceiros. **Soluções tecnológicas utilizadas em múltiplos setores, como plataformas de colaboração, bibliotecas de desenvolvimento e sistemas de gestão corporativa, representam 37,5% dos vetores de comprometimento relacionados à cadeia de suprimentos.**

Além disso, a complexidade das arquiteturas modernas de software cria um problema adicional: dependências transitivas invisíveis. **Estima-se que mais de 60% das vulnerabilidades em aplicações nativas da nuvem estejam presentes em bibliotecas indiretas, muitas vezes desconhecidas pelas próprias organizações que utilizam esses sistemas.**

Figura 3 - Representação da cadeira de suprimentos industrial sendo quebrada

Essa concentração de risco é particularmente evidente em setores industriais. A convergência entre Tecnologia da Informação (TI) e Tecnologia Operacional (OT) ampliou significativamente a superfície de ataque em ambientes de manufatura. Como resultado, **os ataques ao setor industrial cresceram aproximadamente 61% em um único ano**, tornando a indústria um dos principais alvos de ataques à cadeia de suprimentos.

Geopolítica da Cadeia de Suprimentos

A segurança cibernética tornou-se um elemento central da competição geopolítica contemporânea. Cadeias de suprimentos digitais e físicas passaram a

ser vistas como infraestruturas estratégicas, capazes de influenciar relações comerciais, segurança nacional e soberania tecnológica.

Mais de 90% das grandes organizações globais afirmam ter ajustado suas estratégias de segurança em resposta ao aumento das tensões geopolíticas, refletindo a crescente convergência entre riscos cibernéticos e disputas internacionais.

Diversos atores patrocinados por Estados-nação têm adotado estratégias específicas voltadas ao comprometimento de cadeias de suprimentos.

Figura 4 - Representação de grupo APTs ligados à Estado-Nação

Grupos associados à **China** têm priorizado operações de espionagem de longo prazo voltadas para infraestrutura crítica e logística global. Essas campanhas frequentemente exploram dispositivos de borda, como roteadores e firewalls corporativos, que operam com visibilidade limitada de segurança. Em algumas campanhas, até 40% das vulnerabilidades exploradas estavam relacionadas a esses dispositivos.

No caso de grupos associados à **Rússia**, as operações frequentemente combinam espionagem, sabotagem e manipulação informacional. Ataques a infraestruturas críticas e campanhas direcionadas a sistemas logísticos têm sido utilizados como instrumentos de pressão geopolítica, especialmente em contextos de conflito ou tensão diplomática.

A **Coreia do Norte** apresenta um modelo operacional distinto, no qual operações cibernéticas são utilizadas diretamente como mecanismo de financiamento estatal. Grupos associados ao regime têm explorado cadeias de suprimentos de software e plataformas de criptomoedas para conduzir roubos em larga escala.

Um exemplo particularmente relevante envolve a infiltração de desenvolvedores falsos em empresas de tecnologia. Utilizando identidades sintéticas e deepfakes baseados em inteligência artificial, esses atores conseguem ser contratados como desenvolvedores remotos, obtendo acesso privilegiado a repositórios de código e sistemas internos.

A Exposição da América Latina

Embora os ataques à cadeia de suprimentos representem uma ameaça global, a América Latina apresenta características estruturais que amplificam sua exposição a esse vetor de risco.

Figura 5 - Representação da execução de um programa trojanizado.

Diferentemente de economias altamente desenvolvidas, onde ataques à cadeia de suprimentos frequentemente servem como mecanismo para contornar defesas avançadas, a **América Latina enfrenta um vetor de Supply chain 'raiz': o uso de softwares não oficiais ou ferramentas de ativação (cracks) em fornecedores de pequeno e médio porte**. Esses utilitários frequentemente atuam como cavalos de troia para ***Initial Access Brokers*** (**IABs**), que vendem o acesso a essas máquinas para grupos de *ransomware*, criando uma vulnerabilidade sistêmica nas cadeias de suprimentos de grandes corporações que se conectam a esses parceiros menos maturados.

Essa realidade cria um cenário híbrido. Por um lado, empresas da região ainda são frequentemente comprometidas por vetores diretos, como *phishing* e exploração de vulnerabilidades expostas. Por outro, organizações que participam de cadeias de suprimentos globais podem sofrer impactos indiretos significativos quando fornecedores internacionais são comprometidos.

A confiança institucional também representa um desafio relevante. **Pesquisas recentes indicam que apenas 13% dos executivos da América Latina acreditam que seus países possuem capacidade adequada para responder a incidentes graves em infraestruturas críticas, um contraste significativo com outras regiões do mundo.**

Além disso, muitas empresas latino-americanas dependem fortemente de provedores estrangeiros de nuvem, software corporativo e infraestrutura digital. Essa dependência amplia o risco de que incidentes ocorridos em outros mercados tenham impacto direto na operação regional.

Inteligência Artificial como Multiplicador de Ameaças

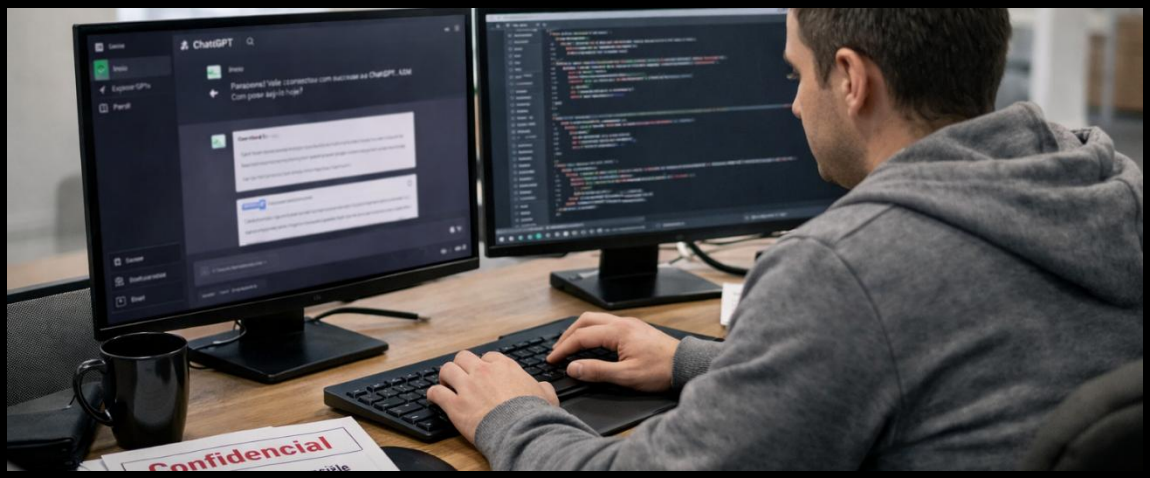
A adoção acelerada de inteligência artificial está redefinindo tanto a superfície de ataque quanto as capacidades operacionais de adversários cibernéticos.

Pesquisas indicam que **94%** dos líderes de segurança consideram a **IA** o principal fator de transformação do cenário cibernético, enquanto **87%** identificam vulnerabilidades relacionadas à IA como o risco de crescimento mais rápido no ambiente digital.

Para os atacantes, a IA representa um poderoso multiplicador de força. Ferramentas baseadas em modelos de linguagem avançados permitem automatizar tarefas que anteriormente exigiam esforço humano significativo, incluindo:

- Desenvolvimento de malware adaptativo
- Reconhecimento automatizado de alvos
- Geração de campanhas de phishing altamente personalizadas
- Análise massiva de código e repositórios públicos

Estima-se que **mais de 80%** das campanhas de engenharia social atualmente utilizem algum tipo de automação baseada em IA.



Além disso, o uso não supervisionado de ferramentas de IA dentro das organizações, fenômeno conhecido como **Shadow AI**, introduz novos vetores de exposição. Aproximadamente **20%** das violações recentes envolveram o uso inadvertido de sistemas de IA por funcionários, resultando em vazamento de dados sensíveis ou propriedade intelectual.

A própria cadeia de suprimentos da inteligência artificial também passou a ser alvo de ataques. Repositórios de modelos pré-treinados e plataformas de compartilhamento de datasets já foram comprometidos em múltiplas ocasiões, levantando preocupações sobre a possibilidade de modelos contaminados com backdoors maliciosos serem incorporados inadvertidamente em sistemas corporativos.

INTELIGÊNCIA TÁTICA

Mecânica Operacional dos Ataques à Cadeia de Suprimentos

Os ataques à cadeia de suprimentos representam uma evolução operacional significativa no cenário de ameaças. Diferentemente das intrusões tradicionais, que buscam acesso direto aos ambientes das organizações, esse modelo explora relações de confiança estabelecidas entre empresas e seus fornecedores para obter acesso indireto a infraestruturas corporativas altamente protegidas.

Do ponto de vista tático, o objetivo central é comprometer pontos de distribuição confiáveis dentro do ecossistema digital, como plataformas **SaaS**, *pipelines* de desenvolvimento, bibliotecas *open source* e sistemas de atualização de software. Ao controlar esses pontos estratégicos, atacantes conseguem inserir artefatos maliciosos que são posteriormente distribuídos por meio de canais legítimos de *software* e integração empresarial, permitindo que o comprometimento se propague de forma silenciosa e escalável, muitas vezes sem disparar alertas nas soluções tradicionais de segurança.

TAXONOMIA TÉCNICA DOS ATAQUES À CADEIA DE SUPRIMENTOS

A cadeia de suprimentos digital moderna expandiu significativamente sua superfície de ataque. O risco não está mais limitado a vulnerabilidades em código, mas inclui também integrações **SaaS**, identidades de aplicações, *pipelines* de desenvolvimento e plataformas de distribuição de software. Entre os vetores mais frequentemente explorados estão *softwares* de transferência de arquivos, plataformas de nuvem corporativa, ferramentas de gerenciamento remoto e repositórios de dependências de software.

***Softwares* de transferência de arquivos representam aproximadamente 14% dos vetores observados**, frequentemente explorados através de vulnerabilidades *zero-day* em plataformas amplamente utilizadas em ambientes corporativos. **Já as integrações SaaS e serviços em nuvem correspondem a cerca de 8,25% dos vetores, geralmente explorados por meio de permissões herdadas e abuso de APIs.**

Ferramentas de gerenciamento remoto, como plataformas **RMM** e **MDM**, também têm sido armamentizadas por atacantes. Como essas soluções possuem privilégios administrativos para gerenciar endpoints corporativos, um comprometimento nesse nível permite executar comandos maliciosos disfarçados de tarefas administrativas legítimas.

Outro vetor relevante envolve subsidiárias e aquisições corporativas. **Aproximadamente 11,75% das violações analisadas envolveram ambientes corporativos conectados após fusões ou aquisições, onde inconsistências de arquitetura e políticas de segurança criam pontos de entrada exploráveis.**

PRINCIPAIS TÉCNICAS DE COMPROMETIMENTO

Abuso de Identidade e Tokens OAuth

No ambiente corporativo moderno, identidades digitais tornaram-se o novo perímetro de segurança.

Integrações SaaS dependem amplamente de mecanismos de autorização baseados em OAuth, APIs e automação de fluxos de trabalho. Quando uma organização integra um aplicativo de terceiros por meio desses mecanismos, o serviço recebe permissões herdadas para acessar dados ou executar ações em nome do usuário ou da organização.

Quando essas plataformas *upstream* são comprometidas, atacantes podem obter tokens **OAuth** ou *session tokens* válidos. Esses artefatos permitem acessar sistemas corporativos downstream sem necessidade de autenticação interativa, contornando controles tradicionais como MFA.

Esse tipo de acesso consolida a técnica de **'Living-off-the-Trust'** (viver da confiança). Diferente do Living-off-the-Land, onde se usam binários nativos, aqui o adversário utiliza a própria infraestrutura de identidade e permissões legítimas do provedor (como **Microsoft 365** ou **Google Workspace**) para manter persistência. Como não há execução de arquivos maliciosos no endpoint, o ataque torna-se virtualmente invisível para soluções tradicionais de EDR/AV, já que o tráfego é indistinguível de operações legítimas de automação via API.

Figura 6 - Representação do fluxo de abuso de OAuth

Um exemplo significativo desse vetor foi observado no comprometimento da integração entre **Salesforce** e **Salesloft-Drift**, onde tokens OAuth válidos foram utilizados para acessar ambientes corporativos de centenas de organizações.

MITRE ATT&CK

- T1078 — Valid Accounts
- T1134 — Access Token Manipulation
- T1552 — Unsecured Credentials

Comprometimento de Pipelines CI/CD

Infraestruturas de desenvolvimento representam um alvo estratégico para atacantes que buscam comprometer cadeias de suprimentos de software.

Ambientes de build e pipelines **CI/CD** frequentemente possuem acesso privilegiado a repositórios de código, artefatos de software e sistemas de distribuição. Quando esses ambientes são comprometidos, atacantes podem modificar processos de build para inserir código malicioso antes que o software seja distribuído aos clientes.

Essa abordagem permite que o código adulterado seja compilado e assinado como parte de processos legítimos, contornando detecções tradicionais.

Figura 7 - Representação do fluxo de Comprometimento de Pipeline

Um exemplo notável foi o ataque à Codecov, no qual invasores modificaram o script Bash Uploader utilizado em pipelines CI/CD de milhares de clientes. O script adulterado exfiltrava variáveis de ambiente contendo credenciais e tokens sensíveis.

MITRE ATT&CK

- T1059 — Command and Scripting Interpreter
- T1552 — Unsecured Credentials
- T1553.002 — Subvert Trust Controls (Code Signing)

Envenenamento de Repositórios Open Source

A dependência massiva de bibliotecas open source introduziu um novo vetor sistêmico de risco no desenvolvimento de software moderno. Aplicações contemporâneas frequentemente incorporam centenas de dependências externas, muitas delas provenientes de repositórios públicos. Quando uma dessas bibliotecas é comprometida, todas as aplicações que a utilizam podem ser impactadas, criando um efeito cascata que amplia significativamente o alcance do ataque dentro de ecossistemas de desenvolvimento.

Atacantes exploram essa dinâmica por meio de técnicas como **typosquatting**, comprometimento de contas de mantenedores e publicação de atualizações maliciosas em repositórios populares. Esses pacotes frequentemente executam scripts maliciosos durante o processo de instalação ou build das aplicações downstream, permitindo a coleta de credenciais, tokens e outras informações sensíveis.

Figura 8 - Representação do Fluxo de Envenenamento de Repositórios

Relatórios recentes identificaram mais de 877 mil pacotes maliciosos publicados em repositórios open source, evidenciando a escala desse vetor de ataque, que tem sido amplamente explorado por grupos associados à **Coreia do Norte** para comprometer ambientes de desenvolvimento.

MITRE ATT&CK

- T1189 — Drive-by Compromise
- T1566 — Phishing
- T1195 — Supply Chain Compromise

Comprometimento de Atualizações de Software

Ataques a **sistemas de atualização de software** representam uma das formas mais eficazes de comprometimento em larga escala dentro de cadeias de suprimentos digitais. Nesse modelo, os atacantes infiltram o ambiente de desenvolvimento ou os mecanismos de distribuição de um fornecedor legítimo e inserem código malicioso em atualizações oficiais do software. Dessa forma, em vez de comprometer diretamente cada organização alvo, os adversários exploram a posição estratégica do fornecedor para alcançar múltiplas vítimas simultaneamente.

A eficácia desse vetor está diretamente relacionada ao modelo de confiança que sustenta os processos de atualização. Atualizações geralmente são **assinadas criptograficamente** e distribuídas por canais oficiais, sendo consideradas confiáveis pelos sistemas das organizações. Como resultado, esses pacotes são frequentemente **baixados e instalados automaticamente**, muitas vezes sem análise aprofundada. Esse mecanismo permite que código malicioso seja introduzido nos ambientes das vítimas sob a aparência de software legítimo, ampliando significativamente o alcance do ataque.

Figura 9 - Representação do fluxo de Comprometimento de Atualizações

O incidente envolvendo a plataforma **SolarWinds Orion** tornou-se um dos exemplos mais conhecidos desse tipo de comprometimento, demonstrando **o impacto potencial da manipulação de processos de atualização em cadeias de**

suprimentos de software, onde uma atualização comprometida foi distribuída para mais de 18.000 organizações em todo o mundo.

MITRE ATT&CK

- T1195 — Supply Chain Compromise
- T1036 — Masquerading
- T1553 — Subvert Trust Controls

Extensões de Navegador Maliciosas

O navegador web tornou-se um componente central do ambiente corporativo moderno, sendo amplamente utilizado para acesso a aplicações SaaS, sistemas internos e serviços em nuvem. Nesse contexto, extensões de navegador passaram a desempenhar um papel relevante na automação de tarefas, integração com ferramentas corporativas e ampliação de funcionalidades. No entanto, essas extensões frequentemente requerem permissões amplas para acessar elementos sensíveis do ambiente do usuário, como sessões autenticadas, cookies, tráfego web e dados de autenticação armazenados no navegador.

Atacantes exploram esse nível de acesso comprometendo contas de desenvolvedores ou publicando extensões aparentemente legítimas em marketplaces oficiais de navegadores. Uma vez instaladas, essas extensões podem operar de forma furtiva dentro do contexto da sessão do usuário, interceptando credenciais, capturando tokens de sessão, monitorando a navegação e até manipulando transações realizadas em aplicações web.

Figura 10 - Representação do fluxo de Extensões Maliciosas

Como essas atividades ocorrem diretamente no navegador e utilizam permissões concedidas pelo próprio usuário ou pela organização, muitas dessas ações se misturam ao comportamento legítimo da aplicação. Isso faz com que extensões maliciosas frequentemente escapem à visibilidade de soluções tradicionais de segurança, como EDRs e antivírus, que geralmente monitoram processos e arquivos no sistema operacional, mas possuem visibilidade limitada sobre atividades internas do navegador.

MITRE ATT&CK

- T1555.003 — Credentials from Web Browsers
- T1056 — Input Capture

Kill Chain de Ataques à Cadeia de Suprimentos

A operação de ataques à cadeia de suprimentos geralmente segue uma sequência estruturada de etapas que permitem aos adversários comprometer um fornecedor e posteriormente propagar o acesso para organizações downstream.

Reconhecimento do Ecossistema

Ferramentas automatizadas e análise de código aberto são utilizadas para identificar bibliotecas utilizadas, provedores SaaS e infraestruturas compartilhadas.

Comprometimento Inicial

Estima-se que aproximadamente 60% dos comprometimentos iniciais envolvam engenharia social ou roubo de credenciais, enquanto cerca de 21% resultam da exploração de vulnerabilidades técnicas.

Inserção de Código Malicioso

Uma vez dentro do ambiente do fornecedor, atacantes modificam artefatos de software, scripts de build ou bibliotecas utilizadas em produtos distribuídos.

Distribuição via Canais Confiáveis

O artefato comprometido é então distribuído por meio de atualizações de software, bibliotecas open source ou integrações SaaS.

Figura 11 - Cadeia de Comprometimento

Reconhecimento do Ecossistema

Os atacantes iniciam mapeando fornecedores, integrações e dependências tecnológicas da organização alvo.

Ferramentas automatizadas e análise de código aberto são utilizadas para identificar bibliotecas utilizadas, provedores SaaS e infraestruturas compartilhadas.

Comprometimento Inicial

O acesso inicial ao fornecedor ocorre principalmente por meio de engenharia social ou exploração de vulnerabilidades em aplicações expostas.

Estima-se que aproximadamente **60%** dos comprometimentos iniciais envolvam engenharia social ou roubo de credenciais, enquanto cerca de **21%** resultam da exploração de vulnerabilidades técnicas.

Inserção de Código Malicioso

Uma vez dentro do ambiente do fornecedor, atacantes modificam artefatos de software, scripts de build ou bibliotecas utilizadas em produtos distribuídos.

Distribuição via Canais Confiáveis

O artefato comprometido é então distribuído por meio de atualizações de software, bibliotecas open source ou integrações SaaS.

Ativação do Payload

Após chegar ao ambiente da vítima, o código malicioso é ativado, muitas vezes utilizando técnicas de execução em memória ou evasão de EDR.

Movimento Lateral

Utilizando permissões herdadas ou credenciais comprometidas, os atacantes expandem o acesso dentro da rede corporativa.

Exfiltração ou Extorsão

A fase final envolve roubo de dados sensíveis ou implantação de ransomware. Em diversos incidentes recentes, a exfiltração começou menos de quatro minutos após o acesso inicial.

Estudos de Caso Relevantes

Incidente	Camada da Cadeia Comprometida	Vetor Técnico Principal	Impacto Operacional
SolarWinds Orion (2020)	Pipeline de build do fornecedor	Inserção de backdoor em biblioteca compilada e assinada digitalmente	Distribuição de malware via atualização legítima para milhares de organizações
MOVEit Transfer (2023)	Software corporativo amplamente distribuído	Exploração de vulnerabilidade zero-day (SQL	Exfiltração massiva de dados em centenas de

		Injection – CVE-2023-34362)	organizações globais
Codecov (2021)	Pipeline CI/CD	Modificação do script Bash Uploader para coleta de variáveis de ambiente	Roubo de tokens, chaves de API e credenciais de ambientes de build
NPM / PyPI (diversos casos)	Ecossistema de dependências open source	Typosquatting, dependency confusion e comprometimento de maintainers	Execução automática de código malicioso durante instalação de bibliotecas
Salesforce / Salesloft (OAuth Abuse)	Integrações SaaS e identidade	Sequestro de tokens OAuth e abuso de APIs legítimas	Acesso indireto a dados corporativos em ambientes Salesforce

Tabela 1 - Tabela de estudo de casos relevantes

SolarWinds Orion (SUNBURST)

Figura 12 - Representação de jornal digital - SolarWind

O comprometimento da plataforma **SolarWinds Orion** é considerado um dos ataques mais sofisticados já registrados contra cadeias de suprimentos de software. A campanha, atribuída ao grupo **APT29**, explorou o ambiente de desenvolvimento da SolarWinds para inserir código malicioso em atualizações legítimas do produto.

Os atacantes comprometeram o pipeline de build da empresa e injetaram um backdoor na biblioteca:

SolarWinds.Orion.Core.BusinessLayer.dll

Como o código malicioso foi compilado e assinado digitalmente pela própria **SolarWinds**, as atualizações comprometidas foram distribuídas através do mecanismo oficial de update do **Orion**. **Entre março e junho de 2020, estima-se que mais de 18.000 organizações tenham instalado versões contendo o backdoor.**

O *malware*, denominado **SUNBURST** (ou ***Solorigate***), foi projetado para operar de forma altamente furtiva. Após a instalação, era executado pelo processo legítimo:

SolarWinds.BusinessLayerHost.exe

A comunicação com a infraestrutura de Comando e Controle (C2) utilizava subdomínios dinâmicos associados ao domínio controlado pelos atacantes:

avsvmcloud.com

O tráfego era disfarçado para se assemelhar às comunicações do Orion Improvement Program (OIP), dificultando a detecção por ferramentas de monitoramento de rede. Durante a fase inicial da infecção, o backdoor coletava informações do ambiente comprometido para permitir que os operadores selecionassem alvos de maior valor estratégico antes de executar cargas adicionais, como o loader TEARDROP, utilizado para implantar payloads em memória.

Embora milhares de organizações tenham recebido a atualização comprometida, apenas um subconjunto foi explorado ativamente, incluindo agências governamentais dos Estados Unidos e grandes empresas de tecnologia.

Entre as principais TTPs observadas destacam-se:

- Supply Chain Compromise – inserção de código malicioso no processo de build do software
- Signed Binary Abuse – distribuição do malware através de binários assinados legitimamente
- Stealthy C2 Communication – uso de infraestrutura dinâmica e mascaramento de tráfego
- Credential Access e Lateral Movement – exploração posterior de ambientes corporativos e serviços em nuvem

O incidente SolarWinds demonstrou como a industrialização da confiança em fornecedores de software pode ser explorada como vetor de ataque, permitindo que atores avançados obtenham acesso inicial privilegiado em larga escala.

MOVEit Transfer (CVE-2023-34362)

Figura 13 - Representação de jornal digital - MoveIT

O comprometimento da plataforma **MOVEit Transfer**, desenvolvido pela **Progress Software**, tornou-se um dos incidentes mais significativos relacionados à exploração massiva de software corporativo amplamente distribuído. Em maio de 2023, o grupo **Cl0p** ransomware explorou uma vulnerabilidade zero-day de SQL Injection (***CVE-2023-34362***) no software de Managed File Transfer (MFT), permitindo acesso não autorizado a bancos de dados e sistemas internos de organizações ao redor do mundo.

A falha permitia que atacantes manipulassem consultas SQL executadas pelo aplicativo web do **MOVEit**, contornando mecanismos de autenticação e obtendo acesso direto às bases de dados do sistema. A exploração levou à instalação de um web shell conhecido como:

LemurLoot

Disfarçado como um arquivo ASP.NET legítimo, o web shell permitia a execução remota de comandos e o acesso aos dados armazenados no sistema.

Após obter acesso ao ambiente comprometido, os operadores do **Cl0p** iniciavam operações automatizadas de exfiltração de dados, coletando informações sensíveis como registros financeiros, dados pessoais e documentos corporativos. Para evitar detecção, os dados eram transferidos em blocos através de canais criptografados.

Diferentemente de campanhas tradicionais de ransomware, o grupo adotou uma estratégia de extorsão baseada exclusivamente em vazamento de dados, ameaçando publicar as informações roubadas caso as vítimas não realizassem o pagamento do resgate.

O incidente impactou mais de 1.000 organizações globalmente, incluindo agências governamentais, instituições financeiras, empresas de tecnologia e organizações do setor de saúde. Entre os casos notáveis estão o comprometimento de dados associados ao U.S. Department of Energy e a

exposição de informações de funcionários através de provedores de serviços de folha de pagamento.

Entre as principais TTPs observadas destacam-se:

- Exploitation of Public-Facing Application – exploração de vulnerabilidade zero-day em software web
- SQL Injection – manipulação de consultas para acesso direto a bancos de dados
- Web Shell Deployment – uso do web shell LemurLoot para persistência e execução remota
- Automated Data Exfiltration – extração em larga escala de dados sensíveis
- Data Extortion – ameaça de divulgação pública dos dados roubados

O caso MOVEit demonstrou como vulnerabilidades em softwares amplamente utilizados podem gerar campanhas de exploração em escala global, reforçando os riscos associados à dependência de soluções de terceiros no ecossistema corporativo.

Envenenamento de Ecossistemas de Pacotes (npm / PyPI)

Figura 14 - Representação de jornal digital - NPM

Ecossistemas de gerenciamento de dependências como **npm** e **PyPI** tornaram-se uma das superfícies mais exploradas em ataques modernos à cadeia de suprimentos de software. Esses repositórios hospedam milhões de bibliotecas utilizadas diretamente em aplicações corporativas, pipelines de integração contínua e ambientes de desenvolvimento, tornando qualquer comprometimento potencialmente escalável para milhares de organizações.

Diversos incidentes recentes demonstram a diversidade de técnicas utilizadas nesse tipo de ataque. Campanhas como ***Shai-Hulud*** (2025) comprometeram contas de mantenedores por meio de phishing direcionado contra usuários do npm, resultando na inserção de **scripts maliciosos em atualizações de mais de 700 pacotes legítimos**. O código adulterado era capaz de coletar credenciais de desenvolvedores, *tokens* de acesso do **GitHub** e chaves de provedores em nuvem, além de utilizar essas credenciais para autopropagação em repositórios adicionais.

Outros ataques exploram técnicas como typosquatting, em que pacotes com nomes semelhantes a bibliotecas populares são publicados para capturar instalações equivocadas, como no caso do pacote mogodb. Também foram observados incidentes de comprometimento de mantenedores, como no caso do pacote event-stream, onde um atacante obteve acesso de commit ao projeto e inseriu código malicioso direcionado a carteiras de criptomoedas.

Além disso, ataques recentes demonstram o uso crescente de scripts de instalação maliciosos, capazes de executar código automaticamente durante o processo de instalação de dependências. Esses scripts frequentemente coletam variáveis de ambiente, credenciais de serviços em nuvem, tokens de APIs e dados armazenados em navegadores ou ferramentas de desenvolvimento.

Entre as principais TTPs observadas destacam-se:

- Supply Chain Compromise (T1195) – inserção de código malicioso em bibliotecas amplamente utilizadas
- Typosquatting e Dependency Confusion – publicação de pacotes maliciosos explorando a resolução automática de dependências
- Credential Access – coleta de tokens de desenvolvimento, chaves de API e credenciais de serviços em nuvem
- Execution via Installer Scripts – execução automática de código durante a instalação de dependências
- Data Exfiltration e Lateral Movement – uso de credenciais roubadas para acessar repositórios privados e sistemas corporativos

O crescimento massivo desses ecossistemas — com milhões de pacotes disponíveis e bilhões de downloads semanais — torna a verificação manual praticamente inviável. Como resultado, aplicações modernas frequentemente dependem de longas cadeias de dependências transitivas, ampliando significativamente a superfície de ataque.

Esse cenário evidencia como a confiança implícita em registries públicos e dependências open source pode ser explorada para comprometer ambientes de desenvolvimento, pipelines de build e aplicações em produção, consolidando o envenenamento de pacotes como um vetor recorrente em ataques à cadeia de suprimentos de software.

CODECOV

Figura 15 - Representação de jornal digital - Codecov

O incidente envolvendo a **Codecov**, plataforma amplamente utilizada em pipelines de integração contínua (CI/CD), demonstrou como ferramentas do ecossistema de desenvolvimento podem se tornar vetores críticos de ataques à cadeia de suprimentos. **Em janeiro de 2021, atacantes comprometeram a infraestrutura da empresa após identificar credenciais expostas em uma imagem Docker da Codecov Enterprise publicada no Docker Hub**. Essas credenciais estavam presentes em uma camada intermediária da imagem e permitiram acesso de escrita a um bucket CDN utilizado para distribuir o script Bash Uploader.

Com acesso à infraestrutura de distribuição, **os invasores modificaram o script Codecov Bash Uploade**r, amplamente utilizado por organizações para enviar relatórios de cobertura de código durante a execução de pipelines CI. O script era normalmente executado automaticamente nos ambientes de integração contínua das empresas, frequentemente por meio de chamadas remotas que baixavam e executavam o script diretamente nos pipelines.

Após a adulteração, os atacantes inseriram código malicioso responsável por enumerar todas as variáveis de ambiente do sistema durante a execução do pipeline. Essas informações eram então enviadas para servidores controlados pelos invasores por meio de requisições externas incorporadas ao próprio script modificado. **Como pipelines CI frequentemente armazenam tokens, chaves de API e credenciais de serviços em nuvem, o comprometimento possibilitou a coleta de segredos sensíveis utilizados em ambientes de desenvolvimento e deploy.**

Entre os dados potencialmente expostos estavam tokens AWS, credenciais de contas de serviço do Google Cloud, chaves de API, chaves GPG e credenciais de bancos de dados, além de informações associadas a repositórios Git privados. Empresas como HashiCorp, Twilio, Rapid7, Confluent, GoDaddy e Washington Post foram identificadas entre as organizações impactadas.

Entre as principais TTPs observadas destacam-se:

- Supply Chain Compromise (T1195) – adulteração de ferramenta distribuída em pipelines CI/CD
- Credential Access – coleta de segredos presentes em variáveis de ambiente
- Trusted Tool Abuse – exploração de ferramenta legítima amplamente adotada por desenvolvedores
- Environment Enumeration – coleta de informações do ambiente de execução
- Data Exfiltration Over Web Services – envio de dados sensíveis para infraestrutura controlada pelos atacantes

O incidente evidenciou os riscos associados à confiança implícita em ferramentas executadas automaticamente em pipelines CI/CD, demonstrando como a manipulação de componentes aparentemente benignos pode resultar na exposição massiva de credenciais e segredos corporativos.

SALESFORCE / SALESLOFT-DRIFT

Figura 16 - Representação de jornal digital - Salesforce

O incidente envolvendo **Salesforce**, Salesloft e Drift ilustra a evolução dos ataques à cadeia de suprimentos para o ecossistema de integrações SaaS baseadas em identidade. No ataque, invasores comprometeram inicialmente o repositório **GitHub** da **Salesloft**, obtendo acesso à infraestrutura da empresa na AWS e extraindo tokens OAuth associados à integração com a plataforma Drift. Como esses tokens representavam identidades válidas dentro das integrações SaaS, os atacantes conseguiram acesso indireto a ambientes corporativos de clientes que utilizavam essas integrações com **Salesforce** e **Google Workspace**.

A exploração baseou-se no sequestro de tokens OAuth válidos, permitindo que os invasores operassem utilizando identidades confiáveis dentro das aplicações integradas. **Dessa forma, foi possível acessar dados e funcionalidades do CRM sem a necessidade de credenciais diretas**, contornando mecanismos de autenticação tradicionais como MFA e cofres de credenciais.

Após obter acesso, os operadores utilizaram APIs legítimas da Salesforce, incluindo a Bulk API 2.0, para executar consultas em larga escala e exfiltrar dados corporativos. Para automatizar o processo, foram utilizadas

bibliotecas Python assíncronas, permitindo a coleta eficiente de grandes volumes de registros. Como o tráfego gerado utilizava chamadas legítimas de API, a atividade se misturava ao comportamento normal das integrações SaaS, dificultando a detecção por mecanismos de segurança tradicionais. Em alguns casos, os atacantes também removiam registros de consultas executadas para reduzir evidências da atividade.

O impacto operacional incluiu o acesso a dados de clientes, registros de CRM, comunicações corporativas e tickets de suporte, além da possibilidade de descoberta de credenciais expostas dentro desses registros, como chaves de acesso da AWS e tokens de serviços externos.

Entre as principais TTPs observadas destacam-se:

- Abuse of OAuth Applications – uso indevido de integrações SaaS confiáveis
- Valid Accounts – operação utilizando identidades legítimas
- Cloud API Abuse – exploração de APIs nativas da plataforma
- Persistence via Access Tokens – manutenção de acesso através de tokens válidos
- Data Collection via SaaS APIs – extração massiva de dados via interfaces legítimas

O caso demonstra como integrações baseadas em identidade e APIs SaaS ampliam significativamente a superfície de ataque da cadeia de suprimentos, permitindo que invasores explorem relações de confiança entre aplicações para obter acesso privilegiado a múltiplas organizações simultaneamente.

A análise desses incidentes demonstra que os ataques à cadeia de suprimentos não se limitam mais ao comprometimento direto de fornecedores de software. A superfície de ataque expandiu-se progressivamente para incluir pipelines de desenvolvimento, ecossistemas de dependências open source e integrações baseadas em identidade. **Em todos os casos analisados, o vetor explorado foi a confiança operacional existente entre componentes do ecossistema digital, seja na distribuição de atualizações, na resolução automática de dependências ou na delegação de acesso entre aplicações SaaS**. Esse padrão evidencia uma transformação estrutural no cenário de ameaças: a confiança tornou-se um recurso operacional crítico e, consequentemente, um alvo prioritário para atores maliciosos.

Lacunas Estruturais em Segurança de Cadeia de Suprimentos na América Latina

Embora ataques à cadeia de suprimentos tenham ganhado destaque global após incidentes como SolarWinds e MOVEit, muitas organizações na América

Latina ainda apresentam lacunas estruturais significativas na gestão desse tipo de risco. A rápida adoção de serviços em nuvem, dependências open source e integrações SaaS ampliou a superfície de ataque regional, enquanto práticas maduras de governança de software e monitoramento de fornecedores ainda estão em estágio inicial em muitos setores.

Essas limitações tornam o ambiente regional particularmente suscetível a ataques que exploram relações de confiança entre fornecedores, dependências de software e integrações tecnológicas. A tabela a seguir resume algumas das principais fragilidades observadas nesse contexto.

Lacunas Críticas em Segurança de Cadeia de Suprimentos na América Latina

Lacuna Estrutural	Descrição	Impacto Operacional	Consequência Estratégica
Ausência de SBOM (Software Bill of Materials)	Muitas organizações não mantêm inventários detalhados das dependências utilizadas em seus sistemas.	Dificuldade em identificar rapidamente se aplicações internas utilizam bibliotecas ou componentes comprometidos.	Resposta lenta a incidentes e exposição prolongada a vulnerabilidades em software de terceiros.
Monitoramento limitado de fornecedores de 3ª e 4ª parte	Programas de gestão de risco de terceiros geralmente se limitam a fornecedores diretos, sem visibilidade sobre dependências indiretas.	Ataques em fornecedores secundários podem se propagar silenciosamente para múltiplas organizações.	Amplificação do impacto de incidentes e maior dificuldade de contenção.
Alta dependência de serviços SaaS e infraestrutura estrangeira	Muitas empresas dependem de plataformas internacionais para CRM, colaboração e infraestrutura cloud.	Comprometimentos em plataformas externas podem afetar simultaneamente múltiplas organizações regionais.	Risco sistêmico e dependência operacional de ecossistemas tecnológicos externos.
Baixa adoção de modelos Zero Trust	Arquiteturas de segurança ainda baseadas em perímetro e confiança implícita entre sistemas internos.	Credenciais ou integrações comprometidas permitem movimentação lateral prolongada.	Persistência furtiva de atacantes e maior dificuldade de detecção.

Gestão limitada de dependências open source	Dependências externas frequentemente são incorporadas sem auditoria de segurança ou controle de integridade.	Instalação automática de bibliotecas comprometidas em pipelines de desenvolvimento.	Ampliação da superfície de ataque em ambientes de desenvolvimento e produção.

Tabela 2 - Tabela das lacunas críticas da cadeia de suprimentos Latam

CONCLUSÃO E PROJEÇÕES

A análise apresentada ao longo deste relatório demonstra que os ataques à cadeia de suprimentos deixaram de ser eventos excepcionais para se tornar um componente estrutural do cenário moderno de ameaças cibernéticas. A transformação da arquitetura digital global, marcada por ecossistemas interconectados, dependências de software distribuídas e integrações contínuas entre plataformas, criou um ambiente no qual a confiança operacional tornou-se um ativo crítico e, simultaneamente, um vetor privilegiado de comprometimento.

Diferentemente de intrusões tradicionais, os ataques à cadeia de suprimentos não dependem da exploração direta das defesas de cada organização individualmente. Ao comprometer pontos estratégicos do ecossistema tecnológico, fornecedores de software, plataformas SaaS, pipelines de desenvolvimento ou bibliotecas open source, adversários conseguem ampliar drasticamente a escala e o alcance de suas operações. Esse modelo operacional representa uma forma de industrialização do comprometimento, em que um único ponto de falha pode gerar impactos sistêmicos em múltiplas organizações.

Os estudos de caso analisados ao longo deste relatório evidenciam essa dinâmica. Incidentes como SolarWinds demonstraram o potencial de comprometer atualizações de software distribuídas globalmente. Explorações como o caso MOVEit revelaram como vulnerabilidades em plataformas corporativas amplamente adotadas podem ser rapidamente transformadas em campanhas de exfiltração massiva de dados. Ao mesmo tempo, ataques envolvendo Codecov, npm e PyPI ilustram como o próprio ecossistema de desenvolvimento de software passou a ser utilizado como vetor para coleta de credenciais e inserção de código malicioso em pipelines de build.

Essa evolução reflete uma mudança fundamental na lógica do ataque cibernético. O alvo primário deixou de ser o perímetro organizacional e passou a ser a infraestrutura de confiança que conecta organizações entre si.

Para os próximos anos, espera-se que essa tendência se intensifique. Três fatores estruturais indicam que ataques à cadeia de suprimentos continuarão a crescer em relevância até 2027:

Expansão da dependência de software e serviços externos.

A adoção acelerada de plataformas SaaS, APIs corporativas e bibliotecas open source continuará ampliando a interdependência entre organizações, criando novas superfícies de ataque baseadas em relações de confiança.

Automação ofensiva baseada em inteligência artificial.

Ferramentas baseadas em IA estão reduzindo o tempo necessário para reconhecimento de ambientes, exploração de dependências vulneráveis e

desenvolvimento de malware adaptativo, permitindo campanhas cada vez mais rápidas e escaláveis.

Convergência entre operações cibernéticas e interesses geopolíticos.

Estados-nação tem incorporado ataques à cadeia de suprimentos como instrumento estratégico para espionagem, sabotagem e influência, ampliando o impacto potencial desse vetor em infraestruturas críticas e cadeias produtivas globais.

Nesse cenário, organizações que continuarem a tratar segurança como um problema estritamente interno enfrentarão dificuldades crescentes para antecipar e conter incidentes. A resiliência operacional passará a depender da capacidade de verificar continuamente a integridade e a segurança de todo o ecossistema digital no qual a organização está inserida.

Entre os pilares fundamentais para essa transição destacam-se:

- **Visibilidade sobre dependências de software**, por meio da adoção de Software Bills of Materials (SBOM) e ferramentas de análise de composição de software.
- **Arquiteturas de segurança baseadas em Zero Trust**, capazes de limitar implicitamente a confiança entre sistemas, identidades e integrações.
- **Verificação criptográfica e controle de integridade** em pipelines de build, distribuição de software e execução de dependências.
- **Integração entre inteligência de ameaças e governança de fornecedores**, permitindo identificar riscos emergentes em componentes críticos da cadeia de suprimentos.

Em última análise, ataques à cadeia de suprimentos representam uma consequência direta da própria arquitetura da economia digital moderna. Quanto mais interconectados se tornam os sistemas que sustentam a operação das organizações, maior será a necessidade de mecanismos capazes de verificar continuamente a confiança em cada elo dessa cadeia.

A segurança cibernética, portanto, deixa de ser apenas um exercício de proteção de perímetro e passa a ser, cada vez mais, **um problema de governança da confiança digital**.

Organizações que compreenderem essa mudança estrutural estarão mais bem posicionadas para antecipar ameaças emergentes. As que não o fizerem continuarão reagindo a incidentes que se propagam silenciosamente através da infraestrutura invisível que sustenta o ecossistema digital global.

ANEXO TÉCNICO

MAPEAMENTO MITRE ATT&CK

Tática	Técnica	ID	Descrição
Initial Access	Supply Chain Compromise	T1195	O adversário compromete fornecedores de software, dependências open source ou pipelines de build para inserir código malicioso em atualizações ou bibliotecas legítimas. Como o software comprometido é distribuído por canais confiáveis, o malware alcança automaticamente múltiplas organizações.
Initial Access	Trusted Relationship	T1199	O atacante explora relações de confiança entre organizações, integrações SaaS ou fornecedores de tecnologia para acessar ambientes corporativos indiretamente, utilizando permissões delegadas ou integrações legítimas entre sistemas.
Execution	Command and Scripting Interpreter	T1059	Scripts maliciosos são executados em pipelines de build, scripts de instalação de pacotes ou automações CI/CD. O adversário insere comandos que coletam dados sensíveis, instalam payloads adicionais ou estabelecem comunicação com infraestrutura de comando e controle.
Execution	User Execution	T1204	O atacante depende da execução de software aparentemente legítimo, como atualizações de aplicações, instalação de bibliotecas ou execução de scripts de automação, para ativar código malicioso dentro do ambiente da vítima.
Persistence	Valid Accounts	T1078	Credenciais legítimas comprometidas — como contas de desenvolvedores, tokens de API ou chaves de autenticação — são utilizadas para manter acesso persistente a repositórios, pipelines de desenvolvimento ou ambientes cloud sem gerar alertas imediatos.
Persistence	Server Software Component	T1505	O adversário insere componentes maliciosos diretamente em aplicações, bibliotecas ou módulos de software distribuídos aos usuários, garantindo execução contínua do código comprometido sempre que o software for utilizado.

Defense Evasion	Signed Binary Proxy Execution	T1218	O atacante utiliza executáveis ou bibliotecas assinadas digitalmente para executar código malicioso por meio de aplicações confiáveis, dificultando a detecção por ferramentas de segurança que confiam em binários assinados.
Defense Evasion	Obfuscated/Encrypted Files or Information	T1027	Código malicioso é ofuscado ou criptografado dentro de scripts, pacotes ou dependências para dificultar análise estática e evitar que mecanismos de segurança detectem a presença do payload.
Credential Access	Steal Application Access Token	T1528	Tokens de autenticação utilizados por APIs, serviços cloud ou integrações SaaS são coletados a partir de variáveis de ambiente, arquivos de configuração ou memória do sistema, permitindo acesso direto a recursos corporativos.
Credential Access	Credentials from Password Stores	T1555	O atacante busca credenciais armazenadas em navegadores, ferramentas de desenvolvimento ou gerenciadores de segredos presentes no ambiente do desenvolvedor ou pipeline CI/CD comprometido.
Lateral Movement	Exploitation of Remote Services	T1210	Após obter acesso inicial, o adversário explora serviços remotos, APIs corporativas ou integrações entre sistemas para expandir o comprometimento para outros recursos dentro da infraestrutura da organização.
Collection	Data from Cloud Storage	T1530	O atacante coleta dados armazenados em serviços de armazenamento em nuvem, repositórios corporativos ou plataformas SaaS acessadas com credenciais ou tokens comprometidos.
Exfiltration	Exfiltration Over Web Services	T1567	Informações sensíveis são exfiltradas utilizando APIs legítimas, serviços web ou plataformas cloud para mascarar o tráfego malicioso como atividade normal da aplicação.

Tabela 3 - Tabela de mapeamento MITRE ATT&CK

Perfil de Atores Relevantes

Ator / Ecossistema	Motivação	Vertor de Supply Chain	Objetivo Operacional	Exemplo de Campanha
DPRK-Nexus (Lazarus, Andariel, BlueNoroff)	Financeira e estatal	Comprometimento de bibliotecas open source, pacotes npm/PyPI e softwares trojanizados	Roubo de criptomoedas, credenciais de desenvolvedores e acesso a infraestruturas de exchanges	campanhas envolvendo pacotes maliciosos em npm/PyPI, ataques a desenvolvedores Web3
China-Nexus (APT41, APT10, Mustang Panda)	Espionagem estratégica e coleta de inteligência	Comprometimento de softwares empresariais, dispositivos de rede e cadeias logísticas de TI	Acesso persistente a redes governamentais e corporativas para coleta de dados estratégicos	campanhas envolvendo softwares corporativos e infraestrutura de telecomunicações
Rússia-Nexus (APT29, Turla, Sandworm)	Espionagem e operações de influência	Inserção de código malicioso em atualizações de software e abuso de certificados digitais	Estabelecimento de acesso furtivo a redes governamentais e infraestrutura crítica	SolarWinds Orion, campanhas envolvendo software corporativo comprometido
Grupos Ransomware-as-a-Service (Cl0p, LockBit, BlackCat)	Financeiro	Exploração de vulnerabilidades em softwares amplamente distribuídos e fornecedores de tecnologia	Comprometimento simultâneo de múltiplas organizações para extorsão em larga escala	MOVEit Transfer, GoAnywhere MFT, Accellion FTA
Atores oportunistas e crimeware	Financeiro ou credenciais	Publicação de pacotes maliciosos, typosquatting e dependency confusion em repositórios open source	Roubo de tokens, credenciais cloud e acesso a ambientes de desenvolvimento	pacotes maliciosos em npm/PyPI e campanhas de dependency confusion

Tabela 4 - Tabela de perfis de atores relevantes

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- World Economic Forum (WEF) - Global Cybersecurity Outlook 2026
- Palo Alto Networks (Unit 42) - Global Incident Response Report 2026
- ENISA (European Union Agency for Cybersecurity) - Threat Landscape 2025
- Gartner - Cybersecurity Trends 2025-2026
- Group-IB: High Tech Crime Trends Report 2026
- Microsoft Digital Defense Report 2025
- ZScaler: State of Cyberthreats and Protection
- TrueSec: Threat Intelligence Report 2026

AUTORES

- **Gustavo Santos – Threat Researcher**

heimdall
security research
A DIVISION OF ISH