TLP: CLEAR

Pesquisa de Cibersegurança Cyber Threat Actors

Ameaças Persistentes Avançadas: Setor Público

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse as análises produzidas pela ISH Tecnologia sobre Táticas, Técnicas e Procedimentos (TTPs) de Threat Actors, malwares emergentes, vulnerabilidades críticas e outros temas relevantes em cibersegurança. Clique na imagem abaixo para conferir nosso blog.

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: CONHECENDO A AMEAÇA

Figura 1 - Congresso Nacional

O Setor Público, englobando a administração direta e indireta, bem como a infraestrutura crítica associada, tornou-se um dos principais alvos no cenário cibernético contemporâneo. Na América Latina, e especialmente no Brasil, a rápida transformação digital, a crescente dependência de serviços online e a complexidade dos ecossistemas tecnológicos ampliaram não apenas a superfície de ataque, mas também o valor estratégico que governos representam para cibercriminosos e atores patrocinados por Estados-nação. A criticidade do setor é evidente: além de concentrar grandes volumes de dados sensíveis, como registros de identificação pessoal de cidadãos, inteligência de Estado e informações financeiras, ele é responsável por assegurar a continuidade de serviços essenciais à população: saúde, educação, transporte, energia e comunicação. Uma interrupção significativa nesses domínios não se limita a prejuízos técnicos ou financeiros, podendo rapidamente se transformar em uma crise social, econômica e política.

O ataque conduzido pelo grupo **WIZARD SPIDER** (**Conti**) contra o governo da Costa Rica, em 2022, exemplifica esse risco ao provocar a suspensão de múltiplas plataformas governamentais e culminar na declaração de estado de emergência nacional. Casos dessa natureza demonstram que ataques cibernéticos direcionados a governos podem paralisar países inteiros, afetar a confiança da população em suas instituições e comprometer pilares de soberania e governança.

Mais recentemente, em março de 2025, o Brasil vivenciou um episódio preocupante com a tentativa de ataque à ***Empresa Brasileira de Hemoderivados e Biotecnologia*** (Hemobrás). Ainda que o **Ransomware** não tenha sido executado com sucesso, a simples detecção da ameaça exigiu a interrupção dos serviços da empresa por semanas, como medida preventiva e de execução do plano de continuidade de negócios. A Hemobrás é a responsável pela produção e distribuição de medicamentos para todo o ***Sistema Único de Saúde*** (SUS), o que evidencia a criticidade de seus sistemas e a gravidade de um possível comprometimento. Esse incidente ressalta um ponto essencial: a dependência digital de serviços públicos vitais aumenta a superfície de ataque e torna a resiliência operacional uma prioridade de segurança nacional. Mesmo uma tentativa frustrada pode gerar impactos substanciais em escala nacional, demonstrando como a indisponibilidade temporária de sistemas públicos essenciais pode afetar diretamente a saúde e o bem-estar da população, além de abalar a confiança institucional e a credibilidade internacional do país.

Esse cenário se agrava diante de desafios estruturais e tendências regionais. Muitos países latino-americanos ainda não alcançaram um patamar uniforme de maturidade em governança de cibersegurança, enfrentando lacunas em orçamento, recursos humanos e capacidade técnica. Paralelamente, há a necessidade de responder a dilemas estratégicos como a dependência tecnológica de fornecedores estrangeiros em setores sensíveis, exemplificada pelos debates sobre o uso de tecnologias chinesas em redes 5G e infraestrutura crítica. Soma-se a isso o uso político de ferramentas digitais e denúncias de espionagem estatal em países como Brasil e Colômbia, além de contextos em que regimes autoritários utilizam incidentes cibernéticos e vigilância digital como instrumentos de controle e repressão.

Outro fator emergente é a ascensão da ***Inteligência Artificial*** (**IA**), que amplia tanto os riscos quanto as oportunidades. De um lado, governos precisam lidar com a intensificação de campanhas de desinformação e manipulação de opinião pública potencializadas por ***IA generativa***, ameaçando processos eleitorais e a estabilidade política. De outro, buscam explorar o potencial da tecnologia para acelerar a transformação digital, otimizar serviços públicos e fortalecer a inovação socioeconômica. Essa dualidade reforça a urgência de estruturas éticas e técnicas que equilibrem inovação e segurança.

Diante desse panorama, o setor público latino-americano encontra-se em uma posição de alta exposição e relevância estratégica, sendo simultaneamente alvo de ataques de motivação financeira, geopolítica e ideológica. A defesa desse ambiente demanda um esforço coordenado que una políticas públicas robustas, parcerias internacionais, amadurecimento técnico e capacidade de resposta ágil. Mais do que proteger sistemas e dados, trata-se de preservar a continuidade do Estado, a confiança da sociedade e a própria soberania nacional.

ESTRATÉGICO: CONHECENDO OS IMPACTOS

O panorama de ameaças ao Setor público na América Latina, especialmente no Brasil, é caracterizado pela convergência de dois eixos dominantes: de um lado, o cibercrime financeiro em larga escala, impulsionado por campanhas de ransomware e extorsão digital; de outro, operações cibernéticas sofisticadas de espionagem, conduzidas por grupos patrocinados por Estados-nação. Essa sobreposição de interesses (econômicos, estratégicos e geopolíticos) cria um ambiente de risco híbrido, no qual as fronteiras entre crime organizado, hacktivismo e operações de inteligência estatal tornam-se cada vez mais difusas.

Os números refletem a gravidade da situação: *o setor público figura como o mais mencionado em fóruns clandestinos da dark web na região* (**18,57%**) e o mais visado em campanhas de phishing (**16,99%**), com o Brasil liderando ambos os indicadores, concentrando 30,98% das menções e mais de 51% das campanhas identificadas. Isso evidencia o papel do país como hub estratégico digital e geopolítico na América Latina, e reforça a necessidade de uma postura de defesa ativa e de inteligência cibernética contínua.

1.1 Diferenciação: APT vs. Cibercrime e Hacktivismo

As **APTs** (**Advanced Persistent Threats**) representam a face mais sofisticada das ameaças cibernéticas. Diferenciam-se do cibercrime tradicional por operarem de forma sustentada e com objetivos estratégicos de longo prazo, geralmente voltados à espionagem, sabotagem ou influência política. São, em sua maioria, patrocinadas por Estados, o que lhes garante financiamento contínuo, acesso a vulnerabilidades ***zero-day*** e capacidade operacional em múltiplos vetores (rede, *endpoint*, ***IoT***, ***OT*** e nuvem).

O cibercrime comum, por sua vez, mantém foco no ganho financeiro direto e imediato, como fraudes, extorsão e sequestro de dados (*ransomware*). No entanto, a distinção entre ambos vem se tornando cada vez mais tênue. Grupos APT restringidos por sanções econômicas ou necessitados de financiamento autônomo têm recorrido a táticas criminosas: o **Lazarus Group** (Coreia do Norte) é o exemplo mais emblemático, misturando espionagem militar com roubo financeiro em larga escala. Paralelamente, grupos criminosos vêm adotando técnicas de ofuscação, movimentação lateral e exfiltração discretas, inspiradas em operações **APT**, o que complica a atribuição e desafia a defesa tradicional.

1.2 As Quatro Categorias de Motivação de Ataques ao Setor

As campanhas APT direcionadas ao setor governamental seguem quatro linhas de motivação estratégica, que frequentemente se sobrepõem em operações híbridas:

- **Espionagem Cibernética**: É a motivação primária e mais recorrente. Busca a coleta de inteligência política, militar e diplomática, bem como o roubo de propriedade intelectual e dados de cidadãos. Essas ações visam gerar vantagem informacional e suporte à política externa e econômica do Estado patrocinador. Exemplo: grupos como ***Mustang Panda*** (China) e ***APT29*** (Rússia) têm histórico de coleta de dados de embaixadas e ministérios em países da América do Sul.
- **Destruição ou Disrupção Operacional**: O foco é provocar impacto físico ou lógico em infraestruturas críticas, como energia, transporte e comunicações. *Malware* destrutivo (como *wiper*) é frequentemente empregado em campanhas de retaliação ou sabotagem. Exemplo: o grupo ***Sandworm*** (ligado ao GRU russo) usou o malware ***Industroyer*** em ataques contra sistemas elétricos, e já foi associado a tentativas de penetração em infraestruturas de energia de países emergentes.
- **eCrime e Monetização de Dados Públicos**: Grupos cibercriminosos regionais, e potencialmente atores estatais, utilizam táticas avançadas para extrair e vender dados governamentais sensíveis (como os vazamentos de informações de chaves PIX, Poder Judiciário e Polícia Federal no Brasil) para fins de fraude e monetização. Alguns grupos **APT** operam em um modelo híbrido, realizando ataques com motivação financeira para sustentar outras frentes. O ***Lazarus Group*** ilustra esse comportamento, combinando espionagem com roubos de criptomoedas e invasões a bancos.
- **Hacktivismo e Operações de Encobrimento**: Ataques com narrativa política ou ideológica que, muitas vezes, mascaram operações estatais. Servem para gerar confusão e dificultar a atribuição direta. O uso de coletivos hacktivistas “fantasmas” tem sido comum em campanhas iranianas e russas. Exemplo: operações recentes de desfiguração de sites governamentais na América Latina, reivindicadas por supostos grupos hacktivistas, mostraram indícios de infraestrutura compartilhada com atores ligados a serviços de inteligência.

1.3 Vitimologia: Alvos Governamentais de Alto Valor

Figura 2 - Imagem representando o blueprint da América Latina

O leque de alvos das **APTs** é vasto, mas o foco no setor público/governamental é determinado pelo valor estratégico dos dados detidos. Esses alvos incluem, mas não se limitam a, organizações governamentais centrais, defesa, serviços financeiros estatais, e infraestrutura crítica.

1.3.1 ALVOS SETORIAIS CRÍTICOS

Figura 3 - Alvos críticos de ataques ao setor público

- **Defesa e Militar**: Alvos clássicos de coleta de inteligência tática, logística e tecnológica. Operações do grupo ***SideWinder APT*** contra forças armadas asiáticas ilustram esse foco, mas campanhas similares já foram detectadas na América Latina com técnicas de spear phishing voltadas a setores de defesa.
- **Relações Exteriores e Diplomacia**: Os Ministérios de Relações Exteriores e embaixadas são focos constantes de espionagem, visando negociações multilaterais e alinhamentos geopolíticos. Grupos como *BackdoorDiplomacy* e *RedDelta* foram observados realizando exfiltrações em embaixadas latino-americanas entre 2023 e 2024.
- **Infraestrutura Crítica (CI/OT):** Setores de energia, transporte, saneamento e comunicações estão entre os mais vulneráveis, dada sua dependência de sistemas legados e o baixo isolamento entre **TI** e **OT**. O ***Sandworm***, o

ChamelGang e o ***Tonto Team*** figuram entre os principais atores com histórico de *targeting* nesse tipo de ambiente.

Alvo	Sub-Alvos	Dados Críticos Visados	Referência Regional
Tecnologia, Aeroespacial e Militar	P&D, Logística, Setor de Comunicações	Propriedade Intelectual (PI), Planos Militares, Segredos de Estado	Brasil (APT10, APT27)
Governo Central e Diplomacia	Ministérios, Órgãos Reguladores, Administração Indireta	Documentos de Negociação, Comunicações Criptografadas, Políticas Governamentais	América Central e do Sul (APT15)
Saúde e Infraestrutura Crítica (CI/OT)	Empresas estatais, Energia, Transporte, Comunicação...	Dados de Cadeia de Suprimentos, Credenciais de Controle (ICS/OT), Disrupção Lógica...	Regional (Conti/Costa Rica), Alerta OT Global
Saúde e Infraestrutura Crítica (CI/OT)	Sistemas de Pagamento (PIX), Polícia Federal, Tribunais	Dados Sensíveis de Cidadãos (PII, LGPD) para Monetização e Fraude, Credenciais...	Brasil (Monetização de dados públicos)

Tabela 1 - Principais Alvos

1.3.2 VETORES DE ACESSO E TENDÊNCIAS OBSERVADAS

Figura 4 - Principais vetores de acesso

Em 2024, os **vetores de acesso inicial mais recorrentes** em ataques contra o setor público latino-americano refletiram um equilíbrio entre exploração técnica e manipulação humana: um cenário que mistura vulnerabilidades conhecidas, engenharia social sofisticada e abuso de identidades legítimas. Os vetores de acesso inicial mais comuns em ataques ao setor público latino-americano foram:

- **Exploração de aplicações expostas na internet**: A exploração de sistemas vulneráveis continua sendo o principal ponto de entrada. Governos ainda operam servidores legados e aplicações desatualizadas, frequentemente sem segmentação adequada ou monitoramento de tráfego. Essa tendência é amplificada pela **exposição massiva de endpoints** e portais governamentais em nuvem pública, criando uma superfície de ataque dinâmica e difícil de proteger.
- **Phishing direcionado**: As campanhas de phishing direcionado (*spear phishing*) evoluíram em sofisticação e personalização. Iscas temáticas simulando licitações públicas, ofícios judiciais, convocações de ministérios ou comunicados de políticas públicas são amplamente utilizados. Em **2024**, observou-se o uso crescente de IA generativa na criação de mensagens com gramática e estilo local, aumentando a taxa de sucesso das campanhas. Muitos ataques combinam phishing inicial com payloads de segunda fase entregues via links encurtados, documentos com macros ou arquivos **PDF** trojanizados, frequentemente hospedados em domínios legítimos comprometidos. Essa abordagem híbrida explora o elo mais fraco da cadeia de segurança: o fator humano.
- **Uso de credenciais válidas**: O uso de credenciais legítimas (obtidas por meio de phishing, infostealers ou vazamentos anteriores) permanece um

vetor crítico. A ausência de autenticação multifator (**MFA**), políticas fracas de IAM (**Identity & Access Management**) e o reaproveitamento de senhas em múltiplos sistemas tornam essa técnica altamente efetiva. Grupos criminosos e ***Initial Access Brokers*** (**IABs**) comercializam essas credenciais na dark web, oferecendo acesso direto a redes de ministérios e órgãos públicos. Esse mercado paralelo serve de ponte entre espionagem e cibercrime, alimentando tanto campanhas de Ransomware quanto intrusões patrocinadas por Estados-nação. Essas técnicas evidenciam tanto a expansão da superfície de exposição digital de governos quanto a carência de políticas estruturadas de gestão de identidade e vulnerabilidades.

- **Engenharia Social e Manipulação Interna:** Além do phishing tradicional, há um aumento perceptível no uso de engenharia social avançada, especialmente contra funcionários de áreas técnicas e administrativas. Atores adversários têm explorado redes sociais profissionais (LinkedIn, Telegram, Discord) para recrutar ***insiders***, obter informações sobre infraestrutura interna ou manipular processos de autenticação. Casos pontuais na região mostram o surgimento de ameaças internas (Insider Threats), com colaboradores coagidos ou motivados financeiramente a fornecer credenciais, tokens de acesso ou informações de rede. Esse vetor humano, muitas vezes negligenciado, é cada vez mais explorado por APTs com foco em espionagem prolongada e exfiltração furtiva.
- **CVEs e Cadeia de Suprimentos:** Outro vetor emergente é o ataque à cadeia de suprimentos digital. Fornecedores terceirizados de tecnologia e infraestrutura de governo frequentemente se tornam o elo mais fraco. Explorações de vulnerabilidades conhecidas (***CVEs***) em software amplamente utilizado, como *Fortinet*, *VMware* e *Microsoft Exchange*, têm sido recorrentes. Esses incidentes ampliam o impacto para múltiplas instituições públicas simultaneamente, expondo dados sensíveis e credenciais de acesso administrativo em larga escala.

Além disso, a profissionalização das operações criminosas tem impulsionado o modelo ***de Ransomware-as-a-Service*** (**RaaS**) e o crescimento de mercados paralelos de ***Initial Access Brokers*** (**IABs**), responsáveis por comercializar credenciais e acessos privilegiados de órgãos públicos na dark web. Paralelamente, campanhas de espionagem ligadas à China, Rússia e Coreia do Norte têm se intensificado na região, refletindo interesses geopolíticos em recursos naturais, acordos de defesa e posicionamento diplomático.

A sobreposição entre **espionagem, extorsão e hacktivismo** cria um ecossistema onde as motivações variam de **lucro rápido a influência geopolítica**. Ataques que começam como **intrusões financeiras** podem evoluir para

operações de coleta de inteligência, enquanto campanhas hacktivistas podem **mascarar ações estatais**.

Esse mosaico de ameaças transforma o **setor público latino-americano** em um **campo de batalha digital estratégico**, onde a informação é o ativo mais visado e a confiança institucional, o principal alvo.

1.3.3 IMPACTOS

Figura 5 - Impactos dos ataques ao setor público

As consequências de uma intrusão bem-sucedida no setor público são **profundas, duradouras e multidimensionais**, afetando não apenas sistemas tecnológicos, mas também a **governança, a estabilidade social e a soberania nacional**. Os impactos se manifestam em diferentes níveis:

- **Interrupção de Serviços Essenciais e Impacto na População:** Ataques a órgãos públicos podem resultar na indisponibilidade de serviços críticos como saúde, educação, transporte, previdência, arrecadação e segurança pública. Um *ransomware* ou ataque à infraestrutura de TI de um ministério, por exemplo, pode paralisar sistemas de emissão de documentos, pagamentos de benefícios ou operação hospitalar, afetando diretamente milhões de cidadãos. Esses incidentes transcendem a esfera técnica e geram crises humanitárias e institucionais, especialmente em países com infraestrutura digital centralizada.
- **Exposição e Vazamento de Dados Sensíveis:** Os governos detêm alguns dos bancos de dados mais sensíveis da sociedade, incluindo registros biométricos, informações fiscais, de defesa e inteligência, além de dados de servidores e cidadãos. A exposição ou comercialização desses dados na dark web pode comprometer a segurança nacional e a integridade de investigações sigilosas, além de facilitar campanhas de desinformação, fraudes e manipulação política. Casos recentes de vazamentos em portais de prefeituras e ministérios mostraram o impacto direto na confiança pública e na credibilidade institucional.
- **Perda de Integridade e Manipulação de Informações:** Ataques direcionados ao conteúdo e integridade de sistemas governamentais, como alterações em cadastros, bases de dados eleitorais, portais de transparência ou documentos oficiais, comprometem a autenticidade das informações estatais. Isso abre espaço para campanhas de desinformação e sabotagem política, explorando a perda de confiabilidade das fontes

oficiais. Em contextos eleitorais ou de instabilidade social, tais ações podem ter efeitos diretos na governabilidade e na legitimidade democrática.

- **Erosão da Confiança Institucional e Repercussões Políticas:** A confiança da população no Estado é um ativo crítico. Quando governos são vistos como incapazes de proteger dados e serviços, ocorre uma erosão da legitimidade institucional. A percepção de vulnerabilidade pode gerar descrédito internacional, perda de credibilidade perante investidores e aliados, além de impactos diretos na estabilidade política. Em países com tensões internas, grupos adversários podem explorar incidentes cibernéticos como ferramentas de pressão ou propaganda ideológica, amplificando o dano reputacional.
- **Riscos à Soberania e Segurança Nacional:** Intrusões que atingem sistemas de defesa, diplomacia, energia ou infraestrutura crítica representam ameaça direta à soberania nacional. Grupos de espionagem patrocinados por Estados-nação podem explorar vulnerabilidades para monitorar comunicações estratégicas, acessar planos militares, manipular políticas externas ou obter vantagens geopolíticas. O impacto vai além do domínio digital, ele pode redefinir alianças internacionais e comprometer operações de segurança.
- **Ameaças Internas e Comprometimento de Confidencialidade:** Os riscos de ameaças internas (***Insider Threats***) crescem à medida que ambientes governamentais permanecem dependentes de acessos privilegiados e autenticação fraca. Colaboradores podem ser coagidos, manipulados ou motivados financeiramente a fornecer informações, credenciais ou até executar ações que facilitem ataques externos. Esse vetor interno é especialmente perigoso em instituições com dados de alta sensibilidade, como agências de inteligência, ministérios da defesa e controladorias.
- **Complexidade na Detecção e Resposta:** A crescente sofisticação das ameaças com uso de ferramentas legítimas (***Living off the Land***), execução em memória, uso de **IA** para evasão e infraestrutura em nuvem descentralizada, torna a detecção e resposta cada vez mais desafiadoras. Muitos órgãos ainda dependem de arquiteturas legadas, sem visibilidade unificada entre *endpoints*, rede e nuvem. Isso gera janela de exposição prolongada e dificuldade na correlação de eventos, retardando a resposta e aumentando o impacto.
- **Dependência Tecnológica e Cadeia de Suprimentos:** O setor público latino-americano depende fortemente de fornecedores estrangeiros de tecnologia, especialmente em áreas de telecomunicações, defesa e gestão de dados. Ataques à cadeia de suprimentos ou exploração de vulnerabilidades em softwares amplamente utilizados (como *Microsoft Exchange*, *Fortinet*, *VMware*) podem comprometer múltiplas entidades públicas simultaneamente, ampliando o alcance do impacto. Além disso, falhas em provedores terceirizados de nuvem e data centers têm o potencial de interromper funções estatais críticas.

- **Impactos Econômicos e Administrativos:** Os custos de reparação, restauração e investigação forense são significativos. Além do impacto financeiro direto, há prejuízos indiretos como perda de produtividade, atrasos em políticas públicas e gastos emergenciais com comunicação e mitigação. Muitos governos acabam realocando orçamentos de projetos estratégicos para cobrir incidentes, prejudicando planos de desenvolvimento e inovação digital.

No setor público, o impacto de um incidente cibernético ultrapassa o domínio técnico: trata-se de preservar a continuidade do Estado e a confiança da sociedade. A cibersegurança, portanto, deve ser tratada como assunto de Estado, e não apenas como responsabilidade técnica. Reforçar governança, visibilidade, capacitação e cooperação internacional é essencial para garantir que ataques cibernéticos não se transformem em crises nacionais. Em um ambiente onde a informação é poder e a confiança é o alicerce do Estado, a proteção cibernética tornou-se um pilar da soberania moderna.

TÁTICO: COMPREENDENDO O ATAQUE

O setor público latino-americano, em especial o brasileiro, tem se consolidado como **um dos principais alvos de operações cibernéticas híbridas**, onde cibercrime, espionagem e hacktivismo convergem em um mesmo ecossistema de ameaça.

Governos detêm **ativos de alto valor estratégico**, como dados pessoais de cidadãos, informações de defesa, comunicações diplomáticas, registros fiscais e infraestrutura crítica. Isso faz com que órgãos estatais sejam alvos tanto de **operações de espionagem patrocinadas por Estados-nação**, quanto de **ataques de ransomware e extorsão conduzidos por grupos criminais**.

A cadeia de ataque direcionada a entidades governamentais costuma se desenrolar em **duas fases complementares**, refletindo a segmentação dos ambientes tecnológicos:

1. A fase **inicial**, focada em comprometer a infraestrutura de **TI corporativa** (ambientes administrativos e ministeriais), onde se obtém acesso, persistência e reconhecimento;
2. A fase **avançada**, que mira **sistemas críticos e redes OT** (*Operational Technology*), como energia, comunicações, transporte e saúde, onde os impactos reais à continuidade do Estado podem ocorrer.

Essa dinâmica representa uma **Kill Chain híbrida**, combinando espionagem, sabotagem e exploração financeira.

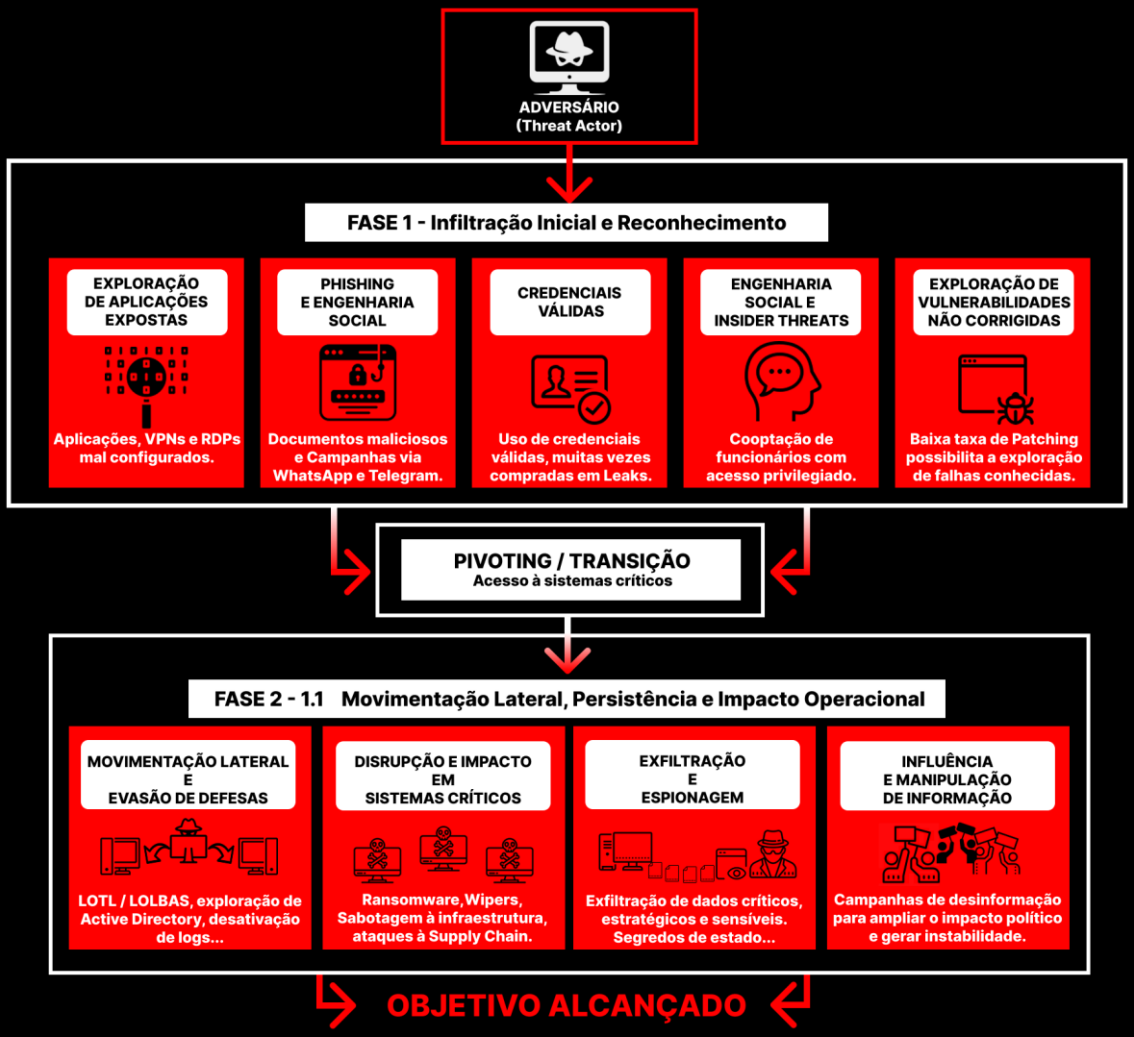

Figura 6 - Kill Chain do Setor Público

2.1 Fase 1: Infiltração Inicial e Reconhecimento

A infiltração inicial é o ponto mais crítico para mitigação. Os adversários exploram uma ampla gama de vetores, aproveitando **vulnerabilidades conhecidas (CVE), fraquezas humanas e lacunas de visibilidade** nos sistemas governamentais.

2.1.1 Exploração de Aplicações e Infraestruturas Expostas

Um vetor predominante, especialmente em órgãos com sistemas legados e datacenters on-premises. Serviços desatualizados, painéis administrativos abertos e aplicações web vulneráveis são rotineiramente explorados.

Exemplos comuns incluem:

- **CVE-2023-34362 (MOVEit Transfer)** e **CVE-2024-3400 (Palo Alto PAN-OS)**, exploradas amplamente em 2024 por grupos ligados à China e à Rússia.
- Exploração de **VPNs** e **RDPs mal configurados**, permitindo acesso direto a redes internas.

- Uso de scanners automatizados (como *Masscan* e *Nmap*) por **Initial Access Brokers (IABs)** que posteriormente vendem o acesso a grupos de ransomware.

2.1.2 Phishing e Engenharia Social

O vetor humano permanece o mais explorado. Campanhas de Spearphishing com **temas governamentais (licitações, editais, comunicados oficiais, intimações jurídicas)** são amplamente utilizadas. O uso de **IA Generativa** ampliou a personalização de e-mails, documentos e até deepfakes de autoridades.

Casos observados incluíram:

- Phishing com **documentos PDF maliciosos** simulando comunicações oficiais.
- Campanhas via **WhatsApp e Telegram** se passando por , em ataques de social engineering a servidores administrativos.

2.1.3 Uso de Credenciais Válidas e Infostealers

O **uso de credenciais legítimas** se tornou um vetor recorrente, especialmente pela **ausência de MFA e má gestão de identidade** (IAM). Infostealers como **Lumma, RedLine e Raccoon** continuam sendo os principais responsáveis pela coleta de logins e tokens de sessão de servidores públicos. Essas credenciais são revendidas por valores entre **US$ 5 e US$ 20** em fóruns clandestinos, sendo reutilizadas em ataques direcionados.

2.1.4 Engenharia Social e Exploração Interna (Insider Threat)

Adversários têm recorrido a **táticas de persuasão e cooptação de insiders**, funcionários ou prestadores com acesso privilegiado, para obter credenciais, documentos ou implantar *backdoors*. A ausência de monitoramento de comportamento e a falta de segregação de privilégios em órgãos públicos favorecem esse tipo de infiltração. Em alguns casos, **funcionários terceirizados de suporte técnico** foram vetores de acesso a ambientes críticos.

2.1.5 Exploração de Vulnerabilidades Não Corrigidas (CVE Weaponization)

Governos sofrem com **baixa taxa de patching** e **janelas longas de exposição**. Grupos APT frequentemente se valem de **vulnerabilidades N-day** já conhecidas, como:

- **CVE-2022-30190** (**Follina**) – usada para execução remota via documentos do Office.
- **CVE-2023-0669** (GoAnywhere MFT) – amplamente explorada para exfiltração de dados governamentais.
- Vulnerabilidades em **Fortinet, VMware e Microsoft Exchange**, usadas por grupos como **APT28 (Rússia)** e **BackdoorDiplomacy (China)**.

2.1.6 Initial Access Brokers e RaaS

Os **IABs** desempenham papel central no ecossistema criminoso, vendendo acessos a redes públicas comprometidas. Esses acessos são depois adquiridos por **grupos de ransomware como LockBit, BlackCat (ALPHV), Play e RansomHouse**, que adaptam o payload conforme o perfil do órgão-alvo. O modelo **Ransomware-as-a-Service (RaaS)** profissionalizou-se e frequentemente reutiliza acessos obtidos de ataques anteriores.

2.2 Fase 2: Movimentação Lateral, Persistência e Impacto Operacional

Após o comprometimento inicial, o adversário busca consolidar controle e preparar terreno para os objetivos finais, **espionagem, disrupção ou extorsão**. O foco muda da infiltração para o **domínio sobre o ambiente**.

2.2.1 Movimentação Lateral e Evasão de Defesas

- Uso de **credenciais válidas** e **ferramentas legítimas (Living off the Land)** como PowerShell, WMI e PsExec.
- Exploração de **Active Directory** e **delegações incorretas de privilégios**, buscando domínio completo da rede.
- Técnicas de evasão incluem **desativação de logs (Wevtutil, Clear-EventLog)** e **injeção de código em memória** para evitar detecção.
- Ferramentas como **Cobalt Strike, Sliver e Brute Ratel** são amplamente observadas em campanhas contra governos latino-americanos.

2.2.2 Disrupção e Impacto em Sistemas Críticos

Nesta fase, o adversário busca impactar serviços essenciais, seja por meio de:

- Ransomware (LockBit, BlackSuit, Akira) – visando criptografar e interromper serviços públicos.
- Wiper Malware – utilizado em operações destrutivas (como o NotPetya e WhisperGate), apagando dados de forma irreversível.
- Sabotagem a Infraestrutura OT/CI, incluindo energia, comunicações, transporte e saúde, com potencial para causar efeitos cascata.
- Ataques à cadeia de suprimentos, comprometendo softwares de gestão e fornecedores de TI governamentais.

2.2.3 Exfiltração e Espionagem

Grupos APT patrocinados por Estados-nação priorizam a coleta de **dados estratégicos**:

- Comunicações diplomáticas e relatórios de inteligência.
- Documentos de defesa, orçamentos e dados de licitação.
- Correspondências internas e metadados de comunicação. A exfiltração é realizada via **túneis HTTPS, DNS over HTTPS (DoH)** e **protocolos ofuscados**, dificultando a detecção por SIEMs e proxies.

2.2.4 Operações de Influência e Manipulação de Informação

Após o vazamento, é comum o uso de **campanhas de desinformação** para amplificar o impacto político e psicológico.
Isso inclui a publicação seletiva de dados em **canais Telegram ou fóruns como BreachForums**, associando o vazamento a narrativas ideológicas ou partidárias.

Essas ações têm duplo propósito: **gerar instabilidade política e mascarar o verdadeiro objetivo do ataque (espionagem ou sabotagem).**

2.3 Fase 3: Persistência, Ocultação e Reinvestida

Muitos ataques contra o setor público não terminam com a extração de dados ou o pagamento de resgate. Adversários mantêm **presença persistente**, criando **backdoors, contas ocultas e acessos secundários**.

Esses pontos de persistência permitem:

- **Reconexão futura para novas campanhas**.
- **Venda de acesso** em mercados de IAB.
- **Acompanhamento de mudanças políticas e administrativas** dentro do órgão atacado.

Grupos como **APT29 (Rússia)** e **Earth Lusca (China)** são conhecidos por manter **campanhas longas (multi-year persistence)** em ministérios e instituições diplomáticas, utilizando táticas stealth de baixo ruído e exfiltração periódica.

A compreensão tática da cadeia de ataque contra o setor público evidencia que **não existe uma linha clara entre espionagem, sabotagem e crime cibernético**. Os adversários operam em **camadas sobrepostas**, utilizando a mesma infraestrutura e os mesmos vetores, mas com objetivos distintos: enriquecimento ilícito, desestabilização política ou coleta de inteligência estratégica.

OPERACIONAL: COMPREENDENDO O ATAQUE

A camada de inteligência operacional visa transformar o comportamento adversário em artefatos observáveis, técnicas rastreáveis e indicadores concretos para as equipes de defesa. Enquanto a inteligência estratégica foca em riscos amplos e a tática descreve o modus operandi, a inteligência operacional mergulha nos **detalhes técnicos específicos**, mapeando como os atacantes realmente agem desde o acesso inicial até a execução, evasão e exfiltração.

No contexto do **setor público e governamental**, essa análise ganha relevância singular, pois os ataques têm frequentemente **motivação política, de espionagem ou sabotagem**, e não apenas financeira. Atores patrocinados por Estados-nação buscam **informações estratégicas**, como comunicações diplomáticas, dados de defesa, projetos tecnológicos, e infraestruturas críticas. Outros grupos, como hacktivistas e cibercriminosos oportunistas, realizam campanhas de **disrupção, desinformação e destruição de dados** para enfraquecer a confiança pública.

A tabela a seguir mapeia os **principais vetores observados** em campanhas contra governos latino-americanos (com destaque para o Brasil), detalhando a **tática**, **técnica**, **contexto de uso** e **atores ou incidentes relacionados**.

Tática	Técnica (MITRE ID)	Contexto	Threat Actors / Incidentes
Initial Access	Phishing / Spear Phishing (T1566)	Campanhas direcionadas a servidores públicos com temas de licitações, políticas públicas, intimações judiciais e sistemas governamentais (ex: eSocial, Gov.br). Uso crescente de IA generativa e deepfakes em 2024–2025.	**APT-C-36 (Blind Eagle), Machete, Guacamaya, NoName057(16), Anonymous Sudan, incidentes em prefeituras brasileiras (2023) e Ministério da Saúde (2022).**
	Exploit Public-Facing Application (T1190)	Exploração de vulnerabilidades em portais e aplicações legadas (ex: Liferay, Joomla, e sistemas internos expostos), aproveitando CVEs não corrigidos.	**LockBit 3.0, Avaddon, ALPHV BlackCat, TA558.**

	Valid Accounts (T1078)	Uso de credenciais comprometidas obtidas em vazamentos ou por infostealers; comum em ambientes sem MFA.	**APT28, APT29, MuddyWater, LockBit, Brokers regionais (IABs) vendendo acessos do gov.br.**
	Supply Chain Compromise (T1195)	Comprometimento de prestadores de serviço de TI e contratos públicos para infiltração em órgãos estatais.	**LockBit (via empresas de software brasileiras em 2024), APT41, Guacamaya.**
Execution	Command and Scripting Interpreter (T1059)	Uso intensivo de PowerShell, WMIC e scripts VBS para execução de payloads e evasão.	**Comum em campanhas de ransomware e espionagem; APT-C-36, Machete, Guacamaya, LockBit 3.0.**
	User Execution (T1204)	Envio de arquivos maliciosos disfarçados de ofícios ou planilhas de licitação.	**APT-C-36, TA558, hacktivistas locais.**
Persistence	Web Shell (T1505.003)	Implantação de webshells em portais públicos vulneráveis para acesso remoto persistente.	**Guacamaya, LockBit, APT41.**
	Account Manipulation (T1098)	Criação de usuários administrativos em domínios governamentais para manter persistência após intrusão.	**Observado em ataques a prefeituras brasileiras e governos estaduais (2023–2024).**
Privilege Escalation	OS Credential Dumping (T1003)	Coleta de hashes e credenciais locais (NTDS.dit, LSASS) em servidores AD de órgãos públicos.	**LockBit 3.0, APT28, APT29, Guacamaya.**
	Exploitation for Privilege Escalation (T1068)	Abuso de vulnerabilidades em drivers e serviços Windows para elevar privilégios.	**LockBit, ALPHV, APT28.**
Defense Evasion	Obfuscated Files or Information (T1027)	Uso de payloads ofuscados em PowerShell/Base64 e compressão dupla em anexos.	**APT28, Mustang Panda, Earth Estries.**

	Living Off The Land (LOTL) (T1564)	Execução de ações com ferramentas nativas (PowerShell, bitsadmin, regsvr32, rundll32).	**Volt Typhoon, APT29, MuddyWater.**
	Masquerading (T1036)	Disfarce de arquivos maliciosos como executáveis de sistema ou ferramentas administrativas.	**Gamaredon, APT41.**
Credential Access	Brute Force (T1110)	Ataques de força bruta e password spraying contra VPNs, RDP e e-mails institucionais.	**APT29, APT40, Volt Typhoon.**
	Stealer Malware (T1555)	Uso de infostealers leves para capturar credenciais de navegadores e clientes de e-mail.	**Gamaredon, RedDelta, SideWinder.**
Discovery	Network Service Scanning (T1046)	Varredura de serviços e portas internas após o comprometimento inicial.	**Volt Typhoon, APT28.**
	System Information Discovery (T1082)	Coleta de informações sobre o sistema, domínio e políticas de segurança.	**MuddyWater, APT29.**
	Remote System Discovery (T1018)	Identificação de outros sistemas e domínios governamentais interconectados.	**Mustang Panda, APT31, Earth Estries.**
Lateral Movement	Remote Services (T1021)	Uso de RDP, SMB e WinRM para mover-se lateralmente em redes ministeriais e agências.	**Volt Typhoon, MuddyWater, APT28.**
	Pass the Ticket (T1550)	Abuso de credenciais NTLM/Kerberos para movimentação lateral.	**APT29, APT28.**
Collection	Data from Local System (T1005)	Coleta de documentos, planilhas e PDFs de diretórios administrativos.	**APT31, Mustang Panda, Earth Preta.**

	Screen Capture (T1113)	Captura de tela de sistemas de alto valor, como estações diplomáticas e ministeriais.	**APT36, Gamaredon, MuddyWater.**
Command and Control (C2)	Application Layer Protocol: Web Protocols (T1071.001)	Comunicação com C2 sobre HTTPS e Cloudflare Tunnels.	**Volt Typhoon, APT28, APT29.**
	Proxy (T1090)	Uso de proxies e VPNs comerciais para mascarar tráfego C2.	**APT41, MuddyWater, Mustang Panda.**
Exfiltration	Exfiltration Over C2 Channel (T1041)	Exfiltração de dados sigilosos via HTTP/HTTPS ou serviços de nuvem (Google Drive, OneDrive).	**APT31, Earth Estries, Mustang Panda.**
	Exfiltration to Cloud Storage (T1567.002)	Upload de arquivos sensíveis para buckets de nuvem comprometidos.	**APT41, Volt Typhoon.**
Impact	Data Destruction (T1485)	Uso de wipers para apagar dados e causar disrupção operacional.	**Sandworm (NotPetya), Moses Staff, Agrius.**
	Defacement (T1491)	Desfiguração de sites governamentais como forma de protesto ou desinformação.	**Anonymous Sudan, NoName057(16), Guacamaya**
	Data Encryption for Impact (T1486)	Uso de ransomware para disrupção e chantagem política.	**DarkBit, ALPHV BlackCat (operações direcionadas a instituições públicas).**
Outros	Ameaça Interna / Colaboração Involuntária	Funcionários enganados ou coagidos a instalar software malicioso ou repassar informações confidenciais.	**Campanhas de engenharia social e deepfakes associadas a TA473 (Winter Vivern) e Mustang Panda.**

Tabela 2 - TTPs relacionadas à ataques ao Setor Público

CONHECENDO OS PRINCIPAIS THREAT ACTORS QUE IMPACTAM O SETOR PÚBLICO LATAM

Após compreendermos, nas seções anteriores, a natureza estratégica dos impactos, as táticas comumente empregadas em ataques e o comportamento operacional de adversários em cenários reais, é essencial identificar quem são os agentes por trás dessas ações. Este tópico apresenta uma visão segmentada dos principais *Threat Actors* que impactam diretamente o setor público latino-americano.

3.1 THREAT ACTORS COM VÍNCULO A ESTADO-NAÇÃO (ESPIONAGEM)

Estes grupos são geralmente focados na coleta de inteligência de longo prazo, muitas vezes visando informações diplomáticas, militares ou dados sensíveis de cidadãos. Eles utilizam táticas altamente direcionadas de *spear phishing* e exploração de vulnerabilidades.

Threat Actor	Motivação	Atividade
APT-C-36 (Blind Eagle)	Espionagem de longo prazo, Roubo de Informação Sensível	Ataca persistentemente instituições governamentais e de infraestrutura crítica na Colômbia, Equador, Chile e Panamá desde 2018. Utiliza *Spear Phishing* (T1566) disfarçado de comunicações oficiais de procuradorias e ministérios para acesso inicial. Emprega RATs e scripts VBS (T1059) para execução.
APT29 (Earth Koshchei, Midnight Blizzard)	Coleta de inteligência, Espionagem (Rússia)	Foca em entidades diplomáticas e governamentais globalmente. Utiliza sofisticadas campanhas de *Phishing* e abusa do protocolo RDP (*Rogue RDP*) para obter acesso inicial e movimento lateral (T1021).

APT41 (Double Dragon)	Espionagem (China), Ganhos Financeiros Oportunistas	Conhecido por ataques à cadeia de suprimentos (*Supply Chain Compromise*, T1195) e exploração de vulnerabilidades em aplicações voltadas para a Internet (T1190) para comprometer redes governamentais.
Machete	Espionagem e Coleta de Inteligência	Atua predominantemente na América Latina, tendo como alvos instituições governamentais e militares. Utiliza fortemente intérpretes de script (T1059) e faz uso de malware para espionagem desde 2014.

Tabela 3 - Threat Actors com vínculo Estado-Nação

3.2 Grupos de Ransomware (RaaS) e Habilitadores do Cibercrime

Esses atores são motivados principalmente por ganhos financeiros, usando a criptografia (T1486) e a extorsão de dados como armas principais. Eles são frequentemente habilitados pela venda de acesso inicial por terceiros.

Threat Actor	Motivação	Atividade
LockBit 3.0	Ganhos financeiros (RaaS), Extorsão (Dupla Extorsão)	É uma das operações RaaS mais ativas no Brasil. O alvo é o setor governamental, explorando fraquezas na rede interna para propagação e máximo impacto. Utiliza acesso inicial por *Phishing*, exploração de vulnerabilidades e cooptação de colaboradores (*insiders*). Responsável por ataques a municípios brasileiros, como Itu, SP.
ALPHV (BlackCat)	Ganhos financeiros (RaaS), Extorsão	Ransomware que utiliza a linguagem Rust.

		Comprometido mais de 1.000 entidades globalmente, incluindo proeminentes entidades governamentais (municipais e de infraestrutura crítica). Conhecido por ser uma ameaça de extorsão ativa na LATAM.
Initial Access Brokers (IABs)	Ganhos financeiros (Comoditização do Acesso)	Não atacam diretamente com *ransomware*, mas vendem acesso não autorizado a redes governamentais (T1078) para grupos como o LockBit. Eles obtêm credenciais válidas via *infostealers* ou exploração de vulnerabilidades, sendo um vetor de ataque provável para entidades LATAM.

Tabela 4 - Grupos de Ransomware e Habilitadores do Cibercrime

3.3 Hacktivismo e Extivismo (Disrupção e Vazamento de Dados)

Estes grupos buscam o impacto ideológico, usando a desfiguração de sites (Defacement, T1491) ou o vazamento de dados sigilosos para fins políticos, sociais ou de protesto.

Threat Actor	Motivação	Atividade
Guacamaya	Ideológica, Exposição de Corrupção	Grupo de hacktivistas com foco em governos e corporações na América Central e Latina (México, Chile, Peru). Ganhador de notoriedade por vazamentos maciços de dados sigilosos de entidades governamentais. Utiliza a exploração de aplicações voltadas para o público (T1190) e *Web Shells* (T1505.003) para persistência.

NoName057	Geopolítica (Pró-Rússia), Disrupção	Grupo hacktivista focado em ataques de Negação de Serviço Distribuída (DDoS) contra infraestrutura crítica e entidades que se opõem à Rússia. Conhecido por causar desfiguração (T1491) e disrupção, utilizando botnets.
Anonymous Sudan	Ideológica (Protesto), Extorsão	Realiza ataques DDoS (T1491) contra agências governamentais, hospitais e universidades. Alega motivação ideológica (pró-palestina), mas há tentativas de extorsão.

Tabela 5 - Hacktivistas e Exfiltradores

CONCLUSÃO

O panorama das ameaças ao Setor Público na América Latina se consolida como um campo de batalha digital de **alto risco estratégico** e **múltiplas motivações**. O setor concentra vastos volumes de dados sensíveis, desde registros de cidadãos e informações financeiras até inteligência de Estado e planos de defesa, e é alvo simultâneo de campanhas sofisticadas de espionagem patrocinadas por Estados-nação (APTs), de operações de extorsão e ransomware conduzidas pelo cibercrime organizado (RaaS), e de ações disruptivas de grupos hacktivistas.

A distinção entre esses atores se torna cada vez mais tênue, resultando em uma **Kill Chain híbrida** onde o acesso inicial obtido por criminosos pode ser reutilizado por grupos de espionagem, e operações de influência podem mascarar objetivos de sabotagem geopolítica. A alta dependência de serviços públicos vitais em ecossistemas digitais complexos e, muitas vezes, vulneráveis, eleva o impacto de um incidente cibernético de um prejuízo técnico para uma **crise social, econômica e política**.

Os impactos de ataques bem-sucedidos transcendem o roubo de dados, manifestando-se na **interrupção de serviços essenciais** que afetam milhões de cidadãos, na **perda de confiança institucional** e no risco direto à **soberania nacional**. O cenário regional é agravado por desafios estruturais, como a maturidade desigual em governança de cibersegurança e a dependência tecnológica de fornecedores estrangeiros.

Conclui-se que a cibersegurança do Setor Público na América Latina é um **pilar da soberania moderna** e da continuidade do Estado. A convergência de ameaças e a criticidade dos alvos exigem que a proteção cibernética seja tratada como um assunto de Estado de urgência máxima.

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **LATAM Regional Cyber Threat Landscape 2025 – CrowdStrike**
- **Insights on Cyber Threats Targeting Brazil – Google Cloud**
- **State of Ransomware 2024 – Kaspersky**
- **LATAM Regional Threat Landscape Report 2024 – SOCRadar**
- **O cenário de ameaças da dark web no Brasil – Kaspersky**
- **Global Threat Landscape 2025 – Fortinet**
- **MITRE ATT&CK**
- **Gov.BR**

AUTORES

- **Gustavo Santos – Security Researcher**

heimdall
security research
A DIVISION OF ISH