Relatório de ransomware de 2024 da ThreatLabz

Índice

Resumo Executivo_

Os ataques de ransomware atingiram novos patamares de ambição e audácia no último ano, marcados por um aumento notável nos ataques de extorsão. Somando-se ao aumento dos ataques de ransomware, a pesquisa da ThreatLabz descobriu um **pagamento de resgate sem precedentes, de US$ 75 milhões**, o maior já pago por uma empresa. Esse valor é quase o dobro do maior pagamento de resgate conhecido publicamente.[1] Só em 2023, os pagamentos de ransomware ultrapassaram US$ 1 bilhão, destacando o crescente impacto financeiro desses crimes cibernéticos.

As táticas dos grupos de ransomware tornaram-se cada vez mais sofisticadas e ousadas. Notavelmente, ultrapassaram os limites tradicionais das empresas que atacam, chegando ao ponto de visar os filhos dos executivos para provocar resgates mais rápidos e mais elevados.[2] Desde infraestruturas críticas[3] e grandes corporações[4] até pequenas e médias empresas, nenhuma organização está imune a ficar na mira da próxima campanha ou evolução dos ataques.

Apesar das operações policiais contra vários agentes de acesso inicial nas operações especiais "Operation Endgame" e "Operation Duck Hunt," muitas das maiores famílias ativas de ransomware continuam a se reagrupar rapidamente e lançar novos ataques quase sem interrupções. Infelizmente, muitos grupos de ransomware estão fora do alcance das autoridades policiais, o que os torna virtualmente imunes a processos criminais. Conforme detalhado neste relatório, as agências de segurança pública aumentaram suas táticas de pressão por meio de recompensas monetárias, sanções, trolling e exposição dos indivíduos por trás do ransomware usando várias formas de táticas psicológicas.

À medida que os grupos de ransomware evoluem continuamente suas táticas, é crucial manter-se atualizado sobre como o cenário de ameaças está mudando.

O Relatório de ransomware de 2024 da Zscaler ThreatLabz oferece uma visão geral do cenário de ameaças de ransomware de abril de 2023 a abril de 2024, detalhando as últimas tendências, alvos, famílias de ransomware e estratégias de defesa eficazes.

A ThreatLabz descobriu que os ataques de ransomware aumentaram 17,8% ano após ano com base em tentativas bloqueadas na nuvem da Zscaler, enquanto os ataques de ransomware identificados através da análise de sites de vazamento de dados aumentaram em 57,8%. Os alvos mais comuns foram empresas dos setores industrial, de saúde e de tecnologia, colocando operações e infraestruturas críticas diretamente na linha de ataque.

As conclusões apresentadas neste relatório destacam a necessidade de as organizações priorizarem a proteção contra a maré implacável de ransomware. Os insights e estratégias do relatório servem como um guia crucial para melhorar suas defesas contra ransomware. Ao compreender as tendências e vulnerabilidades mais recentes e implementar as práticas recomendadas, você pode reduzir significativamente o risco de se tornar uma vítima de ransomware e proteger melhor os ativos e dados críticos da sua organização.

[1] Bloomberg, **CNA Financial pagou US$ 40 milhões em resgate após o ciberataque de março**, 20 de maio de 2021.
[2] Business Insider, **Hackers agora atacam filhos de executivos corporativos em ataques de ransomware**, 12 de maio de 2024.
[3] Dark Reading, **Ascension Healthcare sofre grande ciberataque**, 10 de maio de 2024.
[4] CyberScoop, **Boeing confirma tentativa de extorsão de ransomware de US$ 200 milhões**, 8 de maio de 2024.

Principais_ descobertas

A pesquisa da Zscaler ThreatLabz descobriu um pagamento de resgate recorde, de US$ 75 milhões; o maior pagamento de ransomware feito por uma empresa na história, quase o dobro do maior pagamento conhecido publicamente.

Ataques de ransomware bloqueados pela nuvem da Zscaler aumentaram em 17,8%, e o número de empresas extorquidas em sites de vazamento de dados cresceu 57,8% no mesmo período, ano após ano, apesar das numerosas operações de agências de segurança pública, incluindo a apreensão de infraestruturas, juntamente com detenções, acusações criminais e sanções.

Os setores de manufatura, saúde e tecnologia foram os principais alvos dos ataques de ransomware, enquanto o setor energético registou um aumento de 500% ano após ano, uma vez que as infraestruturas críticas e a suscetibilidade a perturbações operacionais o tornam particularmente atrativo para os cibercriminosos.

Os Estados Unidos continuam sendo o principal alvo de ataques de ransomware, sofrendo 49,95% do total de ataques, seguido pelo Reino Unido, Alemanha, Canadá e França.

A ThreatLabz identificou 19 novas famílias de ransomware durante o período de análise, elevando o número total para 391 desde o início do nosso rastreamento.

As famílias de ransomware mais ativas foram **LockBit (22,1%), BlackCat (também conhecida como ALPHV) (9,2%)** e **8Base (7,9%).**

As vulnerabilidades continuam sendo um vetor de ataque de ransomware muito comum, enfatizando a importância da rápida aplicação de correções e do gerenciamento unificado de vulnerabilidades, sustentado por uma arquitetura zero trust para fornecer proteção mesmo quando as correções não estão disponíveis.

Ataques de engenharia social baseados em voz estão sendo cada vez mais usados para obter acesso a redes corporativas, uma técnica usada pelos grupos criminosos Scattered Spider e Qakbot.

Cenário de ransomware_: principais tendências e alvos

A natureza dinâmica do ransomware colocou-o na vanguarda das preocupações de segurança nos últimos anos. Os criminosos estão constantemente evoluindo seus métodos de ataque e extorsão, aproveitando os avanços na tecnologia de inteligência artificial (IA), código-fonte vazado e criptografia avançada para maximizar seu impacto e lucratividade.

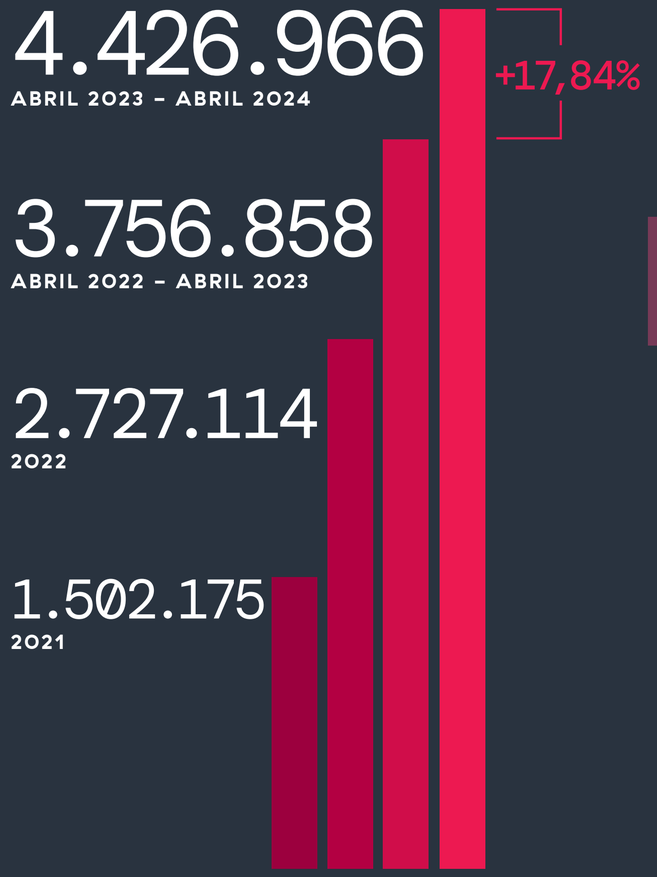
Este relatório examina as seguintes tendências de ataques de ransomware de abril de 2023 a abril de 2024:

- Aumento geral nos ataques de ransomware
- Setores verticais da indústria mais impactados por ransomware
- Distribuição geográfica das organizações vítimas
- Aumento de ações policiais contra grupos de ransomware e agentes de acesso inicial
- Principais ameaças de ransomware e pagamentos de resgate recordes

Aumento geral nos ataques de ransomware

A mais recente análise da ThreatLabz revela uma tendência preocupante, com um aumento de 17,84% ano após ano nos ataques de ransomware, com base nas tentativas bloqueadas observadas na nuvem da Zscaler. O aumento das atividades de ransomware se traduz em interrupções significativas e impactos financeiros nas organizações vítimas de todos os tamanhos. Esses ataques muitas vezes interrompem as operações comerciais, causando longos períodos de inatividade, perda substancial de dados e altos custos de recuperação. O peso financeiro é considerável; não apenas há uma demanda de resgate em jogo, mas a restauração do sistema e o controle de danos podem ter um preço elevado. À luz dessas ameaças crescentes, a necessidade de defesas **robustas contra ransomware** nunca foi tão grande.

NÚMERO DE TENTATIVAS BLOQUEADAS NA NUVEM DA ZSCALER



Setores verticais da indústria mais impactados por ransomware

Os ataques de ransomware representam riscos significativos para empresas de todos os tamanhos e setores. Esses ataques podem comprometer dados sigilosos, levar a pesadas perdas financeiras, interromper a continuidade dos negócios e prejudicar reputações. Diferentes setores enfrentam desafios únicos de ransomware com base na forma como operam, nos dados que manipulam e na sua infraestrutura tecnológica.

Apesar das variáveis, os ataques de extorsão de ransomware têm aumentado consistentemente, com o número de empresas vítimas listadas em sites de vazamento de dados aumentando 57,81% desde o relatório da ThreatLabz do ano passado sobre tendências de ransomware. O setor de manufatura foi de longe o mais visado, somando 653 ataques; mais do dobro do que qualquer outro setor.

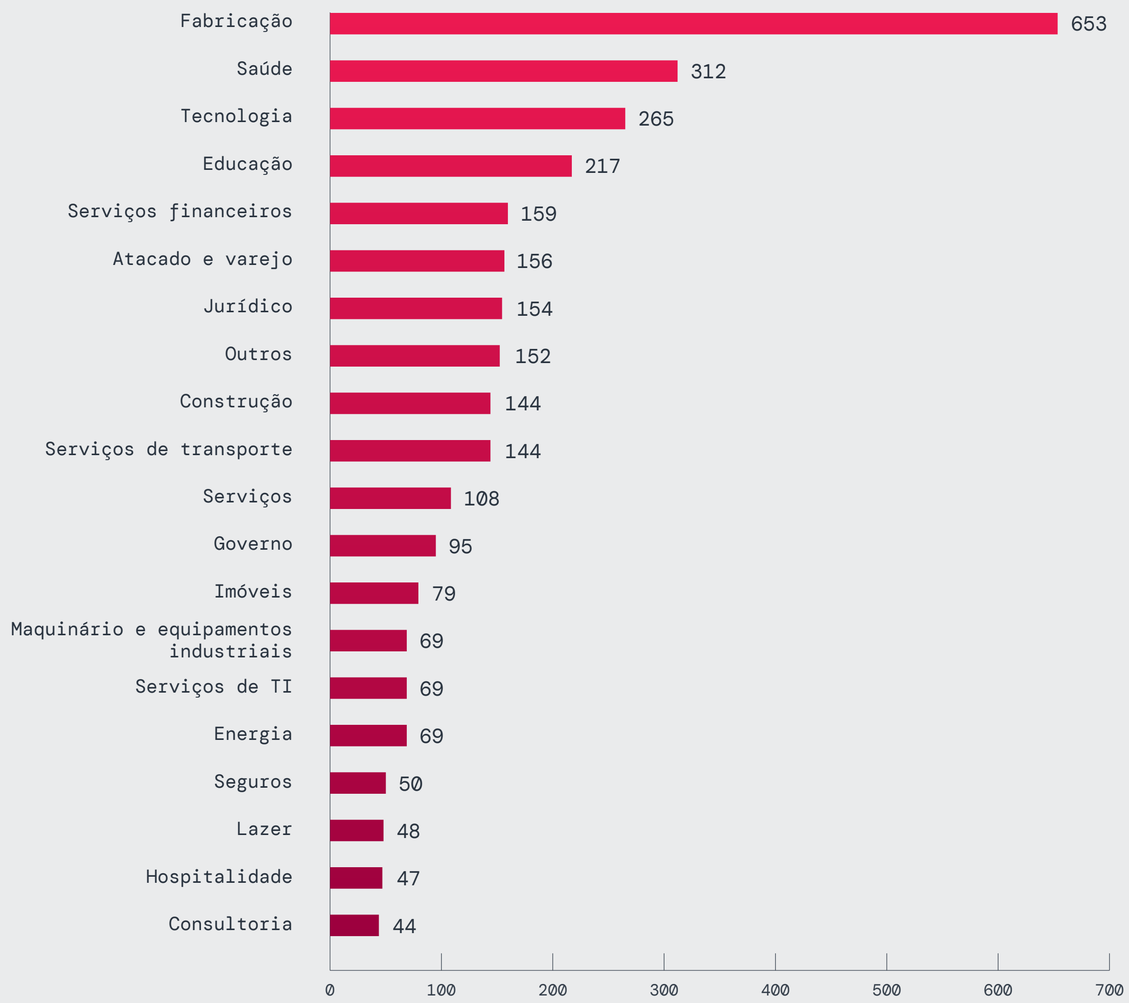


Figura 1: ataques de ransomware por setor com base em sites de vazamento de dados (apenas os 20 principais setores).

Tendências ano após ano

O setor de energia sofreu um aumento de 527,27% ano após ano nos ataques de ransomware, provavelmente devido à sua natureza crítica e ao alto potencial de resgate que oferece aos criminosos.

Da mesma forma, o setor de restaurantes, bares e serviços de alimentação registrou um aumento de 333,33% nesse tipo de ataques. Isso pode ser atribuído à rápida digitalização do setor, impulsionada pela adoção de sistemas avançados de ponto de venda e plataformas de pedidos online. Embora essas tecnologias possam agilizar as operações e melhorar as experiências dos clientes, também podem introduzir possíveis vulnerabilidades.

Embora este aumento destaque a prevalência de ataques de ransomware, ele pode não captar toda a extensão dos incidentes de ransomware. Muitos ataques não são relatados ou são resolvidos em particular por meio do pagamento de resgates, sem divulgação pública. Assim, esses números devem ser vistos como indicativos de tendências mais amplas de ransomware, em vez de uma representação abrangente de todo o cenário de ameaças.

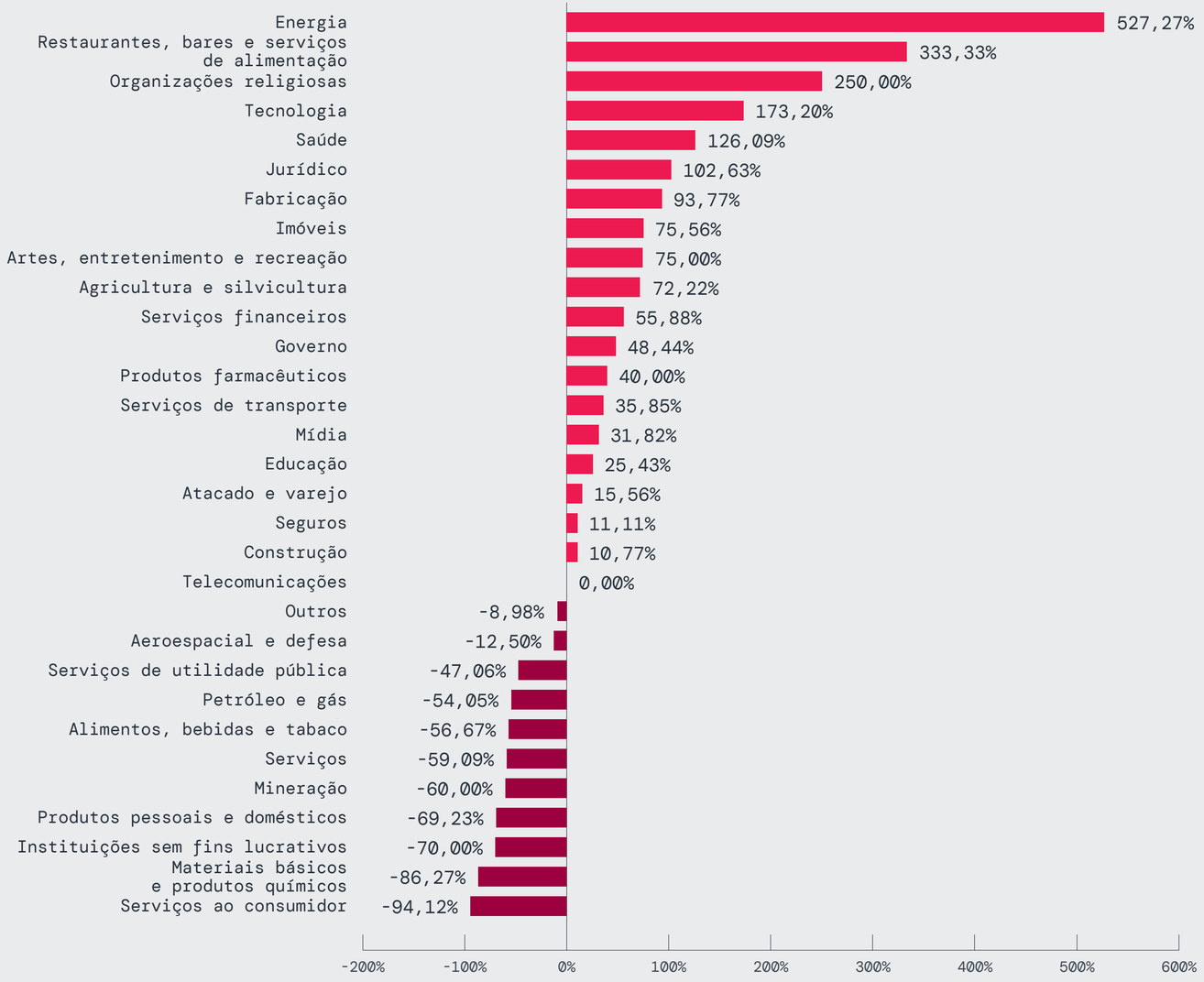


Figura 2: percentual de variação ano após ano nos ataques de extorsão por ransomware por setor. Observe que alguns setores tinham uma base de referência relativamente baixa de ataques no relatório do ano passado, fazendo com que seu crescimento pareça mais substancial.

Distribuição geográfica das organizações vítimas

Os Estados Unidos sofreram um volume significativamente maior de ataques de ransomware do que qualquer outro país, representando cerca de 50% de todos os incidentes a nível mundial. Em comparação, o Reino Unido foi o segundo país mais visado, sofrendo quase 6% dos ataques de ransomware, seguido pela Alemanha (4,09%), Canadá (3,51%), e França (3,26%). A figura 3 mostra um mapa térmico que ilustra os países afetados por extorsões de resgate entre abril de 2023 e abril de 2024.

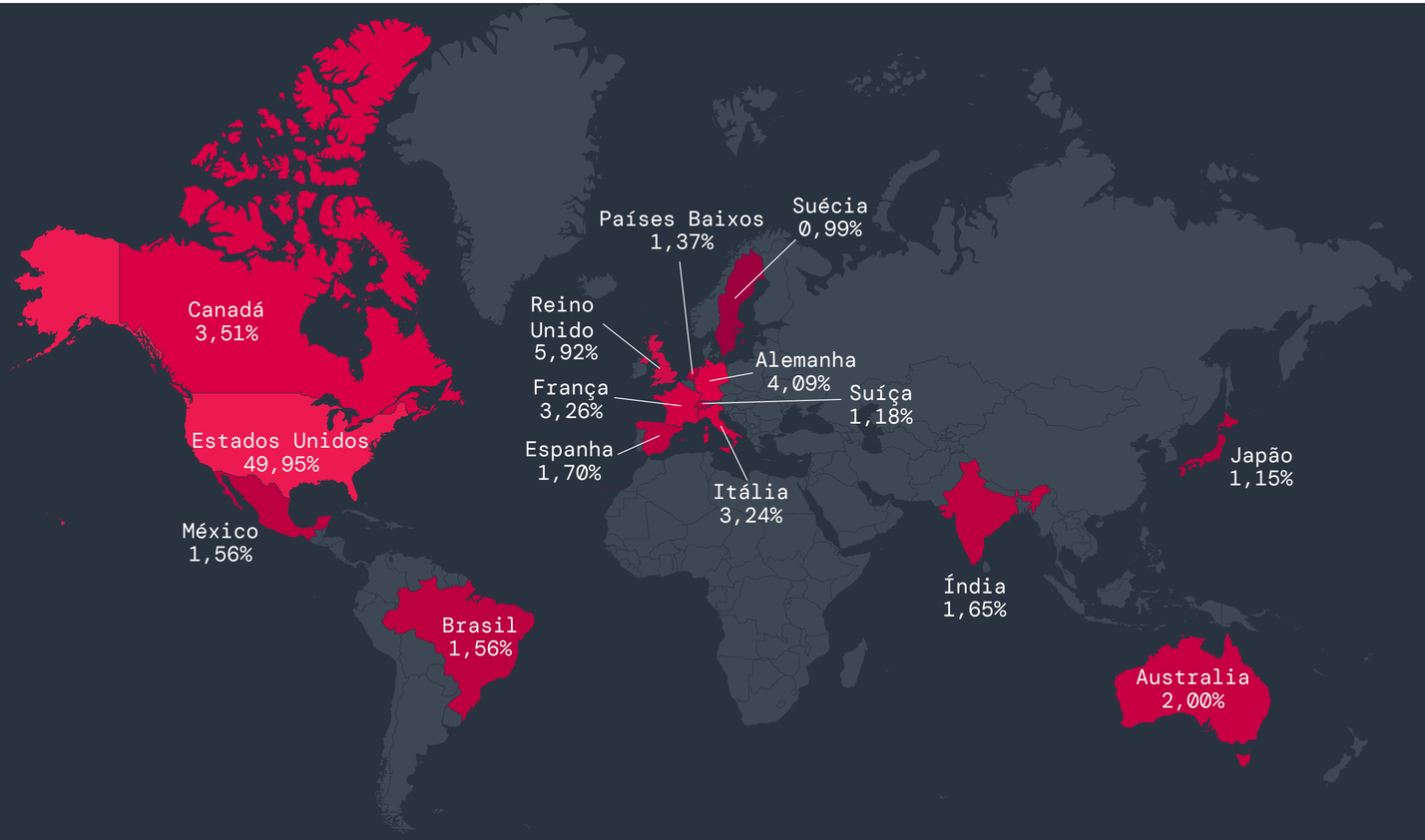


Figura 3: distribuição das vítimas de ransomware por país.

Compreender a distribuição dos ataques de ransomware é essencial para a avaliação de riscos, alocação de recursos, desenvolvimento de políticas, cooperação internacional e esforços de conscientização pública no combate às ameaças de ransomware.

Avaliação de riscos

A análise de regiões fortemente visadas ajuda as organizações nessas áreas a avaliar os seus próprios níveis de risco e a implementar uma segurança cibernética mais forte. Na pesquisa da ThreatLabz, os EUA sofrem 50% dos ataques globais de ransomware, apelando às organizações dentro das suas fronteiras para priorizarem protocolos de segurança rigorosos.

Alocação de recursos

Os dados direcionados permitem que governos e organizações aloquem recursos estrategicamente, melhorando a sua postura de segurança ao priorizar o apoio, o financiamento e a experiência em áreas com os mais elevados níveis de ameaça.

Desenvolvimento de políticas

Os governos podem utilizar informações provenientes de ataques regionais de ransomware para embasar leis, melhorar os padrões de segurança, promover a cooperação internacional e facilitar o compartilhamento de informações do setor público–privado. Como exemplo notável recente, as novas regras de cibersegurança da SEC marcam um passo importante no reforço da transparência e da responsabilização face às ameaças crescentes.

Cooperação internacional

A identificação dos países mais visados permite a execução de esforços coordenados entre autoridades policiais, organizações e governos para combater o ransomware a nível nacional e internacional. A Operação Duck Hunt e a Operação Endgame exemplificam como a cooperação internacional pode perturbar as atividades cibercriminosas.

Conscientização pública

Destacar países frequentemente visados pode incentivar indivíduos, organizações e governos a tomarem medidas mais proativas no que diz respeito ao treinamento em cibersegurança, planejamento de resposta a incidentes e investimento em tecnologias defensivas.

Tendências ano após ano

A ThreatLabz comparou os ataques de ransomware do relatório deste ano com o relatório de ransomware de 2023 da ThreatLabz para avaliar as taxas de variação. Entre os 15 países mais visados, os EUA experimentaram um aumento notável de 101,88% em relação ao ano anterior, e a Suécia viu um aumento impressionante de 350%, embora tenha representado uma parcela significativamente menor dos ataques totais.

Embora a análise das tendências de ransomware a nível global seja inestimável, também é importante examinar os desenvolvimentos específicos em diferentes regiões do mundo. O estudo das divisões regionais ajuda as organizações a criar planos de segurança personalizados e ajuda os governos a desenvolver políticas de segurança cibernética mais eficazes.

MUDANÇAS NOS ATAQUES DE RANSOMWARE NOS 15 PAÍSES MAIS VISADOS

País	Ataques de ransomware por país (2023)	Ataques de ransomware por país (2024)	Alteração percentual
Estados Unidos da América	902	1.821	101,88%
Reino Unido	144	216	50,00%
Alemanha	110	149	35,45%
Canadá	151	128	-15,23%
França	87	119	36,78%
Itália	63	118	87,30%
Austrália	69	73	5,80%
Brasil	38	57	50,00%
Espanha	36	62	72,22%
México	31	57	83,87%
Países Baixos	17	50	194,12%
Índia	62	60	-3,23%
Suíça	32	43	34,38%
Japão	44	42	-4,55%
Suécia	8	36	350,00%

Figura 5: comparação ano após ano dos ataques de ransomware por país.

MUDANÇAS NAS TAXAS DE ATAQUE DE RANSOMWARE NA EMEA

País	Empresas impactadas por ataques de ransomware (2023)	Empresas impactadas por ataques de ransomware (2024)	Alteração percentual
Reino Unido	144	216	50,00%
Alemanha	110	149	35,45%
França	87	119	36,78%
Itália	63	118	87,30%
Espanha	36	62	72,22%
Países Baixos	17	50	194,12%
Suíça	32	43	34,38%
Suécia	8	36	350,00%
Bélgica	16	34	112,50%
África do Sul	13	24	84,62%
Áustria	15	24	60,00%
Emirados Árabes Unidos	12	21	75,00%

Figura 6: comparação ano após ano de ataques de ransomware por país na região da EMEA.

MUDANÇAS NAS TAXAS DE ATAQUE DE RANSOMWARE NA APAC

País	Empresas impactadas por ataques de ransomware (2023)	Empresas impactadas por ataques de ransomware (2024)	Alteração percentual
Austrália	69	73	5,80%
Índia	62	60	-3,23%
Japão	44	42	-4,55%
Tailândia	13	25	92,31%
Indonésia	15	23	53,33%
Malásia	14	20	42,86%
Taiwan	23	17	-26,09%
Filipinas	7	16	128,57%
Singapura	8	16	100,00%
China	21	15	-28,57%
Coreia do Sul	12	10	-16,67%
Vietnã	10	10	0,00%

Figura 7: comparação ano após ano de ataques de ransomware por país na região da APAC.

Grupos de ransomware mais ativos em 2023 e 2024

LockBit (22.,%), BlackCat (9,2%), e 8Base (7,9%) foram os grupos de extorsão de ransomware mais ativos no último ano, cada um responsável por um número significativo de ataques. A figura 8 mostra o número de vítimas de vazamento de dados por família de ransomware durante esse período.

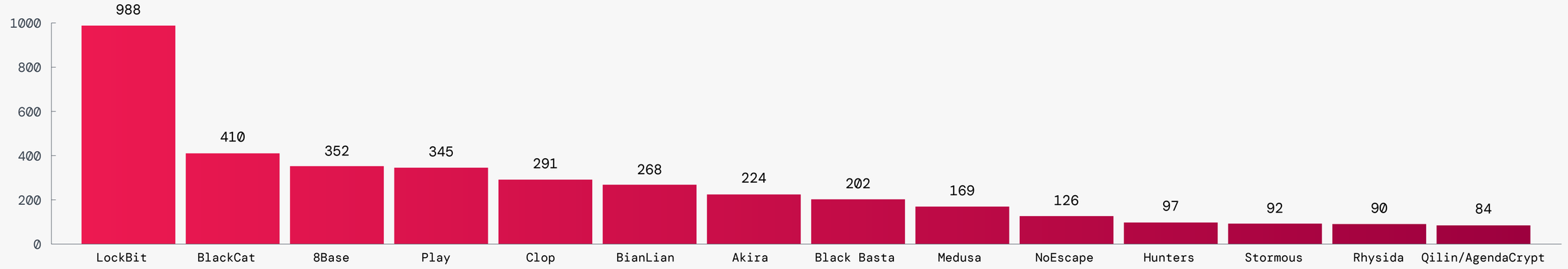


Figura 8: ataques de ransomware revelados em sites de vazamento de dados operados maliciosamente.

Os mais novos grupos de ransomware em cena

A figura 9 mostra uma linha do tempo de novos grupos de ransomware que começaram a publicar dados em sites de vazamento como parte de sua estratégia de extorsão.

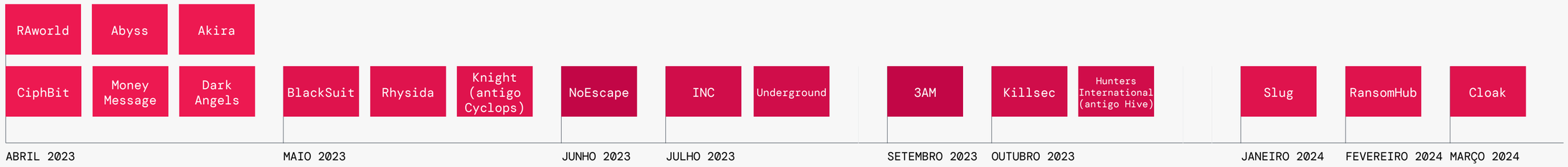


Figura 9: novos grupos de ransomware com sites de vazamento de dados.

Principais vulnerabilidades utilizadas em ataques de ransomware

Vulnerabilidades em software, sistemas e na infraestrutura digital geral podem servir como pontos de entrada críticos para ataques de ransomware. As organizações devem estar cientes dessas vulnerabilidades e tomar medidas proativas para resolvê-las.

A Agência de Segurança Cibernética e de Infraestrutura (CISA) mantém uma lista abrangente de vulnerabilidades,[5] incluindo aquelas ativamente exploradas por grupos de ransomware. É altamente recomendável que as organizações monitorem de perto essa lista e priorizem a mitigação das vulnerabilidades mencionadas nela. O gerenciamento proativo de vulnerabilidades é essencial para fortalecer a postura geral de cibersegurança de uma organização.

Em muitos casos, as vulnerabilidades exploradas por grupos de ransomware impactam os ativos conectados à internet na superfície de ataque externa das organizações, como gateways, VPNs e outras tecnologias de conectividade remota. Por estarem voltadas para a internet, essas vulnerabilidades são significativamente mais fáceis de serem verificadas e exploradas pelos criminosos. A orientação mais recente da CISA[6] enfatiza ainda mais as vulnerabilidades em VPNs e soluções de conectividade remota como pontos críticos de preocupação, aconselhando a adoção das abordagens mais atuais, como arquitetura zero trust, SSE e SASE, que são baseadas em políticas granulares de controle de acesso.

Durante o ano passado, famílias proeminentes de ransomware visaram e exploraram as vulnerabilidades mostradas na figura 10, impactando significativamente uma ampla gama de sistemas.

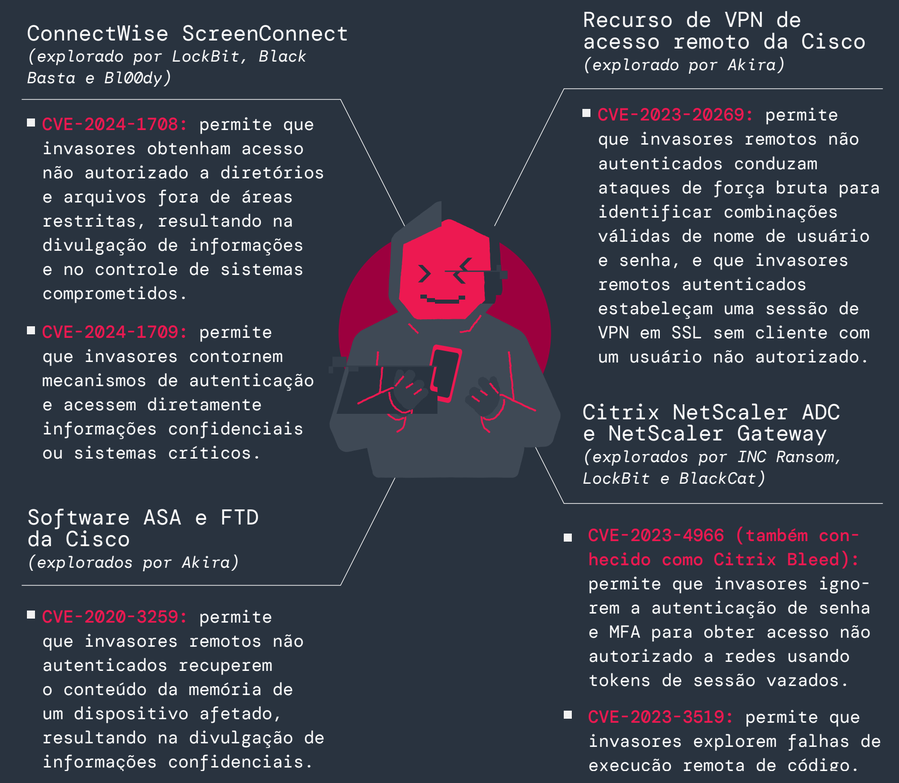


Figura 10: vulnerabilidades predominantes de abril de 2023 a abril de 2024.

As correções disponíveis para essas vulnerabilidades devem ser aplicadas o mais rápido possível, juntamente com as seguintes medidas de mitigação:

- Desativar o acesso remoto aos servidores
- Usar senhas robustas e autenticação multifator
- Monitorar servidores em busca de atividades suspeitas

[5] Agência de Segurança de Cibersegurança e Infraestrutura **Catálogo de vulnerabilidades conhecidas exploradas**, acessado em 25 de junho de 2024.
[6] Agência de Segurança de Cibersegurança e Infraestrutura **Abordagens modernas para a segurança de acesso à rede**, 18 de junho de 2024.

Resumo_de_ransomware: o que está nas manchetes

O ransomware é difundido e transcende setores; e quando um grupo é encerrado, outro renasce ou emerge de novo. Aqui estão algumas histórias recentes que destacam o cenário de ransomware em constante evolução.

A praga do ransomware na área da saúde

O setor de saúde enfrentou desafios significativos ao longo de 2023 e 2024, pois foi fortemente atacado por grupos de ransomware. As repercussões da interrupção das operações de saúde são sérias: ambulâncias são redirecionadas, prescrições são atrasadas e procedimentos médicos essenciais têm de ser adiados. Além disso, o roubo de dados de saúde sigilosos pode ter consequências de grande alcance, incluindo roubo de identidade e fraude em saúde, agravando ainda mais as vulnerabilidades no ecossistema de saúde.

CONSEQUÊNCIAS IMPREVISTAS DOS PAGAMENTOS DE RESGATE

Um fornecedor de tecnologia de saúde para soluções de pagamento foi vítima de um ataque de ransomware orquestrado pelo grupo BlackCat. Apesar de cumprir as exigências dos atacantes e pagar uma quantia impressionante de US$ 22 milhões de resgate, a provação tomou um rumo inesperado. O grupo BlackCat renegou sua promessa de compartilhar uma parte do resgate com o afiliado por trás do ataque (o chamado "golpe de saída"), levando o afiliado a ameaçar o provedor de saúde com a divulgação de dados sigilosos.

Esse é um lembrete claro de que o velho ditado "não há honra entre ladrões" se aplica a ataques de ransomware. Mesmo que os resgates sejam pagos, não há garantia de que o grupo criminosos não publicará ou excluirá os dados roubados. Além disso, algumas ferramentas de descriptografia de ransomware contêm bugs que impedem a recuperação de dados bem-sucedida e podem levar mais tempo para recuperar os dados do que de um backup.

DUPLA EXTORSÃO, DUPLA VITIMIZAÇÃO

Em fevereiro de 2023, um importante distribuidor farmacêutico dos EUA confirmou que os seus sistemas de TI tinham sido comprometidos. A violação afetou uma das subsidiárias do distribuidor, com os arquivos roubados posteriormente vazados pelo grupo de ransomware Lorenz.[7] Então, em fevereiro de 2024, o mesmo distribuidor sofreu outro ataque de ransomware.[8] Isso parece fazer parte de uma tendência crescente observada pela ThreatLabz, em que uma empresa foi sujeita a vários incidentes de ransomware no período de um ano.

[7] BleepingComputer, **Distribuidora de medicamentos AmerisourceBergen confirma violação de segurança**, 8 de fevereiro de 2023.
[8] BleepingComputer, **Gigante farmacêutica Cencora afirma que dados foram roubados em um ataque cibernético**, 27 de fevereiro de 2024.

O impacto da decisão de segurança cibernética da SEC

Em 2023, a SEC introduziu novas regras de divulgação de segurança cibernética para aumentar a transparência e a responsabilização entre as empresas de capital aberto. Em vigor a partir de 15 de dezembro de 2023, essas regras exigem a comunicação oportuna de incidentes materiais de segurança cibernética e requerem informações detalhadas sobre a gestão, estratégia e governança de riscos de segurança cibernética de uma empresa. Os principais componentes das decisões da SEC incluem a adição do Item 1.05 ao 8-K, que exige o relato de incidentes materiais de segurança cibernética no prazo de quatro dias úteis após a determinação da materialidade pela empresa. Além disso, o Formulário 10-K agora exige relatórios anuais sobre gestão e estratégia de riscos de segurança cibernética, começando com os anos fiscais que terminam em ou após 15 de dezembro de 2023. Os emissores estrangeiros privados também devem cumprir com divulgações comparáveis no Formulário 6-K e no Formulário 20-K.

As decisões apresentam um novo desafio para os agentes de ransomware que oferecem serviços privados de resolução de pagamentos a empresas cotadas em bolsa, uma vez que as empresas ainda são obrigadas a divulgar integralmente o ataque. Por outro lado, o novo mandato enfraquece os ataques de extorsão sem criptografia, uma tendência emergente em que os grupos de ransomware contam exclusivamente com a ameaça de vazar dados roubados para exigir resgates.

COMO AS NOVAS REGRAS IMPACTAM AS EMPRESAS

As decisões de segurança cibernética da SEC podem representar sérios desafios para as empresas em termos de conformidade e gestão de riscos. Embora pretendam aumentar a transparência e a proteção dos investidores, essas regras exigem que as empresas cumpram requisitos complexos de comunicação e forneçam divulgação imediata de incidentes materiais.

Um impacto importante é o aumento da pressão sobre as empresas para quantificar e avaliar os incidentes cibernéticos com precisão. Determinar a materialidade e o possível impacto dos incidentes cibernéticos requer uma análise cuidadosa, que pode ser dispendiosa e exigir que as empresas (grandes e pequenas) repensem os seus protocolos de resposta a incidentes e atualizem as suas divulgações para cumprir os requisitos da SEC.

Além disso, os prazos de conformidade variam com base no tamanho e no status dos relatórios das empresas, acrescentando outra camada de complexidade. As pequenas empresas de relatórios muitas vezes têm prazos de conformidade diferentes e normalmente mais longos em comparação com as grandes corporações. E embora as grandes empresas tenham de cumprir prazos mais apertados, a sua escala também lhes proporciona mais recursos para analisar a materialidade de um incidente de segurança cibernética.

Os novos requisitos de divulgação também eliminam a possibilidade de as empresas públicas pagarem resgates discretamente sem incorrer em danos reputacionais e na repercussão que se segue após compartilhar abertamente informações sobre uma violação.

ALGUMAS EMPRESAS JÁ ESTÃO VIOLANDO AS REGRAS DA SEC

Apesar das diretrizes claras da SEC, algumas empresas já não cumpriram as novas regras de segurança cibernética. Divulgações recentes de empresas conhecidas levantaram preocupações sobre o não cumprimento e a adequação dos seus relatórios de incidentes.[9] Muitas dessas divulgações carecem de dados quantitativos e avaliações detalhadas das implicações financeiras e operacionais dos incidentes cibernéticos, que é precisamente o que a SEC exige agora. Essa tendência, em que as empresas fornecem divulgações deficientes de incidentes cibernéticos, apesar da decisão da SEC, pode exigir maior orientação e supervisão regulatória para garantir uma conformidade consistente e eficaz.

As decisões da SEC sobre segurança cibernética representam uma mudança regulatória significativa que visa melhorar a transparência e a responsabilização na comunicação de incidentes. A adesão a essas novas regras de forma consistente e de boa fé exigirá uma colaboração contínua entre reguladores, empresas e partes interessadas da indústria.

[9] Forbes, **Empresas já não estão cumprindo as novas regras de divulgação de incidentes de segurança cibernética da SEC**, 4 de março de 2024.

Impacto das ações de segurança pública

Qakbot interrompido pela “Operação Duck Hunt”

Em 29 de agosto de 2023, em um esforço multinacional coordenado, o Departamento Federal de Investigação (FBI) e o Departamento de Justiça (DOJ) anunciaram a Operação Duck Hunt. A Zscaler ThreatLabz forneceu assistência técnica significativa às autoridades para essa operação.[10] A infraestrutura do Qakbot foi projetada para ser resiliente contra tentativas de remoção por meio de uma infraestrutura de vários níveis, conforme mostrado na figura 11.

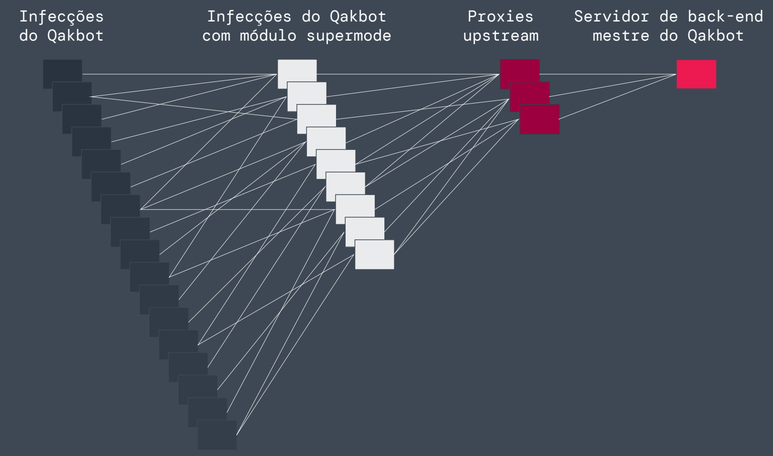


Figura 11: infraestrutura multicamadas do Qakbot.

Essa infraestrutura forneceu várias camadas de resiliência, com cada nível exigindo um esforço coordenado para desmantelar. A primeira camada da infraestrutura do Qakbot incluía sistemas infectados executando um plug-in de supernode que retransmitia o tráfego upstream para vários proxies projetados para ocultar o servidor de backend mestre do Qakbot.

A Operação Duck Hunt redirecionou os servidores proxy upstream do supernode para um conjunto de servidores sinkhole para assumir imediatamente a infraestrutura do Qakbot, como mostrado na figura 12.

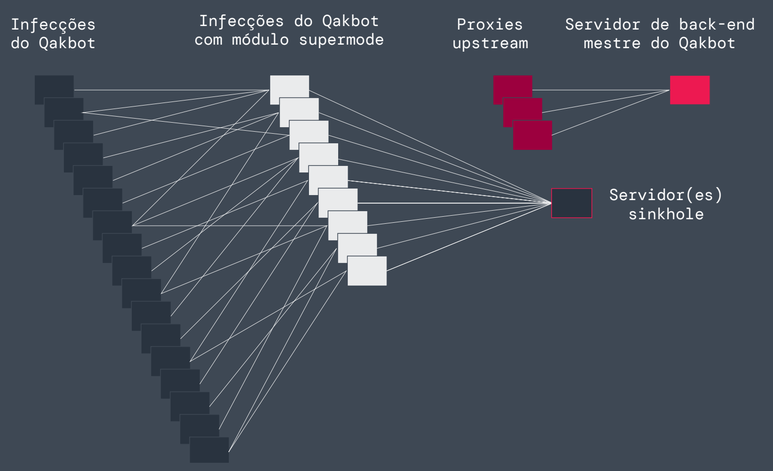


Figura 12: arquitetura do Qakbot após redirecionar os proxies upstream de cada supernó.

Depois que o FBI sequestrou os supernós, os servidores de sinkhole instruíram os computadores vítimas a baixar um código em shell que carregava reflexivamente uma DLL que neutralizava o malware. Isso desinfetou com sucesso os computadores das vítimas e evitou novos ataques.

No momento da remoção, o Qakbot havia infectado mais de 700 mil computadores em todo o mundo, incluindo mais de 200 mil somente nos Estados Unidos.[11] Antes dessa operação, **o Qakbot esteve ativo durante quase 15 anos**, originalmente concebido para facilitar fraudes com cartões de crédito e transferências bancárias. Em 2019, o grupo passou a servir como agente de acesso inicial para grupos de ransomware, incluindo Conti, ProLock, Egregor, REvil, MegaCortex e Black Basta.

O malware Qakbot normalmente era distribuído por meio de e-mails de spam contendo anexos ou links maliciosos. Uma vez infectado, o Cobalt Strike era frequentemente implantado para movimentação lateral e eventual implantação de ransomware.

Infelizmente, não houve prisões ou acusações abertas contra qualquer um dos criminosos, e o Qakbot **ressurgiu em dezembro de 2023**. O grupo atualizou o malware para ser compatível com versões de 64 bits do Windows, alterou o formato de configuração interna e modificou a comunicação de rede para usar criptografia AES. Como discutiremos mais adiante neste relatório, o grupo Qakbot mudou significativamente seus TTPs desde a Operação Duck Hunt.

[10] Departamento de Justiça dos EUA, **Malware Qakbot interrompido em derrubada cibernética internacional**, 29 de agosto de 2023.

[11] TechCrunch, **Como o FBI derrubou o notório botnet Qakbot**, 1º de setembro de 2023.

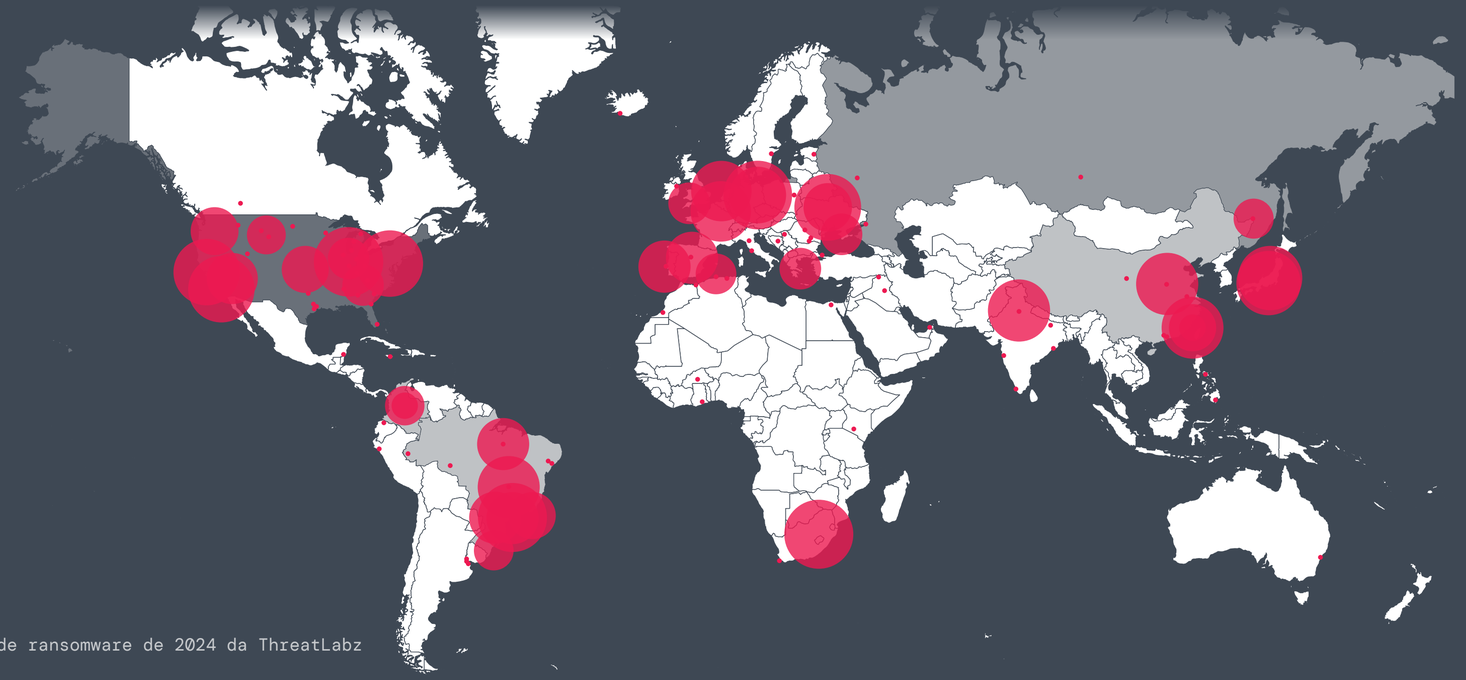
A “Operação Endgame” teve como alvo simultâneo vários agentes de acesso inicial

Em 28 de maio de 2024, em colaboração com inúmeras agências internacionais de segurança pública, a Europol anunciou a Operação Endgame, que visava simultaneamente vários agentes de acesso inicial. Isso levou a mais de uma dúzia de buscas globais, várias detenções e ao encerramento de mais de 100 servidores utilizados para atividades criminosas. Esses servidores eram essenciais para as operações de vários downloaders de malware (também conhecidos como “loaders”) que eram usados para se infiltrar nos computadores das vítimas, implantando software malicioso, incluindo ransomware.

As famílias de malware visadas nessa operação foram responsáveis por infectar milhões de computadores em todo o mundo, inclusive em instalações de saúde e serviços de infraestrutura crítica. Como parte da operação, foram tomadas medidas contra SmokeLoader, Pikabot, Bumblebee e IcedID.

A Zscaler ThreatLabz forneceu assistência técnica essencial para os esforços de sinkhole e remediação do SmokeLoader na Operação Endgame.

O SmokeLoader, ativo desde 2011, foi usado por vários agentes de acesso inicial para ransomware, incluindo Raspberry Robin e a gangue de ransomware Stop (também conhecida como DJVU). A Operação Endgame apreendeu mais de mil domínios do SmokeLoader usados por esses grupos criminosos. Os domínios foram então redirecionados para um servidor controlado pelas autoridades. O mapa da figura 13 mostra sistemas infectados que se comunicaram com o sinkhole do SmokeLoader.



Este mapa demonstra o impacto de longo alcance que o SmokeLoader teve em todo o mundo, com infecções significativas na América Latina, Ásia, América do Norte e Europa.

Figura 13: mapa de infecções do SmokeLoader se comunicando com o sinkhole da Operação Endgame. (Fonte: Zscaler ThreatLabz)

Quando os sistemas infectados com o SmokeLoader se conectavam ao servidor sinkhole, eles recebiam o comando de desinstalação integrado do próprio malware. Até o momento, mais de 40 mil sistemas infectados com o SmokeLoader foram limpos, conforme mostra a figura 14.

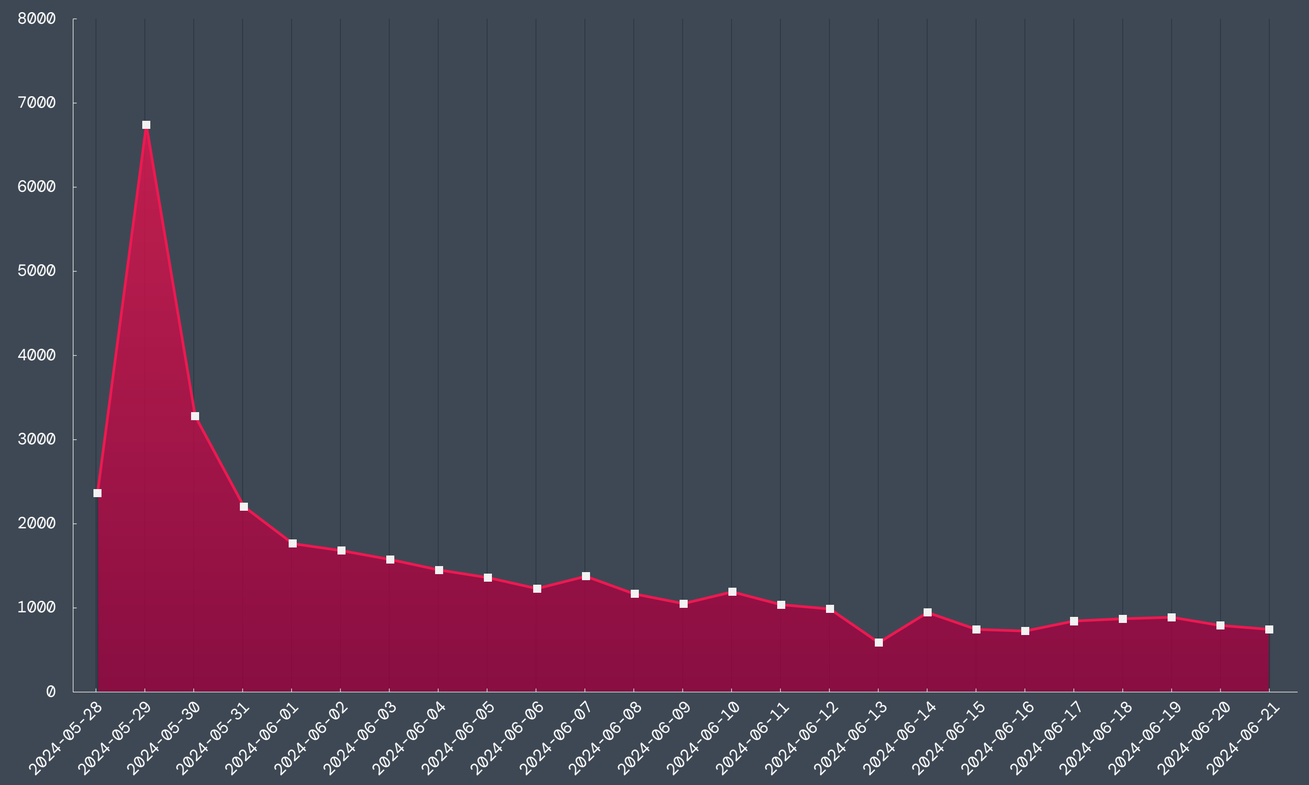


Figura 14: sistemas SmokeLoader limpos pela Operação Endgame.

O Pikabot surgiu originalmente no início de 2023 e exibiu atividade significativa na segunda metade do ano. Esse aumento ocorreu porque o malware se tornou o agente de acesso inicial preferencial do ransomware Black Basta depois que a Operação Duck Hunt interrompeu o Qakbot. Em fevereiro de 2024, **o Pikabot ressurgiu com mudanças significativas** em sua base de código e estrutura. O Pikabot foi observado pela ThreatLabz implantando regularmente **o Cobalt Strikeeo Meterpreter** do Metasploit.

O Bumblebee foi lançado em março de 2022 e tinha ligações com o antigo grupo de ransomware Conti. O malware foi o sucessor da ferramenta de malware BazarLoader do grupo, que eles usaram para acesso inicial para ataques com os ransomwares Conti e Diavol. A ThreatLabz observou frequentemente tanto o BazarLoader quanto o Bumblebee implantando cargas úteis do Cobalt Strike para movimentação lateral. O Bumblebee também foi associado a ataques dos ransomwares Akira e Black Basta.

Semelhante ao Qakbot, o IcedID foi originalmente projetado como um trojan bancário quando apareceu em 2017. No entanto, o grupo posteriormente mudou seu foco para servir como agente de acesso inicial para ransomware. Ao longo dos anos, o código de malware do IcedID foi bifurcado e modificado para diversos fins. Além disso, os mesmos desenvolvedores criaram um novo loader de malware conhecido como Latrodectus, lançado em novembro de 2023, que provavelmente também foi usado para implantar ransomware.

Após a Operação Endgame, houve pouca atividade para a maioria desses agentes de acesso inicial, **com exceção do Latrodectus**, que ressurgiu em menos de um mês. No entanto, a calmaria provavelmente durará pouco, à medida que os criminosos se reagruparem.

Ransomware Hive renascido como Hunters International

Em janeiro de 2023, a infraestrutura do grupo de ransomware Hive foi encerrada. Após uma operação secreta de sete meses, o FBI infiltrou-se com sucesso nos servidores do Hive, recuperando mais de 300 chaves de descriptografia que impediram aproximadamente US$ 130 milhões em pagamentos de resgate. Em funcionamento desde junho de 2021, o coletivo Hive atacou e vitimou mais de 1.500 organizações em todo o mundo, acumulando mais de US$ 100 milhões em pagamentos de resgate.[12] As vítimas incluíram hospitais, distritos escolares, instituições financeiras e várias outras entidades. No entanto, nenhuma prisão associada ao Hive foi feita, e o grupo foi rebatizado como Hunters International em outubro de 2023. Os cibercriminosos costumam usar essa estratégia de rebranding após uma grande interrupção.

O grupo fez uma mudança notável em sua operação: não oferecerá mais descontos nem negociará com as vítimas o pedido inicial de resgate, conforme mostra a figura 15.

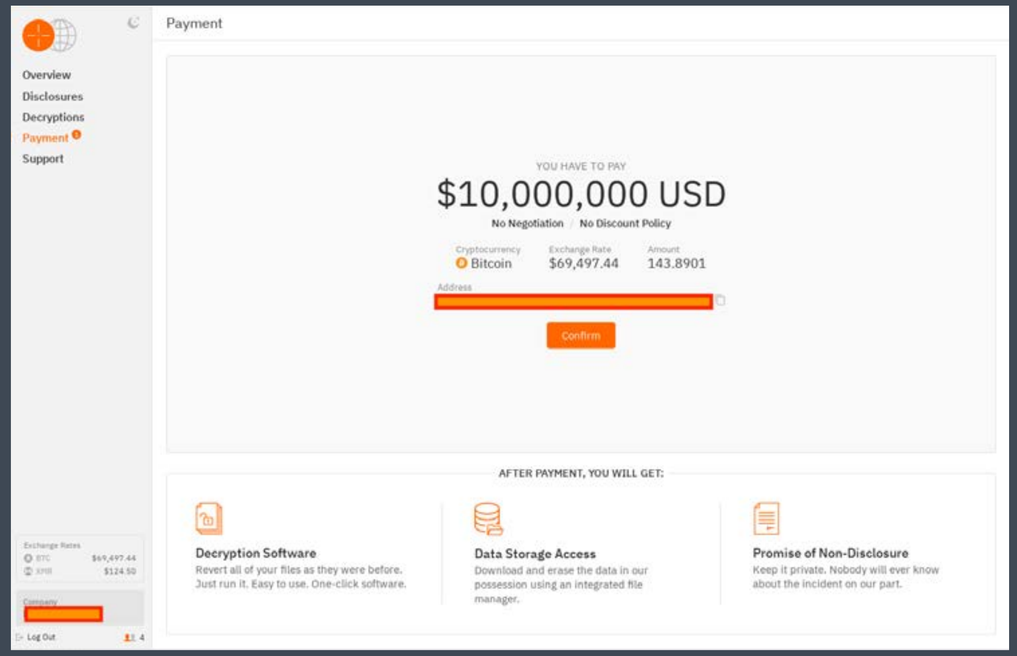


Figura 15: portal de vítimas do Hunters International sem descontos ou negociações de preços.

A política de preços não negociáveis é **muito incomum** em grupos de ransomware, que frequentemente oferecem descontos significativos em relação ao pedido de resgate original. Essa decisão da equipe Hunters provavelmente levará a um volume geral de pagamento menor, mas a valores globais de pagamento mais elevados.

O Hunters International continua a lançar novos ataques e é provável que continue a ser uma grande ameaça, se não houver mais detenções e acusações criminais.

[12] Departamento de Justiça dos EUA, **Departamento de Justiça dos EUA interrompe variante do Hive Ransomware**, 26 de janeiro de 2023.

As 5 principais famílias de ransomware_ a serem observadas em 2024 e 2025

À medida que o ransomware e outras ameaças cibernéticas continuam a evoluir em complexidade e sofisticação, manter-se informado sobre as famílias de ransomware mais prevalentes e perigosas é crucial para manter uma postura de segurança eficaz. Esta seção destaca cinco famílias de ransomware que representam alguns dos riscos mais significativos para as empresas, fornecendo informações sobre suas táticas, impacto potencial e atividades recentes.

#1 Dark Angels

O grupo de ransomware Dark Angels, que opera o site de vazamento de dados Dunghill, surgiu por volta de maio de 2022. O grupo conduziu alguns dos maiores ataques de ransomware, mas conseguiu atrair atenção mínima. No início de 2024, a ThreatLabz descobriu uma vítima que pagou ao Dark Angels US$ 75 milhões, superior a qualquer quantia publicamente conhecida; uma conquista que certamente atrairá o interesse de outros invasores que buscam replicar esse sucesso adotando suas principais táticas (que descrevemos abaixo). O Dark Angels tem como alvo vários setores, incluindo saúde, governo, finanças e educação. Mais recentemente, foram observados lançando ataques contra grandes empresas industriais, de tecnologia e de telecomunicações.

O grupo Dark Angels emprega uma abordagem altamente direcionada, normalmente atacando uma única grande empresa de cada vez. Isso contrasta fortemente com a maioria dos grupos de ransomware, que atacam as vítimas indiscriminadamente e terceirizam a maior parte dos ataques a redes afiliadas de agentes de acesso inicial e equipes de testes de penetração. Depois que os Dark Angels identificam e comprometem um alvo, eles decidem seletivamente se criptografam os arquivos da empresa. Na maioria dos casos, o grupo Dark Angels rouba uma grande quantidade de informações, normalmente na faixa de 1 a 10 TB. Para grandes empresas, o grupo exfiltrou entre 10 e 100 TB de dados, cuja transferência pode levar dias ou semanas.

O ataque de maior destaque conduzido pelo grupo Dark Angels ocorreu em setembro de 2023, quando violou um conglomerado internacional que fornece soluções para sistemas de automação predial, entre outros serviços. O Dark Angels exigiu um resgate de US$ 51 milhões, alegou ter roubado mais de 27 TB de dados corporativos e criptografado as máquinas virtuais VMware ESXi da empresa. Uma variante do ransomware RagnarLocker foi usada para criptografar os arquivos da empresa durante o ataque. A relação entre RagnarLocker e Dark Angels não é clara, mas o grupo estava usando o ransomware antes da ação policial contra o RagnarLocker,[13] que resultou na prisão de um membro importante em outubro de 2023. Observe que quando o Dark Angels apareceu pela primeira vez, ele implantou uma variante do Babuk antes de mudar para o RagnarLocker.

A estratégia do grupo de ransomware Dark Angels de atingir um pequeno número de empresas de alto valor para grandes pagamentos é uma tendência que vale a pena monitorar. A Zscaler ThreatLabz prevê que outros grupos de ransomware tomarão nota do sucesso do Dark Angels e poderão adotar táticas semelhantes, concentrando-se em alvos de alto valor e aumentando a importância do roubo de dados para maximizar seus ganhos financeiros.

[13] Europol, **Gangue de ransomware Ragnar Locker derrubada por uma investida policial internacional**, 20 de outubro de 2023.

#2 LockBit

O LockBit surgiu pela primeira vez em setembro de 2019 e rapidamente ganhou destaque devido à grande rede de afiliados de ransomware do grupo. O LockBit utiliza uma grande rede de afiliados para executar violações, exfiltrar dados e implementar seu ransomware. A infiltração normalmente começa através de e-mails de spam contendo anexos ou links maliciosos. Outros métodos incluem a execução de ataques de senha de força bruta direcionados ao Protocolo de Área de Trabalho Remota (RDP) ou credenciais de VPN, a compra de credenciais roubadas comprometidas por meio de agentes de acesso inicial e a exploração de aplicativos voltados ao público. A rede cibercriminosa do LockBit tem como alvo setores críticos como manufatura, saúde e logística. O grupo atacou coletivamente mais de 2.000 sistemas em todo o mundo e extorquiu mais de US$ 120 milhões de vítimas.

No último ano, o LockBit permaneceu no topo da lista em termos de volume de ataques. Usando uma estratégia marcadamente diferente do Dark Angels, o grupo LockBit incentiva os afiliados a atacar o maior número possível de organizações, independentemente da recompensa potencial. Esse elevado volume de ataques resulta muitas vezes em pequenas empresas que são alvo de exigências de resgate relativamente baixas.

O ransomware LockBit é implantado em sistemas baseados em Windows e Linux. Existem três versões do LockBit para Windows: LockBit Red (o original), LockBit Black (baseado no código-fonte do BlackMatter) e LockBit Green (baseado no código-fonte vazado do Conti). Conforme mencionado no **Relatório de ransomware de 2023 da ThreatLabz**, o builder do LockBit Black vazou e muitos grupos cibercriminosos não afiliados ao LockBit o usaram para seus próprios ataques de ransomware. Curiosamente, o LockBit Black ainda é a variante mais comumente implantada no grupo. A variante específica do ransomware LockBit usada para criptografar os arquivos da vítima agora é mostrada na nota de resgate ao lado do ID da vítima. Isso permite que o criminoso que conduz o ataque identifique facilmente a variante do LockBit implantada para ajudá-lo a fornecer a ferramenta de descriptografia adequada quando um resgate for pago. Observe a figura 16 para ver um exemplo de uma nota de resgate recente do LockBit Black.

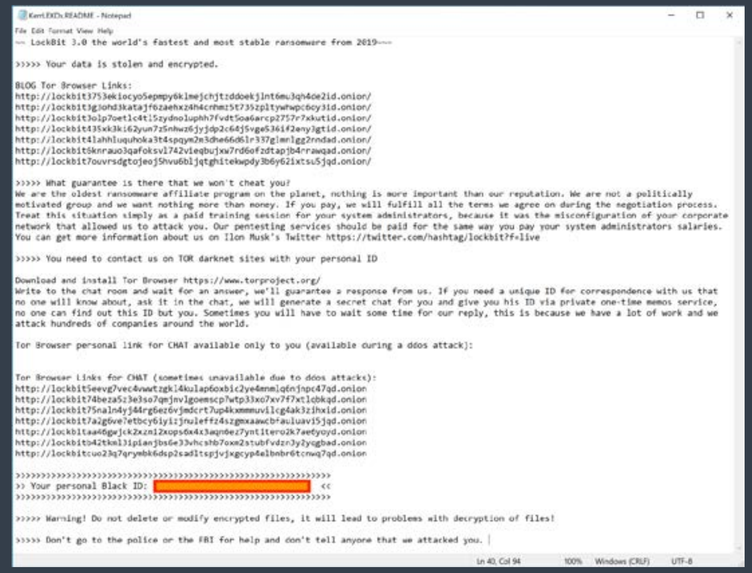


Figura 16: exemplo de uma nota de resgate recente do LockBit Black.

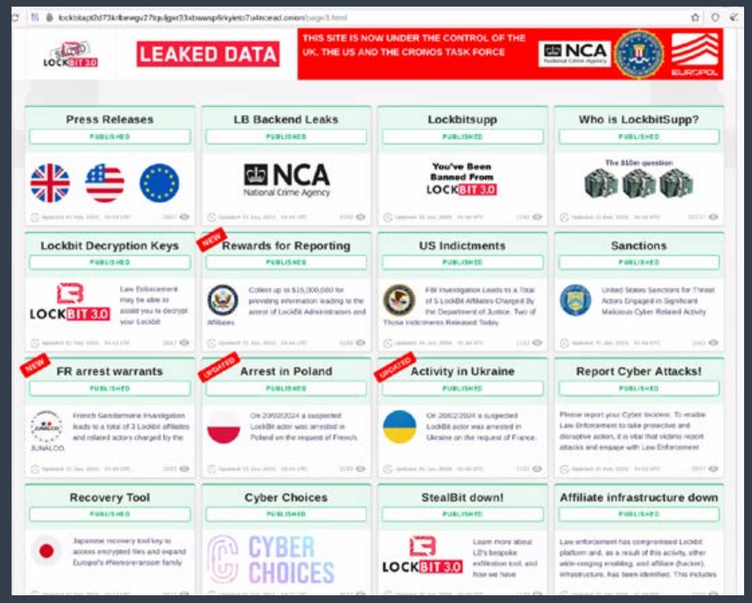


Figura 17: apreensão do site de vazamento de dados do LockBit pelas autoridades.

Em 20 de fevereiro de 2024, o FBI e as autoridades do Reino Unido apreenderam partes da infraestrutura do LockBit, que incluía aproximadamente 7 mil chaves de descriptografia de vítimas. Após a apreensão, as agências de segurança confiscaram o site de vazamento de dados do LockBit e zombaram dos cibercriminosos com uma versão semelhante do antigo site, exibindo vários artigos e cronômetros de contagem regressiva até que novas informações fossem divulgadas, conforme mostrado na figura 17 abaixo.

Infelizmente, poucos dias após a remoção, **a ThreatLabz identificou novos ataques de ransomware** perpetrados pelo LockBit e um novo site de vazamento de dados. O grupo permaneceu ativo e atacou dezenas de novas entidades desde a ação policial.

Em 7 de maio de 2024, o FBI anunciou a acusação do desenvolvedor e operador do LockBit, Dmitry Yuryevich Khoroshev. No entanto, o operador do LockBit negou rapidamente que o FBI o tenha identificado corretamente. Sem mais prisões, os ataques do LockBit provavelmente continuarão no futuro próximo, embora em algum momento a ThreatLabz espere que a marca LockBit possa ser aposentada e a operação ressuscitada sob outro nome devido aoaumento do escrutínio.

#3 BlackCat

O ransomware BlackCat (também conhecido como ALPHV), introduzido em novembro de 2021, foi uma das ameaças mais notórias até ser encerrado em março de 2024. Semelhante ao LockBit, o BlackCat aproveitou uma rede afiliada para lançar ataques e compartilhou uma porcentagem dos pagamentos do resgate.

Indiscutivelmente o afiliado mais famoso do BlackCat é um grupo conhecido como Scattered Spider[14] (também conhecido como Star Fraud). Composto por membros que falam inglês, esse grupo é altamente eficaz em ataques de engenharia social, muitas vezes fazendo-se passar por pessoal de TI ou de suporte técnico em chamadas de voz e realizando ataques de troca de SIM para contornar a autenticação multifatorial. Em 15 de junho de 2024, o suposto líder[15] do Scattered Spider, um cidadão britânico de 22 anos, foi preso. No entanto, é muito cedo para dizer qual o impacto que essa prisão terá na capacidade do grupo de continuar os seus ataques.

A BlackCat foi uma das famílias de ransomware mais compatíveis com várias plataformas, em parte porque usa a linguagem de programação Rust. A figura 18 mostra as ferramentas de descriptografia disponíveis para todas as plataformas compatíveis com o ransomware BlackCat pouco antes de o grupo encerrar as operações. As plataformas incluíam Windows, ESXi, FreeBSD e inúmeras variantes de sistemas operacionais e arquiteturas Linux, como ARM, x86/x64, e PowerPC.

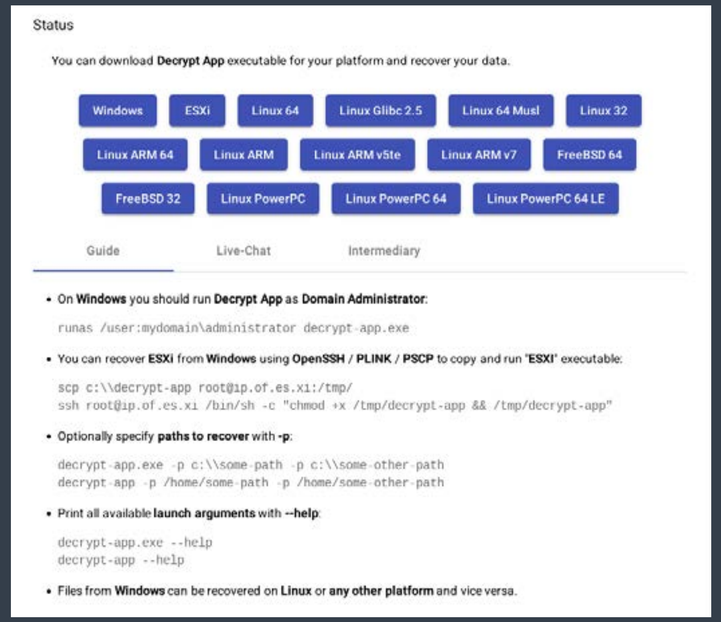


Figura 18: as ferramentas de descriptografia do BlackCat foram fornecidas para 15 sistemas operacionais, arquiteturas e plataformas diferentes.

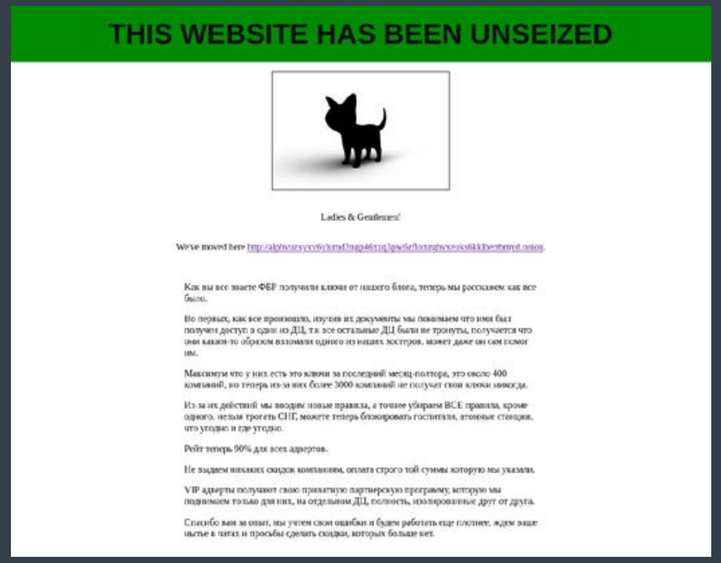


Figura 19: site de vazamento de dados "não apreendidos" do BlackCat após ação policial.

Esse nível de compilação entre plataformas é incomum em comparação com outras famílias de ransomware que normalmente são compatíveis apenas com Windows, ESXi e um pequeno número de plataformas baseadas em Linux. Isso indica que os afiliados do BlackCat podem ter solicitado compatibilidade com plataformas adicionais, a fim de criptografar arquivos no maior número possível de sistemas.

Em dezembro de 2023, o FBI obteve acesso a algumas infraestruturas do BlackCat. O FBI tentou apreender os sites do grupo baseados no Tor, incluindo os portais de negociação de resgate e sites de vazamento de dados. No entanto, em uma reviravolta rápida, o BlackCat publicou uma mensagem dizendo que haviam "desocupado" o site de vazamento de dados e forneceram um link para um novo site de vazamento de dados que o FBI não podia manipular, como mostrado na figura 19 abaixo.

Esse vai e vem entre o FBI e o BlackCat ocorreu durante alguns dias até que o BlackCat tivesse certeza de que o novo site de vazamento de dados estava suficientemente divulgado. Observe que "apreender" um site baseado em Tor não é tão trivial quanto um site tradicional baseado em DNS, porque depende de segredos criptográficos e não de uma autoridade central sujeita a ordens judiciais.

Em março de 2024, o grupo BlackCat anunciou a sua dissolução, citando o comprometimento da sua infraestrutura pelo FBI, o que supostamente os impossibilitou de continuar as suas operações. No entanto, surgiram suspeitas devido ao momento de seu encerramento ocorrer imediatamente após receberem um resgate de US$ 22 milhões e, em seguida, realizarem um golpe de saída em um afiliado que os ajudou a invadir um prestador de serviços de saúde (discutido anteriormente neste relatório).

Embora o ransomware BlackCat não esteja mais ativo, os afiliados por trás dos ataques do grupo provavelmente migraram para outras redes de ransomware como serviço, como o RansomHub (onde os dados roubados do provedor de saúde que pagou o resgate de US$ 22 milhões já foram vazados). Além disso, é improvável que o próprio grupo de ransomware BlackCat tenha realmente cessado suas operações e provavelmente ressurgirá sob uma nova marca.

[14] Agência de Segurança de Cibersegurança e Infraestrutura, **Cybersecurity Advisory: Scattered Spider**, 16 de novembro de 2023.
[15] Krebs on Security, **Suposto chefe do grupo de hackers "Scattered Spider" preso**, 15 de junho de 2024.

#4 Akira

O ransomware Akira entrou em cena em abril de 2023, ganhando rapidamente fama pelo volume de ataques conduzidos por afiliados. O grupo criminoso Akira é provavelmente outra ramificação do extinto grupo Conti. Na verdade, o código do ransomware Akira originalmente compartilhava muitas semelhanças com o código-fonte vazado do Conti. No entanto, o grupo desenvolveu mais recentemente um ransomware baseado em Rust que contém referências a personagens do Power Rangers, como Megazord.

Os afiliados do ransomware Akira empregaram vários mecanismos de acesso inicial, inclusive por meio da exploração da CVE-2023-20269.[16] O grupo criminoso que opera o Bumblebee, que tem ligações com o ransomware Conti, também é conhecido por ser um agente de acesso inicial para o Akira. Conforme mencionado anteriormente no relatório, a Operação Endgame desmantelou o Bumblebee, mas teve um impacto mínimo nas operações do Akira.

Para entender melhor os ataques do Akira, podemos aprender diretamente com as informações que o Akira fornece às vítimas que pagam resgate. A ThreatLabz capturou a seguinte mensagem de bate-papo do Akira, que contém detalhes sobre como eles inicialmente obtiveram acesso à rede da empresa por meio de um agente de acesso inicial e também ofereceu dicas para prevenir ataques de ransomware no futuro:

O acesso inicial à sua rede foi adquirido na dark web. Em seguida, foi realizado o kerberoasting e obtivemos hashes de senhas. Então, nós apenas aplicamos força bruta neles e obtivemos a senha de administrador do domínio. Passando semanas dentro da sua rede, conseguimos detectar algumas falhas que recomendamos eliminar:

1. Nenhum de seus funcionários deve abrir e-mails suspeitos, links suspeitos ou baixar qualquer arquivo, muito menos executá-los em seus computadores.

2. Use senhas robustas e altere-as sempre que possível (pelo menos 1 a 2 vezes por mês). As senhas não devem corresponder ou ser repetidas em recursos diferentes.

3. Instale 2FA sempre que possível.

4. Utilize as versões mais recentes dos sistemas operacionais, pois são menos vulneráveis a ataques.

5. Atualize todas as versões de software.

6. Use soluções antivírus e ferramentas de monitoramento de tráfego.

7. Crie um jump host para sua VPN. Use credenciais exclusivas que sejam diferentes do domínio um.

8. Use software de backup com armazenamento na nuvem compatível com uma chave de token.

9. Instrua seus funcionários com a maior frequência possível sobre as precauções de segurança online. O ponto mais vulnerável é o fator humano e a irresponsabilidade de seus funcionários, administradores de sistemas, etc. Desejamos a você segurança, tranquilidade e muitos benefícios no futuro. Agradecemos por trabalhar conosco e por sua atitude cuidadosa com sua segurança.

Embora esse conselho venha diretamente do Akira, as recomendações são válidas e fornecem uma base para compreender e impedir tais ataques.

O Akira é um dos únicos grandes grupos de ransomware que não foi diretamente sujeito a interrupções de agências de segurança pública. Como resultado, o Akira é agora um dos grupos de ransomware mais ativos que provavelmente continuará a lançar novos ataques durante o próximo ano.

[16] https://nvd.nist.gov/vuln/detail/CVE-2023-20269

#5 Black Basta

O ransomware Black Basta, identificado pela primeira vez em abril de 2022, é outro sucessor do grupo de ransomware Conti. Os afiliados do Black Basta empregaram diversos métodos para obter acesso às redes corporativas. Antes da Operação Duck Hunt (agosto de 2023), o Qakbot era um importante agente de acesso inicial para o Black Basta. Como mencionado anteriormente, o Pikabot interveio para preencher a brecha após a queda. No entanto, o Pikabot foi fechado após a Operação Endgame em maio de 2024.

Desde então, a ThreatLabz tem rastreado novas atividades do grupo criminoso Qakbot, que dinamizou e alterou significativamente seus TTPs. Em vez de usar e-mail de spam para infectar sistemas com o Qakbot, o grupo está atualmente usando uma combinação de técnicas de engenharia social. Em vez de enviar e-mails de spam para milhões de endereços, o grupo criminoso está realizando ataques direcionados. Esses ataques começam com o grupo enviando e-mails de spam para um pequeno número de empresas-alvo. O grupo então liga para um funcionário dessas empresas fingindo ser do seu próprio departamento de TI. O interlocutor instrui a vítima a participar de uma sessão de compartilhamento de tela usando um software de desktop remoto, como a Assistência Rápida da Microsoft, para “atualizar os filtros de spam da empresa” para o funcionário. Depois que o funcionário concede acesso ao criminoso, um script em lote do Windows é executado para realizar o reconhecimento, roubar credenciais e instalar um backdoor no sistema da vítima. O backdoor continua a mudar, mas inclui Qakbot, Cobalt Strike e uma ferramenta de proxy SOCKS. O script em lote contém uma interface de linha de comando semelhante à mostrada na figura 20.

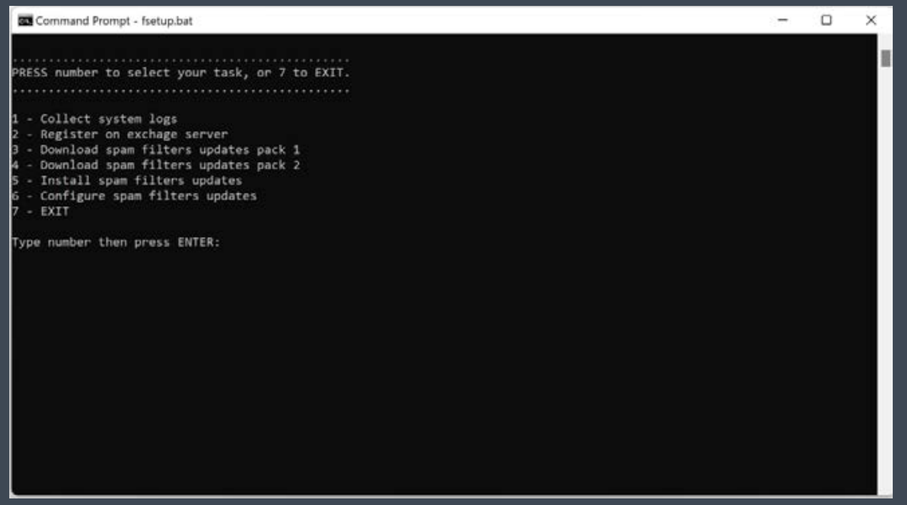


Figura 20: interface de script em lote malicioso do Windows usada para estabelecer um backdoor no sistema da vítima como precursor de um ataque do ransomware Black Basta.

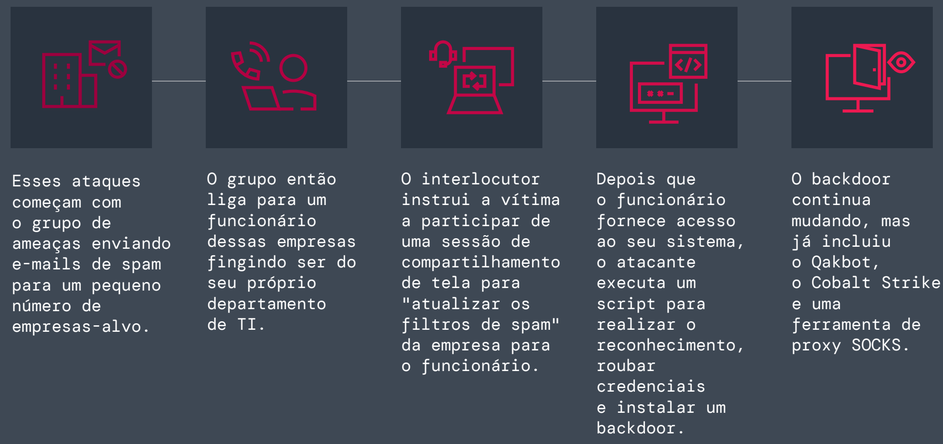


Figura 21: cadeia de ataque do ransomware Black Basta com acesso inicial intermediado pelo grupo de ameaças Qakbot.

Uma vez estabelecido esse acesso de backdoor, o grupo Qakbot transfere o acesso a uma equipe de testes de penetração responsável pela movimentação lateral e pela implantação final do ransomware Black Basta.

Embora a Operação Duck Hunt tenha tido um impacto significativo a curto prazo, o grupo permanece ativo e continua a inovar e experimentar novas técnicas para comprometer organizações. Durante o próximo ano, o grupo criminoso Qakbot provavelmente continuará sendo um importante agente de acesso inicial para ataques de ransomware como o Black Basta.

Arquivo de notas de ransomware_ da ThreatLabz

A Zscaler ThreatLabz mantém um **repositório público no GitHub** que, até o momento em que este relatório foi escrito, rastreia 391 famílias de ransomware e contém um total de 945 notas de resgate, adicionando 19 famílias e 55 notas de resgate entre abril de 2023 e abril de 2024. Esse arquivo pode ser valioso para o rastreamento grupos de ransomware ao longo do tempo, incluindo seus sites de vazamento de dados e táticas de negociação, e para vincular grupos de ransomware que mudam de marca usando análise estilométrica.

A figura 22 mostra uma comparação estilométrica entre um bate-papo de resgate do Conti (acima) e um bate-papo de resgate do Black Basta (abaixo). Isso demonstra que os membros do Black Basta são quase certamente ex-membros do Conti, como fica evidente nas semelhanças na estrutura das frases, na escolha das palavras e até nas instruções específicas.

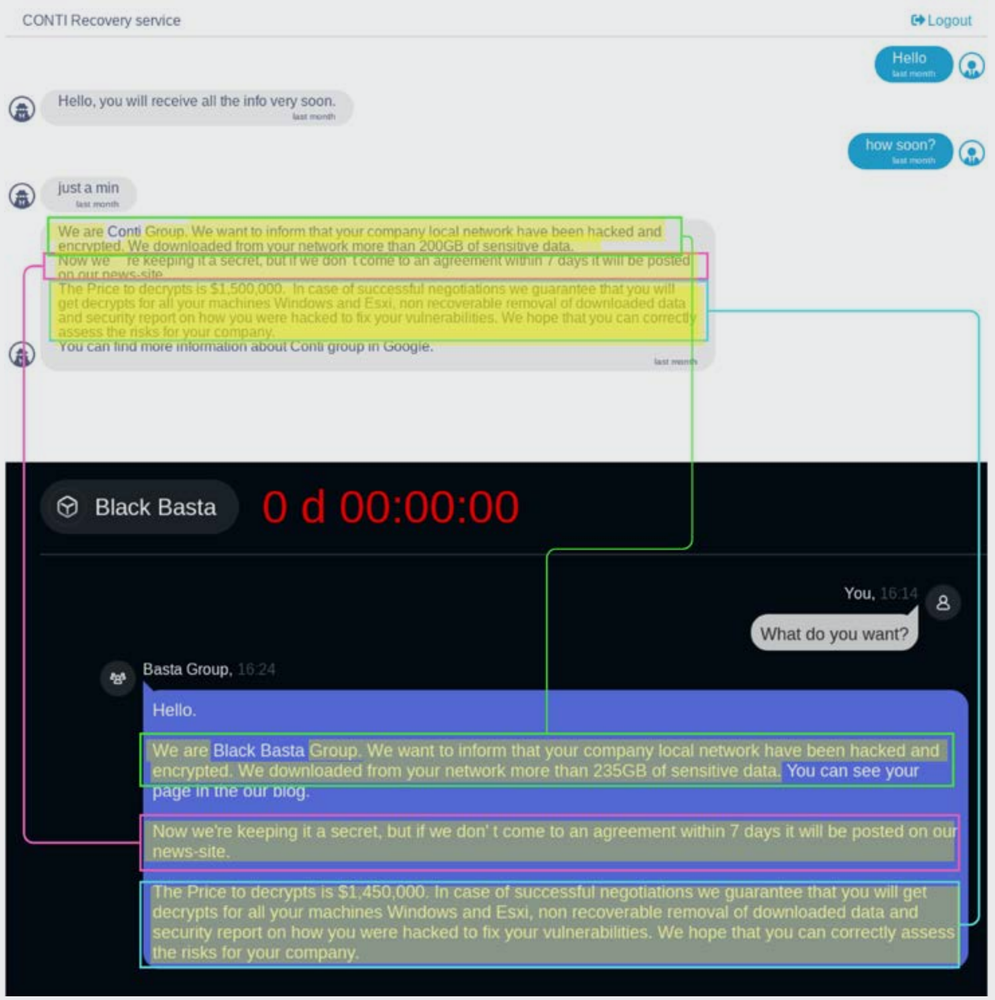


Figura 22: comparação estilométrica entre bate-papos de resgate do Conti (acima) e Black Basta (abaixo).

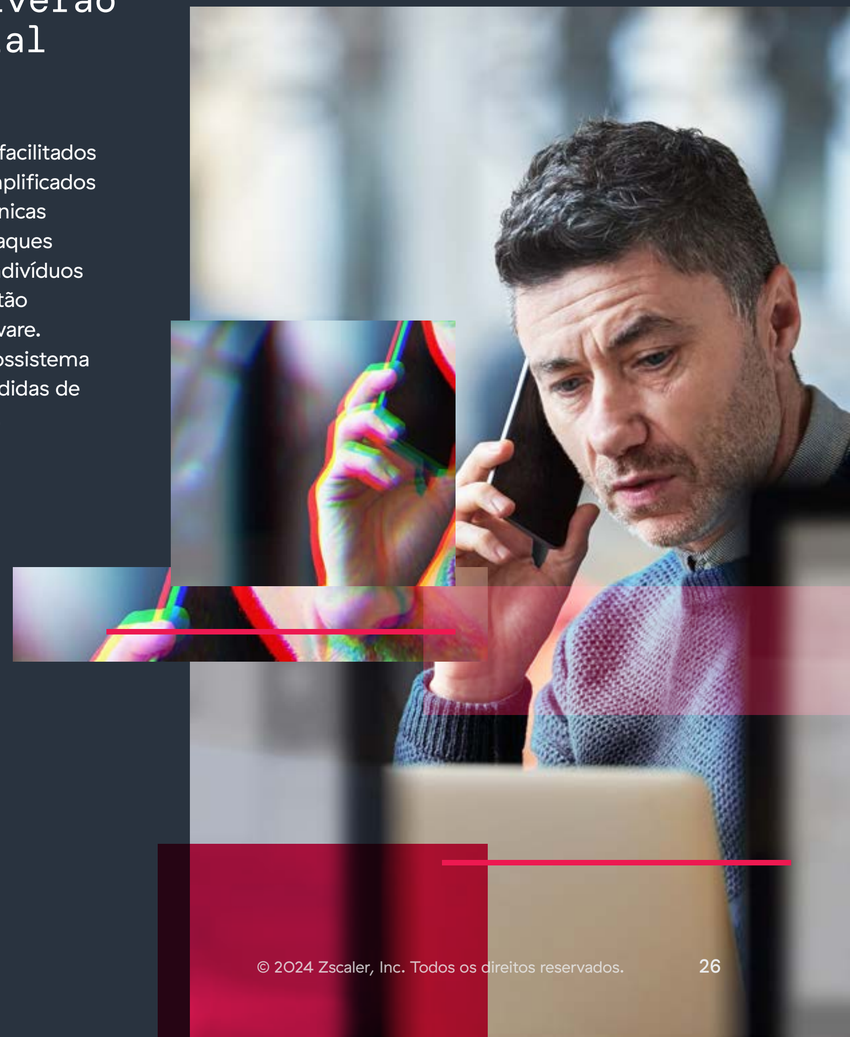
Previsões para_ 2025

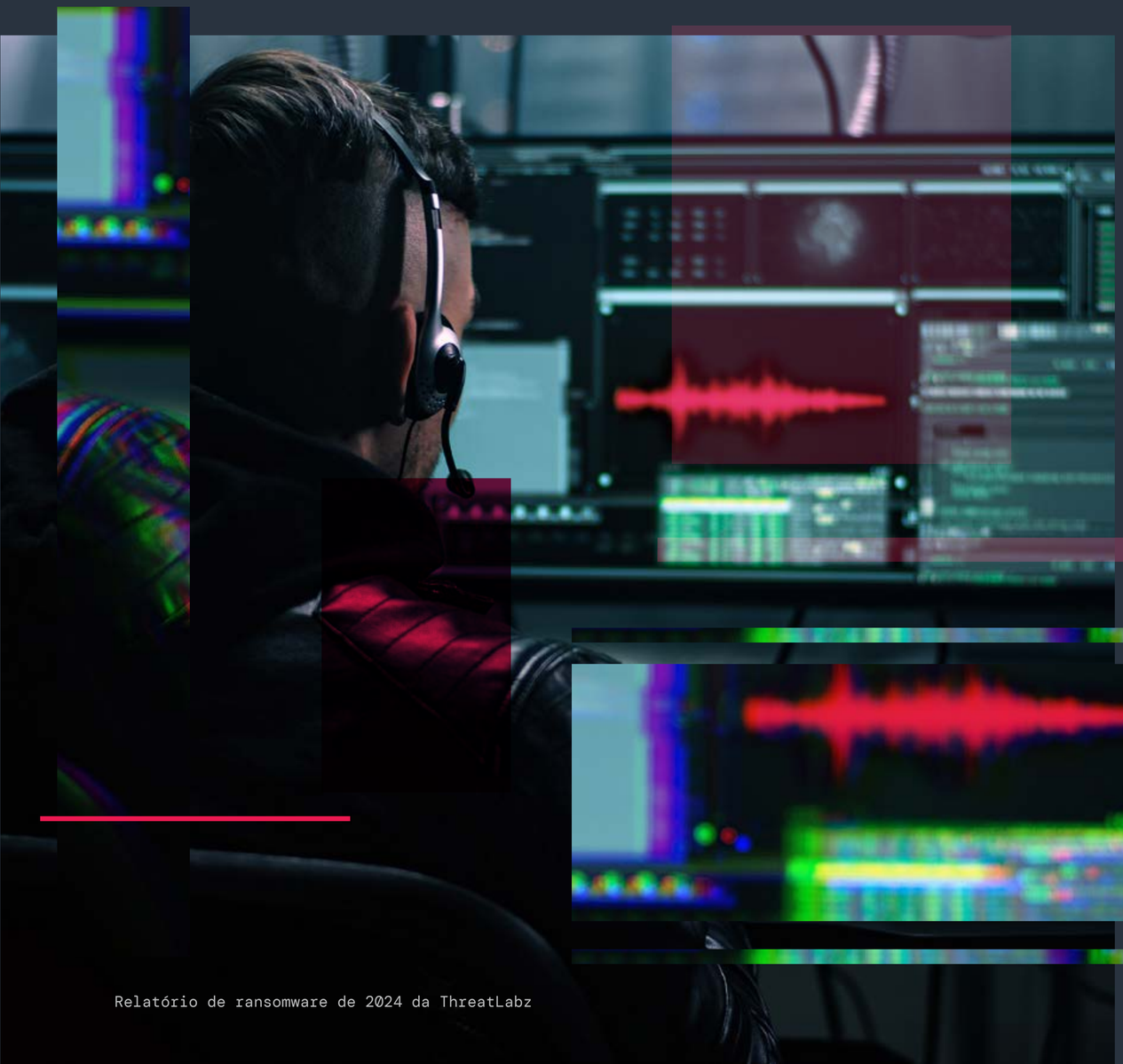
1. Os grupos de ransomware adotarão estratégias de ataque altamente direcionadas.

Nos últimos anos, o Dark Angels tem sido um dos grupos de ransomware mais bem-sucedidos e menos conhecidos, com uma estratégia distinta de atacar um pequeno número de empresas multibilionárias e extorqui-las por resgates substanciais. Essa estratégia serve um duplo propósito: reduzir o escrutínio das autoridades policiais e do setor de segurança, ao mesmo tempo que gasta mais recursos para se infiltrar em grandes empresas que estão dispostas a pagar resgates significativos para proteger enormes volumes de dados roubados. Isso fez com que o grupo recebesse o maior pagamento de resgate já conhecido, de US$ 75 milhões, o que certamente atrairá o interesse de outros grupos de ransomware em 2025 que possam querer replicar seu sucesso.

2. Os ataques direcionados envolverão cada vez mais engenharia social baseada em voz.

Em 2025, esperamos ver um aumento nos ataques direcionados facilitados por agentes especializados de acesso inicial. Esses agentes, exemplificados pelas atividades do Qakbot e do Scattered Spider, empregam técnicas sofisticadas para garantir a entrada, nomeadamente utilizando ataques de engenharia social baseados em voz (“vishing”) para enganar indivíduos e fazê-los conceder acesso a um ambiente corporativo, que é então usado em última análise para exfiltrar dados e implantar ransomware. Essa tendência emergente destaca as colaborações dentro do ecossistema cibercriminoso e sublinha a necessidade de maior vigilância e medidas de segurança avançadas para combater essas ameaças em evolução.





3. Os invasores de ransomware adotarão cada vez mais a IA generativa para criar campanhas mais eficazes, personalizadas e localizadas.

A crescente adoção da IA generativa em 2025 e no futuro permitirá que os criminosos criem e-mails de spam com gramática e ortografia precisas, bem como usem a clonagem de voz para se passar por funcionários, a fim de obter acesso privilegiado. Nos próximos anos, as vozes geradas por IA poderão ser adaptadas com sotaques e dialetos locais para aumentar a credibilidade e aumentar a probabilidade de sucesso, tornando-se um excelente exemplo de como os grupos de ransomware tornarão os ataques mais convincentes e difíceis de detectar.

4. Mais incidentes de segurança cibernética serão relatados de acordo com as novas regras da SEC.

Com a decisão da SEC exigindo relatórios mais rigorosos sobre incidentes de segurança cibernética, o ano de 2025 continuará a testemunhar um aumento no número de organizações que divulgam incidentes de ransomware. Espera-se que isso resulte em maior transparência e promova uma cultura de responsabilidade e defesas proativas, impulsionando melhorias nas práticas de cibersegurança.

5. Os ataques de ransomware de exfiltração de dados em alto volume estarão aumentando.

Ataques que exfiltram grandes quantidades de dados, incluindo incidentes com menos criptografia, aumentarão significativamente no próximo ano. Essa tendência, que começou a ganhar força em 2022, faz com que os criminosos se concentrem exclusivamente na exfiltração de dados, sem criptografar os sistemas. A abordagem permite operações oportunistas mais rápidas e capitaliza o medo de dados sigilosos serem divulgados para coagir as vítimas a pagarem resgates. Isso destaca uma mudança contínua nas estratégias de ransomware em direção a métodos mais eficientes e de alto impacto.

6. As empresas do setor da saúde, especialmente, continuarão a enfrentar ataques persistentes de grupos de ransomware.

O elevado valor dos dados de saúde continuará a atrair a atenção em 2025. Muitas empresas de saúde demoram a substituir sistemas legados por medidas de segurança modernas e avançadas, o que as torna particularmente vulneráveis. Como resultado, essas organizações provavelmente enfrentarão repetidas violações e tentativas de extorsão. Aqueles que não tomarem as medidas adequadas para priorizar estratégias de defesa zero trust poderão ser alvo de grupos de ransomware.

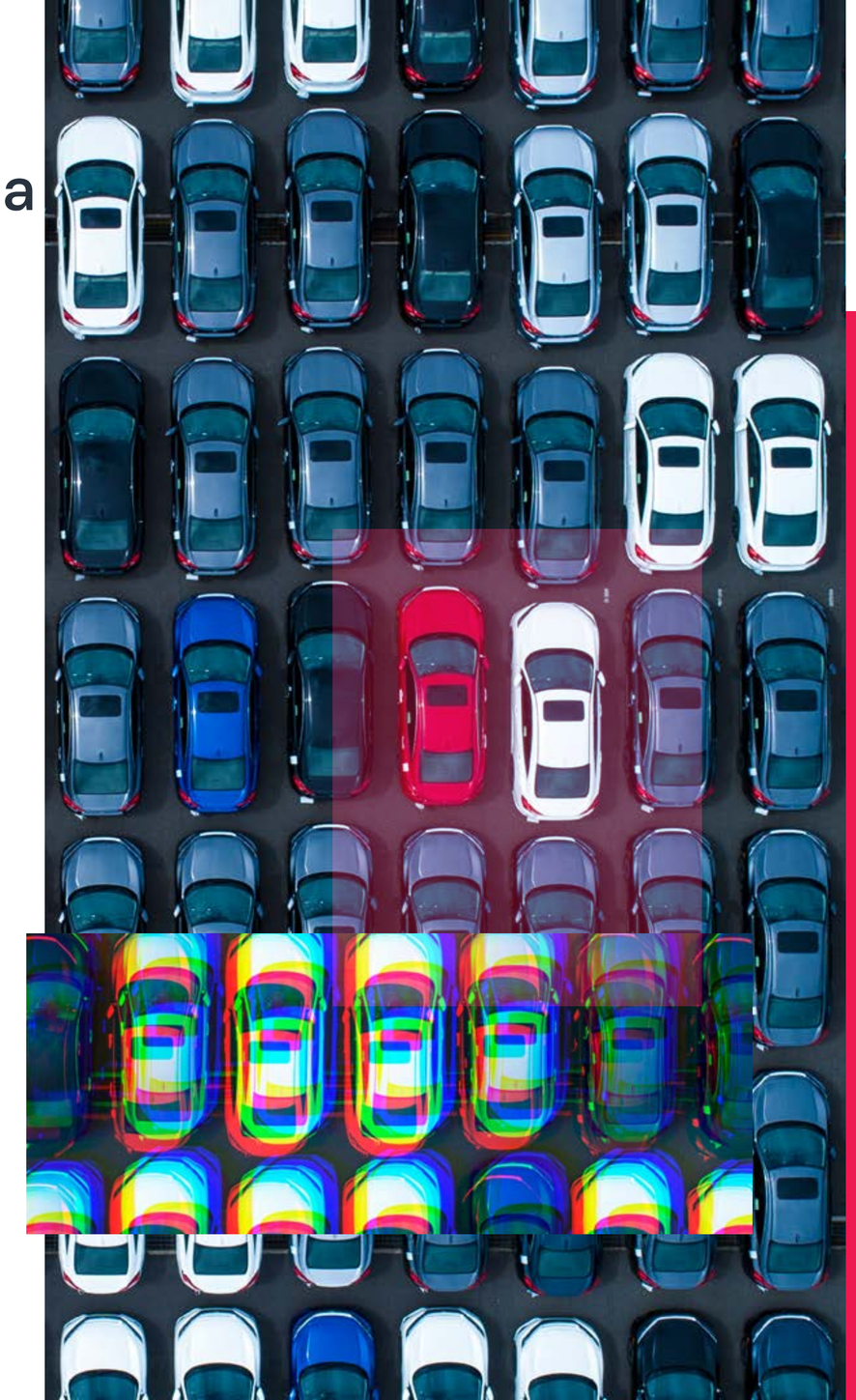
7. A colaboração internacional contra organizações de crime cibernético se baseará em esforços existentes.

As autoridades policiais e o setor privado continuarão a colaborar nos esforços para combater ataques de ransomware, tais como interromper os principais agentes de acesso inicial e grupos de ransomware. A colaboração internacional se tornará cada vez mais vital à medida que a interconectividade global cresce, facilitando a atuação dos cibercriminosos transnacionalmente. Ao compartilhar inteligência e expertise, essas ações coordenadas interromperão mais efetivamente as redes globais de ransomware. A Zscaler ThreatLabz esteve na vanguarda e foi fundamental no fornecimento de assistência técnica para várias dessas operações no último ano.

Como a Zscaler simplifica a proteção contra ransomware

A crescente complexidade e custo dos ataques de ransomware ressaltam a necessidade de defesas zero trust abrangentes. A plataforma **Zscaler Zero Trust Exchange™** simplifica o desafio, oferecendo uma abordagem holística para impedir ransomware.

A Zero Trust Exchange permite que as empresas implementem defesas mais inteligentes em todas as fases de um ataque. Isso começa impedindo que invasores descubram ou explorem usuários e aplicativos, tornando esses usuários e aplicativos invisíveis, acessíveis apenas por usuários ou dispositivos autorizados. Ela inspeciona de maneira integrada todo o tráfego de entrada e saída, seja ele criptografado ou não. Os usuários e dispositivos autenticados conectam-se diretamente aos aplicativos de que precisam, nunca à rede. Assim, mesmo que um invasor consiga acesso, ele não pode se mover lateralmente para roubar ou criptografar dados.



POR QUE O ZERO TRUST É ESSENCIAL PARA A PROTEÇÃO CONTRA RANSOMWARE
As arquiteturas de segurança legadas são ineficazes para impedir ataques de ransomware.

ADEUS, ANTIGO: medidas de segurança tradicionais e soluções específicas, incluindo firewalls e VPNs de "nova geração", muitas vezes introduzem pontos cegos, complexidade e custos significativos. Essas abordagens legadas não conseguem inspecionar arquivos e tráfego criptografados de maneira econômica, deixando as organizações vulneráveis à movimenteção lateral e ataques de ransomware que exploram brechas na visibilidade e no controle, muitas vezes com consequências devastadoras.

OLÁ, ZERO TRUST: uma arquitetura zero trust pressupõe que cada usuário, dispositivo e conexão estão potencialmente comprometidos. Essa abordagem exige verificação contínua e controle de acesso rigoroso. Ao verificar identidades de forma consistente e inspecionar todo o tráfego, incluindo dados criptografados, o zero trust reduz significativamente o risco de propagação de ataques na rede, neutralizando ameaças de ransomware antes que elas possam causar danos.

A ZSCALER INTERROMPE O RANSOMWARE EM TODAS AS FASES DO CICLO DE ATAQUE, desde o reconhecimento inicial e comprometimento até a movimentação lateral, roubo de dados e execução de carga útil.

Minimize a superfície de ataque: devensolvida em uma arquitetura zero trust, a Zero Trust Exchange substitui arquiteturas herdadas de VPN e firewall exploráveis que expandem a superfície de ataque. A Zscaler minimiza efetivamente a superfície de ataque, ocultando usuários, aplicativos e dispositivos atrás de um proxy na nuvem, onde eles não são visíveis ou detectáveis na internet. Semelhante a uma central telefônica que roteia chamadas para destinos autorizados, a Zscaler conecta apenas o usuário ou dispositivo autorizado e correto a um aplicativo específico.

Evite o comprometimento inicial: a Zero Trust Exchange emprega ampla inspeção de TLS/SSL, isolamento do navegador, sandbox avançada em linha e controles de acesso baseados em políticas para impedir que os usuários acessem sites maliciosos, bem como detectar ameaças desconhecidas antes que elas cheguem à sua rede. Isso minimiza o risco de comprometimento em primeiro lugar.

Elimine a movimentação lateral: aproveitando a segmentação de usuário para aplicativo ou de aplicativo para aplicativo, os usuários se conectam diretamente aos aplicativos (e os aplicativos a outros aplicativos), não à rede, eliminando o risco de movimentação lateral. Ao centralizar o gerenciamento de políticas de controle de acesso, a Zscaler atua como um ponto de verificação de segurança para o tráfego da internet, removendo rotas de movimentação lateral. A Zscaler também pode identificar e impedir que possíveis invasores se movam lateralmente, sejam ameaças externas ou agentes internos mal-intencionados, por meio da detecção e resposta a ameaças de identidade (ITDR) e recursos de deception.

Impeça a perda de dados: medidas integradas de prevenção contra perda de dados, combinadas com inspeção total de TLS/SSL, efetivamente frustram tentativas de roubo de dados. A Zscaler garante que os dados sejam protegidos tanto em trânsito quanto em repouso.

COMBATE A AMEAÇAS BASEADAS EM IA COM INOVAÇÃO EM IA + ZERO TRUST

Esses recursos baseados em IA permitem que a Zscaler ofereça proteção robusta contra ransomware, garantindo segurança abrangente para empresas no cenário de ameaças em evolução:

- ***A detecção de phishing e C2 baseada em IA*** usa a detecção integrada baseada em IA do Zscaler Secure Web Gateway para identificar e bloquear sites de phishing nunca antes vistos e infraestrutura de comando e controle (C2).
- ***A sandbox baseada em IA*** oferece prevenção abrangente contra malware e ameaças de dia zero analisando arquivos suspeitos em um ambiente controlado.
- ***A segmentação baseada em IA*** fornece recomendações automatizadas de políticas de acesso para minimizar a superfície de ataque e evitar a movimentação lateral, usando contexto do usuário, comportamento, localização e telemetria de aplicativos privados.
- ***A política dinâmica e baseada em risco*** analisa continuamente o risco associado a usuários, dispositivos e aplicativos para aplicar políticas dinâmicas de segurança e acesso.
- ***O isolamento do navegador baseado em IA*** cria um espaço seguro entre os usuários e o conteúdo malicioso da web, renderizando páginas como fluxos de imagens perfeitas, evitando vazamentos de dados e a entrega de ameaças ativas.
- ***A descoberta e classificação de dados baseadas em IA*** fornecem visibilidade e classificação instantâneas de dados prontas para uso em dados de terminais, em linha e na nuvem, tornando mais difícil para o ransomware direcionar e criptografar dados sigilosos.

Prevenção holística em cada estágio da cadeia de ataque

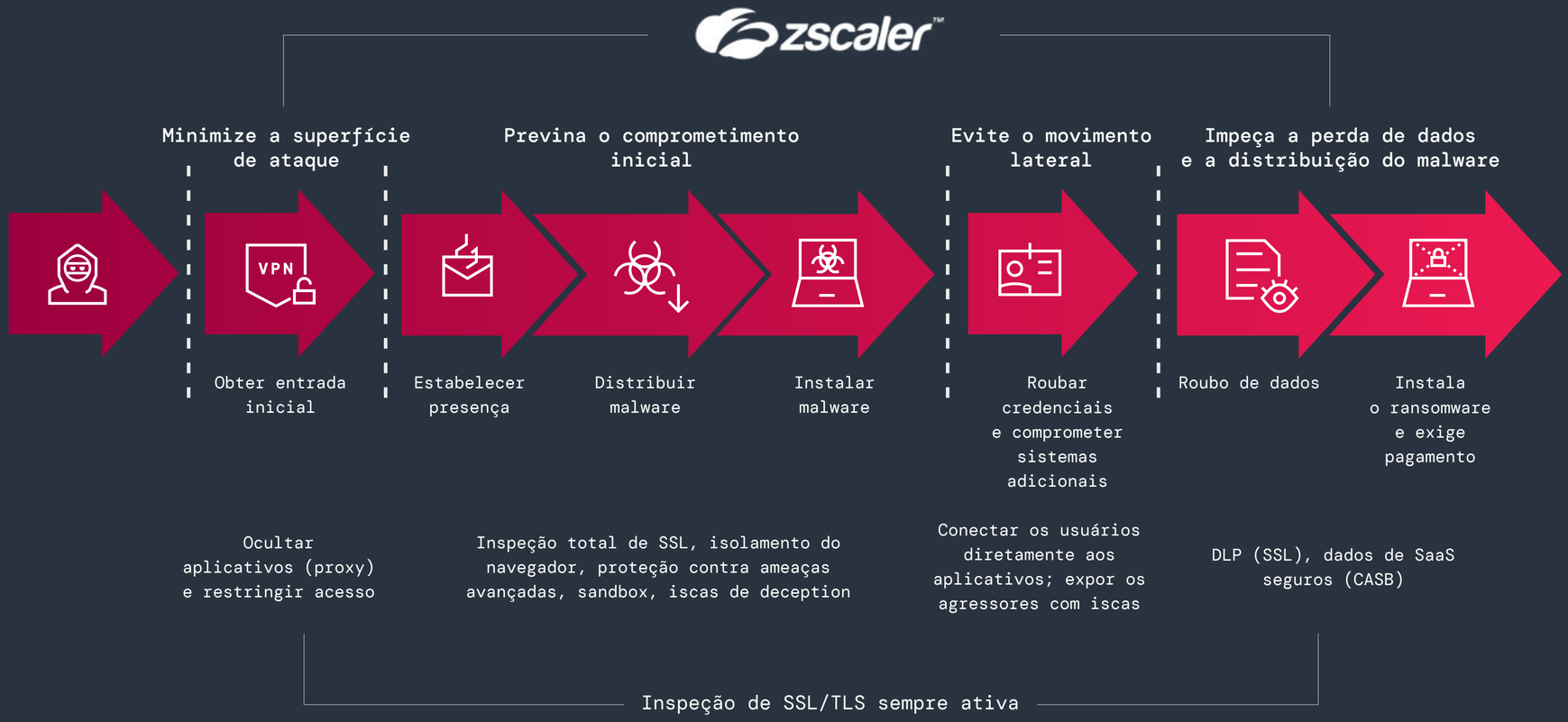


Figura 23: Mapeamento da arquitetura zero trust ao longo da cadeia de ataques de ransomware.

Produtos Zscaler relacionados

Zscaler Internet Access™ (ZIA™): fornece acesso seguro e direto à internet, oferecendo proteção integrada contra ameaças. Os recursos avançados de prevenção de ameaças e sandbox do ZIA ajudam a impedir downloads de ransomware e comunicações de comando e controle (C2), evitando a infiltração de ransomware.

Zscaler Private Access™ (ZPA™): oferece acesso seguro a aplicativos internos sem exposição à internet, empregando um modelo zero trust. O ZPA garante que apenas usuários e dispositivos autorizados possam acessar aplicativos críticos, reduzindo assim a superfície de ataque e evitando tentativas de ransomware.

Zscaler Zero Trust Firewall: intercepta e inspeciona tráfego em TLS/SSL para detectar malware oculto no tráfego criptografado, evitando sua infiltração na rede.

Zscaler Deception: detecta e contém invasores que tentam se mover lateralmente ou escalar privilégios atraindo-os com servidores, aplicativos, diretórios e contas de usuário falsos.

Zscaler Sandbox: analisa arquivos e executáveis suspeitos em um ambiente virtual controlado, ajudando a identificar e bloquear códigos maliciosos, mantendo as organizações à frente de ransomware baseado em arquivos e ataques de dia zero.

Zscaler Cloud Browser: isola sessões da web e transmite apenas pixels para dispositivos para eliminar efetivamente o risco de downloads drive-by e explorações de dia zero que podem ser usadas por operadores de ransomware.

Zscaler ITDR (detecção e resposta a ameaças de identidade): detecta e defende contra ataques baseados em identidade, como roubo de credenciais e abuso de privilégios, assaltos ao Active Directory e permissões de risco.

Zscaler Data Protection: fornece segurança consistente e unificada para dados em trânsito e em repouso em aplicativos SaaS e de nuvem pública, reduzindo a probabilidade de exfiltração de dados e ao mesmo tempo mitigando o impacto potencial de ataques de ransomware.

Orientações de prevenção contra ransomware

Uma estratégia de defesa baseada em arquitetura zero trust é uma medida de segurança comprovada para impedir ataques de ransomware, mas enfrentar essa ameaça multifacetada exige planejamento proativo, colaboração contínua e investimentos estratégicos.

Os especialistas da ThreatLabz compilaram as práticas recomendadas mais recentes para ajudar a reduzir os riscos de ransomware e proteger sua organização contra ameaças existentes e emergentes.

- **Implemente backups de dados frequentes e seguros.** Certifique-se de que o backup de todos os dados seja feito frequentemente e com segurança, incluindo backups offline. Adapte estratégias de backup com base nas ameaças em evolução.
- **Mantenha os softwares atualizados.** Aplique imediatamente as correções de segurança mais recentes para solucionar vulnerabilidades conhecidas. Use plataformas de inteligência sobre ameaças baseadas em IA para priorizar e gerenciar correções de segurança de maneira eficaz.
- **Habilite a autenticação multifator (MFA).** Adicione uma camada extra de segurança às contas de usuário com MFA para reduzir o risco de acessos não autorizados. Integre soluções de MFA para detectar e prevenir invasões de contas de forma eficaz.
- **Estabeleça uma política de segurança corporativa consistente.** Garanta que todos os usuários sigam procedimentos de segurança consistentes, incluindo MFA e atualizações de segurança frequentes, para ajudar a evitar comprometimentos iniciais. Com equipes de trabalho distribuídas, é ainda mais importante implementar uma arquitetura de borda de serviço de segurança (SSE) para proteger os usuários, não importa onde eles estejam.
- **Reforce a segurança dos aplicativos.** Remova aplicativos da internet pública para evitar que grupos de ransomware explorem vulnerabilidades. Implemente uma arquitetura zero trust para aplicativos internos para protegê-los contra tentativas de ransomware.
- **Aplique o acesso de privilégio mínimo.** Implemente políticas de privilégio mínimo para restringir o acesso dos usuários apenas aos recursos necessários para suas funções. Utilize soluções baseadas em IA para analisar dinamicamente o comportamento do usuário e adaptar os privilégios de acesso de acordo.
- **Fortaleça a proteção da identidade.** Use ferramentas de ITDR para obter visibilidade sobre configurações incorretas de identidade, corrigir vulnerabilidades no Active Directory que os adversários exploram para escalar privilégios e mover-se lateralmente e detectar ameaças de identidade furtivas.
- **Inspecione todo o tráfego.** Atualmente, 86% das ameaças são distribuídas através de canais criptografados, que muitas vezes não são inspecionados, facilitando até mesmo que invasores moderadamente sofisticados contornem os controles de segurança. É essencial inspecionar todo o tráfego, criptografado ou não, para evitar comprometimentos.
- **Implemente o acesso à rede zero trust (ZTNA).** Implante a segmentação granular de usuário para aplicativo e de aplicativo para aplicativo, intermediando o acesso por meio de controles de acesso de privilégio mínimo para eliminar a movimentação lateral, minimizar a exposição de dados e aprimorar sua postura geral de segurança.

- **Utilize o isolamento do navegador baseado em IA.** Proteja os usuários contra ameaças da web com o isolamento baseado em IA de conteúdo suspeito da internet e usuários de alto risco. Ao isolar a experiência do navegador e restringir ações potencialmente prejudiciais (como inserir credenciais), os usuários podem acessar URLs e arquivos suspeitos com segurança, sem arriscar a segurança do sistema.
- **Empregue sandbox avançada baseada em IA.** Impeça malwares elusivos e nunca antes vistos com uma sandbox que detecta e coloca automaticamente em quarentena ameaças desconhecidas e arquivos suspeitos, aproveitando a análise de IA/ML.
- **Implante prevenção contra perda de dados (DLP) integrada.** Proteja-se contra exfiltração e exposição de dados implantando medidas de DLP integrada.
- **Utilize tecnologia de deception.** Empregue ferramentas de deception e honeypots para enganar os invasores, fortalecendo as defesas contra a infiltração do sistema.
- **Utilize um agente de segurança de acesso à nuvem (CASB).** Controle e monitore o uso de aplicativos na nuvem com um CASB para evitar atividades maliciosas, como downloads de arquivos e exfiltração de dados.
- **Forneça treinamento contínuo aos funcionários.** Realize treinamentos regulares de conscientização sobre segurança para instruir os funcionários sobre ameaças de ransomware. Empregue simulações de cenários reais de ransomware para melhorar a preparação dos funcionários.
- **Desenvolva um plano abrangente de resposta a ransomware.** Crie um plano de resposta que inclua recuperação de dados, resposta a incidentes e protocolos de comunicação para agir de forma rápida e eficaz no caso de um ataque de ransomware.

Siga a Zscaler ThreatLabz para obter insights regulares sobre as últimas ameaças de ransomware e desenvolvimentos, incluindo indicadores de comprometimento (IOCs) publicados e mapeamentos MITRE ATT&CK. Essas informações podem ser usadas para treinar sua equipe, melhorar sua postura de segurança e ajudar a prevenir ataques de ransomware.

A ThreatLabz também mantém repositórios no GitHub com IOCs, ferramentas (incluindo ferramentas de descriptografia de ransomware de prova de conceito) e um arquivo de notas de ransomware de todos os principais grupos de ransomware.

X @ThreatLabz | Blog de pesquisa de segurança da ThreatLabz

Metodologia do relatório

A metodologia de pesquisa para este relatório é um processo abrangente que usa várias fontes de dados para identificar e rastrear as tendências de ransomware. A equipe do relatório coletou dados de diversas fontes entre abril de 2023 e março de 2024, incluindo:

- **A nuvem de segurança global da Zscaler,** que processa mais de 500 trilhões de sinais diários, bloqueia mais de 9 bilhões de ameaças e violações de políticas por dia e fornece mais de 250 mil atualizações de segurança diárias aos clientes da Zscaler. Analisamos esses dados, que incluem informações sobre endereços IP de origem, endereços IP de destino e tipos de arquivos associados a ataques de ransomware, para identificar atividades de ransomware.

- **Fontes externas de inteligência.** Também coletamos dados de fontes externas de inteligência, como feeds de inteligência sobre ameaças, pesquisas de código aberto e relatórios de segurança pública, que forneceram informações adicionais sobre invasores de ransomware, seus alvos e métodos.

- **A análise da própria equipe da ThreatLabz de amostras de ransomware e dados de ataque.** A equipe de inteligência sobre ameaças da ThreatLabz rastreia famílias de ransomware em grande escala por meio de engenharia reversa e automatização da análise de malware para desenvolver estratégias de resposta eficazes. A ThreatLabz também trabalha em estreita colaboração com agências internacionais de segurança pública e desempenhou um papel significativo em ações recentes, incluindo a Operação Duck Hunt e a Operação Endgame.

Sobre o ThreatLabz

ThreatLabz é o braço de pesquisa de segurança da Zscaler. Essa equipe de classe mundial é responsável por perseguir novas ameaças e garantir que as milhares de organizações que usam a plataforma global Zscaler estejam sempre protegidas. Além da pesquisa de malware e análise comportamental, os membros da equipe estão envolvidos na pesquisa e no desenvolvimento de novos módulos para proteção avançada contra ameaças na plataforma Zscaler, e realizam regularmente auditorias internas de segurança para garantir que os produtos e a infraestrutura da Zscaler atendam aos padrões de conformidade de segurança. A ThreatLabz publica regularmente análises aprofundadas de ameaças novas e emergentes em seu portal, **research.zscaler.com**.

Sobre a Zscaler

A Zscaler (NASDAQ: ZS) acelera a transformação digital para que os clientes possam ter mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange™ protege milhares de clientes contra ciberataques e perda de dados ao conectar com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SASE é a maior plataforma de segurança na nuvem integrada do mundo. Para saber mais, visite **www.zscaler.com.br.**