Ransomware em evolução

Como a ameaça deixou de se limitar à criptografia de dados, incorporou extorsão baseada em vazamentos, ataques de supply chain e um ecossistema criminal cada vez mais sofisticado.

///AXUR

Sumário executivo

A esta altura, ransomware é uma ameaça que dispensa apresentações. Eles já renderam muitas manchetes nos noticiários, mantêm as forças policiais ocupadas e até preocupam políticos e analistas de segurança nacional, que temem a possibilidade de que um ransomware paralise os sistemas responsáveis por serviços críticos como energia e água.

Na maioria das empresas, os analistas de cibersegurança têm preocupações semelhantes. O ransomware tem o potencial de paralisar todos os sistemas, inclusive os mais críticos para a operação, deixando a empresa refém dos criminosos e colocando em risco a continuidade do negócio.

Apesar disso, cada empresa é responsável por traçar uma estratégia de defesa e prevenção contra o ransomware. O que funciona para uma organização nem sempre funcionará para outra, considerando a diversidade de softwares e de processos.

Por esta razão, nem sempre é fácil transformar essas preocupações em um plano de ação efetivo.

Foi pensando nisso que criamos um guia geral e abrangente sobre a ameaça do ransomware, trazendo informações atualizadas sobre as operações desses criminosos e curiosidades sobre o histórico dos golpes de extorsão digital que ajudam a esclarecer como o cenário tomou forma.

Das descrições dos principais grupos operadores de ransomware às recomendações de prevenção e recuperação, trouxemos o que entendemos ser mais importante para que cada empresa formule sua estratégia de acordo com as prioridades da sua gestão de risco, os recursos disponíveis e o grau de exposição a esta ameaça.

Isto dito, é importante compreender desde já que o ransomware não é uma ameaça estática. Os criminosos sempre buscam novos meios para atingir as empresas, tanto na fase inicial e técnica do ataque como na fase final da extorsão. O aperfeiçoamento constante e a adaptabilidade devem fazer parte da estratégia de defesa, pois as melhores defesas de ontem nem sempre são eficazes para prevenir e mitigar os ataques de hoje.

O ransomware não é apenas mais uma ameaça entre tantas outras. Nos últimos anos, o ransomware absorveu quase qualquer atividade de crime cibernético que não envolve fraudes comerciais ou financeiras. Tentativas de extorsão agora vem acontecendo mesmo sem criptografia de dados, pressionando as empresas com base em danos reputacionais e obrigações jurídicas referentes à proteção de dados.

Proteger a empresa contra ransomware não é difícil apenas porque o ransomware é uma ameaça complexa, mas sim porque a maioria dos riscos ligados às fragilidades na infraestrutura de TI converge no ransomware.

Os números do ransomware

Os resgates pagos por empresas às gangues de ransomware somaram **US$ 813 milhões** em 2024 e **US$ 1,25 bilhão** em 2023.
(Chainalysis, 2025)

O resgate médio cobrado em um ataque de ransomware é de **US$ 1,3 milhão**.
(Coalition)

6% dos ataques de extorsão ameaçam as vítimas com vazamento de dados e não utilizam mais a criptografia.
(Sophos, 2025)

25% das empresas pagam o resgate cobrado.
(Veeam, Q4 2024)

Considerando apenas os ataques que só utilizam vazamento de dados, **41% das vítimas** pagam a extorsão em ataques.
(Veeam, Q4 2024)

O que há de novo

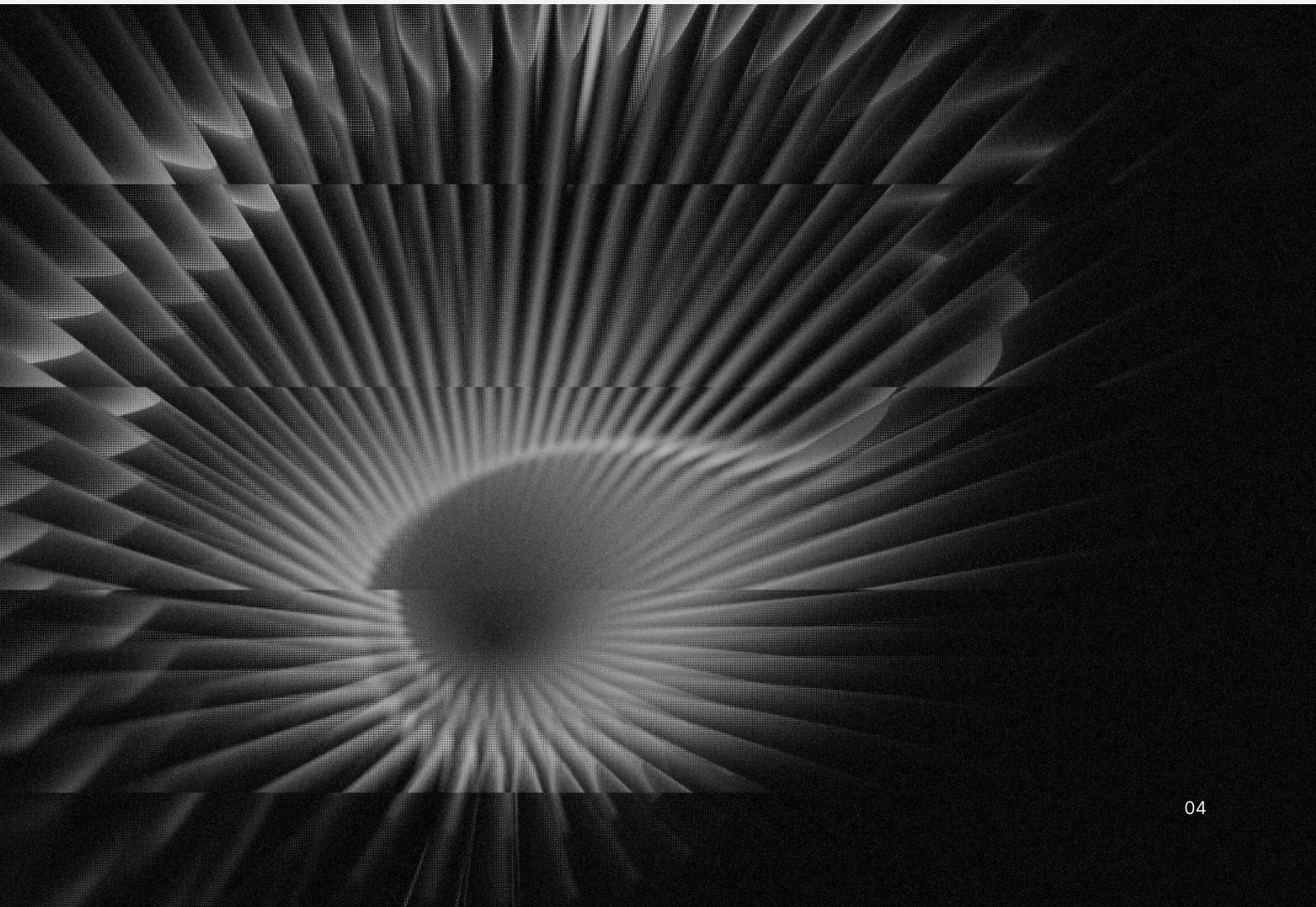
Esta é uma versão revisada e atualizada de um documento que publicamos em 2022. Se você leu a versão original, as principais atualizações estão nos capítulos referentes aos grupos de ransomware e medidas de prevenção.

Ainda que o ransomware tenha consolidado como uma ameaça cibernética ao longo dos últimos 15 anos, as quadrilhas que atacam as empresas não são nada sólidas. Ações policiais, problemas operacionais e conflitos internos levam muitas dessas gangues a encerrar suas atividades — ou pelo menos, a declarar que estão encerrando suas atividades para conseguir despistar autoridades ou ex-parceiros do crime. Por isso, os nomes e atores relevantes no mundo do ransomware não são mais os mesmos.

As prioridades de prevenção também mudaram. Os grupos de ransomware estão apostando cada vez mais na pressão das repercussões jurídicas e danos reputacionais decorrentes da exposição de dados roubados.

Uma estratégia de prevenção e recuperação que considere apenas backups e a reinstalação dos sistemas comprometidos não vai conseguir evitar que a empresa seja pressionada pelos criminosos.

Acreditamos que os capítulos que tratam destes assuntos merecem ser lidos novamente. Certas seções são totalmente novas (como a que trata de ataques de supply chain), enquanto outras tiveram de ser reescritas ou complementadas com dados atualizados.



Evolução do ransomware

Como chegamos ao cenário atual

Direto ao Ponto — O ransomware não é uma ameaça isolada. O ecossistema do crime que sustenta a operação da fraude de ransomware depende de vários "serviços", sendo a capacidade de cobrança, a lavagem de dinheiro e a ocultação de rastros on-line alguns dos exemplos mais importantes. Explicamos aqui como o ransomware evoluiu de golpe que bloqueava a tela do computador e cobrava resgate por meio de SMS para se tornar um malware avançado capaz de derrubar a infraestrutura digital de uma empresa e cobrar resgates de milhões de dólares em criptomoeda.

O 'primeiro' ransomware

Depois de tantas menções no noticiário, o ransomware dispensa apresentações. Enquanto algumas empresas aceitaram pagar milhões de dólares a criminosos para retomar as atividades, outras nem sequer puderam cogitar esta opção e declararam falência ou fecharam as portas. Mas como foi que esta ameaça conseguiu tanta musculatura em apenas uma década?

O primeiro código malicioso que pode ser considerado um "ransomware" surgiu em 1989. Criado pelo biólogo Dr. Joseph Popp, o malware foi distribuído em disquetes que supostamente teriam informações sobre a AIDS, que tomava atenção de médicos depois que foi catalogada, em 1981. Uma vez instalado, esse ransomware travava o sistema **pedindo um resgate de US$ 189.**

Além da cobrança para recuperar o sistema (o mesmo tipo de "mensagem de resgate" que existe no **ransomware moderno**), o malware criptografava o nome dos arquivos e pastas, impossibilitando o uso do computador – algo que também lembra as técnicas mais avançadas em uso hoje, com a **criptografia assimétrica.**

Esse código primitivo é às vezes chamado de "cavalo de troia AIDS" devido aos rótulos nos disquetes que foram distribuídos para disseminar o código, mas também é conhecido como "PC Cyborg", pois esta era a empresa que supostamente receberia a remessa do resgate.

As autoridades não tiveram dificuldade para identificar o autor da praga digital. Contudo, Joseph Popp sofria com problemas mentais foi considerado inimputável pelas cortes.

Cibercrime moderno, criptomoedas e OPSEC

Ainda que as semelhanças saltem aos olhos, não é muito correto procurar explicações para o ransomware moderno olhando para programas maliciosos tão antigos. Essa ameaça, tal como existe hoje, é produto de circunstâncias que vão **além das capacidades técnicas e de software.** Inclusive, **as circunstâncias e obrigações jurídicas** das vítimas das gangues de ransomware têm despontado como um dos principais trunfos nas "negociações" dos criminosos.

Para quem tem o desafio de defender uma rede, conhecer as condições necessárias para um ataque bem-sucedido e **monitorar a atividade criminosa para antecipar ações e preparar uma resposta** pode ser a chave para uma atuação assertiva capaz de desmantelar a capacidade do criminoso de concretizar a fraude.

O primeiro passo é olhar para o que o invasor está buscando e para os meios e ferramentas que ele tem à disposição. Infelizmente, a estrutura do crime que existe hoje, e que é responsável pela existência do ransomware, foi construída ao longo de décadas de fraudes na internet.

Em outras palavras, o ransomware é uma ameaça construída ao longo de pelo menos 15 anos de aperfeiçoamento da atividade criminosa no mundo digital.

Uma das demandas do criminoso profissional é a "OPSEC" (segurança de operação) com o objetivo de reduzir o risco de ser preso e perder acesso aos ganhos ilícitos. Quanto mais fácil for receber dinheiro ilícito ou realizar crimes "tradicionais", como a lavagem de dinheiro e falsidade ideológica, mais ousado o crime digital tende a ser.

A transformação do ransomware em uma ameaça personalizada, na qual os criminosos sabem quem estão atacando e quanto podem cobrar da vítima, foi acelerada pela existência de uma modalidade de pagamento capaz de viabilizar a transferência de cifras milionárias: as criptomoedas.

A relação entre o ransomware e as criptomoedas é realmente profunda. Em 2017, autoridades americanas desmantelaram a corretora de criptomoedas "BTC-e", acusando-a de auxiliar os criminosos. Em 2025, um investigador que se identifica apenas como "GangExposed" alegou que um evento de blockchain seria apenas uma fachada para lavar o dinheiro das fraudes. Embora nenhuma ação das autoridades tenha ocorrido para comprovar essa denúncia, as criptomoedas e a blockchain aparecem frequentemente nessas fraudes, inclusive por meio de serviços de ocultação de origem e lavagem conhecidos como "tumblers".

Apesar dessa relação próxima hoje, o ransomware já existia antes das criptomoedas. Nos antigos países do bloco soviético, os primeiros "bloqueadores" de sistema costumavam realizar cobranças por meio de serviços de SMS Premium: bastava que a vítima enviasse um SMS para o número informado para receber o código de desbloqueio. O valor do "resgate" vinha na conta de telefone.

Em outros casos, a cobrança era feita através de uma plataforma chamada E-Gold, que foi suspensa pelo Departamento de Justiça dos Estados Unidos em 2007. Nessa época, os valores cobrados pelo "resgate" dificilmente passavam dos US$ 300. No caso dos SMSs, o valor costumava ser de US$ 10.

No restante da Europa e na América, onde regras mais rígidas no setor de telecomunicação impediam essa cobrança por SMS, **o "ransomware" costumava vir disfarçado de um antivírus falso.** O pretexto da venda de software permitia que os criminosos realizassem a cobrança do resgate com cartão de crédito. O custo desses "programas" girava em torno de US$ 50.

Foram esses antivírus falsos que, na segunda metade da década de 2000, introduziram as mensagens avisando sobre "problemas" no computador, com técnicas como a troca do papel de parede da área de trabalho – **algo que ransomwares usam até hoje.**

Quando falam com as empresas atacadas para "negociar" o resgate, não é raro que as gangues de ransomware ainda tratem as vítimas como "clientes" ou "pacientes" – algo que lembra essa época em que os criminosos vendiam programas de "segurança". Para reforçar os argumentos jurídicos, os criminosos viabilizaram apoio "jurídico" aos criminosos envolvidos na negociação para aumentar a pressão sobre a vítima.

Alguns vírus de resgate icônicos, como o CryptoLocker e o CryptoWall, usavam a mesma linguagem visual (escudos e cadeados) que aparecia nos programas de segurança falsos.

É claro que nem todos queriam ou conseguiam realizar cobranças por cartão de crédito, inclusive porque as adquirentes envolvidas começaram a ser investigadas pelo excesso de estornos (chargebacks). Havia uma "segunda linha" de bloqueadores que fazia cobranças por cartões pré-pagos e vale-presentes.

Um malware conhecido desta família foi o Reveton. Já considerado um "ransomware", ele não utilizava criptografia. Em vez disso, **aplicava um golpe de extorsão** alegando que a vítima havia cometido um crime e que precisava pagar uma multa. Para isso, usava telas personalizadas, assumindo o nome e a imagem da autoridade policial do país associado ao sistema.

Papel de parede usado pelo ransomware LockBit.

A cobrança era realizada por serviços especializados em simplificar remessas internacionais, como Ukash, Paysafe e MoneyPak. As cobranças eram de cerca de US$ 200.

Mas um nome notório nesse ramo foi a Liberty Reserve, fundada em 2001 e extinta em 2013 por uma ação do FBI após diversas evidências de que o serviço era utilizado para transações entre criminosos.

Segundo o Departamento de Justiça dos Estados Unidos, a Liberty Reserve teria sido usada em um esquema de lavagem de dinheiro em transações que somavam US$ 250 milhões. O fundador do serviço se declarou culpado das acusações e foi sentenciado a 20 anos de prisão em 2016.

Essa queda da Liberty Reserve em 2013 coincidiu com o amadurecimento do mercado de criptomoedas. A corretora Mt. Gox ainda estava em alta, com um repertório de recursos e funções que desenhava o "caminho das pedras" para futuras concorrentes.

CryptoLocker: o malware que definiu uma categoria de extorsão

Foi no mesmo ano de 2013 que especialistas em segurança detectaram o CryptoLocker. Distribuído principalmente por meio de outros códigos maliciosos já existentes (como a botnet Gameover ZeuS) e plataformas de envio de spam, acredita-se que ele tenha faturado cerca de US$ 27 milhões em bitcoin.

As características e o funcionamento do CryptoLocker o colocariam em pé de igualdade com códigos modernos. Ele usava criptografia assimétrica e servidores de controle, sendo categorizado de "crypto-ransomware" para diferenciá-lo de outros tipos de extorsão com resgate digital. Contudo, o êxito do CryptoLocker serviu para **consolidar essa modalidade da fraude, e hoje é o que conhecemos simplesmente como "ransomware".**

Ao contrário do que aconteceu com malwares semelhantes da época, essa função criptográfica do CryptoLocker não foi quebrada. A criação de uma ferramenta de decifragem só foi possível após uma operação das autoridades que permitiu a obtenção das chaves de criptografia usadas na fraude.

Por outro lado, três aspectos do CryptoLocker o diferenciavam das fraudes realizadas hoje: o valor cobrado, a forma de distribuição e a ausência da "extorsão dupla". Todos esses elementos estão vinculados. Enquanto algumas empresas vítimas de ransomware hoje recebem cobranças de centenas de milhares ou até milhões de dólares, o CryptoLocker cobrava cerca de US$ 500.

O valor milionário cobrado por um ransomware contemporâneo é consequência da sua forma de distribuição e da aplicação da extorsão dupla. Os operadores de ransomware comandam de perto cada invasão, adentrando a rede da empresa de forma contundente e reduzindo as chances de uma recuperação por backup. A extorsão dupla, por sua vez, é feita através do roubo das informações antes do ataque de criptografia, de modo que a vítima possa ser ameaçada com um vazamento de dados.

Nada disso acontecia no CryptoLocker. O malware era distribuído em massa através de redes zumbis e por meio do uso dos "exploit kits", que exploravam falhas em navegadores e plugins.

Em outras palavras, era comum que o usuário fosse contaminado após navegar em um site malicioso. As visitas a essas páginas dependiam de motores de busca, de anúncios fraudulentos e da invasão de sites legítimos vulneráveis. Era um tipo de disseminação oportunista, sem direcionamento.

Talvez o último ransomware notório a ser distribuído desta forma foi o WannaCry, em 2017. Programado para explorar uma vulnerabilidade no Windows de forma automatizada, o WannaCry atacaria qualquer sistema que fosse capaz de acessar. Assim, era mais provável que sistemas de backup saíssem ilesos do ataque, facilitando a recuperação.

O WannaCry ainda cobrava um resgate de algumas centenas de dólares (normalmente entre US$ 300 e US$ 600). Quase que paralelamente, outro ransomware menos midiático, o Locky, começava a cobrar cifras de quatro dígitos.

A partir de 2017, algumas transformações importantes ocorrem no mundo do crime de ransomware:

2017

A corretora de bitcoin BTC-e é desmantelada pelo Departamento de Justiça dos Estados Unidos. Acusada de lavagem de dinheiro (o montante seria de US$ 4 bilhões), a corretora era considerada uma das preferidas dos operadores de ransomware. Como o principal acusado não pôde ser extraditado para os Estados Unidos devido a uma disputa judicial envolvendo Grécia, Rússia e França, o caso ainda não teve um desfecho.

2018

Surge o ransomware Ryuk, que concentra os ataques em empresas e organizações. Sistemas individuais, de consumidores e profissionais independentes, ficam em segundo plano. Estimativas apontam que até 81% de todos os ataques de ransomware em 2018 vitimaram empresas. Com alvos mais valiosos, o valor cobrado pelos resgates explodiu: em 2019, o Ryuk chegou a tentar cobrar US$ 12,5 milhões de uma vítima.

2019

Expansão dos serviços de "mixing" ou "cryptocurrency tumblers", que misturam criptomoedas de diversas origens para ocultar ganhos ilícitos. Segundo um relatório da BitFury, o volume de bitcoins transferidos de mercados das darknets, que era de apenas 1% no início de 2019, subiu de forma constante ao longo do ano e alcançou 20% no primeiro trimestre de 2020.

2020

Estratégia de "dupla extorsão" cresce quase 500% e pagamentos são cobrados em criptomoeda Monero. Começamos a observar a consolidação do ransomware também como veículo de vazamento de dados, em que a ameaça de exposição das informações corporativas entra como uma segunda face da extorsão praticada no golpe. Em paralelo, serviços de mixers entraram na mira das autoridades e corretoras de criptomoeda foram obrigadas a adotar processos mais robustos de KYC (know your costumer), levando alguns ransomwares notórios (como o REvil) a iniciar cobranças em Monero, uma moeda mais difícil de rastrear, ou então cobrar até 20% mais caro de quem só poderia pagar em bitcoin. O resultado: em 2020, US$ 692 milhões em transações de criptomoedas foram atribuídas a ransomware.

2023

Grupos de ransomware começam a mirar fornecedores e apostar em vazamento de dados. O sucesso da abordagem da dupla extorsão levou alguns grupos de ransomware a experimentarem ataques com roubo de dados sem criptografia. Ataques centralizados em fornecedores de software ou serviços de TI, seja por meio de vulnerabilidades ou credenciais vazadas, geraram incidentes em centenas de empresas simultaneamente, sem que a rede corporativa destas empresas fosse atacada.

Apesar da evolução na cobrança dos resgates (com cifras maiores e mecanismos mais anônimos), o ransomware ainda tinha uma dependência forte de outros tipos de malware, como se o ransomware "pegasse carona" em outras contaminações. Mas, quando este modelo se mostrou insuficiente, os operadores do crime apostaram em um modelo com mais especialização, compartimentando a atividade criminosa para ganhar escala.

Quando começaram a procurar alvos específicos e de alto valor, os grupos de ransomware conseguiram justificar a cobrança de resgates cada vez mais caros, chegando a milhões de dólares em certas vítimas.

Essa estratégia culminou com ataques contra empresas que atuam em setores críticos. O grupo DarkSide atingiu a Colonial Pipeline em 2021 e cobrou US$ 4,4 milhões em resgate, criando um marco histórico para os ataques cibernéticos. Esse e outros incidentes semelhantes mostraram que o ransomware era capaz de impactar operações de infraestrutura, saúde e energia, o que fez com que o ransomware se destacasse como a maior ameaça digital moderna.

TOTAL ROUBADO POR RANSOMWARE 2020-2024:

US$ 4,8 bilhões

O CUSTO MÉDIO DE UM ATAQUE DE RANSOMWARE EM 2024:

US$ 5,13 bilhões

As organizações criminosas por trás do ransomware

Como uma linha de produção, criminosos se especializaram

Direto ao Ponto — As gangues que operam ataques de ransomware enfrentam vários desafios para expandir sua escala sem comprometer a efetividade do golpe. Conhecer o dia a dia da atividade criminosa é o primeiro passo para traçar a linha de atuação das equipes de segurança, em especial no monitoramento e threat intelligence, visando apoiar a elaboração de medidas preventivas ou até antecipar ações futuras. Analisando grupos como BlackCat, Clop e DragonForce, entenderemos melhor como esses criminosos se especializam, suas disputas internas e as frágeis relações de confiança que se formam a partir da ganância e da busca pelo aumento no volume de ataques.

Clop e Scattered Spider: extorsão através de serviços de TI

As gangues responsáveis por ransomwares não são estáveis. Por diversas razões, como brigas internas, reorganizações, "calotes" e ações da polícia, é comum que as gangues sejam dissolvidas, inclusive com anúncios públicos a respeito da interrupção das atividades. No entanto, os indivíduos que integram essas gangues e as ferramentas utilizadas normalmente continuam na cena do ransomware, seja através da comercialização dos códigos utilizados ou da formação de novas alianças e quadrilhas.

O Clop é uma dessas gangues. Formado como sucessor de um ransomware conhecido como CryptoMix e em atuação desde 2019, o Clop é relevante por ter realizado uma série de ataques e extorsões que fogem de forma significativa ao padrão que se espera de um ransomware.

Uma das características marcantes do Clop são os ataques em massa através de serviços de TI ou softwares usados por várias empresas. Desde o final de 2020, o Clop realizou quatro ataques contra softwares usados para transmissão de dados, roubando informações de milhares de empresas. Uma estimativa chegou a sugerir que uma única ação em massa do Clop, contra o MOVEit Transfer, rendeu mais de US$ 75 milhões para a quadrilha.

O Clop também se destacou por realizar ataques de ransomware sem depender da cifragem de arquivos, apoiando-se exclusivamente na pressão que o vazamento de dados corporativos exerce sobre suas vítimas.

Em um cenário de ransomware mais tradicional, uma empresa atacada estaria preocupada principalmente com seus próprios dados, com a recuperação e com a continuidade do negócio. Em uma fraude centrada no vazamento de dados, as preocupações maiores são as consequências jurídicas e de mercado, como a perda de clientes e vazamento de projetos sensíveis.

O backup dos dados não impacta na capacidade de resposta da empresa. Inclusive, um backup desprotegido pode ser uma brecha a ser explorada, pois os criminosos só precisam acessar uma cópia dos arquivos, não importa onde ela estiver. Isso também difere do ransomware tradicional, em que o malware teria de conseguir acesso a todos os backups para ser efetivo.

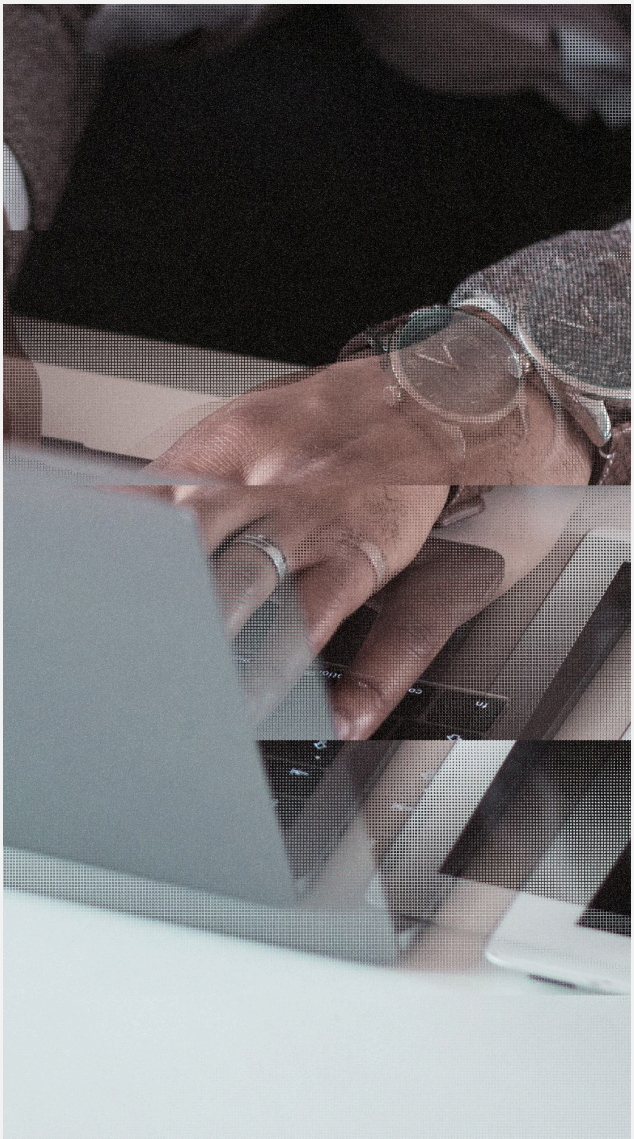
Sem cifrar os arquivos, o Clop facilita o ganho de escala em seus ataques em massa, tornando a ação mais breve. Além disso, não é necessário acesso aos sistemas corporativos ou permissões de escrita nos dados, pois a leitura é suficiente para copiar os arquivos e iniciar a tentativa de extorsão.

Evidentemente, a ausência da etapa de criptografia dos dados também significa que a extorsão tende a ser menos efetiva do que a extorsão dupla (que combina a cifragem e a ameaça de vazamentos). No entanto, o Clop tem mostrado que não é necessário cifrar os arquivos para que a operação criminosa tenha sucesso. Estimativas apontam que o Clop já recebeu cerca de US$ 500 milhões em pagamentos de resgate desde a sua criação.

O Scattered Spider, que possui diversos nomes na comunidade de cibersegurança e está ligado a um coletivo conhecido como "The Com", é mais conhecido por suas táticas de engenharia social. Acredita-se que o grupo tenha muitos cúmplices em países do ocidente, tendo em vista que esses ataques de engenharia social ocorrem também por telefone.

Os alvos da engenharia social do Scattered Spider são quase sempre prestadores de serviço que atuam em helpdesk ou outras funções semelhantes. De modo geral, o grupo é notório por explorar fragilidades em sistemas e processos de autenticação, seja através de phishing, SIM swapping e outras táticas.

Assim como o Clop, indivíduos associados a essa gangue também já realizaram ataques de extorsão sem utilizar um ransomware tradicional para criptografar os dados. Tanto pela forma que obtém acesso às redes corporativas como pela forma que realiza a extorsão, o Scattered Spider vem impondo novas preocupações às empresas.



Dragonforce

Apesar de alguns indícios de que a gangue DragonForce tenha se organizado em 2023 como um grupo hacktivismo em defesa da Palestina, as ações recentes desse grupo têm uma motivação financeira inegável.

O DragonForce cresceu formando alianças em um modelo de ransomware as a service (RaaS, “ransomware como serviço”), ganhando notoriedade pela sua capacidade de absorver afiliados descontentes com outras operações criminosas.

O “RaaS” imita o modelo de "software como serviço" para permitir que os autores de um ransomware se distanciem da operação diária e dos ataques aos alvos.

O modelo RaaS não é novo. Antes mesmo do DragonForce existir, o grupo Conti aperfeiçoou este modelo com uma operação altamente segmentada, deixando os “afiliados” com a tarefa de atacar os alvos. Contudo, o Conti encerrou suas atividades em 2022 após uma série de vazamentos das comunicações internas que escancaram a existência de conflitos e desconfiança.

Um ponto que pode ser considerado particular do DragonForce é a possibilidade de afiliados criarem sites próprios para divulgar os ataques e intermediar as negociações. Isso ajuda a ocultar a relação do afiliado com o DragonForce, permitindo que cada um tenha sua "marca" hospedada na infraestrutura do DragonForce. O grupo chama esse modelo de “cartel” por garantir mais autonomia a cada afiliado.

Em meados de 2025, surgiram indícios de que indivíduos ligados ao Scattered Spider estariam instalando o ransomware do DragonForce em seus alvos, consolidando uma nova aliança no mundo do crime.

Esse tipo de movimentação mostra que os laços no mundo do cibercrime são bastante fluidos e muitas vezes se moldam conforme a conveniência de cada ocasião, ainda que os criminosos busquem se agrupar em torno de organizações razoavelmente sólidas e de boa reputação.

Por mais que o DragonForce seja um nome relativamente novo, a estrutura do grupo e até as táticas e ferramentas utilizadas (como Mimikatz, Cobalt Strike) já foram empregados por outros atores.

Ransomware como serviço: um pilar do ransomware

Com o RaaS, um ransomware possui diversos "afiliados" que realizam as invasões. Contudo, as negociações para a cobrança do resgate ficam sob responsabilidade do núcleo da gangue.

Quando uma operação criminosa ganha esse tipo de escala e precisa gerenciar pessoas e sua própria infraestrutura tecnológica – com o desafio adicional de que a confiança é joia rara no mundo do crime –, não é raro que descuidos, infiltrações e erros exponham detalhes do que está sendo feito.

Essas informações ajudam a construir contramedidas e alertas ágeis sobre uma possível atividade de ransomware nos ambientes cobertos por esse monitoramento.

Alguns exemplos de informações que o monitoramento das ações criminosas pode providenciar:

1. Tactics, techniques, and procedures (TTPs): como o ransomware chega na rede alvo, quais tipos de credenciais podem estar sendo utilizadas (VPN, banco de dados, domínio, provedores de nuvem), quais vulnerabilidades recentes exigem mais cautela, entre outras.

2. Indicators of compromise (IoCs): arquivos endereços de IP e comportamentos de sistema que podem indicar a presença de um ransomware antes de sua ativação.

3. Targets (alvos): empresas e setores que podem estar na mira dos criminosos. Comunicados de grupos como o LAPSUS (que não é estritamente uma gangue de ransomware, embora seus ataques sejam semelhantes) chegaram a nomear empresas específicas que estavam na mira do grupo e foram interceptadas pela Axur.

4. Vazamentos e credenciais: para garantir um retorno máximo pelos seus esforços, criminosos anunciam os dados que possuem para venda, oferecendo inclusive trechos de amostragem. Especialmente quando trazem credenciais, esses dados funcionam como um indício de uma violação ou prenúncio de uma violação futura de interesses.

5. Dados corporativos: além das credenciais, o monitoramento dos criminosos pode indicar a exposição indevida de outros dados de caráter corporativo (financeiros e de contabilidade, dados pessoais de colaboradores e clientes, projetos com parceiros etc.). Esta exposição indica a existência de riscos jurídicos e de reputação, e ainda pode servir para ajudar a rastrear uma violação ocorrida a partir da natureza dos dados que foram expostos (por exemplo, com uma perícia no sistema onde aquela informação é armazenada).

Por que o ransomware tem empregados e fornecedores

Um ataque de ransomware bem-sucedido depende de uma cadeia complexa de eventos e ferramentas.

Um vazamento das conversas da gangue de ransomware Conti, que aconteceu em fevereiro de 2022, se mostrou uma das fontes de informação mais sólidas e interessantes sobre a operação diária de um ransomware. Os chats teriam sido divulgados por um pesquisador de segurança ucraniano como uma forma de retaliação contra o grupo após manifestações em favor da Rússia no confronto militar com a Ucrânia.

Os diálogos comprovaram muito do que já se suspeitava sobre o cotidiano de uma operação de ransomware, mas mostrou também que os líderes das gangues pagam até salários para seus "empregados" (no caso da Conti, eram pelo menos 100) e que há uma espécie de "departamento de RH" para recrutar novos membros e substituir quem não está com desempenho adequado.

Apesar disso, a desconfiança é uma constante neste meio. Um caso notório foi o da gangue **BlackCat**, que encerrou suas atividades em maio de 2024 e deixou afiliados reivindicando comissões que não teriam sido pagas. O risco de calotes e traições mantém as tensões elevadas no mundo do cibercrime.

O modelo de afiliados e de "crime como serviço" começou a ganhar corpo ainda na década de 2000, quando criminosos vendiam acesso a códigos maliciosos e aos "Exploits Kits" (EKs) – códigos prontos para explorar vulnerabilidades em navegadores, vendidos por assinatura ou comissão e controlados por estatísticas e métricas de sucesso.

Foram os EKs e as redes de spam (que também comercializam sua capacidade de envio de mensagens como serviço a outros criminosos) que formaram a base das primeiras contaminações de ransomware, além de distribuírem ladrões de senhas e cartões, mineradores de criptomoeda e outras fraudes.

O golpe do antivírus falso, que aplicava fraudes com o pretexto de venda de software, também já adotava o modelo de afiliados comissionados – uma prática legítima que existe no mercado. De fato, "culpar os afiliados" por toda e qualquer prática duvidosa era uma forma de blindagem para os criminosos, que à época precisavam evitar a represália dos bancos e cartões de crédito.

Com as criptomoedas, este pretexto já não tem utilidade. Mas o esquema de afiliados ajuda a garantir uma motivação clara e sustentar a especialização de cada fase da atividade criminosa.

As especialidades do crime

O modelo "ransomware as a service", que leva esse método para o ransomware, já estava sendo esquematizado em 2012. Naquele ano, um malware chamado de Winlocker, ou " Gimemo", propôs um programa de afiliados com um painel de controle que contabilizava os resgates pagos e a porcentagem da comissão que o afiliado receberia.

O afiliado do ransomware seria o único responsável pela contaminação dos computadores. Havia, portanto, duas figuras: o autor do ransomware, responsável por programar o software e manter a infraestrutura básica de controle da praga para contabilizar estatísticas, e o disseminador, responsável por cuidar de toda a entrega do malware até a vítima.

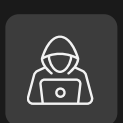
O cenário hoje é mais complexo. Tanto a tarefa do autor do ransomware como a do disseminador foram divididas em partes menores, cada uma delas realizada por indivíduos dedicados à tarefa.

Os cargos de empregados e afiliados de ransomware

Programadores, ou "coders": são os responsáveis por criar os softwares necessários para a operação. Eles criam o ransomware, aplicam os algoritmos de criptografia no código e integram ferramentas.

Testadores: o "controle de qualidade" de um ransomware depende principalmente de sua capacidade de evitar ferramentas de antivírus. Os testes, neste caso, ocorrem por meio da análise do malware em ferramentas de segurança e de alterações voltadas a desviar das proteções.

Administradores de rede: são os responsáveis pela infraestrutura, servidores de controle e de distribuição. Muitos ransomwares utilizam arquivos de configuração dinâmicos, o que os permite alternar para uma nova estrutura caso a antiga seja derrubada. Para tirar proveito dessa funcionalidade, a própria infraestrutura precisa ser refeita periodicamente.



Caçadores de vulnerabilidade: realizam engenharia reversa em softwares e sistemas em busca de falhas de segurança que possam ser exploradas em ataques.

Hackers: utilizam a infraestrutura, os programas e as vulnerabilidades preparados pelo resto da equipe para executar ataques contra os alvos planejados. São responsáveis pelo movimento lateral dentro das organizações, utilizando ferramentas de roubo de senhas e varredura de rede (como Nmap e Mimikatz) para que a execução final do ransomware atinja o máximo de sistemas possível, inclusive em diferentes sistemas operacionais.

Negociadores e 'advogados': indivíduos responsáveis por dialogar com as vítimas do ransomware para obter o pagamento. "Advogados" podem ajudar na negociação para reforçar os riscos jurídicos decorrentes do vazamento dos dados roubados pela quadrilha.

Especialistas em criptomoedas: são os responsáveis por elaborar os mecanismos de lavagem de dinheiro que serão usados para transferir os montantes pagos pelas vítimas ao sistema bancário.

Mesmo com toda essa gama de cargos e especializações, a operação de um ransomware ainda tem outras demandas que precisam ser atendidas por fornecedores.

Em qualquer negócio, o ganho de escala tem seus prós e contras. No caso do ransomware, por mais que o ganho de escala tenha aumentado os ganhos ilícitos por meio da sofisticação da fraude e da especialização dos envolvidos, existe uma demanda considerável por acesso a novos alvos.

É claro que alguns grupos são mais organizados e especializados do que outros. No entanto, todos os criminosos têm à disposição o mesmo ecossistema, do qual podem adquirir informações ou contratar fornecedores. Assim como um programador de ransomware pode contratar um criminoso especializado em spam, outro pode comprar um malware pronto para disseminá-lo por redes sociais ou engenharia social e ser cúmplice do crime sem nenhum conhecimento técnico muito específico.

Para tornar tudo isso possível, os criminosos criaram espaços de negociação relativamente abertos, viabilizando a entrada de novos criminosos capazes de sustentar todo o esquema – independentemente da atividade que saibam realizar.

Para quem conta com um monitoramento especializado dessas redes e espaços, eles se tornam uma grande fonte de dados. Por meio deles, é possível antever ou detectar ataques que ainda estão para acontecer – por exemplo, por meio da detecção de uma credencial vazada.

Como o criminoso que rouba a credencial nem sempre é o mesmo que o utiliza, a interceptação dessas negociatas pode ser decisiva para barrar um ataque antes dele acontecer.

A prevenção de um ataque de ransomware por meio de atividades de inteligência e monitoramento tem um potencial de eficácia altamente relevante nesse cenário.

A extorsão com base em vazamento de dados faz com que medidas de recuperação e restauração (como o backup) sejam insuficientes para aliviar a pressão de pagamento do resgate, pois a empresa ainda pode estar exposta a um vazamento de dados. Vazamentos causam prejuízos à marca e à reputação.

Há casos registrados em que os golpistas utilizaram a base de clientes ou de colaboradores da vítima para comunicá-los do risco de exposição de suas informações pessoais caso a empresa se recusasse a pagar.

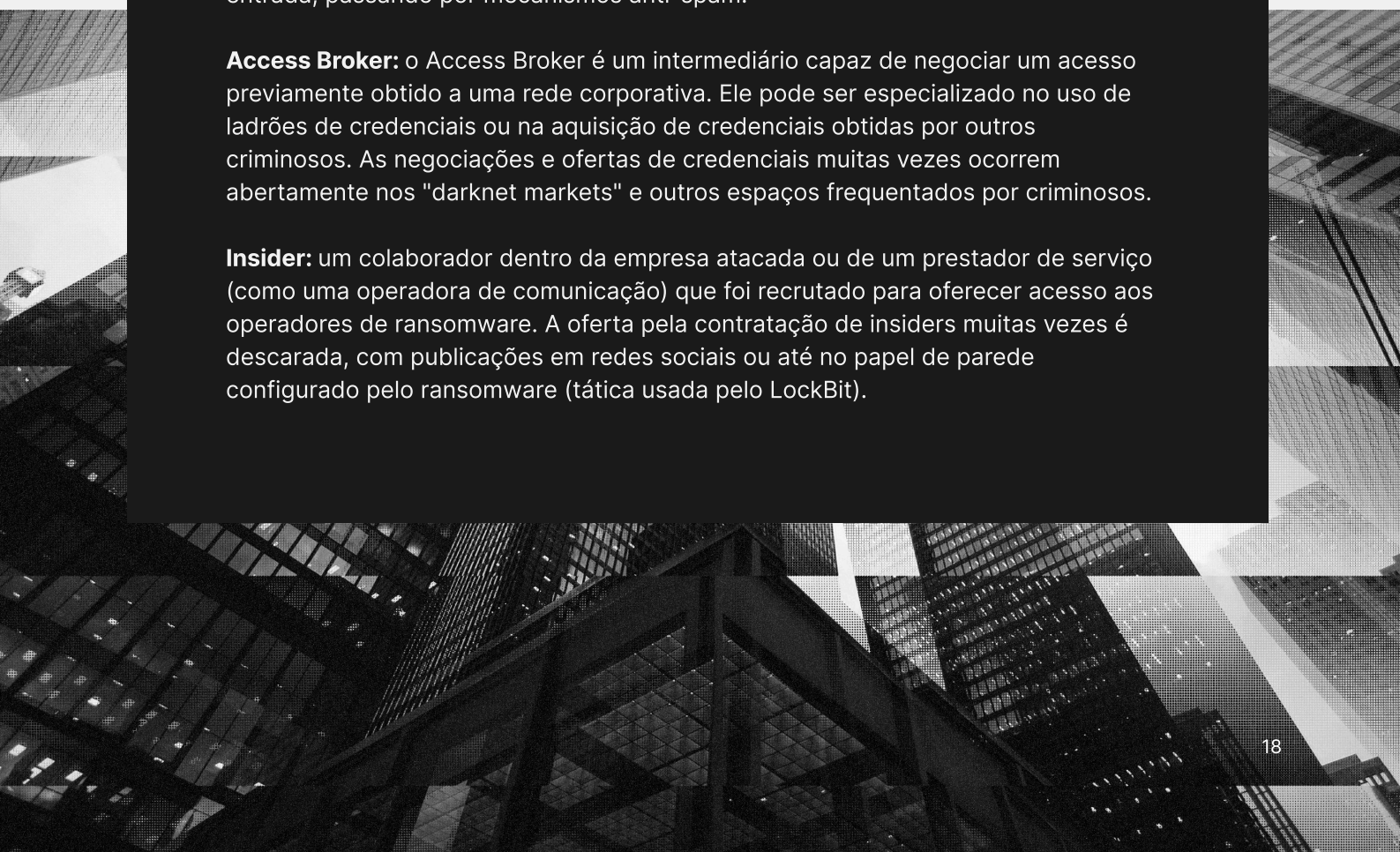
Esta é a grande aposta do ransomware moderno: por mais que uma organização tenha feito a lição de casa com backups e um plano de recuperação robusto, praticamente não há como evitar os danos da exposição de dados. Para piorar, não existe garantia de que os dados realmente serão apagados pelos criminosos.

Os fornecedores do ransomware

Spammer: um criminoso especializado em comprar ou montar uma infraestrutura capaz de enviar e-mails maliciosos. Esses e-mails podem ser em massa ou confeccionados sob medida para atingir um alvo específico. O critério de sucesso para esse fornecedor é a capacidade de fazer com que o e-mail chegue à caixa de entrada, passando por mecanismos anti-spam.

Access Broker: o Access Broker é um intermediário capaz de negociar um acesso previamente obtido a uma rede corporativa. Ele pode ser especializado no uso de ladrões de credenciais ou na aquisição de credenciais obtidas por outros criminosos. As negociações e ofertas de credenciais muitas vezes ocorrem abertamente nos "darknet markets" e outros espaços frequentados por criminosos.

Insider: um colaborador dentro da empresa atacada ou de um prestador de serviço (como uma operadora de comunicação) que foi recrutado para oferecer acesso aos operadores de ransomware. A oferta pela contratação de insiders muitas vezes é descarada, com publicações em redes sociais ou até no papel de parede configurado pelo ransomware (tática usada pelo LockBit).



Prevenção

Colocando na prática o que sabemos sobre o adversário

Direto ao Ponto — Conhecendo o ecossistema do crime e suas fragilidades, é possível atuar de forma incisiva e abrangente na coleta e processamento dos dados expostos pelos criminosos, mapeando o risco da empresa e eliminando os pontos de entrada que seriam utilizados nos ataques. Como o ransomware depende de acesso externo, essas medidas nem sempre precisam envolver apenas a equipe de segurança interna e devem considerar uma ação abrangente com cibersegurança externa.

Hardening contra Ransomware

Guia Rápido

Avalie as proteções existentes contra os vetores de ataque do ransomware

Credenciais roubadas

- Utilize um serviço de monitoramento de credenciais
- Utilize autenticação multifator (MFA) resistente a phishing
- Implemente um sistema de gestão de identidade
- Treine e conscientize usuários sobre o uso correto de credenciais
- Adote uma arquitetura *zero trust*

Malware

- Utilize uma solução de EDR/XDR
- Conecte suas soluções de segurança a plataformas de inteligência
- Implemente soluções de IDS ou restrinja o uso de aplicativos não autorizados

Engenharia social

- Inclua a conscientização dos colaboradores em sua política de segurança
- Adicione proteções aos navegadores, como sandbox ou restrições de acesso externo

Vulnerabilidades

- Utilize uma solução de External Attack Surface Management (EASM) para detectar sistemas expostos à rede e vulnerabilidades
- Aplique atualizações com correções de vulnerabilidades
- Não exponha sistemas de acesso remoto (RDP) à rede
- Mantenha recursos de segurança habilitados
- Proteja recursos da rede corporativa utilizando autenticação Kerberos e recursos de segurança em controladores de domínio

Fornecedores e terceiros

- Acompanhe as práticas de segurança dos fornecedores e terceiros para que elas estejam alinhadas com as práticas adotadas para todo o negócio
- Crie mecanismos de isolamento com privilégios reduzidos e controles de acesso a recursos de nuvem

Como a ameaça de vazamentos mudou o peso da prevenção

Uma boa estratégia de recuperação era suficiente para mitigar os impactos do ransomware até 2020, mas a prática da extorsão dupla (resgate dados com ameaça de vazamentos) mudou esse cenário. Mesmo com a restauração dos sistemas, o risco de vazamento de dados dificulta que se evitem outros prejuízos decorrentes do ataque, como os danos à marca e as possíveis consequências jurídicas previstas na legislação, como as punições da Lei Geral de Proteção de Dados (LGPD).

Com a ameaça da extorsão dupla consolidada, alguns grupos começaram a explorar uma nova abordagem baseada exclusivamente no vazamento de dados. Esses ataques dispensam o atacante de obter acessos de escrita aos dados, abrindo um leque muito maior de possibilidades para realizar ataques de extorsão.

Já há quem prefira utilizar o termo "extorsão de dados" para se referir a todas as formas de extorsão, abandonando o conceito tradicional de ransomware.

O Clop, que já mencionamos, o Hunters International e criminosos ligados ao The Com (Scattered Spider) foram alguns dos atores que obtiveram sucesso com esse tipo de ameaça.

De acordo com dados do relatório State of Ransomware 2025 da Sophos, a quantidade de ataques de extorsão sem criptografia, amparados apenas na ameaça de vazamento de dados, dobrou em um ano. Nesse estudo, esses ataques representam 6% de todos os incidentes de extorsão e 13% dos incidentes desta categoria em empresas com menos de 250 funcionários.

Seja em um contexto de extorsão dupla ou como extorsão única, o roubo de dados seguido da ameaça de expor informações corporativas provoca uma mudança nas prioridades no combate ao ransomware.

Nesse contexto, medidas capazes de prevenir ou interromper um ataque em andamento agregam muito valor à estratégia de defesa. Limitando e cortando o acesso do criminoso à rede da empresa antes do roubo dos dados, a empresa protege seus segredos comerciais e sua reputação – e não terá de tomar qualquer decisão a respeito do pagamento de um resgate milionário.

A prevenção de qualquer ataque cibernético exige uma boa maturidade em segurança da informação, com a aplicação de patches, políticas de segurança e processos adequados. Contudo, esses passos básicos nem sempre são suficientes. Além disso, garantir que não haja nenhum erro ou inconformidade é um desafio diário.

O ransomware é muitas vezes dirigido à cada empresa de forma personalizada, com um operador humano apoiado por uma gangue interessada em derrotar mecanismos de segurança tradicionais (como o antivírus). Por outro lado, os recursos de segurança internos podem ser escassos, inclusive pelo gap de profissionais enfrentado no mercado de segurança.

Por essa razão, é preciso contar com o de equipes especializadas em mitigar riscos específicos, muitos deles visíveis do mundo externo graças às dificuldades que os operadores de ransomware criaram para si próprios ao organizar operações criminosas sofisticadas em larga escala.

Vazamentos de credenciais: o prenúncio do ransomware

De acordo com a edição de 2025 do Data Breach Investigations Report (DBIR) da Verizon, 22% das invasões começam com uma credencial roubada. Esse conjunto inclui ataques de extorsão, sejam eles com ransomware tradicional ou com ameaças de expor informações corporativas.

Apesar do roubo de credenciais representar um grande risco, existem meios para enfrentar esse desafio.

Como o ransomware contemporâneo depende de um verdadeiro ecossistema de cibercrime, há muitas oportunidades para detectar atividades suspeitas através do monitoramento desse ecossistema. São informações que podem indicar que uma organização está em risco ou, no pior dos casos, já está na mira dos criminosos.

Com essa visão privilegiada da atividade criminosa, uma empresa pode agir de forma proativa para eliminar vulnerabilidades ou canais de acesso que podem ter sido comprometidos.

Além de senhas vazadas de bancos de dados comprometidos, os times de CTI (Cyber Threat Intelligence) e ART (Axur Research Team) da Axur acompanham vazamentos decorrentes do uso de malwares dedicados ao roubo de credenciais (os credential stealers). Embora não sejam parte da operação de um ransomware no sentido mais estrito, as credenciais obtidas por esses malware são reunidas em coletâneas com o intuito de vendê-las no submundo do crime. Com essa comercialização, eles se conectam a todo tipo de atividade criminosa.

As credenciais podem ser vendidas aos access brokers ou diretamente para gangues de ransomware, e estas poderão encontrar vítimas do seu interesse ou então credenciais de sistemas (infraestruturas de nuvem, dashboards, bancos de dados) que já conhecem e que sabem que podem garantir um bom ponto de acesso à rede de uma empresa.

O monitoramento da Axur já identificou mais de 17 bilhões de credenciais roubadas e cerca de 700 mil credenciais novas são detectadas mensalmente, representando um risco para milhares de pessoas e para as empresas nas quais elas trabalham.

Esse tipo de trabalho permite interromper uma cadeia de eventos que poderia resultar em um ataque de ransomware. Ao ser alertada sobre as senhas roubadas ou canais que estão vulneráveis a esse tipo de acesso, a organização é capaz de reagir: com o cancelamento da credencial, a escalada das ações maliciosas é interrompida.

Tanto no caso da Colonial Pipeline de 2021 como no ataque à Change Healthcare em 2024, o acesso inicial ocorreu por meio de uma credencial roubada. Pelo que se sabe, a série de ataques que afetou empresas usuárias do sistema de armazenamento Snowflake, também em 2024, foi igualmente resultante de credenciais roubadas.

Um alerta prévio sobre o vazamento das credenciais envolvidas poderia ter mudado o rumo desses incidentes.

Um credential stealer pode ser distribuído por e-mail (com engenharia social e phishing), mas também é muito comum a disseminação em redes sociais. A capacidade desses malwares para roubar sessões de login armazenadas no navegador (muitas vezes derrotando a autenticação multifator) os tornam interessantes para roubar contas de criadores de conteúdo – inclusive daqueles que utilizam todos os recursos de segurança oferecidos pelos grandes prestadores de serviços de internet.

Um colaborador pode colocar a empresa em risco mesmo que o ladrão de credenciais seja instalado em seu computador pessoal a partir de um link em redes sociais. Todas as senhas roubadas, inclusive aquelas que aparentemente não têm vínculo com sistemas corporativos, podem ser usadas nos ataques de credential stuffing, no qual são feitas tentativas de acesso a um alvo usando credenciais adquiridas para outro sistema.

Dito de outro modo, a senha roubada para um serviço qualquer pode ser revalidada e conferida em um sistema corporativo, mais valioso para gangues de ransomware. Por meio dos "access brokers" – os intermediários que comercializam canais de acesso –, a credencial chegará aos operadores mais aptos, dando início ao ataque de ransomware.

Credenciais também podem ser expostas a partir do acesso não autorizado a bancos de dados, sejam da empresa ou de um fornecedor. Implementar tokens de rastreamento pode facilitar a identificação precoce de um vazamento e barrar o ataque por meio do cancelamento de credenciais ou do corte de acesso de fornecedores que podem ter sido comprometidos.

Esse trabalho de monitoramento pode ser integrado à operação de segurança da empresa. Contando com um mecanismo para detectar violações da política de segurança e outras regras de conformidade – inclusive de colaboradores que estejam repetindo senhas ou de fornecedores –, a organização melhora sua proteção contra ransomware enquanto eleva seu nível de maturidade de segurança em toda a sua cadeia de operação.

Monitoramento da superfície de ataque externa

Antes mesmo de obter alguma credencial ou dado corporativo, criminosos podem realizar varreduras nos sistemas da empresa que ficam expostos na internet - servidores web, e-mails, VPN, canais de API, entre outros. Ao encontrar uma vulnerabilidade, erro de configuração ou dado exposto nestes sistemas, é possível que o invasor encontre o caminho para dar o primeiro passo dentro do alvo.

No complexo ecossistema digital corporativo, não é incomum que dashboards, serviços web, armazenamento em nuvem e muitos outros recursos sejam adotados de forma “ad-hoc” - ou seja, para atender uma necessidade específica e até momentânea, sem que haja conexão clara com os demais processos e sistemas. Muitas vezes, estes recursos carecem de documentação clara e sua existência nem sempre é comunicada ao departamento de TI, gerando fenômeno conhecido como “shadow IT”.

Por esta razão, não basta que a empresa esteja atenta apenas à sua superfície de ataque interna e aos seus recursos administrados pelo departamento de TI.

Na maioria dos casos, o invasor está do lado de fora e, portanto, o primeiro contato dele com o ambiente da empresa ocorre justamente por meio dessa superfície externa — inclusive com aqueles recursos não são os oficialmente administrados pela equipe de TI.

O resumo deste cenário é que o invasor pode acabar conhecendo melhor esta superfície externa do que a própria empresa, especialmente se não houve um esforço coordenado para monitorar, mapear e proteger esta superfície externa. Não é possível aplicar um patch de segurança para um sistema cujo uso a própria equipe de TI desconhece.

Soluções de External Attack Surface Management (EASM) ajudam as empresas a enxergar melhor a sua infraestrutura a partir do lado de fora, da mesma forma que um atacante. O EASM colabora com a gestão de vulnerabilidades, detecta erros de configuração e identifica softwares e equipamentos expostos à rede de forma indevida.

Monitorar, mapear e buscar a conformidade de todos estes sistemas externos é essencial para evitar que invasores encontrem “atalhos” para dentro do ambiente corporativo.

O risco de ataques a terceiros e a segurança da supply chain

Em vez de procurar atacar seus alvos diretamente, alguns grupos de ransomware têm buscado pontos comuns de falha em fornecedores de empresas. Ataques a esses terceiros vêm sendo chamados de supply chain attacks, pois atingem as empresas por meio das outras organizações das quais elas dependem.

Como muitas empresas permitem a conexão direta ou indireta desses terceiros à sua infraestrutura de TI, o risco envolvido nesse tipo de campanha não difere muito de um ataque direto à infraestrutura da empresa.

Para o atacante, encontrar uma vulnerabilidade ou falha em um fornecedor pode permitir que ele atinja dezenas ou centenas de empresas com uma única ação. Desta forma, um único ataque cibernético se desdobra em dezenas de tentativas de extorsão, aplicadas a cada vítima separadamente.

Tipos de ataque a terceiros

Não existe uma categorização formal dos diferentes ataques a fornecedores, mas muitas das ações desta natureza podem ser agrupadas com base no tipo de terceiro explorado.

Ataques a infraestrutura terceirizada

Essas ações exploram alguma característica, falha ou ponto comum em um serviço digital utilizado por várias empresas.

O exemplo mais emblemático é o caso do Snowflake, um serviço de armazenamento em nuvem. Embora os responsáveis pelo ataque não tenham explorado nenhuma vulnerabilidade no serviço, a ausência de autenticação multifator (MFA) em várias das contas dos clientes do Snowflake abriu uma brecha para um roubo de dados em massa, atingindo 165 organizações sem adentrar na infraestrutura de nenhuma delas.

Em outros casos, criminosos tentaram explorar fragilidades em provedores de identidade terceirizados e outros tipos de serviços de TI.

Essa estratégia também tem sido adotada por outros grupos de atacantes fora da esfera do ransomware. Um dos casos mais preocupantes foi noticiado em 2023, quando hackers chineses obtiveram uma chave criptográfica da infraestrutura da nuvem da Microsoft para atacar clientes da empresa no governo norte-americano. O caso motivou uma investigação por parte da então recém-formada Cyber Safety Review Board.

Ataques a serviços de apoio

Criminosos têm empregado engenharia social para enganar centros de atendimento ou helpdesk terceirizados para ganhar acesso à infraestrutura corporativa.

Como essas equipes muitas vezes têm permissões para redefinir as senhas dos usuários, elas podem se tornar um ponto fraco do processo de autenticação. O atacante pode se passar por um funcionário da empresa e solicitar a redefinição da senha e até a desativação dos fatores adicionais de autenticação.

Também há registros de ameaças de violência física contra os colaboradores terceirizados que prestam este serviço. Se não houver um meio de acompanhar e registrar esses incidentes, a empresa contratante pode acabar só tendo conhecimento da tentativa de ataque depois que a invasão já aconteceu.

Ataques a softwares

Ataques que exploram vulnerabilidades em softwares não são novidade. No entanto, o tipo de vulnerabilidade explorada nesses ataques e a finalidade da exploração criam um cenário muito específico que deve ser compreendido dentro do contexto geral de ataques a fornecedores.

A principal característica a ser considerada é a finalidade da exploração da falha, ou seja, se ela será utilizada para um golpe de extorsão de dados. Softwares que atendem necessidades particulares das redes corporativas, como serviços de transmissão de dados e programas de administração remota, são os principais alvos dessas ações.

Não é necessário que a ação envolva uma vulnerabilidade no próprio software. Os atacantes também podem tentar atacar diretamente a empresa responsável pelo software para adulterá-lo e conseguir chegar ao alvo. O caso da SolarWinds, em 2020, é o mais conhecido de um ataque deste tipo, porém não envolveu um incidente de ransomware.

Isso não significa que nenhum ransomware utilizará a mesma tática. Em 2017, o software de contabilidade M.E. Doc foi adulterado para iniciar a disseminação de um malware conhecido como NotPetya. O NotPetya é hoje considerado um malware do tipo wiper, já que carecia de uma função genuína para decodificar e recuperar os arquivos.

Apesar disso, as consequências para as vítimas foram muito semelhantes às de um ataque de ransomware da época, e é pouco provável que os operadores de ransomware não estejam procurando softwares que sirvam como porta de entrada para as redes corporativas.

Os casos mais recentes e notórios de ataques de extorsão com exploração de softwares foram realizados pelo grupo Clop, que explorou falhas em serviços como GoAnywhere e MOVEit Transfer, ameaçando centenas de organizações com os dados roubados através desses serviços.

Com ferramentas de cibersegurança externa, empresas podem ganhar visibilidade sobre problemas em suas conexões com terceiros. Por exemplo, o monitoramento de credenciais pode ser ampliado para incluir terceiros que possuem credenciais para sistemas corporativos.

Em paralelo, o acompanhamento de insights de inteligência mantém as equipes de segurança informadas sobre as táticas mais recentes dos grupos de ransomware e quais softwares podem estar sendo explorados em campanhas, oportunizando uma resposta incisiva e ágil para prevenir ou minimizar o impacto dos ataques.

Inteligência em cibersegurança

Acompanhar as movimentações das gangues de ransomware permite mapear as vulnerabilidades e técnicas utilizadas.
Na prática, é possível priorizar as ações que terão mais eficácia para proteger a organização.

- Priorize a aplicação de patches de vulnerabilidades que estão sendo usadas por gangues de ransomware
- Reforce a segurança de canais e serviços (como um cloud provider específico) que estejam envolvidos em ataques recentes
- Aprimore sistemas de segurança preexistentes (como antivírus e firewalls) com dados relevantes de IoCs, como endereços de IP e arquivos maliciosos
- Saiba dos riscos específicos para seu setor de atuação
- Atue para inibir o recrutamento de insiders para colaborar com criminosos
- Adote sistemas de gestão de senha (cofres) e autenticação multifator (MFA) para reforçar a segurança de credenciais e dos canais de acesso. Estas medidas podem evitar a exposição de uma credencial ou reduzir a utilidade de uma credencial roubada.

Como o monitoramento de vazamentos quebra a corrente do ransomware em seu primeiro elo

1. Operadores de ransomware adquirem credenciais e meios de acesso a sistemas corporativos de outros criminosos especializados na violação inicial ou roubo de logins e senhas (estes criminosos são às vezes chamados de “Access Brokers”)

2. Monitorar o fluxo dessas transações e ofertas permite identificar quem mais pode estar em risco e como os invasores podem conseguir acesso à rede corporativa

3. Ao detectar uma credencial vazada, pela pode ser bloqueada pela organização

4. O operador de ransomware não conseguirá o acesso inicial à organização

5. Sem esse acesso inicial, o ataque é dificultado e não poderá prosseguir

Recuperação e resposta

Como reagir a um ataque de ransomware

Direto ao Ponto — Como a empresa muitas vezes depende de sua infraestrutura tecnológica, um ataque de ransomware pode comprometer todo o negócio. A paralisação das atividades exige uma postura proativa, projetando a solidez esperada por investidores, consumidores e outros stakeholders, o que exige preparo, canais de comunicação e um bom checklist capaz de guiar a atuação das equipes envolvidas no momento mais crítico. O checklist Agência de Cibersegurança dos Estados Unidos (EUA) é nossa referência para este guia.

A visão executiva da resposta ao ransomware

Em uma fraude de extorsão dupla (criptografia de arquivos acompanhada de ameaça de vazamento de dados), como é a regra nos golpes de ransomware que estão em evidência, a organização enfrenta dois desafios principais:

1. Restaurar a infraestrutura de TI para retomar as operações e minimizar o prejuízo decorrente da interrupção gerada pela criptografia dos arquivos
2. Proteger a reputação e a marca da empresa diante dos consumidores, colaboradores e demais stakeholders

Embora a proteção da marca não seja uma preocupação direta da equipe que atuará na recuperação do sistema, é importante definir um canal de comunicação adequado para as equipes encarregadas desta responsabilidade.

A equipe de TI também pode priorizar atitudes concretas que demonstrem preocupação com os consumidores, como a proteção das credenciais que podem ter caído na mão dos criminosos. A organização pode fazer isto invalidando as senhas anteriores e exigindo a troca no próximo login, sem alarmar consumidores com uma troca de senhas obrigatória.

Contudo, vale ressaltar que a organização pode ter responsabilidades específicas previstas na legislação. No Brasil, a Lei Geral de Proteção de Dados (LGPD) obriga empresas a comunicar o vazamento de dados pessoais aos respectivos titulares em determinadas situações. Regras semelhantes existem em vários estados norte-americanos e na Europa, com a GDPR.

Caso o ataque não tenha criptografado dados, a extorsão tende a se basear majoritariamente nessas repercussões jurídicas e reputacionais. Os criminosos podem até chantagear a empresa com a divulgação do incidente a clientes e parceiros cujas informações foram obtidas durante o ataque.

Para esses cenários, convém preparar uma estratégia de comunicação robusta que oriente os clientes e parceiros a respeito da situação e evite que os criminosos assumam o protagonismo na divulgação do incidente. A comunicação será mais assertiva se a empresa possuir controles de segurança ou processos capazes de determinar com precisão quais informações foram obtidas e quais medidas devem ser tomadas por todas as partes atingidas pelo vazamento.

O preparo é essencial

A resposta a um incidente de ransomware pode ser facilitada por uma série de preparativos.

Treine a equipe de TI para a resposta inicial a incidentes de segurança.

Não é incomum que, diante de problemas rotineiros, administradores de redes e analistas de TI tomem atitudes como a reinicialização ou o desligamento do sistema. Isso elimina evidências que futuramente ajudariam a elucidar o incidente. São os administradores e analistas que muitas vezes terão o primeiro contato com um sintoma provocado pela invasão, e uma boa resposta inicial pode facilitar muitas das etapas posteriores.

Teste os backups e planeje uma recuperação.

O backup está no centro das preocupações com o ransomware. Contudo, não basta realizar um backup – é preciso que os arquivos estejam protegidos e, preferencialmente, desconectados (offline).

Considere os riscos e particulares dos backups em nuvem.

Para backups em nuvem, deve-se considerar o tempo de restauração, que estará condicionado à velocidade da rede e outras limitações, bem como a dependência que o backup pode ter de um sistema conectado à rede e vulnerável ao ransomware. Usar múltiplas soluções de nuvem e soluções de armazenamento imutável pode ajudar a evitar que os invasores comprometam todos os backups. Como os backups em nuvem podem ser acessados remotamente, é preciso criptografá-los para evitar que os invasores acessem os backups para chantagear a empresa com vazamento de dados.

Determine canais de contato emergenciais.

Os canais de contato da empresa podem não ser confiáveis ou até estarem indisponíveis durante um incidente de ransomware. Esteja preparado para montar uma sala de guerra e estabelecer contato com consultorias de segurança, stakeholders e gestores por meio de canais que não dependam diretamente da infraestrutura corporativa.

Estruture processos de controle de dados e privacidade.

Em vários países, a legislação vigente exige que as empresas protejam dados pessoais e prestem esclarecimentos às vítimas atingidas por um vazamento de dados. Determinar se um atacante obteve ou não acesso a informações pessoais pode ser essencial para evitar que a empresa seja chantageada por ameaças de exposição de dados.

Elabore um plano de recuperação e Gestão de Continuidade de Negócio (GCN) e um Business Impact Analysis (BIA).

Os planos de recuperação de desastre e GCN mapeiam riscos e a interdependência de processos do negócio, facilitando a priorização de sistemas para a recuperação. Sem isso, um sistema considerado crítico durante uma análise apressada realizada durante o incidente pode acabar sendo restaurado e continuar inoperante por alguma dependência desconhecida de um outro sistema que não está na fila de recuperação.

O Business Impact Analysis (BIA), por sua vez, avalia o impacto da interrupção dos serviços para delinear os requisitos operacionais do negócio e recursos associados. Com isso, ele colabora com o desenho dos marcos que a recuperação deve atingir e a estimativa dos prazos em que ela pode ocorrer.

Quanto menos preparada a organização estiver ao se deparar com um incidente de ransomware, maior tende a ser o trabalho da equipe de resposta, prolongando o período de indisponibilidade de sistema e ampliando os prejuízos.

Além disso, quanto mais rápida for a resposta e a retomada da operação regular, menor tende a ser o dano à imagem da empresa, especialmente se ficar demonstrado que não houve o pagamento do resgate.

Checklist: respondendo a um incidente de ransomware

Uma boa referência para elaborar uma estratégia de resposta a um ataque de ransomware é o Ransomware Guide (Guia de Ransomware) elaborado pela CISA, a agência norte-americano responsável por segurança cibernética e de infraestrutura.

O checklist conta com 19 itens em 3 grandes etapas da resposta. Abaixo, temos os 19 itens com alguns comentários adaptados:

Etapa 1: Detecção e Análise

1. Determine os sistemas impactados e isole-os imediatamente

- Se várias subnets podem ter sido impactadas, desconecte todas no switch. Pode não ser viável desconectar individualmente durante o incidente.
- Se não for possível desconectar a rede como um todo, desconecte sistemas individuais desconectando cabos ou removendo-os do Wi-Fi.
- Os sistemas também podem ser desconectados ou isolados por meio da segmentação em VLANs. Em alguns ambientes ou serviços (como na nuvem pública), esta pode ser a opção mais viável.
- Se a invasão teve início em um terceiro ou parceiro, revogue todas as credenciais ou canais de acesso associados a ele.
- Os responsáveis pelo ataque podem tentar monitorar a comunicação interna da empresa. Utilize, preferencialmente, métodos alternativos de comunicação (como ligações telefônicas) e prossiga de forma coordenada para evitar a movimentação lateral dos criminosos ou o agravamento do ataque.

2. Só desligue sistemas caso não seja possível desconectá-los da rede

- O desligamento dos sistemas só deve ser realizado em último caso, pois elimina evidências voláteis (como a memória do sistema) e dificulta a perícia.

3. Faça a triagem dos sistemas que devem ser restaurados e recuperado

- Identifique e priorize sistemas mapeando a natureza dos dados armazenados em cada um e a função desempenhada (segurança, saúde, geração de receita).

Etapa 1: Detecção e Análise

4. Inicie um esforço de Threat Hunting para entender como o ataque aconteceu

- Procure por novas contas criadas no diretório de usuários ou contas cujas propriedades de autenticação foram alteradas
- Verifique os logins em sistemas de acesso remoto e VPNs
- Vasculhe os endpoints pela presença de ferramentas que podem ter comprometido backups e credenciais (como o Mimikatz) ou realizado a exfiltração de dados (ferramentas como Rclone e clientes de serviços de armazenamento não utilizados na organização)
- Registros de atividade do envio de dados para fora da rede, em qualquer porta

Etapa Intermediária: Comunicação, Documentação e Gestão

Embora esta etapa não esteja explicitada no guia da CISA, é neste momento que devem ser compiladas todas as informações mapeadas na fase inicial. Também é nesse momento que se inicia um fluxo de comunicação com gestores e stakeholders, o qual **deverá ser mantido durante todo o processo de resposta de incidente para resguardar danos à marca.**

5. Reúna-se com sua equipe para desenvolver e documentar a compreensão inicial do que ocorreu a partir da análise inicial

6. Usando informações de contato das autoridades e prestadores de serviço da organização, dialogue com equipes internas e externas e stakeholders sabendo o que eles podem providenciar para ajudar você a mitigar, responder e recuperar-se do incidente.
   - Compartilhe as informações que você tem para que a ajuda seja relevante. Mantenha gestores e a alta gestão informados com atualizações regulares sobre o andamento da situação.

Etapa 2: Contenção e erradicação

7. Guarde uma imagem de sistema e cópia da memória de uma amostra dos dispositivos afetados (estações de trabalho e servidores, por exemplo). Colete logs relevantes e cópias de arquivos de malware precursores do ransomware e qualquer outro dado observável que pode ser considerado um IoC (endereços de IP de servidores de comando e controle, entradas de registro suspeitas, entre outros arquivos).
   - Atente-se para a preservação de informações altamente voláteis como logs e dados de memória de sistema para evitar a perda ou alterações.

8. Consulte autoridades policiais sobre a possível existência de ferramentas de decifragem que podem estar disponíveis.
   - Os especialistas da Axur podem ajudar a encontrar uma ferramenta de decifragem. Contudo, a decifragem não será possível na maioria dos casos.

9. Pesquise fontes confiáveis para obter recomendações referentes à variante específica de ransomware e siga os passos indicados para detectar e isolar sistemas ou redes impactadas.

10. Identifique credenciais e sistemas envolvidos na invasão inicial. A credencial pode ser uma conta de e-mail.

11. Com base nos dados da invasão determinados nos passos anteriores, isole qualquer sistema associado que pode ser usado para manter um acesso não autorizado. As invasões são muitas vezes acompanhadas de um roubo em massa de credenciais.
    - Proteger a rede e outras fontes de informação contra novos acessos não autorizados pode exigir a desativação de serviços de VPN e de acesso remoto, de serviços de login único (SSO) e outros ativos de acesso público ou de nuvem.

12. Ação adicional sugerida: passos para identificação de criptografia de dados em servidores
    - Dados em servidores podem ser cifrados por um ransomware instalado no próprio servidor. Mas também há casos em que a criptografia é realizada a partir de um endpoint autorizado, sem que isso implique em uma contaminação do próprio servidor
    - Sessões de acesso a pastas compartilhadas abertas, as informações de proprietário dos arquivos e históricos de login em serviços de RDP podem ajudar a descobrir se dados armazenados em servidores estão sendo criptografados a partir de um ransomware que foi instalado em uma estação de trabalho.
    - O log de segurança do Windows, logs evento do serviço SMB e ferramentas de análise de tráfego (como o Wireshark) podem também ajudar a determinar a fonte do acesso indevido.

Etapa 2: Contenção e erradicação

13. Examine os sistemas existentes para detecção e prevenção de ataques à organização (antivírus, resposta em endpoints, sistemas IDS e IPS etc.) e dos logs. Isto pode revelar evidências adicionais sobre sistemas ou de malwares envolvidos nos estágios iniciais do ataque.
    - Procure por evidências do malware do tipo "Dropper", que atua como precursor do ransomware. Como explicamos na organização do cibercrime, o acesso a redes corporativas é muitas vezes comprado pelos operadores do ransomware, enquanto os "Access Brokers" se especializam no acesso inicial com malwares de acesso remoto ou de roubo de credenciais.

14. Conduza uma extensa análise para identificar mecanismos de persistência de fora para dentro e de dentro para fora.
    - "De fora para dentro": credenciais roubadas ou criadas pelos próprios invasores, vulnerabilidades, sistemas de perímetro contaminados com malware de acesso remoto.
    - "De dentro para fora": ferramentas de acesso remoto instaladas em sistemas internos que vão desde o Cobalt Strike, uma suíte profissional para esse tipo de ação, a ferramentas típicas de suporte remoto, como o AnyDesk.

15. Restaure sistemas priorizando serviços críticos (como os de saúde e segurança ou de geração de receita), preferencialmente usando imagens pré-configuradas.
    - Certifique-se de que os patches apropriados sejam aplicados e que o sistema de segurança adequado (antivírus ou XDR) esteja presente.

16. Depois que o ambiente foi completamente limpo e restaurado (inclusive as credenciais impactadas e a remoção ou erradicação de mecanismos de persistência maliciosas), realize uma redefinição de senhas para todos os sistemas afetados e faça o tratamento de vulnerabilidades e brechas de segurança ou de visibilidade. Isso pode ser feito com a aplicação de patches, atualização de segurança e tomando outras precauções de segurança ainda não adotadas.

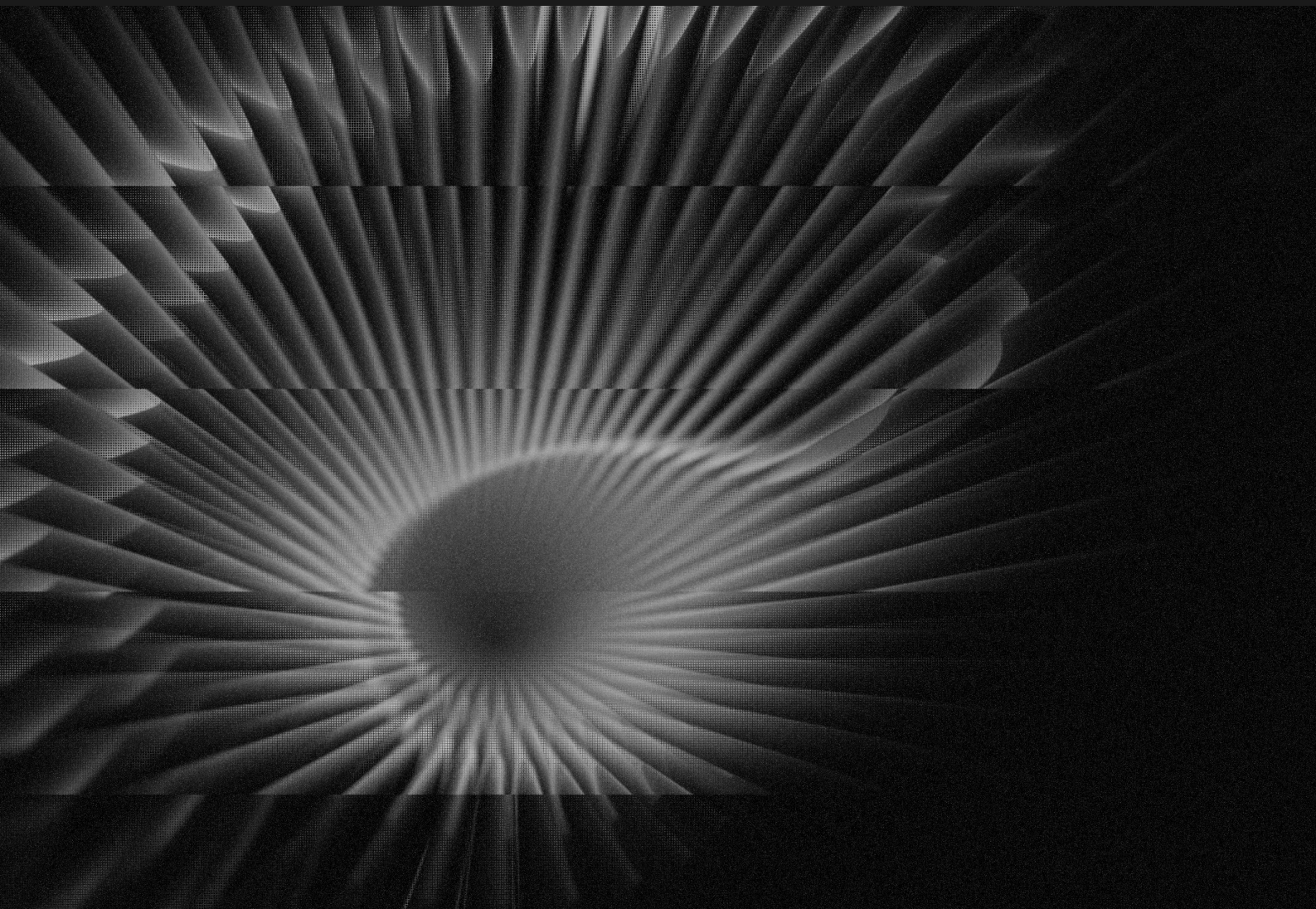
17. A partir de um critério estabelecido, que pode incluir os passos acima ou a busca de uma assistência externa, a autoridade de TI ou de segurança de TI declara o fim do incidente de ransomware.

Etapa 3: Recuperação e atividade pós-incidente

18. Reconecte os sistemas e restaure dados a partir de backups offline e criptografados, priorizando serviços críticos
    - Lembre-se: pagar o resgate não é garantia de que seus dados serão devolvidos.

19. Documente as lições aprendidas com o incidente e as atividades de resposta para amparar atualizações (e refinar) políticas da organização, planos e procedimentos e guiar exercícios futuros referentes a eles.

20. Considere compartilhar as lições aprendidas e indicators of compromise com autoridades ou organizações relevantes do setor para beneficiar a comunidade.



Conte com inteligência externa para antecipar ataques

A Axur fortalece a defesa contra ransomware ao agir onde os criminosos iniciam tudo: fora do perímetro corporativo. Nossa plataforma monitora continuamente credenciais vazadas, dados sensíveis e pontos de exposição na superfície externa da sua organização e de fornecedores, interceptando acessos que poderiam ser vendidos a operadores de ransomware.

Com essa visibilidade antecipada, as equipes de segurança conseguem bloquear credenciais comprometidas, corrigir vulnerabilidades críticas e reduzir drasticamente as chances de invasão antes que o ataque aconteça.

Além da prevenção, a Axur acelera a resposta a incidentes. Nossa inteligência sobre táticas, técnicas e procedimentos de grupos de ransomware alimenta mecanismos de detecção e investigação, facilitando a identificação de acesso não autorizado e a contenção rápida de movimentos laterais.

Com automação de análises, dados acionáveis e dashboards inteligentes, sua equipe ganha vantagem sobre um ecossistema criminoso dinâmico e pode manter continuidade operacional e reputação mesmo em cenários de alta pressão.

Fortaleça sua defesa contra o ransomware

AGENDE UMA DEMO

bsi ISO/IEC 27001 Information Security Management CERTIFIED

CleanDNS Trusted Reporter

Descubra todas as nossas soluções em **axur.com**

///AXUR