EBOOK

Ransomware

Como entender, prevenir e responder a uma das mais graves ameaças digitais à segurança da sua empresa

Sumário

Sumário Executivo

Diversos levantamentos apontam o ransomware como uma das ameaças mais graves ou preocupantes. Um exemplo consta no relatório anual de 2021 do Centro de Cibersegurança Nacional do Reino Unido (NSCS), que reconheceu o ransomware como a maior ameaça digital enfrentada pelo país, especialmente devido aos possíveis danos referentes à indisponibilidade de serviços essenciais (eletricidade, água, esgoto) ou infraestrutura.

A preocupação é legítima. Os impactos de um ataque de ransomware costumam ser dramáticos e visíveis, com longos períodos de indisponibilidade de serviços, paralisação do negócio e tentativas de extorsão com cifras milionárias.

Contudo, pode ser proveitoso entender o ransomware com uma soma de ameaças. Afinal, o que torna o ransomware tão insidioso é o fato de que praticamente qualquer descuido pode desencadear um ataque. Graças ao ecossistema do cibercrime a outros softwares maliciosos há muito conhecidos, como aqueles que geram redes-zumbi, uma única credencial vazada ou vulnerabilidade, ou até um clique indevido em um link de um e-mail, é suficiente para expor a rede a um ransomware.

Depois deste acesso inicial, é a paciência (e especialização) dos criminosos que o transforma em um incidente cujo impacto se alastra por toda a organização. Dos serviços internos e externos ao fator humano, o ransomware estressa todas as camadas da infraestrutura digital.

O desafio, portanto, está na priorização das ações com maior potencial de efetividade. Compreendendo a fraude, pode-se mapear o fluxo e as etapas nas quais ela pode ser interrompida, seja impedindo o primeiro acesso ou detectando um dos outros ataques dos quais o ransomware depende. Pensar apenas na etapa mais emblemática do ransomware (a criptografia, ou o “resgate digital”) não nos ajuda a achar essa resposta.

É por isso que trouxemos um perfil da evolução do ecossistema do crime até os dias atuais, mostrando como os operadores de ransomware se beneficiam dele. É neste ecossistema que existem as melhores oportunidades de atuação de inteligência, monitoramento e, portanto, de prevenção.

Ao final, temos também uma guia para responder a um ataque se ransomware - e vemos como o preparo adequado é a chave para manter este processo ordenado.

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$ 189,00.

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 e 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.

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.

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$ 300,00. No caso dos SMSs, o valor costumava ser de US$ 10,00.

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.**

Papel de parede usado pelo ransomware LockBit.

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". Alguns vírus de resgate icônicos, como o CryptoLocker e o CryptoWall, usavam a mesma linguagem visual (escudos e cadeado) 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.

A cobrança era realizada por serviços que se especializavam em simplificar remessas internacionais, como Ukash, Paysafe e MoneyPak. As cobranças eram de cerca de US$ 200,00.

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 fraude

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 os códigos usados em 2022. 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”.

Até hoje, não existe uma ferramenta de decodificação para recuperar arquivos criptografados pelo CryptoLocker. Quem não pagou o resgate e não tinha backup jamais recuperou os dados perdidos.

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$ 500,00.

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 plug-ins.

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$ 300,00 e US$ 600,00). Quase que paralelamente, outro ransomware menos midiático, o Locky, começava a cobrar cifras de quatro dígitos.

A partir deste momento, de 2017 a 2020, algumas transformações importantes ocorrem no mundo do crime de ransomware:

1. 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.

2. 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.

3. 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.

4. 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 autoridade 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 criptomoeda foram atribuídas a ransomware.

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.

Linha do tempo do ransomware

O ransomware é uma ameaça construída ao longo de quase duas décadas de aperfeiçoamento da atividade criminosa no mundo digital. Embora o primeiro ransomware tenha surgido em 1989, a fraude como existe hoje foi desenhada ao longo da segunda metade da década de 2000. Transformada pela chegada das criptomoedas, passou a ser considerada uma das maiores preocupações de cibersegurança.

1989

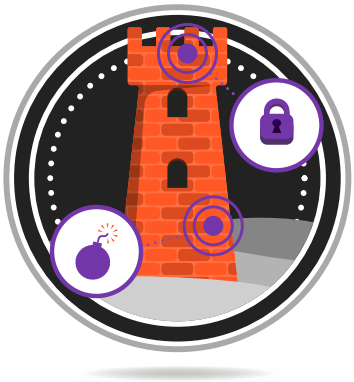
Lançado o **malware AIDS**, primeiro código malicioso que pode ser considerado um "ransomware". Foi distribuído em disquetes que supostamente teriam informações sobre a AIDS, por isso seu nome. Congelava o sistema e pedia um resgate de US$ 189.

2004

É detectado pela primeira vez o vírus **GPCode**, que criptografava arquivos para cobrar um resgate através de um serviço de pagamento russo.

2009

É criado o primeiro bloco do **Bitcoin**, método de pagamento que seria adotado para cobrar os resgates do ransomware nos anos seguintes.

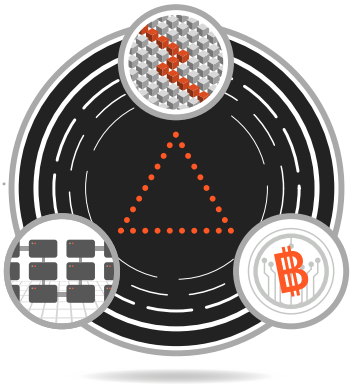


2012

É criado o malware **Citadel**, um ladrão de credenciais que também instalava o ransomware Reveton e produzia relatórios de rendimentos e instalação para o controle de afiliados, consolidando o modelo "malware como serviço", em que cada fase do ataque é realizada por indivíduos diferentes.

Primeira detecção do **CryptoLocker**, que combinava criptografia assimétrica, servidores de controle e opção de pagamento por Bitcoin, formando os pilares do golpe de ransomware para toda a década.

2013



2015

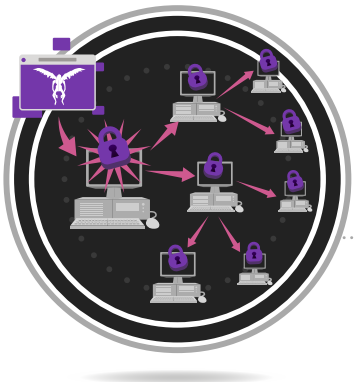
O modelo de **ransomware como serviço** abre as portas para criminosos sem habilidade técnica. O golpista ganharia uma comissão por cada vítima que pagasse o resgate a partir da versão do malware gerada em um site da Deep Web.

Paralisação de serviços e empresas devido ao **WannaCry**, o último ransomware notório a ser distribuído de forma indiscriminada, sem procurar alvos específicos.

2017

2017 a 2020

Grandes transformações no crime de ransomware

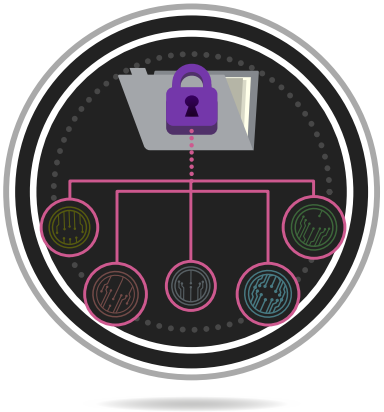


2018

Surge o ransomware **Ryuk**, que concentra os ataques em empresas e organizações.

Expansão dos serviços de **cryptocurrency tumblers**, que misturam criptomoedas de diversas origens para ocultar ganhos ilícitos.

2019



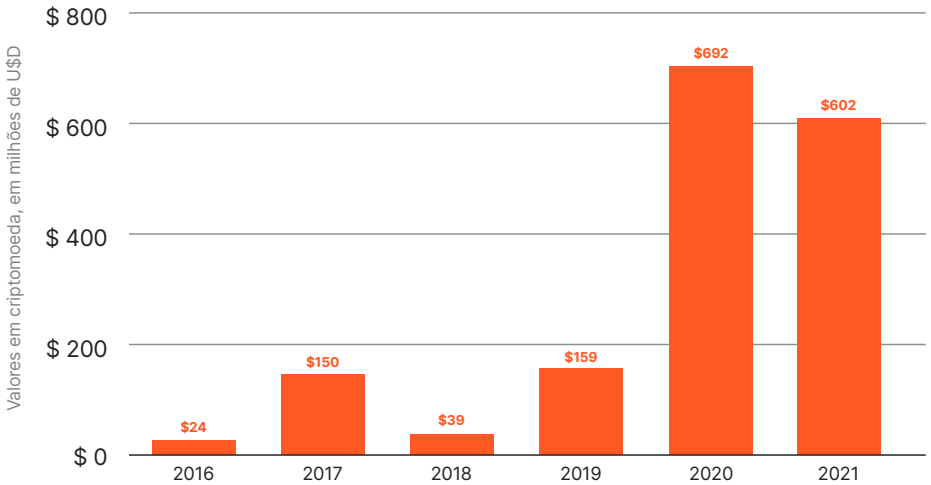
2020

Cresce a estratégia de **extorsão dupla**, que ameaça vítimas com vazamento de dados, e pagamentos são cobrados também em criptomoeda Monero.

HOJE

O ransomware continua trazendo prejuízos, mas a **prevenção** por meio de atividades de inteligência e **monitoramento** tem um potencial de eficácia altamente relevante, assim como saber com quem contar na hora mais crítica da recuperação.

Valores totais em criptomoeda recebidos por endereços de ransomware



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 o Conti e o DarkSide, 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.

DarkSide: o ransomware que deflagrou uma emergência

Em maio de 2021, a Colonial Pipeline, um oleoduto dos Estados Unidos, suspendeu o fornecimento de combustível após ter seu sistema de cobranças derrubado por um **ataque de ransomware.** O resgate cobrado (e pago) foi de US$ 4,4 milhões.

A investigação revelou que o ransomware não havia chegado à rede corporativa por meio de outro malware ou por um phishing direcionado. Em vez disso, os criminosos

haviam explorado uma credencial antiga e exposta que dava acesso ao serviço de VPN da companhia para iniciar a invasão.

Foi o próprio presidente da empresa, Joe Blount, que revelou o método usado pelos invasores em depoimento para um comitê do Senado norte-americano. Uma questão técnica normalmente invisível para a alta direção de um oleoduto havia causado um prejuízo milionário e risco de falta de combustível na região abastecida pelo serviço.

O depoimento do executivo deixa duas marcas:

1. A alta gestão precisava olhar para a ameaça representada pelo ransomware.

2. A **nova modalidade** de ransomware – com ataques dirigidos e personalizados ao ambiente alvo – tinha amadurecido e podia trazer consequências reais até para o cotidiano das pessoas.

O ransomware que atingiu a Colonial Pipeline se chamava DarkSide. A exposição do caso acabou jogando luz do sol também sobre as operações dessa gangue, pressionando também uma resposta das autoridades. Toda a operação foi encerrada ainda no mês maio, depois que a infraestrutura foi confiscada por autoridades e os líderes do DarkSide decidiram se afastar.

O caso, porém, podia ser um “golpe de um golpe”. O DarkSide funcionava como “ransomware-as-a-service” (RaaS), um sistema que 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.

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. Ao “encerrar” suas atividades, o DarkSide, na prática, podia estar aplicando um calote em seus “afiliados”.

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).

Após “encerrar” suas operações, o DarkSide ressurgiu como um ransomware chamado BlackMatter. O estabelecimento do vínculo entre famílias supostamente distintas de ransomware permite prever certos aspectos do comportamento do invasor, o que também pode ajudar na resposta a incidentes.

Porquê 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. Como aconteceu no caso do DarkSide, em que os líderes podem ter aplicado um golpe em seus afiliados, os líderes das gangues de ransomware precisam lidar com o receio de serem roubados por seus sócios e colaboradores.

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 em 2022 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.

Existem ainda os auxiliares responsáveis pelo estudo dos alvos (estimando o faturamento e a capacidade de pagamento) e pela negociação com as vítimas.

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 a 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 dupla 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.

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 impactar a equipe de segurança existente, permitindo que esta continue focada nos ativos internos.

Como a extorsão dupla mudou o peso da prevenção

Se uma boa estratégia de recuperação era suficiente para mitigar os impactos do ransomware até 2020, a prática da extorsão dupla (resgate de dados com ameaça de vazamentos) significa que a restauração dos sistemas não vai evitar outros prejuízos decorrentes do ataque, como os danos à marca e as possíveis consequências jurídicas previstas na legislação, como a Lei Geral de Proteção de Dados (LGPD).

É por isso que medidas capazes de prevenir ou interromper um ataque em andamento agregam muito valor à defesa contra a ameaça do ransomware. 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 apoio 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

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.

Os times de CTI (Cyber Threat Intelligence) e ART (Axur Research Team) da Axur conseguiram acessar arquivos de “log” de quase uma dezena 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 (os já mencionados “logs”) com o intuito de vendê-las no submundo do crime. Com essa comercialização, eles se conectam a todo tipo de atividade criminosa.

Os logs podem ser vendidos 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 trabalho de monitoramento da Axur já identificou mais de 170 milhões de credenciais roubadas por estes códigos maliciosos. Destas, 18,2 milhões puderam ser vinculadas ao Brasil. Além disso, várias destas senhas dão acesso a serviços críticos ou que notoriamente são utilizados como porta de entrada para ransomware.

Um dos credential stealers mais notórios monitorados pela Axur é o RedLine. A análise dos logs realizada pela Axur identificou dezenas de milhões de credenciais roubadas e 305,6 mil delas puderam ser atribuídas diretamente a empresas brasileiras - e tudo isso é fruto da atividade de um único malware.

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.

No caso da Colonial Pipeline, por exemplo, o acesso inicial ocorreu por meio de uma credencial de VPN. Um alerta prévio sobre o vazamento desta credencial poderia ter mudado o rumo do incidente. E o risco não é apenas hipotético: entre todas as credenciais expostas nos logs dos credential stealers monitorados pela Axur, 374 mil puderam ser atribuídas a sistemas de VPN.

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 o 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 que 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.

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

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

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”).

1. 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.

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

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

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 pró-ativa, 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 — caso do checklist da CISA, uma agência do governo norte-americano, que trazemos como referência.

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.

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). 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, dificultando o acesso aos dados ou, no pior dos casos, permitindo que o ransomware cifre também o backup.

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.

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 dos especialistas da Axur:

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.

- 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 recuperados.

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

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.

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

5. 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

6. 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.

7. 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.

8. 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.

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

10. 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.

11. 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.

12. 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.

13. 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, à ferramentas típicas de suporte remoto, como AnyDesk.

14. 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.

15. 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.

16. 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

17. 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.

18. 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.

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

A Axur dispõe de especialistas em cyber threat intelligence para conduzir o processo de resposta a incidente que podem integrar a sua sala de guerra (war room) e fornecer orientações efetivas de acordo com o ransomware envolvido e as especificidades do seu negócio.

Clique para baixar o nosso case de sucesso War Rooms: Estratégia e Reação e saiba como apoiamos nossos clientes em incidentes de alto impacto.

Em qualquer incidente, como o próprio guia da CISA sugere no caso do ransomware, é importante saber quem pode apoiar a sua empresa.

Experiências digitais mais seguras

Protegemos a presença digital de milhares de empresas ao redor do mundo

Agende uma demo

Sobre a Axur

A Axur possibilita a escala e automatização do tratamento de ameaças cibernéticas para apoiar os times de segurança da informação e proporcionar experiências digitais mais seguras. A nossa plataforma de Threat Intelligence tem o tempo de reação mais rápido do mercado, solicitando takedowns automáticos, 24x7.

Isso é possível porque a plataforma Axur atua em quatro camadas: além da detecção, as tecnologias de inspeção, automação e remoção diminuem muito o tempo médio de contenção (MTTC) dos times de segurança. Além disso, nossos especialistas em Inteligência Cibernética expandem a investigação tanto na Surface como na Deep & Dark Web, tornando a Axur a empresa líder em Cyber Threat Intelligence na América Latina.

Contato para a imprensa
press@axur.com

Endereços

EUA
535 Mission Street – 14th floor
San Francisco, CA 94105

Singapura
109 North Bridge Road
Cityhall District, 179097

Brasil
Rua Mostardeiro, 322 – 15º andar
Porto Alegre, RS 90430-000

axurbr Axur AxurBrasil AxurBrasil AxurBrasil Axur