The bridge to possible

Proteção contra ransomware

Segurança Zero Trust para uma força de trabalho moderna

Conteúdo

O ransomware chegou para ficar 2

O perímetro expande 6

Phishing, ataques direcionados e vulnerabilidades 7

Guia passo a passo para um ataque de ransomware 8

Como impedir o comprometimento do ransomware antes que comece 10

Conclusão 11

Atualize a defesa além do MFA com o Duo 12

Referências 13

The bridge to possible

O ransomware chegou para ficar

O ransomware evoluiu rapidamente como uma estratégia de ataque. Antes era apenas uma aquisição hostil de computadores isolados; atualmente, as apostas estão aumentando. Cada vez mais os agentes mal-intencionados visam alvos geopolíticos, sistemas de negócios e infraestruturas essenciais (por exemplo, buscam empresas de grande porte), o que pode resultar em danos sem precedentes. Hoje, o ransomware é uma das maiores ameaças à segurança cibernética, aumentando em 150% no ano de 2020 devido à mudança repentina para o trabalho remoto.

Agora, o ransomware é classificado como terrorismo cibernético, e a recente ordem executiva do presidente dos EUA, Biden, confirma que medidas devem ser tomadas imediatamente para manter os sistemas seguros. Uma abordagem Zero Trust é o padrão ouro para proteger contra ransomware. O National Institute of Standards and Technology (NIST) afirma que "a implementação de uma arquitetura Zero Trust se tornou um compromisso de segurança cibernética e uma obrigação comercial".

A ficha informativa da Casa Branca declara que: “incidentes recentes de segurança cibernética, como SolarWinds, Microsoft Exchange e o incidente da Colonial Pipeline, são um lembrete esclarecedor de que as entidades dos setores público e privado dos EUA enfrentam cada vez mais atividades cibernéticas mal-intencionadas avançadas de agentes do estado-nação e criminosos cibernéticos”.

> **“Incidentes recentes de segurança cibernética, como SolarWinds, Microsoft Exchange e o incidente da Colonial Pipeline, são um lembrete esclarecedor de que as entidades dos setores público e privado dos EUA enfrentam cada vez mais atividades cibernéticas mal-intencionadas avançadas de agentes do estado-nação e criminosos cibernéticos."**

Ficha informativa da Casa Branca dos Estados Unidos da América.

O que é o ransomware?

Simplificando, o ransomware usa diversas táticas para atingir os usuários predominantemente por meio de infecções por malware, começando com phishing por e-mail, uma senha roubada ou um ataque de força bruta. Um ataque de ransomware pode ser realizado ao criptografar arquivos ou pastas, impedir o acesso do sistema ao disco rígido e manipular o registro de inicialização mestre para interromper o processo de inicialização do sistema. Uma vez que o malware foi instalado e espalhado, os hackers podem obter acesso a dados confidenciais e dados de backup, que eles criptografam para manter as informações reféns. Os hackers podem agir rapidamente ou passar meses bisbilhotando sem serem detectados para entender a infraestrutura de rede, antes de lançar um ataque.

O sequestro de dados é feito para causar medo e urgência nas vítimas. As informações ficam inacessíveis até que o pagamento (principalmente em Bitcoin) possa ser feito. Mesmo assim, as empresas podem não recuperar todos os dados. Existem muitas variantes de ransomware; porém, na maior parte, o cryptoransomware é a principal ameaça. Devido ao polimorfismo (malware em constante mudança), existem muitas variantes que podem evitar a detecção.

O cryptoransomware que bloqueia os dados está melhorando rapidamente. Em 2006, o ransomware usava 56 bits com criptografia artesanal. A versão avançada de ransomware atual usa algoritmos simétricos de AES e criptografia de chave pública RSA ou ECC para bloquear dados.

O ransomware se tornou um negócio

À medida que o ransomware continua a ganhar força, ele se tornou um negócio profissional administrado por organizações criminosas (principalmente localizadas na China, Rússia, Coreia do Norte e Europa Oriental) dedicadas a mirar e causar interrupções em alvos de alto valor, além de extrair dinheiro em troca de dados. Para fazer isso de forma eficaz, essas organizações chegaram ao ponto de configurar call centers para orientar os alvos no processo de compra de Bitcoin e pagamento do resgate. Alguns recebem até uma alta classificação dos alvos devido ao bom atendimento ao cliente.

Às vezes, para incentivar o pagamento, os invasores fornecem um "relatório de segurança" passo a passo, que detalha exatamente como eles conduziram o ataque após a troca do resgate. Embora seja inteligente que as gangues descriptografem os arquivos em troca de dinheiro para manter sua reputação intacta para o próximo alvo, esse nem sempre é o caso. The State of Ransomware 2021 da Sophos afirma que apenas 8% das vítimas recuperam os dados e 29% recuperam mais da metade deles. Às vezes, os dados são coletados e negociados com outros invasores ou retidos para outra oportunidade futura de resgate.

Nos últimos anos, os agentes mal-intencionados estabeleceram o ransomware como serviço (RaaS), uma solução pronta para uso totalmente integrada, que permite que qualquer pessoa implante um ataque de ransomware sem saber codificar. Assim como os produtos de software como serviço (SaaS), o RaaS oferece acesso relativamente barato e fácil a esses tipos de programas mal-intencionados a uma taxa menor do que o custo de criar o seu próprio programa. Os provedores de RaaS geralmente têm uma redução de 20% a 30% do lucro gerado pelo resgate. Agora, existem modelos de assinatura e de afiliados para ajudar a concluir ataques de sucesso. O grupo de hackers REvil tinha um modelo de afiliados que lucraria com qualquer pessoa que contribuísse com um ataque de ransomware de sucesso. Esse modelo levou ao aumento substancial no volume de ataques de ransomware.

Atribuída inicialmente à gangue Maze, outra tendência é a dupla extorsão, em que os hackers pegam as informações sequestradas e ameaçam publicá-las na dark Web e/ou Internet, caso suas exigências não sejam atendidas. Eles têm uma infraestrutura integrada para lidar com esses despejos de dados, de acordo com o Relatório de investigações de violação de dados de 2020 da Verizon. A tática de "nome e vergonha" agora é popular para a maioria das gangues de ransomware, assim como o modelo de "penalidade", em que o preço aumenta à medida que o tempo passa.

À medida que as empresas fortalecem a postura de segurança para computadores e redes contra ataques de ransomware, os hackers estão voltando sua atenção para a exploração de dispositivos móveis. Os dispositivos móveis têm uma tela muito menor e não fornecem informações completas à primeira vista (e-mail, por exemplo), o que faz com que as vítimas cliquem com mais facilidade em links mal-intencionados. Os ataques à Internet das Coisas (IoT) também estão aumentando, pois o ransomware e a falta de segurança podem transformar dispositivos e objetos em pontos de entrada para ferramentas de ransomware. Em 2020, os ataques de ransomware direcionados a dispositivos de IoT aumentaram em 109% nos EUA.

Esses fatores, juntamente com os países que atuam como refúgios seguros para invasores, levaram ao aumento do crime de ransomware. Ocorreu um ataque de ransomware de sucesso a cada dez segundos em 2020 e, de acordo com uma pesquisa da Anomali Harris Poll, um a cada cinco americanos é vítima de ataques de ransomware. Além disso, a Infosecurity Magazine relata que o método de ataque mais popular "foi de longe o tráfego de botnet (28%), seguido de mineradores de criptografia (21%), ladrões de informações (16%), malware de dispositivos móveis (15%) e do setor bancário (14%)". Em resposta, as empresas estão se esforçando para gastar mais dinheiro em segurança (US$ 150 bilhões em 2021, de acordo com o Gartner).

Os ataques a indivíduos estão diminuindo, à medida que os hackers se concentram em alvos específicos mais lucrativos. Os provedores de serviços gerenciados (MSPs) estão relatando um aumento de 85% nos ataques contra SMBs. As corporações, juntamente com empresas de infraestrutura, saúde, governo e manufatura, estão sendo mais visadas do que nunca, com preços na casa dos milhões em troca de dados. O tamanho de um resgate dobrou no ano passado, quando os invasores atacaram empresas de grande porte. Os ataques a fornecedores, contratados e software de terceiros também aumentaram de forma exorbitante. As empresas tiveram que confiar na segurança dessas partes externas que têm acesso aos sistemas.

A ascensão das gangues de ransomware	O primeiro caso conhecido de ransomware veio de disquetes que continham pesquisas sobre AIDS e malware, distribuídos em todo o mundo em 1989 pelo dr. Joseph Popp. Os discos criptografavam os arquivos no sistema da vítima e negavam o acesso até que enviassem um pagamento de US$ 189 para uma caixa postal no Panamá. CDs de isca foram distribuídos na conferência sobre AIDS da Organização Mundial da Saúde. O pagamento e o envio de CDs eram problemáticos e caros.
2006	Os criminosos cibernéticos começaram a usar uma forma mais eficaz de criptografia de chave pública 660 RSA para criptografar arquivos com mais rapidez. Os principais agentes naquela época eram o Trojan Archiveus e o GPcode, que usavam e-mail de phishing como pontos de entrada.
2008-2009	Um novo software antivírus carregado com malware ransomware surgiu, e um software de segurança não autorizado usou o FileFix Pro para extorquir dinheiro para descriptografia.
2010	O Bitcoin mudou tudo. Dez mil variantes de ransomware foram detectadas, e o ransomware de bloqueio de tela fez sua primeira aparição.
2013	Havia um quarto de milhão de amostras de ransomware, e o Cryptolocker e o Bitcoin se tornaram rapidamente o principal método de pagamento. O ransomware usou a criptografia RSA de 2048 bits para aumentar as exigências, provando ser lucrativo para gangues.
2015	O trojan ransomware Teslacrypt surgiu; agora, havia 4 milhões de variantes de ransomware, e o ransomware como serviço (RaaS) foi lançado.
2016	O JavaScript e o ransomware Locky eram populares, e o Locky infectava 90.000 vítimas por dia. Os invasores visavam empresas de grande porte, como hospitais e instituições acadêmicas. O ransomware alcançou mais de US$ 1 bilhão em lucros. O malware Petya causou mais de US$ 10 bilhões em perdas financeiras.
2017	O criptoworm WannaCry surgiu neste ano, evoluindo para diversas variantes todos os dias e se espalhando rapidamente para 300.000 computadores em todo o mundo por meio de um exploit da Microsoft.
2018	O Katsuya foi lançado. A SamSam encerrou vários serviços municipais que impactavam a cidade de Atlanta.

2019	A REvil, uma gangue privada de RaaS, surgiu na Rússia. O Ryuk, uma variante de ransomware avançada e cara, integrada a anexos e e-mails de phishing mal-intencionados, exigiu pagamentos mais altos em comparação a ataques semelhantes e fechou de fato todos os principais jornais dos EUA.
2020	Darkside, Egregor e Sodinokibi se estabeleceram como os principais agentes. O Ryuk passou de um caso por dia para 19,9 milhões em setembro, o equivalente a oito casos por segundo.
2021	Os kits de REvil/Sodinokibi, Conti e Lockbit atingiram fortemente o setor de saúde. O CryptoLocker extorquiu US$ 40 milhões da grande seguradora CNA Financial em um dos maiores pagamentos de ransomware até hoje. O DarkSide conseguiu atacar a Colonial Pipeline Company, marcando a maior invasão divulgada publicamente da infraestrutura essencial dos EUA.

O perímetro expande

Como o ransomware se tornou tão predominante? Anteriormente, o perímetro era um muro fechado que gerenciava dados e aplicações centralizadas por meio de firewalls de rede virtual privada (VPN) e soluções de gerenciamento de dispositivos móveis (MDM), como um fosso em torno do castelo da rede. Atualmente, o trabalho acontece em qualquer lugar e em qualquer dispositivo (incluindo dispositivos móveis pessoais), e os dados precisam ser acessados em aplicações de terceiros na nuvem. Não há fosso, e sim muitas entradas para o castelo. O aumento do trabalho remoto durante a pandemia transformou o perímetro tradicional no "perímetro definido por software". Na correria de manter os funcionários trabalhando, a segurança foi uma reflexão tardia para muitos, o que levou a oportunidades de ransomware para agentes mal-intencionados.

Acesso Remoto

As principais tendências de segurança e risco do Gartner para 2021 relatam que 64% dos funcionários agora podem trabalhar em casa e dois quintos da força de trabalho estão trabalhando em casa. Durante o período obrigatório de permanência em casa da pandemia, a maioria dos funcionários teve que se tonar 100% remoto e precisava da capacidade de trabalhar em seus próprios dispositivos, enquanto acessava aplicações de SaaS na nuvem e no local. Muitas empresas não tinham infraestrutura para sustentar essa mudança. Atualmente, o acesso remoto é a nova realidade da força de trabalho. À medida que as empresas se adaptam a esse padrão de operação, prevê-se que a força de trabalho seja um modelo híbrido de funcionários remotos e funcionários que retornam ao escritório.

Peter Firstbrook, analista e vice-presidente do Gartner, afirma em uma publicação no blog: "à medida que o novo normal toma forma, todas as empresas precisarão de uma postura defensiva sempre conectada e clareza sobre quais riscos comerciais os usuários remotos elevam para permanecerem seguros".

As empresas que não fortaleceram a postura de segurança para essa mudança nem melhoraram a educação de segurança interna criam um caminho fácil para os invasores. O Gartner relata que 57% das violações envolvem negligência de funcionários/terceiros. De acordo com o ZDNet, o Remote Desktop Protocol (RDP) é o principal método usado por agentes de ameaças para obter acesso a computadores Windows e instalar ransomware e outros programas de malware, seguidos de phishing de e-mail e exploits de erros de VPN.

Restrições de VPN

O uso de exploits em VPNs é o terceiro método de entrada mais popular para hackers de ransomware. O ataque que desligou a Colonial Pipeline Company foi o resultado de uma senha comprometida de uma VPN não utilizada. Embora as VPNs possam limitar o acesso a aplicações locais, há inconsistência no acesso a aplicações em nuvem que pode levar a vulnerabilidades. Uma vez comprometidas, as VPNs podem levar ao acesso de backdoor à rede, no qual os hackers podem instalar malware nos sistemas internos.

Uma abordagem Zero Trust em camadas de VPN e firewall com MFA evita 100% dos bots automatizados, 99% dos ataques de phishing em massa e 90% dos ataques direcionados, de acordo com a pesquisa do Google.

Endpoints desprotegidos

À medida que cada vez mais dispositivos são conectados a redes corporativas, o número de dispositivos pessoais e dispositivos sombra aumenta. Como esses dispositivos podem não ser monitorados ou atualizados, eles podem levar a violações nos principais endpoints, sem serem detectados. À medida que os hackers procuram meticulosamente uma entrada, os endpoints desprotegidos e a falta de insights sobre quem e o que está se conectando à rede e sobre a integridade do dispositivo podem levar a uma violação.

Phishing, ataques direcionados e vulnerabilidades

Quais técnicas são usadas em ataques de ransomware? É um processo de várias etapas que pode ser relativamente curto ou realizado ao longo de meses para acessar e criptografar os dados mais importantes e que causarão mais danos, caso sejam mantidos reféns. O CSOonline.com relata que 94% dos programas de malware são entregues por e-mail, e os ataques de phishing são responsáveis por mais de 80% dos incidentes de segurança. Outros pontos de entrada incluem atualizações não corrigidas e vulnerabilidades de dia zero. Quase todos eles começam com o roubo de credenciais.

Técnicas de ransomware

Spray and Pray ou phishing geral

Os agentes de ameaças adquirem listas de e-mail no mercado negro, analisam as credenciais e distribuem e-mails de phishing. Apenas algumas credenciais são necessárias para ter sucesso, geralmente adquiridas por e-mail com anexos mal-intencionados, sites fraudulentos que parecem legítimos ou uma identidade falsa direcionada a funcionários de alto valor.

Spear phishing

Esse ataque coordenado e direcionado a um grupo específico de usuários é realizado por meio do envio de mensagens personalizadas com engenharia social, valendo-se de curiosidade, medo ou recompensa de uma fonte que parece legítima. Os e-mails e o site contêm malware usado para roubar credenciais. O malware também pode ser distribuído por meio de mídia social e aplicações de mensagens instantâneas.

Força bruta

De acordo com uma pesquisa do LastPass, 91% dos entrevistados reconheceram que reutilizam senhas. Os hackers têm pleno conhecimento disso e coletam senhas de despejos de credenciais ou da dark Web. Eles usam ferramentas automatizadas para testar senhas em diferentes sites, conhecidas como preenchimento de credenciais ou força bruta. Uma vez dentro, o ataque pode começar.

Exploração de vulnerabilidades conhecidas

Além de obter insights sobre quais dispositivos se conectam à rede, é importante conhecer a integridade do dispositivo e saber se as correções e atualizações são atuais para manter um perfil de alta segurança. O Security Boulevard relata: “componentes de código aberto desatualizados e ‘abandonados’ são disseminados. E 91% das bases de código continham componentes que estavam desatualizados há mais de quatro anos ou não tiveram atividades de desenvolvimento nos últimos dois anos”.

The bridge to possible

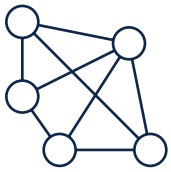
Guia passo a passo para um ataque de ransomware

Criptografia de ransomware

É muito comum que os ataques de ransomware criptografem os dados nos sistemas de destino, tornando-os inacessíveis até que um resgate seja pago pela descriptografia. A tática mais recente é a criptografia dupla, em que os hackers criptografam um sistema duas vezes ou duas gangues diferentes visam a mesma vítima. Com essa abordagem, os invasores têm a chance de coletar dois resgates ao receber o pagamento da primeira camada de criptografia e, em seguida, surpreender as vítimas com outra camada após receber o pagamento da primeira. A criptografia mais comum é assimétrica ou simétrica.

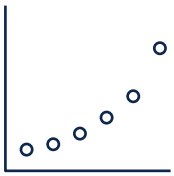
Coordenação do ataque

A essa altura, os hackers de ransomware fazem a lição de casa sobre as empresas específicas que estão atacando. Eles podem comprar listas de e-mails na dark Web, identificar líderes importantes, ler os dados financeiros da empresa, pesquisar perfis de mídia social e compilar uma lista das principais partes interessadas, como prestadores de serviços, fornecedores e parceiros. Quais táticas os hackers usam para entrar? Os três principais ataques de 2020 vieram de endpoints de RDP protegidos de forma inadequada, ataques de phishing por e-mail e exploração de vulnerabilidades de VPN de dia zero. Credenciais comprometidas são a principal maneira pela qual os agentes mal-intencionados obtêm acesso.



Movimento vertical

Na fase de infiltração e infecção, o movimento vertical é quando os agentes da ameaça passam de uma posição externa para uma posição interna. Uma vez dentro, eles verificam arquivos e executam códigos mal-intencionados em endpoints e dispositivos de rede. O malware se move pelo sistema infectado, desativando firewalls e programas de software antivírus. A essa altura, os invasores assumiram os dados, mas eles ainda não foram criptografados. Os pontos de entrada comuns para movimento vertical incluem contas de e-mail com phishing, servidores Web de baixo nível e endpoints protegidos de forma inadequada.



Base de dados lateral	Exfiltrar os dados	Pagamento e desbloqueio
O sucesso das ameaças persistentes avançadas (APTs) aumentou devido ao movimento lateral. Para estabelecer uma base de dados, os criminosos precisam criptografar computadores e distribuir o ransomware para o maior número possível de sistemas. Depois de obter acesso, a busca do invasor começa. Eles começam o movimento lateral, sem serem detectados, por semanas ou meses pela rede para identificar alvos importantes, como o centro de comando e controle (C2), chaves assimétricas e arquivos de backup. Ao mesmo tempo, eles elevam o acesso e as permissões infectando outros sistemas e contas de usuários e preparam uma presença mal-intencionada persistente para sequestrar os dados. Alguns exemplos de movimento lateral incluem a exploração de serviços remotos, o spear phishing interno e o uso de senhas roubadas, também conhecidas como “pass the hash”.	Quando a avaliação do inventário estiver concluída, a criptografia será iniciada. Os backups do sistema são excluídos, os arquivos e pastas locais são corrompidos, as unidades de rede não mapeadas são conectadas a sistemas infectados, e a comunicação com o centro de comando e controle é feita para gerar as chaves criptográficas usadas no sistema local. Os dados da rede são copiados localmente, criptografados e carregados, substituindo os dados originais. Dados exfiltrados podem ser usados para extorsão dupla. Nesse caso, é exigido um resgate para descriptografar os dados criptografados e, em seguida, um segundo resgate é exigido para não vazar os dados roubados.	Os invasores ativam o malware, bloqueiam os dados e anunciam as exigências de um resgate nos locais comprometidos, com instruções específicas sobre como fazer o pagamento, normalmente em Bitcoin. Uma ocorrência de ransomware cria um problema de tempo de inatividade muito caro, que é extremamente difícil de resolver. As ameaças são feitas e a contagem regressiva começa. As empresas devem decidir se querem sofrer um viés e pagar, tentar restaurar os arquivos por conta própria ou usar o seguro de segurança cibernética, que recuperará apenas parte do resgate. É uma escolha entre opções ruins e, por isso, é essencial que as empresas implementem uma arquitetura Zero Trust e reforcem as melhores práticas de segurança para evitar essa situação.

Setores vulneráveis

Serviços de saúde, municípios e governo, bem como varejo, educação e finanças são os setores mais afetados pelos ataques de ransomware. Esses setores possuem soluções antigas complexas e podem não aproveitar a segurança robusta da nuvem. Os serviços de saúde, educação e governo são lentos para adaptar a postura de segurança com atualizações e novas tecnologias, o que os torna alvos fáceis e lucrativos.

The bridge to possible

Como impedir o comprometimento do ransomware antes que comece

Em um ataque de ransomware, os invasores precisam primeiro obter acesso. Eles podem fazer isso obtendo credenciais comprometidas, como foi o caso da violação da Colonial Pipeline.

O Duo MFA (autenticação multifator) pode ajudar a impedir que o ransomware obtenha acesso. O MFA exige que um usuário apresente uma combinação de duas ou mais credenciais para verificar a identidade para login. Por exemplo, além de um nome de usuário e uma senha, o Duo MFA solicita algo que você tenha, como um dispositivo confiável ou um token de software ou hardware, antes de conceder acesso aos recursos. Graças a essa exigência adicional, o MFA torna muito mais difícil para o ransomware obter essa base de dados inicial.

O ransomware também está interessado em usar serviços remotos, como RDP e VPNs, para obter acesso a uma rede. Darkside, o suposto autor do ataque a Colonial Pipeline, é suspeito de ter usado o acesso à VPN corporativa para entrar no ambiente da vítima. Mais do que apenas o MFA, a combinação de Duo MFA, Duo Device Trust, Duo Network Gateway (DNG) e Duo Trust Monitor forma uma solução de acesso confiável e pode ajudar a proteger o acesso remoto à infraestrutura local e impedir que o ransomware obtenha acesso.

O Duo MFA exige mais do que um nome de usuário e uma senha para autenticação. O DNG permite que os usuários acessem sites locais, aplicações Web, servidores SSH e RDP, sem precisar se preocupar com credenciais de VPN. O Duo Device Trust verifica se o dispositivo que acessa recursos remotamente é um computador confiável e não o dispositivo de um invasor. Por fim, o Duo Trust Monitor chama a atenção para solicitações de autenticação que parecem suspeitas, como as provenientes de países em que agentes de ransomware são conhecidos por serem ativos e países em que uma empresa não tem funcionários.

O uso de malware também é uma técnica popular de infecção por ransomware. A Cisco fornece soluções complementares adicionais, como Secure Endpoint e Email Gateway, que podem inspecionar, detectar e bloquear o ransomware no malware, antes que ele infecte os endpoints.

Como o Duo ajuda a proteger contra ransomware

O Gartner relata que 90% dos ataques de ransomware podem ser evitados. O Duo está posicionado de forma única para ajudar as empresas em três frentes:

1. Impedir que o ransomware obtenha uma base de dados inicial em um ambiente
2. Prevenir ou retardar a propagação de ransomware, caso ele consiga se infiltrar em uma empresa
3. Proteger recursos e partes essenciais da empresa, enquanto um invasor ainda estiver presente no ambiente e até que a correção total seja realizada

Como evitar a propagação

O ransomware que afeta um pequeno número de sistemas tem um impacto limitado e provavelmente não fará com que uma empresa pare e se disponha a pagar um resgate. É por isso que a propagação de ransomware é essencial para derrubar eficazmente uma parte considerável de uma empresa e obrigá-la a pagar o resgate para voltar aos negócios rapidamente. Em 2017, o WannaCry e o NotPetya usaram o exploit External Blue para aproveitar uma vulnerabilidade da Microsoft e distribui-lo sem intervenção do usuário.

O Device Health Application do Duo pode manter os dispositivos corrigidos e atualizados, dificultando a distribuição automática do ransomware. Além disso, fornece visibilidade ao verificar o status de integridade do dispositivo, incluindo a atualização do dispositivo, a cada tentativa de login. Com o recurso de autocorreção do Duo, os usuários podem manter os dispositivos corrigidos com facilidade, sem a ajuda da TI.

Correção em segurança

Recuperar-se de um ataque de ransomware e colocar os sistemas on-line novamente não significa necessariamente que o invasor saiu do ambiente. Ele pode ter tentado estabelecer persistência para voltar mais tarde. Uma técnica comum é comprometer as contas atuais ou criar novas contas, geralmente acessando o Active Directory ou outros diretórios que contenham contas de usuário. O Duo MFA pode trazer a tranquilidade de que um invasor que ainda está na rede não poderá fazer articulações e movimento lateral com facilidade usando credenciais comprometidas. Também pode ganhar tempo e impedir que um invasor cause mais danos, enquanto o ataque é totalmente corrigido, removendo todos os vestígios de persistência.

Implementação de um modelo de segurança Zero Trust

De acordo com o princípio de "nunca confiar, sempre verificar", o Zero Trust é um modelo de segurança que pode ajudar as empresas a implementar proativamente as melhores práticas conhecidas para proteger contra ataques cibernéticos, incluindo o ransomware.

O Zero Trust é tão essencial que a Casa Branca emitiu uma ordem executiva exigindo especificamente o Zero Trust e o MFA.

O Duo fornece um MFA fácil de usar e implementar. Ele também permite que as empresas só concedam acesso caso um usuário e seu dispositivo possam ser verificados e considerados confiáveis. Essa capacidade de controlar e gerenciar o acesso é um dos pilares fundamentais do Zero Trust, e o Duo MFA é um dos primeiros passos para implementar uma estrutura Zero Trust.

Conclusão

O ransomware será mais predominante e as empresas devem estar mais atentas. A engenharia social e o spear phishing obtêm sucesso porque exploram o elemento humano da segurança de uma empresa. Adotar e implementar uma filosofia de segurança Zero Trust, que começa com um MFA forte e uma plataforma de acesso confiável, é importante para se antecipar aos ataques de ransomware.

The bridge to possible

Atualize a defesa além do MFA com o Duo

As empresas podem se defender contra o impacto do ransomware por meio de ataques de phishing sociais e direcionados, implementando políticas de acesso condicional que aproveitam fatores contextuais, como localização e postura do dispositivo, para estabelecer confiança nos usuários e nos dispositivos.

A plataforma de segurança na nuvem do Duo protege o acesso a todas as aplicações, para qualquer usuário e dispositivo, em qualquer lugar. Simplificamos o acesso seguro para lidar com os riscos de identidade e dispositivo usando seis recursos essenciais:

1. Verifique as identidades dos usuários com métodos de autenticação multifator seguros e flexíveis.
2. Ofereça uma experiência de login coerente com o logon único do Duo, que oferece acesso centralizado às aplicações no local e na nuvem.
3. Obtenha visibilidade de cada dispositivo e mantenha um inventário detalhado de todos os dispositivos que acessam as aplicações empresariais.
4. Estabeleça a confiança no dispositivo por meio de verificações de integridade e postura para dispositivos gerenciados ou não gerenciados, antes de conceder acesso à aplicação.
5. Aplique políticas de acesso granulares para limitar o acesso aos usuários e dispositivos que atendem aos níveis de tolerância a risco da empresa.
6. Monitore e detecte comportamentos de login de risco usando o Duo Trust Monitor ou exporte os registros para o SIEM, a fim de corrigir eventos suspeitos, como inscrição de novos dispositivos para autenticação ou login em um local inesperado.

Motivos para escolher o Duo

Velocidade com segurança

O Duo oferece os componentes básicos de Zero Trust em uma solução rápida e fácil de implantar para os usuários. Dependendo do caso de uso específico, alguns clientes podem ser executados em questão de minutos.

Facilidade de uso

Para se inscrever, basta que os usuários baixem um aplicativo na App Store e se conectem. Os controles de manutenção e política são fáceis para que os administradores controlem e obtenham uma visibilidade clara.

Integra-se a todas as aplicações

Nosso produto foi criado para ser independente e funcionar com sistemas antigos. Independentemente dos fornecedores de TI e de segurança usados, com o Duo, você ainda pode proteger o acesso a todas as aplicações de trabalho, para todos os usuários, em qualquer lugar.

Menor custo total de propriedade (TCO)

Como o Duo é fácil de implementar e não exige a substituição de sistemas, ele requer muito menos recursos de tempo e custo, iniciando as operações rapidamente e começando a jornada para um modelo de segurança Zero Trust.

Referências

The Pandemic-hit World Witnessed a 150% Growth of Ransomware, https://cisomag.eccouncil.org/growth-of-ransomware-2020/, CISO Magazine, 5 de março de 2021

Exclusive: U.S. to give ransomware hacks similar priority as terrorism, https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/, Reuters, 3 de junho de 2021

NIST Announces Tech Collaborators on NCCoE Zero Trust Project, https://www.hstoday.us/industry/emerging-innovation/nist-announces-tech-collaborators-on-nccoe-zero-trust-project/, Homeland Security Today, 24 de setembro de 2021

FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware, https://www.whitehouse.gov/briefingroom/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware, The White House, 13 de outubro de 2021

Types of Encryption: Symmetric or Asymmetric? RSA or AES?, https://preyproject.com/blog/en/types-ofencryption-symmetric-or-asymmetric-rsa-or-aes/, Prey Project, 15 de junho de 2021

What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast, https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hackergroup-just-wreaked-havoc, The Heritage Foundation, 20 de maio de 2021

What We Can Learn From Ransomware Actor "Security Reports," https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports, Coveware, 24 de junho de 2021

The State of Ransomware 2021, https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx, Sophos, 2021

Data Mining Process: The Difference Between Data Mining and Data Harvesting, https://www.import.io/post/the-difference-between-data-mining-data-harvesting, Import.io, 23 de abril de 2019

Ransomware: Enemy at The Gate, https://ussignal.com/blog/ransomware-enemy-at-the-gate, US Signal, 3 de setembro de 2021

2020 Data Breach Investigations Report, https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf, Verizon, 2020

Malware is down, but IoT and ransomware attacks are up, https://www.techrepublic.com/article/malwareis-down-but-iot-and-ransomware-attacks-are-up/, Tech Republic, 23 de junho de 2020

One Ransomware Victim Every 10 Seconds in 2020, https://www.infosecurity-magazine.com/news/oneransomware-victim-every-10/, Infosecurity Magazine, 25 de fevereiro de 2021

Terrifying Statistics: 1 in 5 Americans Victim of Ransomware, https://sensorstechforum.com/1-5-americansvictim-ransomware/, Sensors Tech Forum, 19 de agosto de 2019

Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021, https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwidesecurity-and-risk-managem, Gartner, 17 de maio de 2021

1 in 5 SMBs have fallen victim to a ransomware attack, https://www.helpnetsecurity.com/2019/10/17/smbsransomware-attack/, Help Net Security, 17 de outubro de 2019

Ransomware – how to stop this growing, major cause of downtime, https://polyverse.com/blog/ransomware-how-to-stop-this-growing-major-cause-of-downtime, Polyverse.com

The strange history of ransomware, https://theworld.org/stories/2017-05-17/strange-history-ransomware, PRI The World, 17 de maio de 2017

Ransomware Timeline, https://www.tcdi.com/ransomware-timeline, tcdi.com, 27 de dezembro de 2017

A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time, Digital Guardian, 2 de dezembro 2020

One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack, https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5, Business Insider, 22 de maio de 2021

Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare, https://www.wired.com/story/atlantaspent-26m-recover-from-ransomware-scare, Wired.com, 23 de abril de 2018

Cyber-attack: US and UK blame North Korea for WannaCry, https://www.bbc.com/news/world-uscanada-42407488, BBC.com, 19 de setembro de 2017

Ransomware: Now a Billion Dollar a Year Crime and Growing, https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646, NBCNews.com, 9 de janeiro de 2017

The Untold Story of NotPetya, the Most Devastating Cyber Attack in History, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world, Wired.com, 22 de agosto de 2018

Ransomware in Healthcare Facilities: The Future is Now, https://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=mgmt_faculty, Marshall University Digital Scholar, outono de 2017

New ransomware holds Windows files hostage, demands $50, https://www.networkworld.com/article/2265963/new-ransomware-holds-windows-files-hostage--demands--50.html, NetworkWorld.com, 26 de março de 2009

Preventing Digital Extortion, https://subscription.packtpub.com/book/networking_and_servers/9781787120365/4/ch04lvl1sec24/the-advancement-of-locker-ransomware-winlock, PackIt, maio de 2017

The Irreversible Effects of Ransomware Attack, https://www.crowdstrike.com/blog/irreversible-effectsransomware-attack, CrowdStrike, 20 de julho de 2016

New Era of Remote Working Calls for Modern Security Mindset, Finds Thales Global Survey of IT Leaders, https://www.businesswire.com/news/home/20210914005014/en/New-Era-of-Remote-Working-Calls-for-Modern-Security-Mindset-Finds-Thales-Global-Survey-of-IT-Leaders, Business Wire, 14 de setembro de 2021

FBI sees spike in cyber crime reports during coronavirus pandemic, https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic, The Hill, 16 de abril de 2020

Symantec Security Summary - September 2021, https://symantec-enterprise-blogs.security.com/blogs/featurestories/symantec-security-summary-september-2021, Symantec Security, 27 de setembro de 2021

INTERPOL report shows alarming rate of cyberattacks during COVID-19, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, Interpol, 4 de agosto de 2020

Gartner Top Security and Risk Trends for 2021, https://www.gartner.com/smarterwithgartner/gartner-topsecurity-and-risk-trends-for-2021, Gartner, 5 de abril de 2021

Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time, https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time, Gartner, 14 de julho de 2020

Gartner Highlights Identity-First Security as a Top Security Trend for 2021, https://www.attivonetworks.com/blogs/gartner-identity-first-security-in-2021, Attivo, 27 de abril de 2021.

2021 SonicWall Cyber threat Report, https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyberthreat-report.pdf, SonicWall, 2021

Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme, https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme, ZDNet.com, 23 de agosto de 2020

VPN exploitation rose in 2020, organizations slow to patch critical flaws, https://www.cybersecuritydive.com/news/trustwave-network-security-remote-access/602044/, Cybersecurity Dive, 18 de junho de 2021

New research: How effective is basic account hygiene at preventing hijacking, https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html, Google Blog, 17 de maio de 2019

Top cybersecurity statistics, trends, and facts, https://www.csoonline.com/article/3634869/top-cybersecuritystatistics-trends-and-facts.html, CSOonline.com, 7 de outubro de 2021

Protecting Companies From Cyberattacks, https://www.inc.com/knowbe4/protecting-companies-fromcyberattacks.html, Inc.com, 20 de setembro de 2021

ThreatList: People Know Reusing Passwords Is Dumb, But Still Do It, https://threatpost.com/threatlistpeople-know-reusing-passwords-is-dumb-but-still-do-it/155996/, Threatpost, 25 de maio de 2020

Synopsys Study Shows 91% of Commercial Applications Contain Outdated or Abandoned Open Source Components, https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-ofcommercial-applications-contain-outdated-or-abandoned-open-source-components, Security Magazine, 12 de maio de 2020

Ransomware's Dangerous New Trick Is Double-Encrypting Your Data, https://www.wired.com/story/ransomware-double-encryption/, Wired.com, 17 de maio de 2021

Combating Lateral Movement and the Rise of Ransomware, https://www.msspalert.com/cybersecurityguests/combating-lateral-movement-and-the-rise-of-ransomware, MSSP Alert, 24 de junho de 2021

Lateral Movement, https://attack.mitre.org/tactics/TA0008/, MITRE| ATT&CK, 17 de outubro de 2019

Industries Impacted by Ransomware, https://airgap.io/blog/industries-impacted-by-ransomware, AirGap.com

Defend Against and Respond to Ransomware Attacks, https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks, Gartner Research, 26 de dezembro de 2019

Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, The White House. 12 de maio de 2021

C11-3233828-00 10/22