TREND MICRO | research

EM DIREÇÃO A UM NOVO MOMENTO

PREVISÕES DE TREND MICRO SECURITY PARA 2022

TREND MICRO RESEARCH

EM DIREÇÃO A UM NOVO MOMENTO

PREVISÕES DE TREND MICRO SECURITY PARA 2022

05

Ameaças na Nuvem

As empresas irão garantir que o básico da segurança em nuvem seja implementado para defender seus ambientes contra uma série de ameaças à segurança em nuvem e atingir um nível gerenciado de risco

08

Ameaças de Ransomware

Para permanecerem protegidas contra a evolução das ameaças de ransomware, as empresas irão se concentrar em proteger seus servidores com políticas de proteção de servidor e controle de aplicativos rigorosas

11

Vulnerabilidade Exploits

As equipes de segurança precisarão estar bem equipadas para lidar com atores mal-intencionados que buscam se aproveitar de vulnerabilidades antigas e explorá-las como recém-descobertas em questão de dias, se não horas

14

Ataques de malware de commodities

Os agentes mal-intencionados continuarão a pensar nas empresas menores como presas fáceis, mas como pequenas e médias empresas que usam muita nuvem virão preparadas com medidas de segurança que podem evitar de commodities

17

Ameaças no IoT

As empresas se irão se esforçar para melhorar o monitoramento e a visibilidade da rede para proteger seus ambientes de TI contra ameaças decorrentes da adoção de IoT

20

Ameaças na cadeia de abastecimento

À medida que as empresas se concentram em tornar suas cadeias de abastecimento mais robustas por meio da diversificação e regionalização, inicia-se a implementação dos princípios de zero trust com a intenção de manter seus ambientes mais seguros

23

Velocidade total para cibersegurança

Published by Trend Micro Research

Stock images used under license from Shutterstock.com

EM DIREÇÃO A UM NOVO MOMENTO

PREVISÕES DE TREND MICRO SECURITY PARA 2022

2021 foi um marco para grandes e pequenas empresas, pois o lockdown levou muitas delas a acelerarem suas transformações digitais e adotarem o modelo de trabalho híbrido. Agora, há mais de um ano na pandemia de Covid-19, essas empresas devem se preparar para mudar de marcha mais uma vez, conforme o mundo vive em seu novo normal - um que prioriza o modelo de trabalho híbrido e está, esperançosamente, no final de uma crise global de saúde.

Agentes mal-intencionados estão prontos para aproveitar as oportunidades que surgiram de um cenário de negócios ainda em evolução. Novos pontos problemáticos estão prestes a surgir à medida que a pressão por transformações digitais continua a redefinir as superfícies de ataque das organizações. No entanto, as empresas estarão preparadas para conter essas ameaças fortalecendo suas defesas com uma infinidade de ferramentas e práticas recomendadas.

Em 2022, as ameaças emergentes continuarão a testar a resiliência das cadeias de suprimentos em todo o mundo. O modelo de extorsão quádruplo que vem ganhando popularidade entre os agentes mal-intencionados, resultando em interrupções operacionais com impacto de longo alcance - não apenas nas próprias vítimas, mas também em seus clientes e parceiros.

Os que utilizam nuvem precisarão reforçar suas defesas em várias frentes, especialmente se quiserem resistir a ataques de agentes que usam metodologias testadas e comprovadas e inovam seguindo as tendências de tecnologia. A introdução de novas criptomoedas em 2022 exigirá que as equipes de segurança estejam atentas a quaisquer cibercriminosos que tentem se infiltrar e abusar dos recursos corporativos para seus recursos de computação em nuvem. Também acreditamos que os agentes mal-intencionados visarão cada vez mais os sistemas de construção e as credenciais do desenvolvedor como pontos de entrada para serviços e aplicações em nuvem. Consequentemente, os desenvolvedores terão que garantir que suas credenciais fiquem fora do alcance de invasores que procuram comprometer seus sistemas.

Esperamos que um número sem precedentes de vulnerabilidades seja descoberto no próximo ano, como resultado do número de caçadores de vulnerabilidades, que procuram coletar grandes recompensas através de bugs e do aumento da atenção da mídia sobre as vulnerabilidades. Prevemos que isso levará a um aumento de exploits de zero day que irá ultrapassar o número recorde de 2021 em uso ativo.[2] O patch gap deixará as empresas desprotegidas à mercê de agentes mal-intencionados ansiosos para localizar quaisquer pontos fracos em infraestruturas de TI, acumulando vulnerabilidades múltiplas para criar novas ameaças multiplataforma.

Vemos duas tendências se formando no ecossistema de ransomware em 2022. As empresas terão que se proteger contra ameaças de ransomware modernas, que são mais direcionadas e proeminentes. E os operadores de ransomware estarão empregando métodos de extorsão cada vez mais complexos, como extração de dados. Seus ataques representarão um desafio para as equipes de segurança, já que muitas empresas ainda precisam investir na proteção de seus servidores tanto quanto investiram na proteção de seus endpoints.

Enquanto as empresas estarão ocupadas se defendendo de ataques direcionados, os agentes mal-intencionados, equipados com ferramentas atualizadas, terão mais sucesso com empresas menores, em grande parte graças aos corretores de malware que vendem ferramentas mercantilizadas do comércio. A nova onda de malware deve chegar no ano que vem, provavelmente incluirá uma introdução a um modelo de botnet como serviço particularmente insidioso, capaz de comprometer várias plataformas.

Novos desenvolvimentos em dispositivos inteligentes irão alimentar o interesse crescente do submundo do crime cibernético na Internet das coisas (IoT), expandindo-se para além dos próprios dispositivos inteligentes. Em vez disso, os cibercriminosos irão lançar seus olhos sobre o volume cada vez maior de dados de carros conectados, uma mercadoria procurada que promete ser um novo fluxo de receita para as montadoras. Isso representará uma oportunidade para os fornecedores de segurança e fabricantes de automóveis se reunirem para redigir o roteiro para uma nova classe de carros inteligentes seguros.

Em última análise, 2022 será um período de transição repleto de possibilidades para empresas e cibercriminosos. Este relatório detalha as percepções e previsões de segurança de nossos especialistas em ameaças para o próximo ano, com o objetivo de ajudar as organizações a tomarem decisões fundamentadas em várias frentes de segurança.

Ameaças na Nuvem

As empresas irão aplicar pelo menos o básico de segurança na nuvem para defender seus ambientes contra uma série de ameaças de segurança e alcançar um nível de risco gerenciado.

Os invasores da nuvem irão dar uma volta e permanecer no local; eles mudarão para a esquerda para seguir as tendências de tecnologia e continuarão a usar ataques testados e comprovados para causar estragos em quem adota a nuvem.

A nuvem,[3] com sua capacidade aparentemente infinita de armazenar e processar grandes quantidades de dados, permitiu que as empresas fizessem a transição para o trabalho remoto com relativa facilidade após o início da pandemia Covid-19.[4] E no próximo ano, a migração para a nuvem continuará a ser um aspecto fundamental da nova norma de operações de negócios. A Gartner prevê que os gastos globais com serviços em nuvem chegarão a mais de US $ 482 bilhões em 2022, um aumento de 54% em relação aos US $ 313 bilhões de 2020.[5] E, à medida que os usuários migram continuamente para a nuvem, os agentes mal-intencionados devem seguir o exemplo.

Para maximizar seu ganho financeiro, os agentes mal-intencionados se certificarão de cobrir todas as bases. Eles continuarão a realizar tipos de ataques testados e comprovados e, ao mesmo tempo, irão realizar ataques focados nas novas tendências em tecnologia para se manter à frente do jogo.

Não apenas as empresas continuarão a usar aplicativos e soluções de software como serviço (SaaS), mas a adoção deverá se expandir no próximo ano. A Gartner prevê que os usuários de SaaS gastarão cerca de US $ 172 bilhões em 2022, o maior gasto entre todos os serviços de nuvem pública.[6] E porque as táticas, técnicas e procedimentos (TTPs) empregados por agentes mal-intencionados ainda estão funcionando - e provavelmente ainda funcionarão para uma nova safra de usuários de SaaS - eles continuarão a usá-los em 2022.

Agentes mal-intencionados continuarão usando estratégias de baixo esforço, mas de alto impacto para obter acesso a aplicações e serviços em nuvem. O uso de e-mails de phishing para roubar credenciais é um exemplo de método que persistirá no próximo ano. Eles também continuarão a comprometer aplicativos e serviços SaaS por meio de segredos não protegidos,[7] chaves de acesso não rotacionadas, imagens de contêiner não seguras obtidas de fontes não confiáveis[8] e políticas de gerenciamento de controle de acesso de identidade imaturas ou mal implementadas. Na verdade, os cibercriminosos geralmente gravitam em torno de estratégias que funcionam. Agentes mal-intencionados, por exemplo, ainda estão explorando vulnerabilidades conhecidas de anos anteriores porque muitos ambientes ainda não foram corrigidos. Além de explorar novas vulnerabilidades que serão descobertas no próximo ano, eles continuarão a usar as antigas que ainda funcionam.

Esperamos continuar vendo grupos cibercriminosos como o TeamTNT visando o poder da computação em nuvem para extrair criptomoedas ilicitamente no próximo ano.[9] À medida que mais moedas digitais surgem, as unidades cibercriminosos continuarão pegando carona nos recursos de computação em nuvem das vítimas e usando iterações de ataques vistos anteriormente.

Por outro lado, os cibercriminosos também seguirão as tendências de tecnologia. Qualquer tecnologia amplamente adotada torna-se um alvo lucrativo para os invasores, por exemplo, em como os agentes mal-intencionados têm como alvo tecnologias como Java,[10] Adobe Flash[11] e WebLogic.[12]

Um efeito colateral interessante, embora nefasto, do movimento shift-left é que os invasores começarão a usar cada vez mais essa abordagem em seus ataques. Já estamos vendo agentes mal-intencionados visando ferramentas e pipelines DevOps[13] em ambientes de desenvolvimento integrado em nuvem (IDEs).[14] Prevemos que os cibercriminosos farão mais campanhas usando os princípios DevOps em cadeias de suprimentos, ambientes Kubernetes, implementações de infraestrutura como código (IaC) e pipelines. Também prevemos que os desenvolvedores e sistemas de construção servirão como pontos de entrada inicial para invasores que procuram espalhar malware por várias empresas por meio de ataques à cadeia de suprimentos. Os tokens e senhas dos desenvolvedores são as chaves para as operações das empresas, e usar as credenciais comprometidas de desenvolvedor aumenta as chances de um invasor implantar malware sob o radar.

A adoção da nuvem é um elemento fundamental da transformação digital. Assim, é importante para as empresas manterem seus ambientes de nuvem seguros, voltando aos fundamentos da segurança em nuvem, que incluem a compreensão e aplicação do modelo de responsabilidade compartilhada,[15] usando uma estrutura bem arquitetada,[16] criptografando, corrigindo,[17] e trazendo o nível certo de especialização. As empresas também precisarão aplicar protocolos de segurança mais rígidos em torno dos sistemas de construção e do código que os desenvolvedores verificam, especialmente se o código enviado tiver participação em processos de produção importantes. Para esse fim, as equipes de segurança podem aplicar medidas como o gerenciamento de privilégios com tokens de acesso de curta duração, o desenvolvimento de uma trilha de auditoria usando ferramentas de linha de comando e o monitoramento do pipeline por meio de software de gerenciamento de segurança de código aberto.

Ameaças de Ransomware

Para permanecer protegido contra a evolução ameaças de ransomware, as empresas visam proteger seus servidores com medidas de segurança rigorosas e políticas de controle de aplicativos

Os servidores serão o principal playground do ransomware

Como qualquer ameaça cibernética insidiosa, o ransomware[18] sobrevive e prospera evoluindo constantemente. Antes, os incidentes de ransomware geralmente envolviam endpoints como pontos de entrada primários, com as vítimas sofrendo ataques através da abertura de e-mails maliciosos ou visitando sites maliciosos que distribuem cargas úteis de ransomware clandestinamente.[19] Mas quando a pandemia chegou, vimos uma mudança óbvia na forma como os operadores de ransomware realizavam seus ataques.

Agentes mal-intencionados, que desejam obter acesso a organizações-alvo, estão se concentrando em serviços expostos e abrangências de serviços. E como o trabalho híbrido, um modelo em que os funcionários trabalham remotamente e também nas empresas, se torna o novo normal das organizações,[20] prevemos que essa tendência continue no próximo ano. O modelo de trabalho híbrido tem muitos prós, como maior flexibilidade e produtividade, mas também vem com alguns contras inegáveis para a segurança cibernética. Devido ao aumento da superfície de ataque e servidores domésticos menos seguros, é difícil identificar como os agentes mal-intencionados estão entrando e realizando ataques - e como as equipes de segurança cibernética podem interromper os ataques de ransomware no momento inicial.

Com base nos incidentes de segurança que observamos este ano, também esperamos ver dois grandes desenvolvimentos de ransomware no próximo ano.[21] Primeiro, os ataques de ransomware se tornarão mais direcionados e altamente proeminentes, dificultando a defesa de redes e sistema contra esse ataques. Como o ransomware moderno é relativamente novo, é muito possível que as empresas ainda tenham que fazer os mesmos investimentos em mitigação e defesa de ransomware para servidores que fizeram para seus enpoints. Além disso, a contínua falta de especialistas qualificados em segurança cibernética é um fator agravante no que diz respeito à proteção das organizações contra ameaças de ransomware.[22] Os TTPs usados pelos operadores de ransomware provavelmente permanecerão os mesmos, mas serão usados para perseguir alvos mais complexos, superando as principais metas dos anos anteriores.

O segundo desenvolvimento que prevemos é que os métodos de extorsão utilizados pelos operadores de ransomware ficaram mais modernos e sofisticados, se assemelhando a ataques de ameaças persistentes avançadas (APT) do estado-nação.[23] Assim que os invasores conseguirem se infiltrar nos ambientes de suas vítimas, eles poderão optar por apenas exfiltrar dados confidenciais e ir direto extorquir suas vítimas, pulando a criptografia ou a etapa de bloqueio de acesso. Em termos de meios primários de extorsão bem-sucedida, o foco mudará da negação de acesso a dados críticos em detrimento do vazamento e mineração de dados roubados para uso em armas. Os vetores de ataque usados por operadores de ransomware para visar empresas, como redes privadas virtuais (VPNs), e-mails de spear-phishing e portas expostas de protocolo de desktop remoto (RDP), permanecerão em jogo. No entanto, em 2022, a nuvem será direcionada com mais frequência. À medida que mais empresas migram para a nuvem,[24] elas trazem seus dados e recursos confidenciais, fazendo com que os cibercriminosos façam o mesmo.[25]

Além de empregar as melhores práticas de segurança para manter os servidores seguros, as empresas se beneficiarão da adesão estrita às diretrizes de proteção de servidor para todos os sistemas operacionais e aplicativos pertinentes. Garantir que seus servidores estejam configurados corretamente ajudará a defender as empresas contra ataques de ransomware e outras ameaças.

Como os servidores têm um conjunto previsível de aplicações com base em suas funções específicas, também é aconselhável que as organizações empreguem o controle de aplicações. Essa prática de segurança permite o bloqueio e restrição de aplicativos, exceto aqueles que foram colocados na lista de segurança pelas equipes de TI.

Vulnerabilidade Exploits

As equipes de segurança devem estar bem equipadas na luta contra os agentes, que vem se adaptando as vulnerabilidades antigas e explorando novas em um questão de dias, se não horas

Devido ao recorde de exploits de zero day em 2021, as empresas se tornaram mais vigilantes, elas estão alertas em relação às potenciais lacunas de patch e esperam que mais vulnerabilidades sejam ser descobertas

O ano que vem promete rivalizar com o recorde histórico de exploits de zero que ajudou a moldar o cenário de ameaças de 2021: 66 exploits de zero day foram encontrados à solta no momento da redação deste relatório, maior número já registrado.[26] Prevemos que ainda mais exploits in-the-wild zero-day serão descobertos em 2022, o que não irá necessariamente sugerir uma queda na qualidade do código, pois será alimentado por vários fatores. Esses fatores incluirão o crescente interesse da mídia na cobertura de explorações que fazem manchetes, caçadores de vulnerabilidade ansiosos por obter recompensas lucrativas por bugs[27] como aquelas oferecidos pela Zero Day Initiative (ZDI) da Trend Micro em um esforço para evitar ataques de zero day,[28] e erros de implementação e omissões que surgirão à medida que mais empresas passarem por transformações digitais. É possível que apenas uma parte das vulnerabilidades exploradas ativamente seja encontrada pela indústria de segurança cibernética, então a descoberta de mais vulnerabilidades também apontará para métodos de detecção cada vez mais eficazes e mudanças de atitudes em torno da divulgação.[29] Programas de recompensa por bugs deram grandes passos em direção ao início detecção de vulnerabilidades para o benefício das empresas, conforme evidenciado pelos incentivos da ZDI, que contribuíram para o desenvolvimento de patches virtuais para os clientes da solução de segurança Trend Micro™ TippingPoint™, com uma média de 81 dias de antecedência do lançamento público do patch lançado por um fornecedor em 2020.[30]

No entanto, se o sucesso de concursos de hacking anteriores Pwn2Own[31] seguisse qualquer indicação, a janela para vulnerabilidades como arma seria reduzida para uma questão de dias, se não meras horas, e exploits seriam escritos para bugs corrigidos em beta antes que seus patches fossem lançados para o consumidor em geral. A lacuna do patch -o tempo entre a descoberta de uma vulnerabilidade e quando um patch é lançado para resolvê-la- permaneceria uma mina de ouro para atores oportunistas, que sem dúvida contariam com atrasos no lançamento das correções de bugs críticos e teriam mais tempo para desenvolver suas façanhas. Atrasos na implantação programada de patches podem ocorrer quando as correções de bugs precisam passar por testes de software, como foi o caso de uma correção para o mecanismo V8 JavaScript do Google Chrome, que foi disponibilizada aos usuários do navegador com o lançamento do Chrome 77 em setembro de 2019, um mês depois que o bug do V8 foi corrigido.[32] Isso deixou as empresas em uma posição difícil, pois enfrentaram o desafio duplo de antecipar exploits acelerados durante o período de espera do lançamento das correções do bug e então implementá-las assim que fossem lançados. Lidar com essas vulnerabilidades não é um processo uniforme; por exemplo, aplicar patches em endpoints é mais simples do que aplicar patches em servidores, o que muitas vezes acarreta mais custos de inatividade.[33]

Ao invés de estudar ativamente as linhas do código em busca de falhas, os agentes mal-intencionados começaram a recorrer aos patches como ponteiros convenientes para falhas do sistema para adaptar seu código de malware. Em 2022, um segmento dedicado de cibercriminosos ficará de olho nas empresas em antecipação a quaisquer vulnerabilidades divulgadas e patches implantados, o que os ajudará a agilizar seus ataques.

Os malfeitores não estão apenas planejando tirar proveito das vulnerabilidades recém-descobertas, mas também continuarão a capitalizar sobre as falhas mais antigas. Isso enfatizará ainda mais a necessidade de as empresas e seus fornecedores parceiros priorizarem o gerenciamento de patches. As vulnerabilidades encontradas nos anos anteriores permanecerão relevantes, pois os agentes mal-intencionados irão redirecioná-las e combiná-las para aumentar seus ataques no próximo ano.

Da mesma forma, haverá um influxo de ataques combinados que terão como alvo vários softwares por encadeamento, por exemplo, as vulnerabilidades no Google Chrome com as vulnerabilidades no Microsoft Windows, obtendo assim acesso privilegiado aos sistemas. Uma vantagem desse aumento de ataques é que ele inevitavelmente atrairá a atenção dos analistas de segurança para as superfícies de ataque menos exploradas. Esperamos ver mais pesquisas dedicadas à tecnologia do lado do servidor que irão lançar uma luz sobre pontos fracos das plataformas como Microsoft Exchange e SharePoint, mitigando o impacto de quaisquer ataques futuros em seus usuários finais.

A segurança nativa da nuvem também precisará ser uma prioridade entre as empresas, muitas das quais adotaram a nuvem depois que a pandemia acelerou suas transformações digitais. A dependência de muitos projetos nativos da nuvem em bibliotecas que são construídas em software de código aberto pode deixá-los expostos a ataques focados em vulnerabilidades conhecidas, visto que essas bibliotecas não são frequentemente atualizadas ou rotineiramente avaliadas quanto a falhas divulgadas publicamente.34 Para segurança equipes, é fundamental encontrar fontes confiáveis de falhas na nuvem para proteger os ativos digitais, pois ainda há uma falta de relatórios de vulnerabilidades e exposições comuns relacionadas à nuvem (CVE) relativos a bugs locais.[35]

Mais do que nunca, as empresas precisarão garantir que suas equipes de segurança de TI estejam bem posicionadas para se adaptar e lidar com esse aumento iminente dessas explorações. Isso envolverá fornecer a essas equipes o suporte e os recursos necessários para fazer o inventário dos dispositivos em um ambiente de TI por meio do gerenciamento de ativos, monitorar as atualizações de segurança dos fornecedores para que possam responder assim que as vulnerabilidades forem divulgadas publicamente e praticar o patching virtual[36] ou isolamento da máquina para proteger quaisquer pontos de entrada de uma ameaça potencial.

Ataques de malware de commodities

Agentes maliciosos irão continuar vendo pequenas empresas como presas fáceis, mas SMBs com muita nuvem virá preparado com segurança medidas que podem afastar ataques de commodities

Enquanto todos os olhos estão voltados para o ransomware, os ataques tradicionais de commodities e os ataques como serviço terão tempo para inovar ferramentas mais sofisticadas.

As empresas continuarão sendo presas lucrativas para os operadores de ransomware em busca de grandes pagamentos, então os caçadores de grandes jogos deixarão as pequenas e médias empresas (SMBs) ficam a mercê do ransomware como serviço (RaaS) e pequenos criminosos cibernéticos usando malware de commodities e mantendo perfis discretos.[37]

A atenção do público foi firmemente fixada no ransomware nos últimos anos, e o ransomware é considerado um tipo de malware comum e um modelo como serviço. Mas há outros tipos de malware disponíveis no mercado, como trojans de acesso remoto (RATs), ladrões de informações, mineradores de criptomoedas, droppers e carregadores de malware, que estarão circulando nos círculos cibercriminosos. Isso transformará o mercado de malware de commodities em uma ameaça insidiosa, mas formidável. Operadores de ransomware tiraram proveito de ferramentas de malware de commodities para tornar seus ataques mais eficazes,[38] enquanto outros agentes maliciosos usaram ferramentas de ataque de commodities para lançar campanhas politicamente motivadas.39 Operadores de ransomware também foram observados usando ferramentas de malware de commodities como Cobalt Strike, Koadic, PowerShell Empire e Metasploit[40] em conjunto com utilitários de administração de sistema existentes - uma técnica chamada “viver da terra” - para evitar a detecção.[41]

Essas ferramentas vêm com funcionalidades mais avançadas e preços acessíveis, tornando esse malware acessível a agentes mal-intencionados.[42] Muitas peças personalizadas de malware acabam sendo comoditizadas no submundo do crime cibernético,[43] o que nos leva a prever a próxima geração de cibercriminosos como sendo mais inovadora e melhor equipada do que a responsável pelo desenvolvimento de ransomware há cerca de 15 anos.[44] Prevemos que o mercado em torno de ferramentas de ataque de commodities não apenas amadurecerá ao lado de novos agentes mal-intencionados, como também irá expandir suas redes e se conectar com criminosos cibernéticos que pensam da mesma forma. Afinal, os vendedores não só fornecem malware pronto para uso, mas também aprimoram o negócio com instruções, dicas e guias de solução de problemas.[45]

O modelo de serviço, no qual o malware comum é vendido como parte de contratos de serviço ao invés uma compra única de malware, será adequado para agentes de nível inferior, que estão fadados a abandonar as ferramentas de malware para buscar parceiros confiáveis no crime à medida que se tornam invasores mais experientes. Essas colaborações levarão a atividades criminosas mais resilientes, conforme evidenciado pela forma que os agentes mal-intencionados reconstruiriam o botnet do malware Emotet usando o do trojan bancário Trickbot, poucos meses após a derrubada da própria infraestrutura da Emotet pelas autoridades policiais.[46] Com isso, prevemos que os ataques de commodities chegarão a um ponto em 2022 em que os agentes mal-intencionados começarão

a ter pouca necessidade de desenvolver um malware personalizado, pois esse malware só será necessário para o gerenciamento de suas afiliadas em um ataque direcionado complexo.

Considerando isso, o malware de commodities está muito atrasado para uma oferta mais sofisticada com a qual os agentes mal-intencionados possam atualizar seu arsenal. O próximo ano provavelmente verá a estreia de um botnet-as-a-service projetado para comprometer e controlar plataformas baseadas em nuvem e IoT simultaneamente, muito parecido com uma versão aprimorada do botnet ZeuS.[47] É possível que tal A ferramenta sairá do cenário da língua russa no submundo do cibercriminoso, devido ao seu cenário de malware notoriamente inovador, [48] mas o botnet FreakOut também está se preparando para ser um candidato à medida que continua a evoluir com recursos adicionais.[49]

Prevemos o mercado de ataque de commodities, cujo modelo de negócios depende do código de malware fazendo o trabalho braçal ao invés de um invasor se movendo dentro de uma rede, sendo amplamente ineficaz contra as defesas mais robustas mais comumente encontradas em configurações corporativas, como sistemas de segurança que usam aprendizado de máquina.[50] No entanto, prevemos que as ferramentas de malware de commodities terão mais sucesso em 2022, visando SMBs, empregadas por agentes mal-intencionados na esperança de encontrar menores defesas de segurança e menor concorrência de outros cibercriminosos. Especificamente, prevemos que os dispositivos IoT usados por SMBs serão os principais alvos de tais ataques. As SMBs, portanto, terão que ser mais criteriosas ao escolher os fornecedores, comprando seus dispositivos IoT de fabricantes que possuem um sólido histórico de patch.

Raramente as pequenas e médias empresas têm equipes de segurança dedicadas e, quando o fazem, essas equipes provavelmente são limitadas por recursos limitados, nos quais a segurança cibernética é apenas uma despesa operacional. Globalmente, os gastos com cibersegurança devem ultrapassar US$ 150 bilhões até o final de 2021,[51] mas as SMBs gastam apenas mais de US$40 bilhões anuais em soluções de segurança de TI, permanecendo em um mercado carente, no qual apenas as SMBs mais maduras retêm talentos internos de segurança .[52] Por causa de suas restrições de orçamento, prevemos que muitas SMBs farão da proteção de endpoints sua principal prioridade, seguida pela proteção de suas redes. Algumas pequenas e médias empresas podem estar ainda mais preparadas do que outras. Aquelas que são focadas no online, dependendo fortemente de plataformas e serviços baseados em nuvem, estarão mais cientes dos riscos representados pelo malware de commodity em suas operações de missão crítica, devido à natureza de seus negócios. Essas empresas são mais propensas a incluir a segurança em sua agenda, escrevendo soluções de segurança cibernética como parte de seu custo de vendas.

Ameaças no IoT

As empresas irão se esforçar para melhorar o monitoramento e a visibilidade da sua rede para proteger seus ambientes de TI contra ameaças decorrentes da adoção de IoT

As informações associadas à IoT se tornarão uma mercadoria quente no submundo do crime cibernético, levando as empresas a se preocupar com as lacunas de segurança que podem levar ao vazamento de dados ou adulteração.

Dispositivos inteligentes há muito tempo tem chamado atenção de agentes mal-intencionados, pois a capacidade computacional limitada da maioria dos dispositivos IoT deixa pouco espaço para segurança integrada.[53] Dispositivos IoT comprometidos têm sido usados em diferentes tipos de ataques, como ataques distribuídos de negação de serviço (DDoS).[54] Com mais organizações levadas a passar por transformações digitais para se manterem competitivas ou pelo menos operacionais durante o lockdown global, prevemos que as empresas, especialmente aquelas de manufatura inteligente, estarão mais expostas a ameaças cibernéticas à medida que transição para o modelo de trabalho híbrido caminha e elas continuam utilizando os serviços de conexão remota.

Para manter suas operações herméticas, mais empresas cujas forças de trabalho dependem de dispositivos IoT se voltarão para sistemas de prevenção e detecção de intrusão (IPSs / IDSs), ferramentas de perícia de rede (NFTs), ferramentas de detecção de anomalia de comportamento de rede (NBAD) e detecção e resposta de rede (NDR) ferramentas que podem ajudá-los a acompanhar de perto o que está acontecendo em suas redes no próximo ano. Os que adotaram a nuvem e dependem de fornecedores de segurança terceirizados terão que rastrear vigilantemente o uso de recursos para qualquer atividade anômala e proteger sua nuvem privada virtual (VPC) de ataques que podem ocorrer em sua infraestrutura e revisar os recursos de fornecedores em potencial para garantir que eles atendam às suas necessidades.

Mas em 2022, os agentes mal-intencionados terão aspirações mais elevadas que vão além do sequestro de dispositivos IoT como uma base de ataque para suas atividades criminosas ou como um meio de se mover lateralmente em uma rede. Os cibercriminosos logo se juntarão à corrida do ouro, à medida que mais montadoras - incluindo grandes nomes como General Motors, Honda e Toyota[55] - lucram com o tráfego de dados fornecido por carros conectados. Esses veículos vêm equipados com uma série de câmeras, lasers e outros sensores que registram coletivamente as condições de direção e o comportamento do motorista, incluindo as velocidades e distâncias de direção de um carro e os tipos de mídia de entretenimento consumidos por seus passageiros. Esses insights em tempo real têm uma infinidade de aplicações para clientes comerciais, dentre elas: medir o sucesso da publicidade, medir a demanda do consumidor e determinar descontos em seguros de automóveis com base em dados de direção.[56] Para montadoras, esses dados também podem ser usados para monitorar o desempenho de componentes de veículos, o que aumentaria suas próprias cadeias de abastecimento.[57]

A demanda por informações sobre carros inteligentes deve se tornar um novo negócio em expansão que está estimado em cerca de US$450 a US$ 750 bilhões até 2030,[58] sem sinais de perder força: 10 exabytes de dados estão previstos para vir de carros conectados mensalmente até 2025.[59] À medida que mais desses veículos pegam a estrada, os agentes mal-intencionados estão se preparados para lucrar com o aumento dessa conectividade, acreditamos que isso aumente a demanda por filtros de dados ilegais capazes de bloquear a comunicação de dados de risco ou hackers que podem limpar os registro de má direção de um carro inteligente. A arquitetura de carros inteligentes também pode ser simplificada se suas funções e processos de coleta de dados mais complexos forem transferidos para a nuvem-na verdade, muitos aplicativos e sistemas usados pelos modelos de carros inteligentes mais recentes já estão hospedados em servidores de back-end em nuvem[60] - mas isso pode deixar montadoras mais suscetível a outras ameaças, como ataques de negação de serviço (DoS) e man-in-the-middle (MitM).

Para que seus produtos sejam preparados para o futuro, os fabricantes de automóveis em 2022 precisarão trabalhar em estreita colaboração com os fornecedores de segurança para decidir coletivamente como irão se proteger. Exemplos dessa parceria já estão em andamento. Houve iniciativas iniciais como a Open EV Software Platform, liderada pelo Mobility in Harmony (MIH) Consortium e seus parceiros Arm, Microsoft e Trend Micro.[62] Há também uma colaboração entre a Volkswagen e a Microsoft que busca criar uma plataforma de nuvem baseada nos fabricantes de automóveis, que pode ser utilizada no desenvolvimento de soluções de direção automatizadas mais avançadas e seguras para carros conectados.[63] Mais projetos como esses estabelecerão as bases para a indústria automotiva desenvolver um sistema operacional dedicado para veículos inteligentes, com o objetivo final de um automotivo ecossistema construído em um sistema operacional unificado que possibilitará que futuros modelos de carros conectados venham equipados com recursos de segurança padronizados.

Ameaças na cadeia de abastecimento

À medida que as empresas se concentram em tornar suas cadeias de abastecimento mais robustas por meio da diversificação e regionalização, inicia-se a implementação de princípios de zero trust com a intenção de manter seus ambientes mais seguros

Cadeias de abastecimento globais estarão na mira de técnicas de extorsão quádrupla conforme as empresas evoluem suas operações.

A pandemia Covid-19 lançou um forte holofote sobre a fragilidade das cadeias de abastecimento. Enorme escassez econômica e atrasos surgiram por causa de vários fatores, incluindo aumento da demanda,[64] contêineres de embarque, escassez de trabalhadores,[65] e dependência de longa data de sistemas de produção mais enxutos, que é resultado do modelo de manufatura just-in-time.[66] Quando os problemas na cadeia de suprimentos se tornou um fardo mundial, o valor delas se ficou ainda mais evidente - não apenas para empresas em dificuldades, mas também para cibercriminosos desonestos, indiferentes, mas alimentados por uma pandemia global. Em particular, os ataques à cadeia de suprimentos estão cada vez mais interconectados com campanhas de ransomware neste ano, como exemplificado pelos ataques REvil/Sodinokibi[67] de alto perfil a grandes organizações, incluindo Quanta Computer,[68] JBS Foods,[69] e Kaseya.[70]

Se aproveitando da grande interrupção da cadeia de abastecimento, haverá um aumento no modelo de extorsão quádrupla[71] em 2022. Os agentes mal intencionados se aproveitarão seus ataques cibernéticos ao máximo, armando fortemente as vítimas de grandes nomes para elas paguem grandes somas de dinheiro por meio de um Técnica de extorsão quádrupla: reter os dados críticos da vítima para resgate, ameaçar vazar os dados e divulgar a violação, ameaçar ir atrás dos clientes da vítima e atacar a cadeia de suprimentos ou fornecedores da vítima.

Este ano, o grupo cibercriminoso DarkSide teve como alvo o Colonial Pipeline, o maior sistema de oleoduto refinado dos Estados Unidos. O grupo impediu que a empresa acessasse seus sistemas de computador e roubou mais de 100 GB de dados corporativos.[72] Foi observado que o grupo tem inovado constantemente suas estratégias de ataque, oferecendo também DDoS e serviços de call center.[73] Isso habilita os afiliados do DarkSide para lançar técnicas de extorsão quádrupla que podem afetar fortemente as cadeias de abastecimento. Consequentemente, os agentes mal-intencionados podem negar o acesso a dados críticos, como segredos de fabricação, impedir o acesso às máquinas usadas na produção ou entrar em contato com clientes e partes interessadas para pressionar as organizações vítimas a pagar.

As mudanças econômicas provocadas pela pandemia levarão as empresas a investir em seus processos de desenvolvimento da cadeia de abastecimento. Elas deverão focar na construção de operações de cadeia de suprimentos mais robustas por meio da diversificação. Por anos, os países têm favorecido a globalização, que tem sido criticada como a causa da excessiva dependência de muitos países na obtenção de suprimentos de uma única fonte geográfica.[74] Ao invés da globalização, as operações da cadeia de abastecimento serão regionalizadas, isso irá garantir que as empresas sejam capazes de lidar com demandas maiores e custos de produção voláteis. As estratégias de diversificação serão diferentes para todas as empresas - alguns elos da cadeia de abastecimento

serão locais, enquanto outros estarão em diferentes países ou regiões.

No entanto, a diversificação não é tarefa simples, realizá-la de forma adequada e segura pode ser um empreendimento caro e que consome muitos recursos. À medida que as organizações procuram fornecedores e fornecedores mais próximos de casa para reduzir os riscos econômicos e ajudar a manter as operações de negócios à tona, elas também podem estar inadvertidamente abrindo suas portas para riscos de segurança. Os fornecedores de longo prazo com os quais eles trabalham há anos serão substituídos por novas empresas que eles precisarão avaliar. Esses novos fornecedores podem oferecer aplicativos e serviços em nuvem com políticas de segurança que podem não estar à altura ou nem priorizar a segurança na nuvem.

O período durante o qual duas organizações alinham seus processos é crítico - e os agentes mal-intencionados podem realizar ataques direcionados para aproveitar as mudanças e o desconhecimento associado às novas parcerias. Por exemplo, um agente pode fingir ser alguém de um novo fornecedor e enviar um e-mail de spear-phishing pedindo ao destinatário que preencha informações relevantes da empresa em um site malicioso.

Para manter as cadeias de abastecimento seguras à medida que as empresas desenvolvem suas estratégias, elas devem aplicar a abordagem de Zero Trust em suas práticas de segurança.[75] O modelo de zero trust ajuda a proteger a maneira como as organizações interagem com outras empresas e trocam dados por meio de verificação contínua ao longo de toda a vida da conexão. Por meio desse modelo, as organizações podem ter certeza de que a saúde dos usuários, dispositivos, aplicações e serviços com os quais interagem é constantemente monitorada e avaliada.

Velocidade total para a segurança cibernética

Nossas previsões de segurança para 2022 descrevem as ameaças e riscos que surgiram baseada em pesquisas, observações e percepções de nossos especialistas sobre questões de segurança iminentes e tecnologias de segurança. Ao lidar com essas questões, as organizações se beneficiarão de uma estratégia de segurança cibernética holística e com multicamadas, que envolvem as seguintes recomendações:

Volte para o básico. Pode parecer extremamente simples, mas aderir às práticas recomendadas de segurança pode ajudar as organizações a combater a maioria das ameaças novas e antigas. Agentes mal-intencionados continuarão a explorar vulnerabilidades antigas em sistemas e aplicações, por isso é importante que as organizações estejam atentas às suas políticas de gerenciamento de patches. Isso as ajudará a evitar violações de dados e, subsequentemente, multas caras e danos à reputação. As empresas também devem compreender e aplicar o modelo de responsabilidade compartilhada e criptografar regularmente os dados críticos.

Aplique o modelo Zero Trust para manter as aplicações e ambientes seguros. As empresas podem melhorar sua postura de segurança aplicando o modelo Zero Trust, em que qualquer usuário ou dispositivo que tente se conectar a suas aplicações e então os sistemas precisarão ser verificados antes de receberem o acesso e continuamente depois disso - independentemente se o usuário ou dispositivo estiver dentro da rede ou não.

Aumente a segurança do servidor e use o controle de acesso. À medida que as organizações avançam em direção a um modelo de trabalho híbrido, é preciso implementar políticas de segurança que levem em consideração a natureza sem perímetro do local de trabalho pós-pandêmico. O acesso e o controle de aplicações permite que as organizações obtenham um controle melhor de sua segurança, mesmo quando os funcionários acessam aplicativos de trabalho confidenciais ou críticos e dados de qualquer lugar e de diferentes dispositivos.

Priorize a visibilidade. À medida que os funcionários continuam acessando aplicações, serviços, sistemas e bancos de dados em nuvem remotamente no próximo ano, é importante que as organizações tragam a visibilidade para ajudar a fortalecer suas defesas de segurança cibernética. As equipes de segurança devem estar cientes de todos os provedores de nuvem, contas e serviços, certificando-se de que estão configurados da forma mais segura possível. Isso ajudará a minimizar o risco de exposições indesejadas e configurações incorretas.

Mude para uma segurança mais forte com as soluções e nível de especialização corretos. Para proteger com sucesso seus sistemas e ambientes de ameaças em constante evolução, as organizações exigem soluções de segurança flexíveis, automatizadas e avançadas que detectem ataques em e-mails, endpoints, redes, servidores e workloads em nuvem com eficiência. A Trend Micro fornece detalhes de investigação completos e insights de um time de segurança que têm acesso a análises abrangentes, soluções de segurança poderosas e inteligência global de ameaças.

Referências

1. Julie Steenhuysen. (Nov. 3, 2021). *Reuters.* "Analysis: Country by country, scientists eye beginning of an end to the COVID-19 pandemic." Accessed on Nov. 25, 2021, at https://www.reuters.com/business/healthcare-pharmaceuticals/country-by-country scientists-eye-beginning-an-end-covid-19-pandemic-2021-11-03/.
2. Joe Devanesan. (Oct. 20, 2021). *TechHQ.* "2021 was a record-breaking year in zero-day exploits – that's both good and bad news." Accessed on Nov. 19, 2021, at https://techhq.com/2021/10/2021-was-a-record-breaking-year-in-zero-day-exploits-and-thats both-good-and-bad-news/.
3. Trend Micro. (Oct. 24, 2019). *Trend Micro Security News.* "The Cloud: What it is and what it's for." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/the-cloud-what-it-is-and-what-it-s-for.
4. Trend Micro. (Oct. 7, 2020). *Trend Micro Security News.* "CSO Insights: DataBank's Mark Houpt on Looking Beyond Securing Infrastructures in the New Normal." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/news/security technology/cso-insights-databank-mark-houpt-on-looking-beyond-securing-infrastructures-in-the-new-normal/.
5. Bernard Marr. (Oct. 25, 2021). *Forbes.* "The 5 Biggest Cloud Computing Trends In 2022." Accessed on Nov. 10, 2021, at https://www.forbes.com/sites/bernardmarr/2021/10/25/the-5-biggest-cloud-computing-trends-in-2022/.
6. Gartner. (Aug. 2, 2021). *Gartner.* "Gartner Says Four Trends Are Shaping the Future of Public Cloud." Accessed on Nov. 10, 2021, at https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public cloud.
7. David Fiser and Alfredo Oliveira. (June 29, 2021). *Trend Micro Research, News, and Perspectives.* "Secure Secrets: Managing Authentication Credentials." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/21/f/secure_secrets_ managing_authentication_credentials.html.
8. Chuck Losh. (May 18, 2021). *Trend Micro Research, News, and Perspectives.* "Container Security First Steps: Image and Registry Scanning." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/devops/21/e/container-security-first-steps-image and-registry-scanning.html.
9. Trend Micro. (July 20, 2021). *Trend Micro Security News.* "TeamTNT Activities Probed: Credential Theft, Cryptocurrency Mining, and More." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ teamtnt-activities-probed.
10. 10. Trend Micro. (Sept. 10, 2013). *Trend Micro Research, News, and Perspectives.* "How the Java Security Situation Quietly Got Much Worse." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/13/i/java-security-situation-quietly-got-much worse.html.
11. Trend Micro. (Feb. 2, 2015). *Trend Micro Research, News, and Perspectives.* "New Adobe Flash 0-Day Exploit Used in Malvertisements." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/15/b/trend-micro-discovers-new adobe-flash-zero-day-exploit-used-in-malvertisements.html.
12. Catalin Cimpanu. (May 1, 2020). *ZDNet.* "Oracle warns of attacks against recently patched WebLogic security bug." Accessed on Nov. 10, 2021, at https://www.zdnet.com/article/oracle-warns-of-attacks-against-recently-patched-weblogic-security-bug/.
13. Trend Micro. (n.d.). *Trend Micro Security News.* "DevOps Definition Page." Accessed on Nov. 10, 2021, at https://www.trendmicro. com/vinfo/us/security/definition/devops.
14. David Fiser. (March 4, 2020). *Trend Micro Research, News, and Perspectives.* "Security Risks in Online Coding Platforms." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/research/20/c/security-risks-in-online-coding-platforms.html.
15. Trend Micro. (May 14, 2020). *Trend Micro Security News.* "Cloud Security: Key Concepts, Threats, and Solutions." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/cloud-security-key-concepts threats-and-solutions.
16. Melissa Clow. (Dec. 16, 2020). *Trend Micro Research, News, and Perspectives.* "A Guide to the Well-Architected Framework." Accessed on Nov. 10, 2021, at https://www.trendmicro.com/en_us/devops/20/l/well-architected-framework-guide.html.
17. Trend Micro. (March 4, 2021). *Trend Micro Security News.* "Security 101: Virtual Patching." Accessed on Nov. 10, 2021, at https:// www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching.
18. Trend Micro. (n.d.) *Trend Micro Security News.* "Ransomware Definition Page." Accessed on Nov. 8, 2021, at https://www. trendmicro.com/vinfo/us/security/definition/ransomware.

19. Trend Micro. (Sept. 28, 2017). *Trend Micro Security News.* "Spam, BEC, Ransomware: The Continuing Abuse of Email by Old and New Threats." Accessed on Nov. 8, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-spam-bec-ransomware-the-continuing-abuse-of-email-by-old-and-new-threats.
20. Dinesh Malkani. (June 4, 2021). *Forbes.* "Going Hybrid: The Future Of Work Is Here." Accessed on Nov. 8, 2021, at https://www.forbes.com/sites/forbestechcouncil/2021/06/04/going-hybrid-the-future-of-work-is-here/.
21. Trend Micro. (Sep. 14, 2021). *Trend Micro.* "Attacks From All Angles: 2021 Midyear Cybersecurity Report." Accessed on Nov. 19, 2021, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles 2021-midyear-security-roundup.
22. Robert Lemos. (Oct. 27, 2021). *Dark Reading.* "Cybersecurity Talent Gap Narrows as Workforce Grows." Accessed on Nov. 22, 2021, at https://www.darkreading.com/careers-and-people/cybersecurity-talent-gap-narrows-as-workforce-grows.
23. Trend Micro. (June 8, 2021). *Trend Micro Security News.* "Modern Ransomware's Double Extortion and How to Protect Enterprises Against Them." Accessed on Nov. 19, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.
24. Trend Micro. (April 14, 2020). *Trend Micro Security News.* "Undertaking Security Challenges in Hybrid Cloud Environments." Accessed on Nov. 8, 2021, at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/undertaking-security challenges-in-hybrid-cloud-environments.
25. Claudia Glover. (Oct. 11, 2021). *Tech Monitor.* "Ransomcloud: How and why ransomware is targeting the cloud." Accessed on Nov. 8, 2021, at https://techmonitor.ai/technology/cybersecurity/ransomcloud.
26. 26. Patrick Howell O'Neill. (Sept. 23, 2021). *MIT Technology Review.* "2021 has broken the record for zero-day hacking attacks." Accessed on Nov. 5, 2021, at https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons.
27. Trend Micro. (July 13, 2021). *Trend Micro Security News.* "Trends and shifts in the underground N-day exploit market." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/trends-and-shifts-in-the underground-n-day-exploit-market.
28. Trend Micro. (May 19, 2021). *Trend Micro Newsroom.* "Trend Micro's Zero Day Initiative Enhances Position as World's Largest Vulnerability Disclosure Player." Accessed on Nov. 25, 2021, at https://newsroom.trendmicro.com/2021-05-19-Trend-Micros-Zero Day-Initiative-Enhances-Position-as-Worlds-Largest-Vulnerability-Disclosure-Player.
29. Clement Lecigne and Maddie Stone. (July 14, 2021). *Google.* "How we protect users from 0-day attacks." Accessed on Nov. 5, 2021, at https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks.
30. Jon Clay. (April 28, 2021). *Trend Micro Research, News, and Perspectives.* "How Trend Micro Helps Manage Exploited Vulnerabilities." Accessed on Dec. 3, 2021, at https://www.trendmicro.com/en_us/research/21/d/how-trend-micro-helps-manage exploited-vulnerabilities.html.
31. Charlie Osborne. (July 14, 2021). *ZDNet.* "Microsoft July 2021 Patch Tuesday: 117 vulnerabilities, Pwn2Own Exchange Server bug fixed." Accessed on Nov. 5, 2021, at https://www.zdnet.com/article/microsoft-july-2021-patch-tuesday-117-vulnerabilities pwn2own-exchange-server-bug-fixed.
32. Catalin Cimpanu. (Sept. 10, 2019). *ZDNet.* "Security researchers expose another instance of Chrome patch gapping." Accessed on Dec. 1, 2021, at https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping.
33. Trend Micro. (April 7, 2021). *Trend Micro Research, News, and Perspectives.* "The Nightmares of Patch Management: The Status Quo and Beyond." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond.
34. 34. Magno Logan. (Oct. 8, 2021). *Trend Micro Security News.* "Minding the Gaps: The State of Vulnerabilities in Cloud Native Applications." Accessed on Nov. 17, 2021, at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/minding-the-gaps-the-state-of-vulnerabilities-in-cloud-native-applications.
35. Shaun Nichols. (Nov. 2, 2021). *TechTarget.* "Why cloud bugs don't get CVEs, and why it's an issue." Accessed on Nov. 17, 2021, at https://searchsecurity.techtarget.com/news/252508948/Why-cloud-bugs-dont-get-CVEs-and-why-its-an-issue.
36. Trend Micro. (March 4, 2021). *Trend Micro Research.* "Security 101: Virtual Patching." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching.
37. Trend Micro. (Aug. 28, 2018). *AP News.* "Trend Micro Report Reveals Criminals Increasingly Drawn To Low-Profile Attacks." Accessed on Nov. 5, 2021, at https://apnews.com/press-release/pr-businesswire/7f2907b6661b426c855e4875511266e1.

38. BSI Staff. (July 26, 2021). *The British Standards Institution.* "How your business can adapt to cybersecurity trends." Accessed on Nov. 21, 2021, at https://shop.bsigroup.com/articles/how-your-business-can-adapt-to-cybersecurity-trends.
39. David Agranovich and Mike Dvilyanski. (Nov. 16, 2021). *Meta.* "Taking Action Against Hackers in Pakistan and Syria." Accessed on Nov. 21, 2021, at https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria.
40. VMWare. (Oct. 11, 2021). *VMWare Security Blog.* "Moving Left of the Ransomware Boom." Accessed on Nov. 25, 2021, at https://blogs.vmware.com/security/2021/10/moving-left-of-the-ransomware-boom.html.
41. Lucian Constantin. (March 19, 2021). *CSO Online.* "Ryuk ransomware explained: A targeted, devastatingly effective attack." Accessed on Nov. 25, 2021, at https://www.csoonline.com/article/3541810/ryuk-ransomware-explained-a-targeted-devastatingly effective-attack.html.
42. Jaromir Horejsi and Daniel Lunghi. (Sept. 13, 2021). *Trend Micro Research, News, and Perspectives.* "APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html.
43. National Cyber Security Centre. (Oct. 6, 2016). *National Cyber Security Centre.* "Common Cyber Attacks: Reducing The Impact." Accessed on Nov. 21, 2021, at https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact.
44. Trend Micro. (n.d.). *Trend Micro Security News.* "Ransomware Definition." Accessed on Nov. 21, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/ransomware.
45. Numaan Huq et al. (June 28, 2019). *Trend Micro Research.* "Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground.
46. Lawrence Abrams. (Nov. 15, 2021). *BleepingComputer.* "Emotet malware is back and rebuilding its botnet via TrickBot." Accessed on Nov. 22, 2021, at https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via trickbot.
47. Bernadette Caraig. (n.d.). *Trend Micro Threat Encyclopedia.* "The ZeuS, ZBOT, and Kneber Connection." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/16/the-zeus-zbot-and-kneber-connection.
48. Joshua Yaffa. (May 23, 2021). *The New Yorker.* "How Hacking Became a Professional Service in Russia." Accessed on Nov. 21, 2021, at https://www.newyorker.com/news/news-desk/how-hacking-became-a-professional-service-in-russia.
49. Catalin Cimpanu. (Jan. 19, 2021). *ZDNet.* "New FreakOut botnet targets Linux systems running unpatched software." Accessed on Nov. 5, 2021, at https://www.zdnet.com/article/new-freakout-botnet-targets-linux-systems-running-unpatched-software/.
50. Trend Micro. (n.d.). *Trend Micro Security News.* "Machine Learning." Accessed on Nov. 22, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/machine-learning.
51. Gartner. (May 17, 2021). *Gartner.* "Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021." Accessed on Nov. 22, 2021, at https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts worldwide-security-and-risk-managem.
52. Bharath Aiyer, Venky Anant, and Daniele Di Mattia. (March 24, 2021). *McKinsey.* "Securing small and medium-size enterprises: What's next?" Accessed on Nov. 22, 2021, at https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/securing-small-and-medium-size-enterprises-whats-next.
53. Trend Micro. (May 28, 2020). *Trend Micro Security News.* "Smart Yet Flawed: IoT Device Vulnerabilities Explained." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device vulnerabilities-explained.
54. Trend Micro. (July 22, 2021). *Trend Micro Security News.* "IoT Security Issues, Threats, and Defenses." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses.
55. Trend Micro. (Oct. 11, 2021). *Trend Micro Research, News, and Perspectives.* "Honda to Start Selling Smart Car Data." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/j/honda-to-start-selling-smart-car-data.html.
56. Kotaro Abe and Ryotaro Yamada. (Sept. 29, 2021). *Nikkei Asia.* "Honda joins $400bn gold rush to monetize smart car data." Accessed on Nov. 5, 2021, at https://asia.nikkei.com/Business/Technology/Honda-joins-400bn-gold-rush-to-monetize-smart car-data.
57. Anthony Spadafora. (Nov. 18, 2020). *TechRadar.* "Amazon and NXP team up on smart car cloud computing deal." Accessed on Nov. 17, 2021, at https://www.techradar.com/news/amazon-and-nxp-team-up-on-smart-car-cloud-computing-deal.

58. Mark Minevich. (July 13, 2020). *Forbes.* "The Automotive Industry And The Data Driven Approach." Accessed on Nov. 5, 2021, at https://www.forbes.com/sites/markminevich/2020/07/13/the-automotive-industry-and-the-data-driven-approach/.
59. Toyota Motor Corporation. (Aug. 10, 2017). *Toyota Motor Corporation.* "Industry leaders to form consortium for network and computing infrastructure of automotive big data." Accessed on Nov. 5, 2021, at https://global.toyota/en/detail/18135029.
60. Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). *Trend Micro Research.* "In Transit, Interconnected, At Risk: Cybersecurity Risks of Connected Cars." Accessed on Nov. 17, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.
61. Trend Micro. (Feb. 6, 2021). *Trend Micro Research, News, and Perspectives.* "Connected Cars, 5G, the Cloud: Opportunities and Risks." Accessed on Nov. 17, 2021, at https://www.trendmicro.com/en_us/research/21/b/connected-cars-5g-the-cloud opportunities-and-risks.html.
62. MIH Consortium. (Oct. 20, 2021). *MIH Consortium.* "MIH Unveils Open EV Software Platform and Announces key partnerships with Arm, Microsoft and Trend Micro." Accessed on Nov. 5, 2021, at https://www.mih-ev.org/en/news-info/?id=695.
63. Microsoft. (Feb. 10, 2021). *Microsoft News Center.* "Volkswagen Group teams up with Microsoft to accelerate the development of automated driving." Accessed on Nov. 17, 2021, at https://news.microsoft.com/2021/02/10/volkswagen-group-teams-up-with microsoft-to-accelerate-the-development-of-automated-driving.
64. Garth Friesen. (Sep. 3, 2021). *Forbes.* "No End In Sight For The COVID-Led Global Supply Chain Disruption." Accessed on Nov. 25, 2021, at https://www.forbes.com/sites/garthfriesen/2021/09/03/no-end-in-sight-for-the-covid-led-global-supply-chain disruption/.
65. Elizabeth Harris. (Oct. 4, 2021). *The New York Times.* "'The Beginning of the Snowball': Supply-Chain Snarls Delay Books." Accessed on Nov. 25, 2021, at https://www.nytimes.com/2021/10/04/books/book-publishing-supply-chain-delays.html.
66. Peter S. Goodman and Niraj Chokshi. (June 1, 2021). *The New York Times.* "How the World Ran Out of Everything." Accessed on Nov. 25, 2021, at https://www.nytimes.com/2021/06/01/business/coronavirus-global-shortages.html.
67. Trend Micro Research. (Jan. 26, 2021). *Trend Micro Research, News, and Perspectives.* "Examining A Sodinokibi Attack." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html.
68. Michael Novinson. (April 23, 2021). *CRN.* "Apple Menaced After REvil Ransomware Attack Against Supplier." Accessed on Nov. 5, 2021, at https://www.crn.com/news/security/apple-menaced-after-revil-ransomware-attack-against-supplier.
69. Trend Micro Research. (May 12, 2021). *Trend Micro Research, News, and Perspectives.* "What We Know About the DarkSide Ransomware and the US Pipeline Attack." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/e/what we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html.
70. Trend Micro Research. (July 4, 2021). *Trend Micro Research, News, and Perspectives.* "IT Management Platform Kaseya Hit With Sodinokibi/REvil Ransomware Attack." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/en_us/research/21/g/it management-platform-kaseya-hit-with-sodinokibi-revil-ransomwa.html.
71. anus Agcaoili et al. (June 15, 2021). *Trend Micro Security News.* "Ransomware Double Extortion and Beyond: REvil, Clop, and Conti." Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.
72. Trend Micro. (Sept. 14, 2021). *Trend Micro.* "Attacks From All Angles: 2021 Midyear Cybersecurity Report." Accessed on Nov. 25, 2021, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles 2021-midyear-security-roundup.
73. Brian Krebs. (May 11, 2021). *Krebs On Security.* "A Closer Look at the DarkSide Ransomware Gang." Accessed on Nov. 25, 2021, at https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/.
74. Chad P. Bown and Douglas A. Irwin. (Oct. 14, 2021). *The New York Times.* "Why Does Everyone Suddenly Care About Supply Chains?" Accessed on Nov. 6, 2021, at https://www.nytimes.com/2021/10/14/opinion/supply-chain-america.html.
75. Trend Micro. (Aug. 13, 2021). *Trend Micro Research, News, and Perspectives.* "What Is Zero Trust and Why Does It Matter?" Accessed on Nov. 9, 2021, at https://www.trendmicro.com/en_us/ciso/21/h/what-is-zero-trust-and-why-does-it-matter.html.

EM DIREÇÃO A UM NOVO MOMENTO

PREVISÕES DE TREND MICRO SECURITY PARA 2022

TREND MICRO | research

TREND MICRO™ RESEARCH

A Trend Micro, líder global em segurança cibernética, ajuda a tornar o mundo seguro para a troca de informações digitais.

A Trend Micro Research é desenvolvida por especialistas apaixonados por descobrir novas ameaças, compartilhar ideias importantes e apoiar os esforços para impedir os cibercriminosos. Nossa equipe global ajuda a identificar milhões de ameaças diariamente, lidera o setor em divulgações de vulnerabilidades e publica pesquisas inovadoras sobre novas técnicas de ameaças. Trabalhamos continuamente para antecipar novas ameaças e fornecer pesquisas estimulantes.

www.trendmicro.com