TENDÊNCIAS EM CIBERSEGURANÇA PARA 2021:

mantendo a segurança
em tempos de incertezas

ÍNDICE

INTRODUÇÃO
3 — 4

1 **O FUTURO DO TRABALHO:** abraçando o novo normal
5 — 7

2 **RANSOMWARE COMO FORMA DE CHANTAGEM:**
pague pelos seus dados ou eles serão divulgados
8 — 10

3 **PARA ALÉM DAS TECNOLOGIAS DE PREVENÇÃO:**
Acompanhando de perto as areias movediças das ameaças cibernéticas
11 — 13

4 **MÁS VIBRAÇÕES:**
As diversas vulnerabilidades dos brinquedos sexuais inteligentes
14 — 17

CONCLUSÃO
18 — 19

INTRODUÇÃO

A pandemia de Covid-19 causou um choque no "sistema", empurrando muitos de nós para uma onda de preocupação e dando um novo significado à permanência da mudança. E agora? Uma das grandes perguntas é: como será 2021?

O ano de 2020 não foi previsto por ninguém, e é claro que não estamos falando apenas de segurança da informação. A pandemia de Covid-19 foi um choque para todos nós, e representou uma mudança de paradigma e hábitos que certamente acarretará consequências muito profundas, as quais ainda não podemos estimar. A questão então é: como falar sobre o que pode acontecer em 2021 depois de um ano como o que acabamos de viver? E a verdade é que apesar de representar um desafio, acreditamos que a melhor forma de estimar tendências é relatando alguns acontecimentos que vêm ocorrendo para melhor entendê-los e, assim, tentar estabelecer um possível desdobramento do que podemos esperar para o futuro.

Durante 2020, um campo em que vimos uma das maiores mudanças é o do trabalho, e poderíamos dizer que algo que vinha surgindo há bastante tempo se concretizou. O problema é que a implementação do trabalho remoto de forma massiva, em vez de ocorrer gradativamente, aconteceu de forma brutal, apressada e em meio a um cotidiano e uma situação social sem controle. Soma-se a isso o fato de que os cibercriminosos se adaptaram rapidamente a essas situações e começaram a explorar as oportunidades que a adoção improvisada do trabalho remoto lhes apresentou. Empresas mal preparadas a nível técnico e de conhecimento, colaboradores sem consciência do uso seguro e correto das ferramentas à sua disposição e uma situação extrema nos obrigam a adaptar e repensar algumas das lógicas e paradigmas que até então eram usados no ambiente de trabalho. No capítulo *"O futuro do trabalho"*, Jake Moore nos apresenta os diferentes aspectos de segurança de um dos temas mais debatidos durante 2020, que certamente continuará sendo discutido no próximo ano.

A essa altura, não restam dúvidas sobre o fato de que a tecnologia está entrelaçada em todos os aspectos da vida humana, e o ano de 2020 foi o exemplo mais claro de como hoje a vasta maioria dos processos e práticas humanas têm alguma conexão com a tecnologia. Já faz alguns anos que falamos da Internet das Coisas (IoT), mas uma faceta que talvez não seja muito mencionada é a aplicação da tecnologia na sexualidade. O surgimento de brinquedos sexuais conectados à Internet não foi uma novidade em 2020, embora o aumento nas vendas desse tipo de dispositivo tenha sido resultado das diferentes medidas de distanciamento social geradas pela pandemia de Covid-19. Além disso, já sabemos que os cibercriminosos estão constantemente procurando obter acesso a informações confidenciais e privadas de usuários, algo que conseguem acessando um dispositivo vulnerável, como um computador, um telefone celular ou um brinquedo sexual. Em *"Más vibrações"*, Denise Giusto e Cecilia Pastorino investigam o tema e o que o futuro reserva para nós.

O ransomware, por sua vez, vem se fortalecendo há vários anos. Uma vez que a infecção se torna evidente para os usuários, seu funcionamento é bastante impressio-

nante. Trata-se de um código malicioso que não passa despercebido, tal como acontece com muitos outros. Mas além de sua "popularidade", cujo ponto mais alto pode ter sido o WannaCry e sua infecção global em 2017, temos acompanhado algumas mudanças no comportamento daqueles que criam e espalham esse tipo de ameaça nos últimos anos. Sua operação "tradicional", que implicava o sequestro de informações e o pedido de resgate para restaurar o acesso a elas, agora ganhou mecanismos de extorsão e ameaça de divulgação das informações roubadas. No capítulo *"Ransomware como forma de chantagem"*, Tony Anscombe analisa essa tendência e o que ela reserva para o futuro a respeito desse código malicioso.

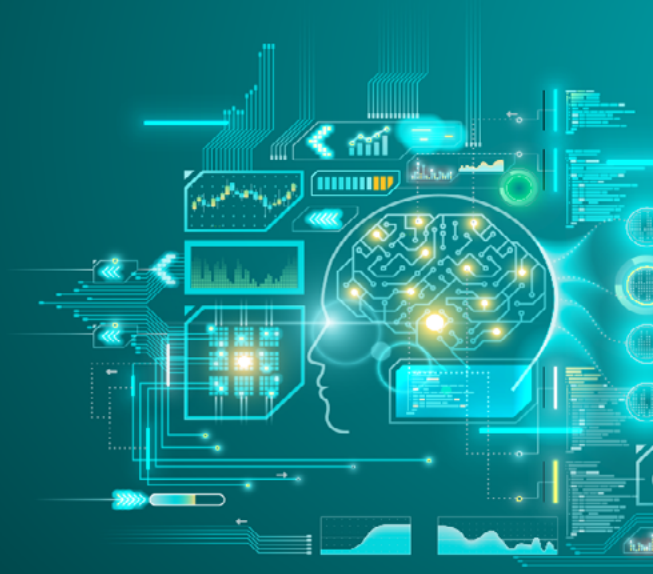
E assim como os criadores de ransomwares não ficam parados, aqueles que adotam outros códigos maliciosos para obterem créditos fraudulentos tampouco param. É por isso que, recentemente, temos testemunhado o uso cada vez mais comum de LOLBaS (Living Off the Land Binaries and Scripts), que consiste no uso de binários do próprio sistema para realizar atividades maliciosas. Em *"Para além das tecnologias de prevenção"*, Camilo Gutiérrez conta como funciona esse tipo de ameaça, que se tornou um desafio para as organizações devido à dificuldade de ser detectada, podendo se tornar um problema ainda maior se não for levada em consideração ao definir os controles de segurança correspondentes.

Depois de um ano que no futuro certamente será visto como um ponto de inflexão para muitas transformações sociais, acreditamos que rever diferentes situações, como as que surgem nos quatro capítulos deste relatório, torna-se uma tarefa imprescindível para tentarmos revelar o que podemos esperar no futuro próximo.

1

O FUTURO DO TRABALHO:

ABRAÇANDO O NOVO NORMAL



2020 foi o ano em que as empresas fizeram a transição para o trabalho remoto, mas quem de fato ajudou a levar essas empresas por meio da digitalização acelerada? Foram os CEOs, CTOs ou, para ser mais sincero, foi a Covid-19? E como será o trabalho após a pandemia?

Jake Moore
ESET Security Specialist

Desde que os governos ao redor do mundo implementaram os isolamentos pela Covid-19, a realidade do trabalho mudou drasticamente, de tal forma que a maioria das pessoas não poderia ter imaginado. E o resultado? *Implementação em massa do trabalho remoto,* que depende da tecnologia mais do que nunca, juntamente com a disrupção resultante das infraestruturas de tecnologia de diversas empresas. Os sistemas centrais de TI foram substituídos por uma rede de indivíduos distintos, todos com maior responsabilidade pelo uso de sua própria tecnologia e necessidades de segurança cibernética. Um sistema de segurança com falhas não apenas deixa as empresas vulneráveis, mas também a confiança dos funcionários em lidar com a segurança cibernética é um risco sério.

Em um momento em que as empresas dependem da resiliência, pessoas mal-intencionadas exploram continuamente as vulnerabilidades de segurança que acompanham o trabalho remoto. É claro que existem maneiras de tornar nossos novos ambientes mais seguros. Medidas simples podem ser postas em prática para ajudar a reduzir a chance de sofrermos ataques cibernéticos – mas ir de um ou dois escritórios para dezenas, até mesmo centenas de escritórios em casa, geralmente tem um preço.

O QUE A COVID-19 NOS ENSINOU

A pandemia não só nos ensinou como é possível trabalhar em casa, mas também como as empresas podem criar e aplicar políticas em questão de semanas. Realocar toda a força de trabalho normalmente levaria meses de planejamento, revisões intermináveis e, ainda, mais planejamento antes de ser aprovado por múltiplas partes. Mas quando o próprio governo é quem informa que não se tem mais permissão para entrar nos escritórios, é surpreendente a rapidez com que essas mudanças podem entrar em vigor e até mesmo manter a empresa operando sem interrupção quando as coisas ficam difíceis.

Algumas questões, no entanto, ainda pairam sobre nós: como podemos garantir a segurança da informação quando os funcionários trabalham de forma remota? Trabalhar de casa é tão seguro quanto no escritório? Será que algum dia voltaremos à vida de escritório de 2019?

Para serem resilientes contra ataques cibernéticos, muitas empresas têm políticas fortes e avaliações de risco em andamento. Muitas também possuem proteção para resistir à grande maioria das ameaças que qualquer empresa normal esperaria sofrer. No entanto, é improvável que qualquer organização no mundo estivesse inteiramente preparada para essa enorme e rápida mudança no trabalho quando a pandemia provocada pela Covid-19 começou. As paredes físicas do escritório atuam como um grande firewall, e qualquer movimento anormal na rede pode ser facilmente descoberto. Mas quando todos na organização passam a se conectar a uma rede de fora da malha de segurança do perímetro usual, o diretor de segurança da informação (CISO) e outras partes envolvidas podem enfrentar algumas tarefas assustadoras.

De uma forma ou de outra, o trabalho remoto claramente veio para ficar por um longo tempo, mas realizá-lo de forma eficiente requer contar com uma excelente gestão corporativa, assim como políticas de segurança perfeitamente integradas. Para que as empresas funcionem sem problemas com disrupção mínima, é necessário garantir que as práticas de gerenciamento e segurança desempenhem um papel igual, o que, por sua vez, protege seus funcionários e os negócios. Algumas organizações não souberam muito bem como proceder quando as instruções diziam para alocarem suas equipes em casa, mas outras aceitaram a mudança e até mesmo a consideraram mais produtiva.

O treinamento pode ajudar muito na proteção das equipes de trabalho, e funciona melhor quando é realizado com frequência e de forma gradual. Isso pode ser, por exemplo, por meio de lembretes rápidos sobre a importância das ***redes privadas virtuales (VPN)*** e da conscientização sobre e-mails de phishing para manter as pessoas atentas, mas sem frustrá-las ou assustá-las.

ANTES *VERSUS* DEPOIS

Antes da Covid-19, os ataques cibernéticos já estavam aumentando, e a pandemia e o isolamento resultante apenas aumentaram esse risco. De golpes de phishing a malware relacionados à Covid-19, os cibercriminosos têm se aproveitado de vulnerabilidades que surgem do trabalho descentralizado e dos sistemas de TI para encontrar falhas e explorá-las.

O trabalho remoto trouxe flexibilidade, mas também alterou drasticamente os processos e sistemas de negócios para atender a uma força de trabalho distribuída. O acesso dos funcionários aos departamentos de TI, e vice-versa, mudou. A colaboração e o trabalho em equipe são facilitados virtualmente, e a falta de comunicação face a face pode prejudicar os canais diretos de comunicação. Algumas das medidas básicas de segurança tidas como certas nos escritórios devem ser compensadas em casa, como exigir que os funcionários remotos usem ***autenticação em dois fatores*** ou VPN para acessar redes internas. Lembrá-los de que devem habilitar atualizações automáticas e verificar a segurança de suas próprias redes Wi-Fi também é crucial enquanto primeira linha de defesa contra cibercriminosos. Idealmente, os funcionários que trabalham de forma remota devem utilizar dispositivos fornecidos pela empresa, ficando sempre atentos a essas ameaças constantes e persistentes.

A mudança repentina em nossa cultura de trabalho remoto foi crítica para muitas organizações para provar que funciona e continuará funcionando. A mudança repentina em nossa cultura de trabalho remoto foi fundamental para muitas organizações, pois demonstrou que o trabalho remoto é útil e continuará sendo no futuro. No entanto, não

devemos nos tornar complacentes. Após pouco tempo de isolamento, já sentíamos falta das conversas ao redor do bebedouro da empresa ou durante o almoço, em que discutimos o golpe de phishing mais recente ou outras dicas práticas de segurança que, muitas vezes, ajudam as pessoas a fazerem as escolhas certas.

PREPARANDO A ORGANIZAÇÃO PARA O FUTURO

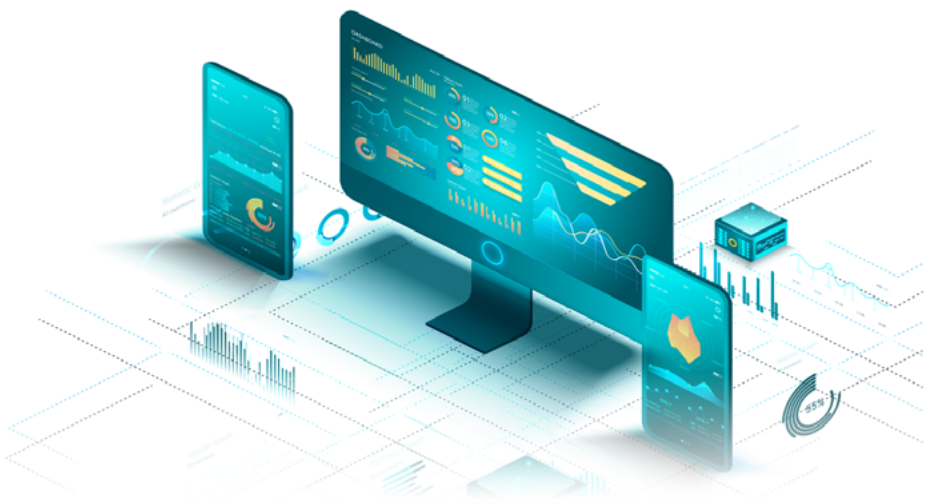
As empresas totalmente digitais estavam claramente mais adaptadas e preparadas para mudar sua força de trabalho para o formato remoto, mas nem todas tiveram a mesma sorte. Devemos lembrar que milhares de empresas exigem que seus funcionários trabalhem de casa, mas se a segurança está bem integrada com a política organizacional, não há razão para que a maioria das empresas do mundo não possa continuar a trabalhar com segurança longe de seus escritórios.

Mas e se houver uma vacina? Será que tudo voltará ao normal? Penso que não. Todos nós aprendemos que o trabalho remoto pode beneficiar as organizações e que essa transição pode ser feita com segurança. Contudo, não acredito que trabalharemos remotamente cinco dias por semana. O que descobrimos é que, enquanto funcionar, seguiremos trabalhando de casa quando nos for conveniente... o que, sem dúvida, irá beneficiar nossa saúde e bem-estar.

Pessoalmente, descobri que essa mudança para trabalhar de casa melhora muito minha vida familiar. Nunca passei tanto tempo com meus filhos pequenos, e eles comentaram várias vezes como é bom que eu esteja em casa com mais frequência. A ladainha de 'segunda à sexta, das 9h às 17h' já é passado, e devemos dar os créditos à Covid-19 por *ter acelerado substancialmente esse processo*, que teria levado anos para acontecer, se é que aconteceria. Mais funcionários em todo o mundo migrarão naturalmente e sem esforço para o que funciona para eles e seus negócios, o que, por sua vez, cria um ambiente melhor para todos nós. O fato de que o processo possa ser levado a sério e com segurança permite que isso seja feito.

Independentemente do que o futuro trará, duas coisas são certas – a maneira como trabalhamos foi permanentemente alterada e os ataques cibernéticos não estão desaparecendo. A pandemia de Covid-19 apenas acelerou a implementação da tecnologia em todas as facetas de nossa vida e, à medida que cada vez mais nossa vida profissional e privada é digitalizada, a segurança cibernética continuará sendo o eixo da segurança dos negócios.

Ataques cibernéticos são uma ameaça persistente às organizações, e as empresas devem formar equipes e sistemas de TI resilientes para evitar as consequências financeiras e de reputação desses ataques. A compreensão da força de trabalho pode desempenhar um papel fundamental na estratégia de segurança cibernética de qualquer empresa, aumentando a eficácia do treinamento e incentivando os funcionários a investirem mais em sua autoconsciência e habilidades. Compreender que o elemento humano da segurança cibernética é tão importante quanto o técnico é o primeiro passo na construção de protocolos holísticos que levem em conta os pontos fortes e fracos de cada um de nós.



2

RANSOMWARE COMO FORMA DE CHANTAGEM:

PAGUE PELOS SEUS DADOS OU ELES SERÃO DIVULGADOS

Com os atacantes de ransomware buscando cada vez mais poder para coagirem as vítimas a pagar, além de aumentar a quantia pedida pelo resgate dos dados, a situação das vítimas está ainda mais difícil. Como será o cenário de ransomwares em 2021?

Tony Anscombe
ESET Chief Security Evangelist

Algo que prevejo que precisa mudar em 2021 é a *definição de "ransomware" no dicionário*:

> ***"Ransomware é um software ilegal que impede o funcionamento adequado de um computador ou impede o usuário de obter informações até que tenha pago algum dinheiro."***
>
> ***(Collins English Dictionary)***

E por que a definição deveria mudar?

A década de 1980 é lembrada por diversos fatores: mixtapes, ombreiras, o cubo mágico de Rubik e o festival beneficiente do Live Aid, para citar alguns, mas poucas pessoas associariam essa década ao ransomware. Em 1989, uma nova ameaça digital chamada o "trojan da AIDS" foi criada, infectando dispositivos por meio de um disquete, escondendo diretórios e criptografando os nomes e extensões de arquivos armazenados no disco rígido. Os usuários recebiam uma mensagem para renovar sua licença e resolver o problema, e para isso deviam enviar US$ 189 à uma caixa postal no Panamá. Trinta e um anos depois, com diversas reviravoltas ao longo de sua evolução, o termo "ransomware" é comumente utilizado em todo o mundo.

Hoje, o ransomware é associado a um programa malicioso que criptografa arquivos e dados, e bloqueia o acesso até que o usuário pague o resgate solicitado em troca do método de descriptografia – ou pelo menos esperamos que se limite a isso. Durante sua evolução, o ransomware assumiu diferentes formas, incluindo o bloqueio de todo o dispositivo sem criptografar nada e exibir uma mensagem que exige um pagamento para recuperar o acesso, bloqueio de tela, exibição de fotos pornográficas e a exigência de um pagamento através de um SMS Premium para recuperar o acesso e impedir que as imagens sejam exibidas.

A participação de mercado do Microsoft Windows cria um ambiente de ataque ideal para os cibercriminosos que desejam extorquir dinheiro de suas vítimas. No entanto, é importante observar que outras plataformas não estão imunes, com exemplos de ataques de ransomware no OS X da Apple e nos sistemas operacionais Android da Google.

NOVOS MÉTODOS DE PRESSÃO SOBRE AS VÍTIMAS

A exfiltração e a extorsão podem não ser técnicas novas, mas certamente são uma tendência crescente. Os ataques estão adotando uma nova modalidade: os criminosos primeiro exfiltram uma cópia de dados confidenciais e a guardam em seu próprio ambiente. Em seguida, criptografam e bloqueiam o acesso aos dados nos servidores das vítimas. Então, os atacantes ameaçam publicar e vender os dados confidenciais, ou até mesmo leiloá-los, caso nenhum resgate seja pago. Essa técnica costuma ser um processo de longo prazo para os atacantes, pois precisam obter acesso à rede, identificar os dados confidenciais e, em seguida, exfiltrar uma cópia para seu próprio ambiente.

Considere, por um momento, como isso ocorre sob a perspectiva do cibercriminoso: as empresas estão se tornando mais inteligentes, implantam tecnologias que impedem ataques, criam processos de backup e restauração resilientes e estão menos dispostas a pagar o resgate. Os atacantes então precisam de um "Plano B" para conseguirem monetizar seus esforços e criar resiliência ao ataque, em vez de dependerem de uma única forma de ameaça: infecção e criptografia de dispositivos. Ao salvar os dados, os cibercriminosos criam resiliência e um argumento de venda para fechar o negócio com seu "cliente", ou seja, a vítima.

O grupo de cibercriminosos Maze, por exemplo, se tornou famoso com ataques de exfiltração e extorsão. No fim de 2019, o grupo publicou detalhes dos dados que alegou ter roubado da Southwire, uma fabricante de cabos com sede nos Estados Unidos, que se recusou a pagar o resgate de dados de US$ 6 milhões. Desde então, continuaram suas atividades nada agradáveis publicando uma lista de empresas que se recusaram a cooperar e ameaçaram publicar documentos e dados confidenciais. Em março de 2020, enquanto o mundo sofria com o caos criado pela pandemia de Covid-19, o grupo Maze publicou no Twitter que, devido à crise global, ofereceriam um desconto a todas as empresas que não haviam cooperado e se absteriam de atacar organizações médicas até que a situação melhorasse.

O cenário de longa duração de exfiltração e extorsão exige que os atacantes tenham uma série de habilidades diferentes e uma certa dose de paciência. Embora muitos ataques de ransomware tenham como objetivo negar acesso, seja por bloqueio ou criptografia, essa tendência crescente de fazer uma cópia leva os atacantes a se infiltrarem em uma rede e se moverem sem serem detectados para que os dados confidenciais possam ser identificados e copiados. Não se trata mais de um simples link ou anexo de phishing em um e-mail que funcionários ou consumidores desavisados abrem involuntariamente desencadeando um ataque de ransomware. Ainda precisa haver um ponto inicial de entrada, utilizando técnicas para explorar o Remote Desktop Protocol (RDP), forçando a entrada por meio de ataques de preenchimento de credenciais ou pelos mecanismos mais tradicionais de phishing e engenharia social.

Uma vez que se entre na rede, é uma questão de permanecer nela sem ser detectado, reunindo informações e coletando credenciais e senhas adicionais para garantir que, mesmo que a rota inicial seja fechada, o acesso seja mantido. A base e a inteligência para mapear uma rede e entender o que é valioso levam tempo e requerem recursos qualificados para atingir o objetivo final de identificar as joias digitais da empresa que, se violadas, bloqueadas ou publicadas, causariam um nível altíssimo de perturbação. Assim que os dados são extraídos furtivamente, os atacantes podem passar para a implantação mais tradicional do ransomware. Com o acesso privilegiado existente, podem até mesmo ter aproveitado a oportunidade para desativar o software de proteção e garantir um ataque bem-sucedido.

AS NOVAS EXIGÊNCIAS

O conjunto de habilidades adicionais e o tempo necessário para completar o processo precisam ser financiados pelos cibercriminosos, o que pode ser constatado pelo aumento dos valores dos regates exigidos. Em 2018, a cidade de Atlanta sofreu um ataque de ransomware tradicional. Os servidores de infraestrutura chave foram criptografados, e os atacantes exigiram US$ 51 mil por um método de descriptografia. Atlanta fez a coisa certa – recusou-se a pagar e reconstruiu seus sistemas, o que dizem ter custado US$ 9,5 milhões.

Nos últimos 18 meses, as quantias exigidas aumentaram e, infelizmente, com uma inflação fora do normal. Lake City e Riviera Beach City, na Flórida, *pagaram US$ 500 mil e US$ 600mil*, respectivamente. Lion, uma empresa australiana de bebidas, recusou-se a pagar a exigência de US$ 1 milhão, e a Universidade da California, em São Francisco, sofreu com a quantia exigida de US$ 3 milhões, pagando US$ 1,1 milhão no fim das contas. Em pouco mais de dois anos, as quantias exigidas no caso de Atlanta parecem pequenas, mas, sem dúvidas, há um aumento indesejado no valor exigido – uma tendência que provavelmente continuará.

A exigência por pagamento em bitcoins não é a única métrica que demonstra que esse cenário está sempre mudando. A Coalition, uma empresa de seguros cibernéticos que atende 25 mil pequenas e médias empresas na América do Norte, recentemente *publicou um relatório* resumindo os pedidos de regaste do primeiro semestre de 2020, que obviamente inclui o início da pandemia. O relatório mostra que "a gravidade média dos pedidos de regate relatados pelos segurados da Coalition aumentou 65% de 2019 a 2020, em grande parte impulsionada pelos custos crescentes do ransomware". O relatório detalha ainda que 41% de todos os processos são relacionados a ransomware e afirma que "mais recentemente, diversos grupos de ransomware estão roubando os dados das organizações antes de criptografá-los e ameaçam expor publicamente os dados roubados se o resgate não for pago". Os dados independentes do relatório da Coalition fornecem uma perspectiva diferente e confirmam a mudança no modus operandi adotado pelos cibercriminosos e o aumento nas quantias exigidas.

AS APOSTAS SOBEM

Avance rapidamente para agosto de 2020, e encontraremos mais uma história de vazamento de dados: Blackbaud, uma empresa de serviços em nuvem que fornece software de arrecadação de fundos para organizações em todo o mundo, *anunciou que conseguiu se defender de um ataque de ransomware*. Em cooperação com um especialista forense digital e com a polícia, a equipe de segurança cibernética da Blackbaud impediu que o cibercriminoso criptografasse dados e os bloqueassem em seus próprios sistemas. No entanto, o atacante rapidamente partiu para um Plano B, oferecendo, por uma certa quantia, a exclusão dos dados confidenciais do cliente que tinham roubado dos sistemas Blackbaud antes de serem removidos com sucesso pela equipe de segurança cibernética.

Blackbaud, surpreendentemente, pagou uma quantia não revelada ao extorsionário com a condição de que a prova de exclusão dos dados fosse fornecida. A resiliência de ter um Plano B rendeu dividendos ao cibercriminoso, apesar dos esforços heróicos das equipes que impediram o ataque. Se o ataque tivesse sido limitado ao cenário mais tradicional de infectar e criptografar, talvez nunca tivéssemos ouvido falar dele. No entanto, como os dados copiados (roubados) incluíam informações pessoalmente identificáveis de indivíduos, a empresa foi obrigada, em alguns locais pela legislação de privacidade, a informar clientes e reguladores que uma violação de dados havia ocorrido.

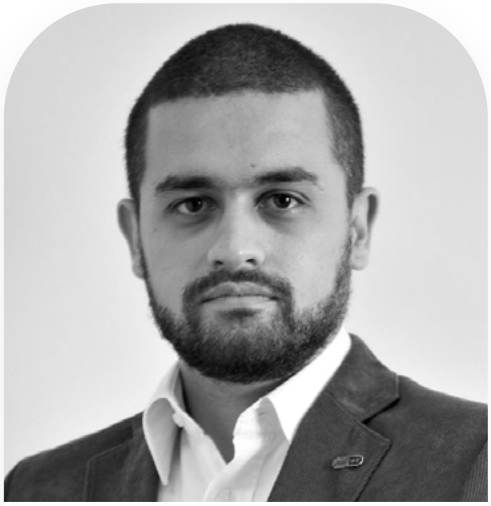
Ataques frustrados ou processos diligentes de backup e restauração podem não ser mais suficientes para afastar um cibercriminoso decidido a receber um pagamento de resgate de dados. O sucesso na monetização devido à uma mudança de técnica – apesar de exigir mais recursos e paciência – oferece aos cibercriminosos uma chance maior de retorno sobre o investimento (ROI) – sim, é um "negócio" avaliado com base em ROI. Na situação da Blackbaud, o ataque de ransomware não implantou nenhum software malicioso nem bloqueou o acesso a sistemas ou dados, outra evolução do termo "ransomware". É uma tendência que, infelizmente, tenho a certeza de que iremos vivenciar ainda mais em 2021.

3

PARA ALÉM DAS TECNOLOGIAS DE PREVENÇÃO:

ACOMPANHANDO DE PERTO AS AREIAS MOVEDIÇAS DAS AMEAÇAS CIBERNÉTICAS

Os cibercriminosos sempre procuram maneiras de tornar seus ataques mais difíceis de detectar e de serem impedidos, inclusive através do uso de ferramentas legítimas de um sistema para fins nefastos. Como devemos nos preparar?



Camilo Gutiérrez Amaya
ESET Head of Awareness & Research LATAM

Desde que o conceito de "vírus de computador" *apareceu há mais de 30 anos*, as ameaças à segurança cibernética não pararam de evoluir. Aliás, de acordo com o *Global Risks Report 2020* (Relatório de Riscos Globais, em tradução livre) do Fórum Econômico Mundial, as ameaças cibernéticas figuram entre os principais riscos para a humanidade nos próximos dez anos. Acrescente a isso a pandemia de Covid-19, que além de todas as suas consequências terríveis, também aumentou os riscos de sofrermos incidentes de segurança, fato que foi confirmado pelo aumento nas tentativas de ataque no início de 2020, conforme observado por diversas organizações, incluindo a *Organização das Nações Unidas* e o *Centro Nacional de Cibersegurança* (*National Cyber Security Center* - NCSC) do Reino Unido.

Nesse contexto, testemunhamos como grupos cibercriminosos passaram a usar técnicas cada vez mais complexas para implantar ataques a cada dia mais direcionados durante os últimos anos. Há algum tempo, a comunidade de segurança começou a falar sobre ataques "Fileless Malware", que pegam carona nas próprias ferramentas e processos do sistema operacional e os utilizam para fins maliciosos. Em outras palavras, as incursões cooptam aplicativos pré-instalados sem a necessidade de soltar executáveis adicionais no sistema das vítimas. Esses executáveis foram apelidados de LOLBaS (Living Off the Land Binaries and Scripts) e, des-

de o final de 2017, o termo começou a ser utilizado para se referir a técnicas evasivas em que os atacantes aproveitam executáveis binários que já estão pré-instalados em um sistema. Como esses ataques podem ser difíceis de detectar, os adversários adotam essas técnicas para maximizar a furtividade e a eficácia de seus ataques.

ONDE TUDO COMEÇOU

É importante ressaltar que o uso dessas técnicas não é algo novo. Vimos como algumas famílias de malware começaram a explorar essas características em 2001, quando o *worm CodeRed* apareceu. Nos últimos anos, no entanto, essas técnicas ganharam mais força, tendo sido empregadas em várias campanhas de ciberespionagem e por diversos agentes maliciosos, principalmente para atingir alvos de alto perfil, como órgãos governamentais. Foi o caso da *Operação In(ter)Ception*, que envolveu ataques contra empresas militares e aeroespaciais na Europa e no Oriente Médio, assim como contra o grupo *Evilnum* e seus ataques ao setor financeiro.

Muitas das técnicas, táticas e procedimentos (TTP) aproveitados por esses grupos são descritos na estrutura *MITRE* ATT&CK®. Os TTPs mais bem documentados incluem, indiscutivelmente, aqueles alavancados pelo *APT34*, também conhecido como Lazarus Group, que se destacou no crime cibernético com incursões como o *ataque à Sony Pictures* em 2014, por meio de *ataques contra um cassino on-line na América Latina* em 2017 e, mais recentemente, devido a *ataques direcionados a instituições financeiras* na Europa. Conforme os pesquisadores da ESET descobriram, o *grupo Invisimole* também baseia suas operações no uso de técnicas de "living off the land" com um conjunto completo de ferramentas para realizar campanhas de ciberespionagem. As incursões aproveitam, por exemplo, aplicativos vulneráveis como o *Total Video Player* ou *speedfan.sys*, além de componentes legítimos como *rundll32* e *womapiexec* para tentar burlar as tecnologias de defesa.

Dito isso, até mesmo uma pesquisa rápida na estrutura MITRE ATT&CK® sobre o uso malicioso de binários como *certutil*, *esentutl* ou *regsvr32*, para citar apenas alguns, revela um grande número de atacantes que utilizam essas técnicas. Mesmo uma olhada rápida nos grupos que adotam esses três binários revela mais de 100 atacantes diferentes, incluindo alguns dos grupos de Advanced Persistent Threat (Ameaça Persistente Avançada - APT) mais conhecidos do mundo, como Turla, Machete, Fancy Bear e Cobalt Group.

Com isso em mente, podemos esperar que 2021 seja um ano em que os incidentes que adotam essas técnicas terão um impacto ainda maior, e setores como o de infraestrutura crítica ou financeiro possivelmente serão os mais visados.

COMPREENDENDO OS MODELOS DE ATAQUE PARA REFORÇAR AS DEFESAS

Graças ao uso de programas legítimos, um dos principais diferenciais desses ataques é que eles reduzem significativamente os vestígios de atividade criminosa, uma vez que as ações maliciosas são carregadas e executadas na memória do computador sem afetar o sistema de arquivos. Como resultado, esses ataques geram nenhum ou poucos artefatos forenses que podem ser analisados posteriormente.

Sem dúvida, isso pode dificultar a detecção e, consequentemente, a prevenção desses ataques. Os ataques também são particularmente eficazes quando a segurança de uma organização é voltada para tecnologias de detecção baseadas em listas brancas ou quando falta uma heurística que forneça recursos de detecção avançados.

Uma vez que esses ataques procuram contornar a maioria das soluções de segurança e impedir a análise forense, outro recurso principal que sustenta essas técnicas é o sigilo. Os atacantes contam com as ferramentas nativas do sistema, como PowerShell e WMI (Windows Management Instrumentation), que são projetadas para facilitar a automação de tarefas e o gerenciamento de configurações do sistema operacional.

Os atacantes também costumam adotar esses métodos para alcançarem persistência, aumento de privilégios e até mesmo exfiltração de dados, ao passo que o acesso inicial ainda é comumente associado à exploração de vulnerabilidades ou campanhas de engenharia social. Portanto, é necessário considerar outras estratégias de gerenciamento de segurança que vão além das tecnologias de prevenção e que consideram a detecção e a resposta a incidentes.

DESAFIOS DE SEGURANÇA PARA EMPRESAS

O papel principal da abordagem de uma organização para combater qualquer tipo de ataque em 2021 envolve o fortalecimento de processos e procedimentos internos que permitam integrar tecnologias e pessoas a fim de monitorar todo o ciclo de vida de uma ameaça, a partir do momento em que um atacante busca o acesso inicial a um sistema, incluindo todos os caminhos até atingir a exfiltração de dados ou algum outro tipo de ação nefasta. Como resultado, é essencial considerar diversas camadas de tecnologias que permitam a visibilidade antes, durante e depois de um ataque.

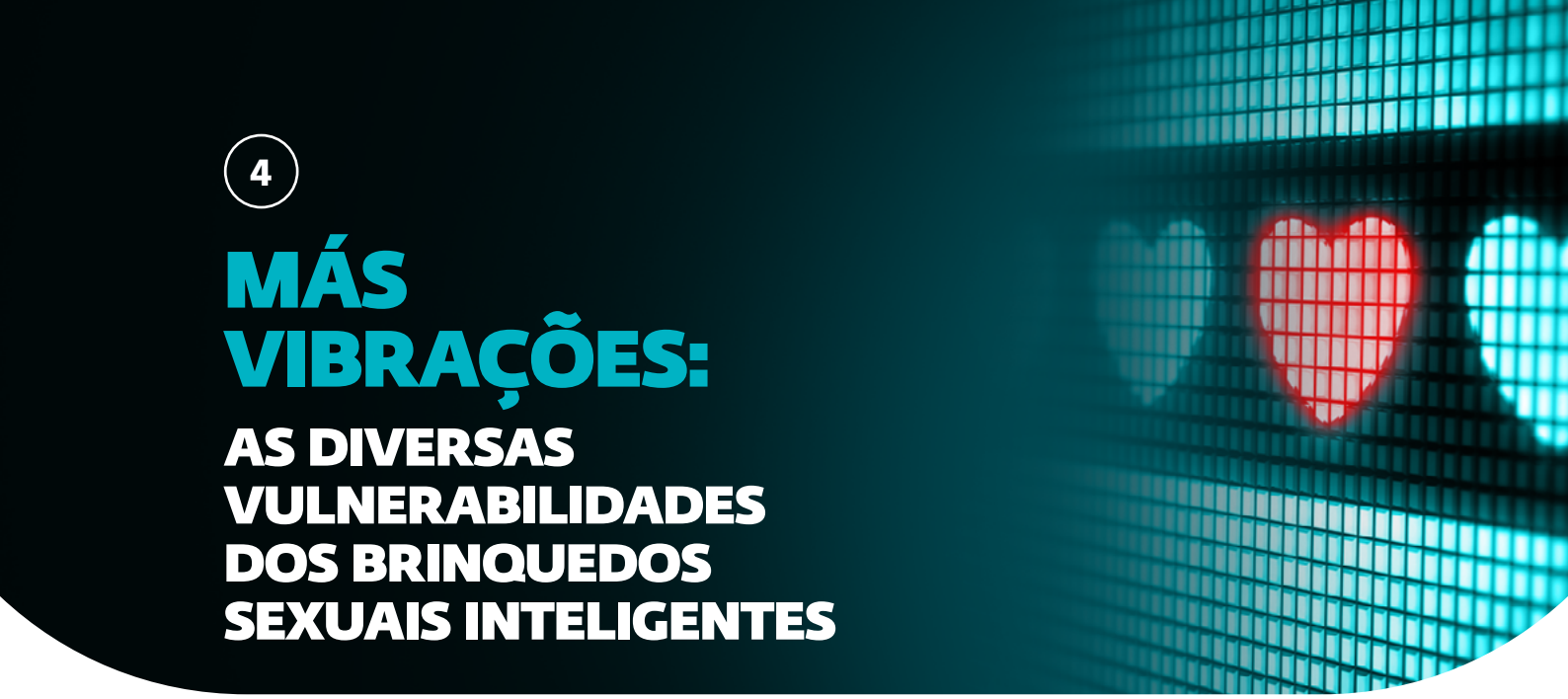
Esses tipos de recursos são obtidos com tecnologias como detecção e resposta de endpoint (EDR), que aumentam a visibilidade dos defensores sobre o que está acontecendo em uma rede de computadores. Juntamente com as tecnologias de detecção, a EDR pode aumentar a capacidade de uma organização de detectar atividades suspeitas e interromper comportamentos considerados perigosos, ao mesmo tempo que possibilita investigar possíveis incidentes que podem fazer parte de um ataque maior e isolar dispositivos que possam estar comprometidos.

Ameaças sem arquivo têm evoluído rapidamente, e espera-se que, em 2021, esses métodos sejam usados em ataques cada vez mais complexos e em larga escala. Essa situação destaca a necessidade de as equipes de segurança desenvolverem processos que utilizem ferramentas e tecnologias não apenas para evitarem que códigos maliciosos comprometam os sistemas, mas também para contarem com recursos de detecção e resposta – mesmo antes desses ataques cumprirem sua missão. As mudanças geradas pela pandemia de Covid-19 aceleraram a transformação digital em 2020, mas o próximo ano traz novos desafios para as organizações, que devem continuar adotando tecnologias que lhes permitam expandir sua visibilidade e monitorar comportamentos anômalos. Portanto, é vital que as organizações estejam equipadas com as ferramentas técnicas adequadas e uma equipe de profissionais treinados para ajudar a detectar incidentes com antecedência e fornecer respostas rapidamente.

4

MÁS VIBRAÇÕES:

AS DIVERSAS VULNERABILIDADES DOS BRINQUEDOS SEXUAIS INTELIGENTES



Que segurança os brinquedos sexuais oferecem e o que ainda está por vir? Os fornecedores estão fazendo o suficiente para proteger os dados e a privacidade das pessoas? E por que a segurança é tão crucial quando falamos de brinquedos para adultos?

Cecilia Pastorino
ESET Security Researcher

Denise Giusto Bilić
ESET Security Researcher

Não é novidade para ninguém que os dispositivos da Internet das Coisas (IoT) possuem vulnerabilidades. A ESET analisou falhas graves encontradas em *centrais* e *câmeras inteligentes*. Além disso, *pesquisadores da ESET descobriram recentemente o KRØØK*, uma vulnerabilidade grave que afetou a criptografia de mais de um bilhão de dispositivos Wi-Fi.

Embora os dispositivos IoT tenham sido sujeitos a inúmeros vazamentos de segurança, levando à exposição dos detalhes de login, informações financeiras e localização geográfica das pessoas, entre outros, existem poucos tipos de dados com maior potencial de prejudicar os usuários, se publicados, do que aqueles relacionados a seu comportamento sexual.

Com um crescente número de novos modelos de brinquedos inteligentes para adultos entrando no mercado, podemos imaginar que há avanços no fortalecimento de mecanismos que garantem as boas práticas no processamento das informações dos usuários. No entanto, diversas pesquisas mostraram que estamos muito longe de poder usar brinquedos sexuais inteligentes sem nos expormos ao risco de um ataque cibernético. Agora, essas descobertas são mais relevantes do que nunca, pois estamos observando *um rápido aumento nas vendas de brinquedos sexuais* como reflexo de uma crise de saúde global e das medidas de distanciamento social relacionadas à pandemia de Covid-19.

Então, até que ponto os brinquedos para adultos são seguros atualmente e o que ainda está por vir? As precauções necessárias para proteger os dados e a privacidade das pessoas foram tomadas? E por que a segurança é tão crucial quando falamos de brinquedos para adultos?

COMO A SEGURANÇA ENTRA EM JOGO

Como se pode imaginar, as informações processadas por brinquedos sexuais inteligentes são extremamente sensíveis: nomes, preferências e orientações sexuais, lista de parceiros sexuais, informações sobre o uso do dispositivo, fotos e vídeos íntimos – todas essas informações podem resultar em consequências desastrosas se caírem em mãos erradas.

Quem poderia se interessar por esse tipo de informação? Muitos países têm *leis que proíbem expressamente que seus cidadãos se envolvam em determinadas práticas sexuais*. O que aconteceria se as autoridades locais lançassem uma campanha opressora baseada na expropriação forçada de dados das empresas que os processam, ou na exploração de falhas em dispositivos sexuais como forma de identificar, localizar e perseguir gays, adúlteros ou qualquer outra pessoa que pertença a uma minoria ou grupo social em razão de suas escolhas sexuais? Além disso, os brinquedos sexuais não estão isentos da possibilidade de serem comprometidos por ataques cibernéticos. Novas formas de *sextorção* aparecem todos os dias se considerarmos o material íntimo acessível por meio dos aplicativos que controlam esses dispositivos.

Além das preocupações com a confidencialidade dos dados, devemos considerar a possibilidade de que vulnerabilidades nos aplicativos poderiam permitir que malwares sejam instalados no telefone ou que firmwares sejam alterados nos brinquedos. Essas situações podem levar a ataques de negação de serviço (DoS), que bloqueiam a entrega de qualquer comando, como o que aconteceu com uma *gaiola de castidade masculina inteligente que, recentemente, mostrou que é vulnerável* a explorações por cibercriminosos que poderiam bloquear os dispositivos de forma massiva, fazendo com que os milhares de usuários deixassem de ter acesso ao equipamento. Um dispositivo também pode ser transformado em arma para realizar ações maliciosas e propagar malwares, ou também ser deliberadamente modificado para causar danos físicos aos usuários, gerando sobreaquecimento e explosão, por exemplo.

Paralelamente, não podemos falar sobre as implicações de um ataque a um dispositivo sexual sem também reavaliar o significado do abuso sexual no contexto da transformação digital pela qual a sociedade está passando. Quais são as consequências de alguém ser capaz de assumir o controle de um dispositivo sexual sem que haja consentimento? Isso poderia ser descrito como um ato de agressão sexual? A noção de crime cibernético assume uma aparência diferente se adotarmos uma perspectiva de invasão de privacidade, abuso de poder e falta de consentimento para um ato sexual. O consentimento obtido por meio de fraude não configura nenhum tipo de consentimento, e essa lacuna legislativa nas leis atuais precisará ser resolvida para garantir a segurança sexual, física e psicológica dos usuários no ambiente digital.

SUPERFÍCIE DE ATAQUE DOS BRINQUEDOS SEXUAIS INTELIGENTES

Em termos de arquitetura, a maioria desses dispositivos pode ser controlados via Bluetooth Low Energy (BLE) por um aplicativo instalado em um smartphone. Dessa forma, os brinquedos sexuais atuam como sensores, que apenas coletam dados e os enviam para o aplicativo para serem processados. O aplicativo é então responsável por definir todas as opções no dispositivo e controlar o processo de autenticação do usuário. Para isso, ele se conecta por Wi-Fi a um servidor na nuvem, que armazena as informações da conta da pessoa. Em alguns casos, o aplicativo também atua como um intermediário entre diferentes usuários que buscam usar recursos como chat, videoconferência e transferência de arquivos, ou que desejam dar o controle

de seu dispositivo a usuários remotos, compartilhando seus tokens.

Alguns fornecedores oferecem aos usuários a possibilidade de se conectarem aos seus dispositivos instalando um software em seus computadores e usando um dongle BLE especial. Também é possível utilizar a API BLE em certos navegadores para se conectar aos brinquedos sexuais por um aplicativo web. As diferentes maneiras pelas quais você pode se conectar aos dispositivos fornecem mais flexibilidade, mas também aumentam a superfície de ataque.

Então, o que pode dar errado? Essa arquitetura apresenta vários pontos fracos que podem ser empregados para comprometer a segurança dos dados sendo processados: interceptação da comunicação local entre o aplicativo de controle e o dispositivo, entre o aplicativo e a nuvem, entre o telefone remoto e a nuvem ou ataque direto ao backend. É claro que nem todos os ataques ocorrem em conexões de rede, e alguns cenários maliciosos podem ser lançados por meio de malwares previamente instalados no telefone ou explorando falhas no sistema operacional.

Diversos pesquisadores de segurança (*[1]*, *[2]*, *[3]*, *[4]*, entre outros) comprovaram que esses dispositivos contêm falhas que poderiam ameaçar a segurança de dados armazenados, assim como a segurança do usuário. As brechas variam de procedimentos de autenticação inadequados a dispositivos que divulgam constantemente sua presença, permitindo que qualquer pessoa possa se conectar a eles.

Em 2016, dois pesquisadores apresentaram a palestra "*Breaking the Internet of Vibrating Things.*" Eles demonstraram como informações como intensidade, padrões, temperatura e hábitos do usuário foram coletados pelo aplicativo *We-Connect* e enviados de volta aos servidores sem anonimato. No ano passado, um pesquisador *mostrou como é fácil para um atacante hackear um plug anal* controlado por BLE. Foi também a primeira prova de conceito em que um dispositivo sexual inteligente pode ser usado como um instrumento para prejudicar o usuário.

Neste ano, a equipe de pesquisa da ESET América Latina apresentou na DEF CON IoT Village *uma nova pesquisa sobre brinquedos sexuais inteligentes não seguros*. O estudo utilizou dois dispositivos como base: um dispositivo portátil chamado Jive, fabricado pela We-Vibe, e o masturbador masculino Max, da Lovense.

Descobrimos que ambos os dispositivos continham vulnerabilidades na implementação de comunicações BLE, permitindo que atacantes interceptassem os dados enviados e controlassem remotamente os dispositivos por meio de ataques BLE MitM (Man-in-the-middle). Isso implica que qualquer pessoa consiga utilizar um scanner Bluetooth simples para localizar e controlar esses brinquedos sexuais inteligentes nas proximidades, semelhante ao que o pesquisador Alex Lomas fez em 2017, enquanto *caminhava pelas ruas de Berlim e descobria brinquedos sexuais*. Essa vulnerabilidade é muito comum em dispositivos IoT, pois a maioria dos modelos disponíveis no mercado não implementa pareamento seguro, o que permite que qualquer pessoa os conecte e os controle.

Em relação ao aplicativo *Lovense Remote*, encontramos algumas opções de design controversas que podem ameaçar a confidencialidade das imagens íntimas enviadas pelos usuários. Não havia criptografia de ponta a ponta, as capturas de tela não estavam desabilitadas, a opção "excluir" no chat não apagava de fato as mensagens do telefone remoto, e os usuários poderiam baixar e encaminhar conteúdo de outras pessoas sem avisá-las. Além disso, usuários mal-intencionados poderiam descobrir os endereços de e-mail associados a qualquer nome de usuário e vice-versa. Essas descobertas constituem questões sérias de privacidade, principalmente em um aplicativo projetado especificamente para compartilhar conteúdo sexual.

O aplicativo permite que os usuários concedam controle remoto de seus dispositivos por meio de uma URL, que inclui um token de 4 dígitos. Também encontramos problemas de segurança com esse token que permitiria que atacantes sequestrassem dispositivos remotos aleatórios sem consentimento.

No aplicativo *We-Connect*, percebemos que metadados confidenciais não estavam sendo retirados dos arquivos antes de serem enviados, o que significa que os usuários podem ter enviado, sem se darem conta, informações sobre seus dispositivos e sua geolocalização exata ao trocar mensagens de texto sexuais com outros usuários. Isso pode ser muito perigoso, pois muitos usuários concedem o controle de seus dispositivos a estranhos, compartilhando seus tokens on-line, tanto como uma preferência pessoal ou como parte de um serviço de "cam girl/boy".

BOAS PRÁTICAS PARA EVITAR RISCOS

Os brinquedos sexuais inteligentes estão ganhando popularidade como parte do conceito de "sexnologia", uma combinação de sexo e tecnologia. Essas práticas podem ter vindo para ficar, mas não devemos esquecer as ameaças potenciais à privacidade e intimidade dos usuários.

Para minimizar os riscos associados ao uso de dispositivos sexuais inteligentes, recomendamos ter em conta as seguintes dicas:

1. Alguns aplicativos oferecem a possibilidade de controlar dispositivos localmente via BLE sem criar uma conta de usuário. Se você não planeja permitir que outros usuários controlem seu dispositivo remotamente pela Internet, procure um desses dispositivos.

2. Na medida do possível, evite compartilhar fotos ou vídeos nos quais seja possível identificar você e não poste tokens de controle remoto na Internet.

3. Evite registrar-se em aplicativos de sexo usando um nome oficial ou endereço de e-mail que permita identificar quem é você.

4. Sempre leia os termos e condições dos aplicativos e sites nos quais você se registra.

5. Utilize brinquedos sexuais inteligentes em ambientes protegidos e evite seu uso em locais públicos ou em áreas com pessoas só de passagem (como hotéis).

6. Baixar os aplicativos e testar seus recursos antes de comprar o dispositivo pode dar a você uma visão geral de como o produto é seguro. Utilize os mecanismos de busca para descobrir se o modelo que você está pensando em comprar já apresentou alguma vulnerabilidade.

7. Sempre proteja os dispositivos móveis que você utiliza para controlar esses brinquedos, mantenha-os atualizados e tenha uma solução de segurança instalada neles.

8. Proteja a rede de Wi-Fi doméstica que você utiliza para se conectar com senhas fortes, algoritmos criptografados com segurança e atualização regular do firmware do roteador.

O QUE AINDA ESTÁ POR VIR?

A era dos brinquedos sexuais inteligentes está apenas começando. Os avanços mais recentes na indústria incluem *modelos com recursos de RV (Realidade Virtual)* e robôs sexuais com tecnologia de inteligência artificial (AI) que incluem câmeras, microfones e recursos de análise de voz baseados em técnicas de AI. O *uso desses robôs como substitutos de profissionais do sexo em bordéis* já é uma realidade.

Esses brinquedos sexuais são apenas uma pequena expressão da sexualidade no mundo digital, uma área que poderíamos dizer que também inclui aplicativos de relacionamento e outros dispositivos como as "*namoradas virtuais*", a manifestação tecnológica de um fenômeno sociológico maior que está transformando nossa sociedade enquanto dispositivos IoT continuam se infiltrando em nossa realidade.

Como já se comprovou diversas vezes, o desenvolvimento seguro e a conscientização pública serão fundamentais para garantir a proteção de dados confidenciais enquanto capacitamos os usuários a se tornarem consumidores inteligentes, capazes de exigir aos fabricantes a implementação de melhores práticas para manter o controle de sua intimidade digital nos próximos anos.

CONCLUSÃO

Mesmo quando a maré começa a mudar e começamos a retomar uma vida mais próxima do que era antes da pandemia, não devemos "baixar a guarda".

Está claro que a pandemia gerou mudanças em praticamente todas as nossas atividades e, com caráter transitório, no nosso uso e relacionamento com a tecnologia. Algumas dessas mudanças foram mais óbvias e diretas, como o trabalho remoto ou aulas à distância devido ao isolamento social, ao passo que outras surgiram como efeito colateral das anteriores, alterando nossos hábitos de consumo e comportamento de maneiras que não havíamos imaginado anteriormente. Tudo isso teve e terá um forte impacto na segurança cibernética, apresentando novos desafios para empresas e organizações - além dos desafios já existentes - para tentarem se proteger de ataques e impondo a necessidade de acelerar os tempos de ação diante de um cenário tão dinâmico como a própria Covid-19, com consequências que, em alguns casos, vieram para ficar.

Nesse contexto, a tecnologia desempenhou um papel de destaque, pois foi o recurso que nos permitiu enfrentar as consequências do isolamento social da forma mais normal possível. No entanto, muitas tecnologias e organizações, assim como pessoas, não estavam suficientemente preparadas do ponto de vista da segurança para enfrentar uma nova realidade que, embora não fosse completamente nova, permitiu-se constatar com clareza algo que já vem acontecendo há muito tempo: a velocidade e o dinamismo com que os cibercriminosos se adaptam para aproveitar as oportunidades. Entre as particularidades de 2020 que realçaram esse comportamento está o aumento da adoção de serviços e tecnologias por uma massa crítica, que obrigou os usuários e as empresas a reagirem rapidamente às mudanças para não serem comprometidos.

Nesse sentido, conforme explicitado no capítulo "O futuro do trabalho", a pandemia forçou a aceleração dos processos de transformação digital e deixou clara a necessidade de a segurança ser o centro de muitas decisões. As atividades maliciosas tiveram um crescimento significativo em 2020 com cibercriminosos de todos os tipos tentando tirar proveito de um cenário que apresentava mais usuários conectados, por mais tempo, e dispostos a adotarem o uso de tecnologias e serviços on-line, os quais não tinham tanta demanda anteriormente.

O caso do Zoom é um bom exemplo para descrever as consequências do impacto acelerado dessa transformação, não só pelo crescimento repentino do número de usuários, que passou de 10 milhões em dezembro para 200 milhões em março deste ano, mas também porque essa demanda e a atenção dada por usuários e empresas também atraiu o interesse de cibercriminosos que lançaram campanhas de engenharia social e descobriram diversas falhas de segurança e privacidade que, apesar de sua popularidade e adoção em massa, fizeram várias empresas proibírem seu uso.

Outro exemplo que mostra o oportunismo dos cibercriminosos durante a pandemia de Covid-19 tem sido o ransomware e seu crescimento desde que se decretou um estado de pandemia, atingindo até mesmo hospitais e organizações do setor de saúde em um momento muito delicado. Além do fato de que diferentes grupos de ransomware aumentaram suas tentativas de explorar o Remote Desktop Protocol (RDP) que as pessoas utilizam para se conectarem de casa às redes corporativas, diferentes famílias de ransomware já modificaram sua estratégia desde o ano passado, adicionando ataques mais direcionados e criptografia de arquivos, exfiltração de informações confidenciais de empresas e subsequente extorsão caso elas decidam não pagar o resgate exigido.

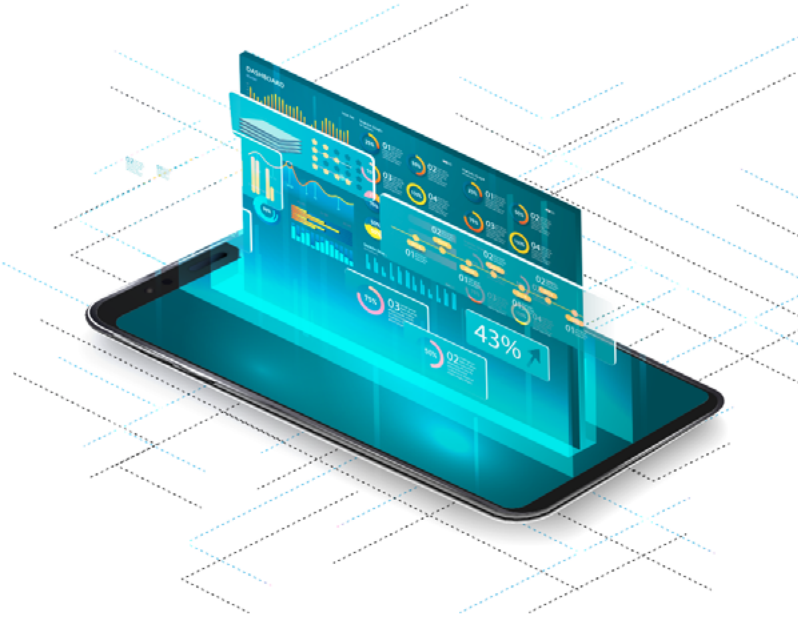
Além de ser uma tendência que se consolidou em 2020, trata-se também de estratégias mais complexas em que os atacantes entram na rede e se movem com paciência, sem serem detectados, até que identifiquem as informações sensíveis e façam cópias para depois evidenciar sua presença, desencadeando o ataque. No capítulo "Ransomware como forma de chantagem", explicamos como as mudanças implementadas pelos grupos criminosos que operam esses códigos maliciosos são um exemplo claro da evolução constante dos cibercriminosos e sua tentativa de adotarem novas estratégias e desenvolverem novas habilidades para se manterem atualizados e atingirem seus objetivos, desafiando o mecanismos de defesa de forma permanente e deixando claro a importância de analisar o cenário atual, mas se projetando para o futuro, deixando a porta aberta para a necessidade de medidas rápidas que se adaptem à realidade criminal do momento.

Outro exemplo da dinâmica com a qual os cibercriminosos trabalham e dos desafios para o futuro pode ser visto no capítulo "Para além das tecnologias de prevenção". Nele, fazemos referência aos desafios atuais e aos que virão se tomarmos como exemplo a rápida adoção dos chamados LOLBaS (Living Off the Land Binaries and Scripts). Esse conceito se refere ao uso de binários específicos do sistema para realizar atividades maliciosas empregando elementos pré-instalados. O uso de LOLBaS torna a tarefa de detecção difícil e, portanto, também a de prevenção de ataques, e eles são muito eficazes quando a segurança de uma organização é direcionada a tecnologias de detecção baseadas em listas brancas e não possui recursos de detecção avançados.

Embora muitos de nós possamos imaginar um aumento no uso de nossos dispositivos para nos comunicarmos com nossos familiares ou para nos entretermos depois que as medidas de isolamento social foram determinadas, o crescimento na venda de brinquedos sexuais inteligentes nos faz pensar sobre o aumento da superfície de ataque e a complexidade envolvida na proteção da vida digital dos usuários com as diferentes possibilidades que os cibercriminosos têm para realizar um ataque.

Nesse sentido, as especialistas Denise Giusto e Cecilia Pastorino, respaldadas por uma pesquisa que realizaram e na qual descobriram diversas vulnerabilidades em dispositivos sexuais inteligentes, mostram com outro exemplo a importância de pensar hoje — e ainda mais no futuro — sobre segurança de forma proativa. Esses dispositivos processam grandes quantidades de informações confidenciais dos usuários e fazem parte de uma indústria crescente de brinquedos sexuais inteligentes, que está avançando e inclui modelos com tecnologia de realidade aumentada e inteligência artificial com câmeras e microfones. Trabalhar para aumentar a conscientização sobre o valor e a importância da segurança já era uma necessidade, mas hoje se torna mais evidente do que nunca.

Assim que a pandemia de Covid-19 acabar, muitas organizações terão confirmado que, com o trabalho remoto, a produtividade não é afetada, podendo até mesmo melhorar. O mesmo pode acontecer em setores como educação ou a área da saúde com consultas médicas virtuais, para citar alguns. Como dissemos no início, algumas mudanças provavelmente vieram para ficar e, junto delas, os desafios pós-pandemia estão definidos do ponto de vista da segurança cibernética. Esperamos que este documento ajude na compreensão de algumas das mudanças ocorridas e que seja possível visualizar quais serão os próximos passos para o que ainda está por vir.



CYBERSECURITY
EXPERTS ON YOUR SIDE