TREND MICRO™ | research

MAPPING THE FUTURE

Dealing With Pervasive and Persistent Threats

TREND MICRO SECURITY PREDICTIONS FOR 2019

CONTEÚDO

Published by Trend Micro Research

Stock images used under license from Shutterstock.com

PREVISÕES DE SEGURANÇA DA TREND MICRO PARA 2019

Os avanços trazidos pela Inteligência Artificial e o Machine Learning figuram entre as tendências mais esperadas a impactar a tecnologia e a segurança no ano de 2019 e nos anos subsequentes, seja no âmbito corporativo ou residencial.

Entre os principais motivos para esse cenário estão o contínuo crescimento do volume de dados que podem ser processados e analisados, a contínua adoção da computação em nuvem por empresas em todo o mundo e o desenvolvimento de dispositivos inteligentes, tanto em domicílios, como em fábricas – sem contar o iminente lançamento da tecnologia 5G em 2020, a mais recente fase de comunicações móveis voltadas para o aumento da velocidade da internet. Além disso, 2019 será um importante ano para processos políticos, incluindo a finalização do Brexit e a realização de eleições em vários países. Estas tecnologias e mudanças sociopolíticas terão impacto direto em temas relacionados à segurança em 2019.

Espera-se que os cibercriminosos, como de costume, usem essa tendência - onde a oportunidade de lucro é provável, rápida e relativamente fácil de se conquistar. Em 2019, as consequências das ameaças digitais irão mais longe em planejamento e efeitos: fraudes usando credenciais violadas irão aumentar, mais pessoas serão vítimas de extorsão, efeitos colaterais serão observados conforme o ambiente virtual crescerá conforme o aumento da presença cibernética de diversos países. Ainda, o sucesso da propaganda virtual e das fake news terão o poder de decidir o destino de nações. Consequentemente, para empresas, novos desafios incluirão a falta de mão de obra qualificada, o que causará o aumento do orçamento na procura de especialistas em segurança em TI. A terceirização irá aumentar. Do mesmo modo, o ciberseguro terá uma expansão sem precedentes, já que as penalidades pelo não cumprimento de normas também devem crescer.

Nossas previsões de segurança para o ano que virá são baseadas em análises realizadas por nossos especialistas no atual progresso das tecnologias emergentes, comportamento de usuários, tendências do mercado e seus impactos em cenários de ameaças. Dividimos este material em categorias baseadas nas principais áreas que poderão ser afetadas, levando em consideração o desenvolvimento de diferentes tecnologias e mudanças no cenário sociopolítico.

CONSUMIDORES

04

Engenharia social via phishing irá substituir Exploit kit como vetor de ataque

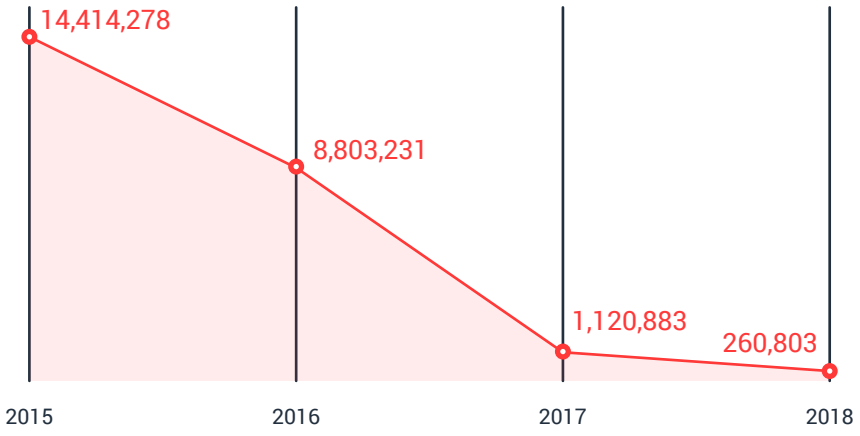
Casos de phishing aumentarão consideravelmente em 2019. Esse cenário onde atacantes fingem ser alguém com uma certa reputação ou identidade para que assim seja possível enganar a vítima e conseguir informações sensíveis existe há um bom tempo. No entanto, com o passar dos anos os invasores estão encontrando novas formas de otimizar seus ataques. Exploit kit, por exemplo, ganharam popularidade pela possibilidade de identificar a versão do software usada por sua vítima e escolher o exploit relevante para tal operação.

Porém, recentemente, dispositivos que usam softwares e sistemas operacionais (SO) diferentes dificultam a criação de Exploit kits modernos. Há 5 anos, por exemplo, Windows dominava, mas agora nenhum SO domina mais da metade do mercado.

Cibercriminosos terão que fazer uma escolha: passar horas construindo um exploit que funcionaria somente numa pequena parcela de dispositivos e que poderão ser atualizados para remover a falha explorada ou voltar para a antiga e conhecida técnica que nunca teve uma solução certeira: a engenharia social.

Continuaremos a ver a queda do uso de Exploit kit, algo que notamos em nossos dados sobre o tema:

Figura 1. Atividades de Exploit kit caíram ao longo dos anos, baseado em dados da infraestrutura Trend Micro™ Smart Protection Network™ em 2018.Protection Network™ em 2018.



Ataques de phishing estão crescendo, baseados em nossos dados, e essa tendência irá continuar em 2019.

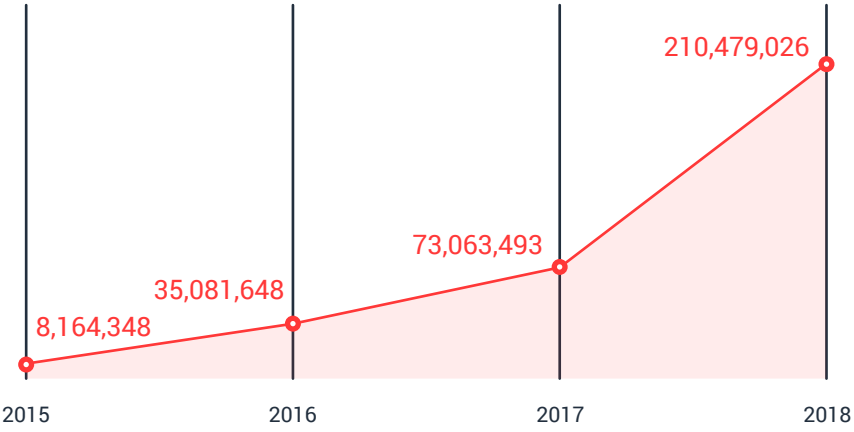


Figura 2. URLs relacionadas a phishing bloqueadas cresceram no passar dos anos, baseados nos dados da infraestrutura Trend Micro™ Smart Protection Network™ em 2018.

Veremos possivelmente tentativas de phishing não só em e-mails, mas também via SMS e meios de mensagens. Cibercriminosos irão mirar em credenciais de bancos online, e também irão atrás de contas usadas para armazenamento de dados na nuvem ou outros serviços de nuvem. Também veremos novos tipos de ataques como SIM-jacking (Sequestro de chip), que confia muito no método de engenharia social. No ataque de SIM-jacking, criminosos se passam por uma equipe de suporte técnico que busca a portabilidade para um chip "perdido" que eles já possuam, efetivamente tomando controle da conta online, que na maioria das vezes é associada ao número de celular.

Em termos de conteúdo de engenharia social, prevemos que essa técnica será usada em eventos esportivos ou políticos, como a copa mundial de Rugby no Japão, as Olimpíadas em Tokyo no ano de 2020 e em eleições em vários países. Cibercriminosos poderão, por exemplo, criar sites falsos de vendas de ingressos, publicar falsos anúncios ou produtos com descontos, enviar links maliciosos sobre as eleições ou algo relacionado a esportes.

Chatbots serão explorados

As comunicações online expandiram-se para além do e-mail. Quanto mais os jovens usam tecnologias e estão sempre online, aplicativos de mensagem tornam-se um canal socialmente aceito de comunicação entre pessoas ou em um canal direto com empresas que disponibilizam algum tipo de atendimento online. Esta nova tendência, combinada com a preferência aos ataques de engenharia social discutidos anteriormente, cria novas oportunidades para os cibercriminosos.

Nós prevemos que ataques que usam chatbots ficarão desenfreados em 2019. Da mesma maneira que ataques via telefone que tiram vantagens de mensagens gravadas e sistemas de interação de voz, atacantes criarão chatbots que irão iniciar uma conversa com a vítima como pretexto para enviar um link de phishing ou obter informações pessoais. Atacantes irão explorar uma grande possibilidade de vetores, incluindo manipulação de pedidos, instalação de um Trojan de acesso remoto (Remote Access trojan, conhecido também como RAT) no computador da vítima ou até extorsão.

Contas de E-Celebs serão exploradas

Na mesma linha da tendência de criar táticas de engenharia social, **cibercriminosos irão comprometer contas de YouTubers famosos e de outras "celebridades virtuais".** Os atacantes irão mirar contas com milhões de seguidores e trabalharão para tomar controle delas via ataques direcionados de phishing e afins. Esses ataques irão acender um holofote na mídia tradicional, mas não antes que milhões de usuários que seguem essas contas tenham sido afetados por qualquer tática que os invasores tenham reservado para eles. Os seguidores terão seus computadores infectados para roubo de dados, para serem usados em ataques distribuídos de negação de serviço (DDOS) ou para mineração de criptomoedas.

Uso massivo de credenciais violadas e vazadas

Um recente relatório publicado pelo instituto Ponemon e pela Akamai destacou que testes de credenciais vazadas em sites populares usando ferramentas automatizadas estão se tornando cada vez mais severos. Por conta do volume de dados vazados nos últimos anos e pela probabilidade de cibercriminosos acharem vários usuários que usam as mesmas credenciais em diversos serviços, nós acreditamos que **surgirão transações fraudulentas usando dados que cibercriminosos conseguiram via vazamentos.**

Cibercriminosos irão usar credenciais violadas para adquirir vantagens no mundo real, como registrar-se em programas de milhas para receber recompensas. Eles também usarão essas contas em redes sociais para publicar propagandas, fake news ou adicionar votos inválidos em comunidades que realizam votações – as aplicações são diversas.

Casos de sextorsão irão aumentar

Teremos um grande crescimento de adolescentes e jovens adultos que serão extorquidos por razões não-monetárias, como a sextorsão (ato em que ameaça-se a divulgação de fotos íntimas, seja para obrigar uma ação específica ou vingança). Mesmo que não se tenha certeza que um blackmail venha a ocorrer, a natureza altamente pessoal deste tipo de ataque fará com que a vítima considere seriamente o cumprimento das demandas do atacante. Com a sextorsão, em particular, ficando cada vez mais difundida, este tipo de ataque irá afetar, e, eventualmente, até reivindicar mais vidas em 2019.

ENTERPRISES

Redes domésticas em cenários de trabalho remoto irão abrir empresas para riscos de segurança semelhantes ao BYOD.

A TI corporativa observará cada vez mais ataques em que os pontos de entrada são os dispositivos domésticos conectados às redes residenciais dos funcionários. Essa é uma interseção inesperada, porém inevitável, de duas tendências: a ascensão de contratações de trabalho remoto e a crescente adoção de dispositivos inteligentes em casa.

Mais funcionários estão aproveitando a opção de trabalhar desde suas casas (também conhecido como teletrabalho, trabalho remoto ou trabalho em casa). Conforme relatado pela Gallup, 43% dos funcionários americanos trabalharam remotamente em 2016, e 39% em 20128. De acordo com uma pesquisa global conduzida pela Polycom, quase dois terços dos funcionários tiraram vantagem da possibilidade de "trabalhar em qualquer lugar" em 2017, contra aproximadamente 14% em 2012. Com BYOD (Bring Your Own Device, em inglês, ou Traga Seu Próprio Dispositivo, em tradução livre), o trabalho em casa desafia a visibilidade dos movimentos de dados corporativos sempre que os funcionários usam sua internet doméstica para acessar aplicativos baseados em nuvem, softwares de bate-papo, videoconferência e compartilhamento de arquivos.

As redes domésticas normalmente têm impressoras e dispositivos de armazenamento instalados, que os funcionários consideram convenientes para o trabalho bem como para uso doméstico, resultando em um cenário de uso misto (ou seja, pessoal e comercial). Além disso, o compartilhamento da rede doméstica do funcionário remoto com dispositivos inteligentes os torna mais inteligente do que nunca. A IDC projeta crescimento de dois dígitos em todas as categorias de dispositivos domésticos inteligentes até 2022. Infelizmente, em termos de segurança, isso significa que todos os dispositivos desprotegidos na rede doméstica de um funcionário serão um possível ponto de entrada para invasores na rede corporativa.

Nossos pesquisadores já provaram como os alto-falantes inteligentes, por exemplo, podem vazar dados pessoais. **Veremos alguns cenários de ataques direcionados em 2019 que usarão os pontos fracos dos alto-falantes inteligentes para acessar redes corporativas por meio das redes domésticas dos funcionários.**

Reguladores GDPR penalizarão o primeiro violador de alto perfil – total de 4%

Reguladores do GDPR (General Data Protection Regulation) da União Europeia não exerceram imediatamente seus novos poderes. Contudo, eles darão muito em breve um exemplo com uma grande empresa não-aderente, multando-a em 4% de seu faturamento anual global.

O GDPR é um modelo mais maduro de conformidade de privacidade. De fato, muitas organizações já haviam pagado multas sob a Diretiva de Proteção de Dados anterior por mais de uma década12, e assim os infratores puderam sentir as garras do regulamento mais cedo do que eles esperavam. A tendência é que ocorram mais divulgações de vazamento de dados em 2019 do que no ano anterior, devido ao GDPR. Já há relatos de que algumas agências estão inundadas com novas divulgações que precisam de investigação. Pelo lado positivo, as divulgações também darão às empresas maior visibilidade e insights sobre como as ameaças estão comprometendo outras organizações.

Isso terá o efeito inevitável de enfatizar a dificuldade prevalente em cumprir os pontos mais sutis do regulamento e forçar os regulamentadores a esclarecer ou acrescentar mais detalhes sobre quais tecnologias de segurança são realmente necessárias. **As empresas também serão forçadas a repensar o valor das atividades de mineração de dados inerentes aos modelos atuais de publicidade, dado o alto preço de uma possível violação. Na verdade, prevemos que, até 2020, mais de 75% dos novos aplicativos de negócios terão que tomar a difícil decisão de escolher entre conformidade e segurança.** Embora a privacidade e a segurança não sejam mutuamente exclusivas, os esforços para garantir a conformidade com a privacidade de dados terão um efeito prejudicial na capacidade de uma empresa de determinar adequadamente a origem e os detalhes de uma ameaça à segurança.

Eventos do mundo real serão usados em ataques de engenharia social

Na seção anterior, previmos que os ataques de phishing se tornarão ainda mais predominantes. No contexto empresarial, **eventos do mundo real como as próximas eleições em vários países em 2019, cerimônias esportivas como os Jogos Olímpicos de Tóquio em 2020 e até mesmo instabilidade política e questões separatistas como Brexit, serão usados como premissa para ataques de engenharia social contra empresas.** Prevemos que haverá muitas atividades cibercriminosas aproveitando tais eventos. Eles serão usados em cibercrimes regulares, fraudes por e-mail e engenharia social contra corporações.

Os cibercriminosos irão se concentrar principalmente em obter informações sobre os funcionários, usando a sua presença nas mídias sociais para criar ataques de phishing cada vez mais convincentes.

O comprometimento de e-mail empresariais irá cair 2 níveis na tabela Org

O comprometimento de e-mail empresarial (BEC) continua sendo um meio muito potente e lucrativo de desviar dinheiro das empresas. Acreditamos que, como resultado do foco em chefes "C level" como alvos de fraude em artigos de notícias sobre a BEC, **cibercriminosos irão atacar funcionários mais abaixo na hierarquia da empresa.** Eles terão como alvo, por exemplo, o secretário ou assistente executivo do CxO'S ou de um diretor ou gerente do alto escalão no departamento financeiro.

A automação será um novo problema no comprometimento de processos de negócios

O comprometimento de processos de negócios (BPC) - no qual os processos de negócios específicos são silenciosamente alterados para gerar lucro para os invasores - será um risco contínuo para as empresas. **A automação irá adicionar uma nova camada de desafio na proteção de processos de negócios no BPC.** A Forrester prevê que isso resultará na perda de 10% dos empregos em 2019.

À medida que mais aspectos de monitoramento e função são conduzidos por meio de softwares ou aplicativos online, os agentes de ameaças terão mais oportunidades de se infiltrar nos processos que não forem seguros desde o início. O software de automação terá vulnerabilidades e a integração com sistemas existentes irá introduzir brechas. Além disso, como os agentes de ameaças tentarão encontrar pontos fracos nos fornecedores ou parceiros de uma empresa-alvo para atingir suas metas, a automação também irá introduzir riscos na cadeia de suprimentos.

O vasto campo de aplicações da extorsão digital será explorado

Dados os insights da nossa pesquisa voltada para o futuro da modalidade de chantagem online ou extorsão digital, esperamos ver execuções mais refinadas ou repetição do mesmo modelo cibercriminoso de negócios. Em 2019, **observaremos cibercriminosos usando a multa máxima por descumprimento do GDPR como uma diretriz ou teto para o resgate exigido.** Eles farão isso na esperança de que empresas em pânico prefiram pagar o resgate do que divulgar a violação.

Também veremos alguns casos de uma versão de extorsão no cenário corporativo na forma de campanhas de difamação online contra marcas. Nesses casos, os agressores exigirão resgate para cessar a divulgação propaganda em estilo de "Fake news" contra marcas-alvo.

GOVERNO

A luta contra as notícias falsas irá resistir sob a pressão de várias eleições

Na União Europeia, espera-se uma "profunda reorganização radical" nas importantes eleições para o Parlamento Europeu em 2019, segundo Carnegie Europe, mesmo que países europeus como Grécia, Polónia e Ucrânia realizem suas próprias eleições nacionais. Nigéria e África do Sul também terão suas eleições, juntamente com vários países da Ásia, como Índia e Indonésia. **Acreditamos que, em 2019, as melhorias que as mídias sociais fizeram para combater as fake news pós-2016 não serão suficientes para acompanhar o dilúvio da ciberpropaganda em torno desses exercícios democráticos.**

Como observado em nosso artigo "The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public", a tríade necessária para notícias falsas se proliferarem só pode ser interrompida se qualquer um dos elementos (plataformas, motivação, ferramentas, etc) for desmontado ou inadequadamente gerenciado. A motivação nunca some e as ferramentas são difíceis de serem esquecidas, uma vez que as mesmas ferramentas podem ser usadas para fins legítimos. Os governos manifestaram interesse em regulamentar as plataformas de mídia social, mas acreditamos que não haverá tempo suficiente para esses sites limparem as "ondas" de notícias falsas. Além disso, existe a dificuldade técnica de compactar notícias falsas na presença de diferentes idiomas em grandes áreas geográficas, como acontece na Europa - ao contrário dos EUA, onde o inglês é o principal idioma usado em publicações de mídia social.

Infelizmente, o lado da tecnologia que permite que propagadores de notícias falsas influenciam o sentimento público tornou-se ainda mais poderoso. O caso em questão é o chamado "Photoshop para áudio" da Adobe, que pode muito bem ser usado como uma ferramenta para enganar o público. Embora a Adobe não tenha divulgado nenhuma informação adicional sobre este software, ele antecipa onde as coisas estão indo em termos da crescente dificuldade de distinguir fato real de falsidade.

Vítimas inocentes serão apanhadas no fogo cruzado à medida que os países aumentam sua presença virtual

Os ataques direcionados continuarão entre as vítimas tradicionais, mas, em 2019, até os países que não costumam ser alvo também estarão envolvidos. As nações que estão firmando suas capacidades cibernéticas por qualquer motivo irão procurar apoiar e capacitar os hackers domésticos, seja como preparação ou como resposta a ataques percebidos ou anteriores. **A má notícia é que esses desenvolvimentos terão efeitos colaterais sobre vítimas inocentes completamente alheias a essas respostas cibernéticas.** Indivíduos, empresas e até grandes organizações, incluindo aquelas que têm efeitos abrangentes sobre o público em geral, serão pegos no fogo cruzado à medida que os países lidarem com a maneira de conduzir suas operações. Nós já vimos isso acontecer com o WannaCry e o NotPetya - o dano colateral só aumentará.

Supervisão regulatória será intensificada

As conversas existentes em torno da segurança levarão os governos a aumentar a supervisão regulatória não apenas dos assuntos de privacidade, mas também dos segmentos de consumo e industrial da Internet das Coisas (IoT). Nos EUA, um projeto de lei na Califórnia exige que fabricantes imponham o uso de senhas fortes em seus dispositivos inteligentes mostra-se ser um passo importante nessa direção. Esperamos ver os governos nacionais proibindo o uso de dispositivos de IoT industriais e de consumo inseguros, começando com a legislação a ser introduzida em 2019.

SEGMENTO DE SEGURANÇA

Os cibercriminosos irão utilizar mais técnicas para se disfarçar

Em resposta aos fornecedores de tecnologias de segurança, especialmente o interesse renovado no machine learning para cibersegurança, **criminosos irão utilizar mais táticas maliciosas para se "disfarçar"**. Novas maneiras de utilizar objetos de computação normais para outros propósitos que não os de uso pretendido ou projetados – uma prática conhecida como "living off the land" – irão continuar sendo descobertas, documentadas e compartilhadas. Nós estamos observando algumas dessas, incluindo:

- O uso de extensões de arquivos não convencionais como .URL, .IQY, .ISO, .PUB, e .WIZ
- Menor confiança nos executáveis atuais, como no uso de componentes "sem arquivo", Powershell, scripts, e macros.
- Malware assinado digitalmente como observado anteriormente em nossa pesquisa "Exploring the Long Tail of (Malicious) Software Downloads", uma técnica já muito usada e que continuará sendo explorada devido sua eficácia.
- Novos métodos de ativação, além de técnicas previamente observadas, como o uso de Mshta, Rundll32, Regasm, or Regsvr32.
- O abuso de contas de e-mails ou serviços de armazenamento online em aplicações de pontos de acesso, como comando e controle ou sites de download ou exfiltração.
- Arquivos do sistema legítimos minimamente modificados ou infectados.

Empresas que dependem somente de tecnologias de IA como sua única solução de segurança vão ter desafios, conforme os criminosos começam a usar estas técnicas, e outras, para infectar sistemas. Nós esperamos que essas táticas cibercriminosas se tornem muito mais divulgadas em 2019.

99,99% dos ataques baseados em exploração ainda não serão baseados em vulnerabilidades de Zero day

Explorações de Zero day - pedaços de malware in-the-wild que usam vulnerabilidades de software os quais os fornecedores afetados desconhecem, têm sido um ponto de foco em segurança de TI, fazendo manchetes sempre que um novo ataque é descoberto, pois eles são relativamente raros.

Por um lado, é difícil para os cibercriminosos encontrarem vulnerabilidades de software não descobertas devido à infraestrutura existente de divulgação responsável, que premia pesquisadores de vulnerabilidades por seus resultados, incluindo a Zero Day Initiative (ZDI) da Trend Micro. E mesmo se o fizerem, bastará a descoberta do ataque para que os fornecedores sejam levados a tomar as medidas adequadas. Por outro lado, a oportunidade mais acessível para os cibercriminosos é a janela de exposição que se abre entre o lançamento de um novo patch e quando este é implementado nos sistemas corporativos. Os administradores de patch precisarão da estratégia adequada e do tempo necessário para aplicar os patches, e esses problemas de eficiência fornecerão tempo suficiente para que os cibercriminosos

montem um ataque. Uma vez que os detalhes da vulnerabilidade tenham sido publicados por meio de uma divulgação, o tempo de pesquisa para usar um ponto fraco é significativamente reduzido.

Em 2019, ataques baseados em exploits bem-sucedidos irão envolver vulnerabilidades para as quais os patches estão disponíveis por semanas ou até meses, mas ainda não foram aplicados. Continuaremos a ver casos de explorações do dia zero sendo utilizados na segurança da rede.

Ataques altamente direcionados começarão a usar técnicas baseadas em Inteligência Artificial

Ataques direcionados por agentes de ameaças bem financiados começarão a usar técnicas baseadas em Inteligência Artificial (IA) para reconhecimento. O uso da IA dará aos atacantes a capacidade de prever os movimentos de executivos ou outras pessoas de interesse. Eles podem utilizar a IA para determinar quando e onde os executivos da empresa devem estar no futuro como, por exemplo, os hotéis em que as empresas normalmente os registram, os restaurantes escolhidos para reuniões e outras preferências que podem ajudar a restringir seus próximos locais prováveis.

Por sua parte, os fornecedores de segurança irão desenvolver suas próprias técnicas defensivas de IA. As equipes de segurança também usarão inteligência artificial, da mesma forma que o machine learning, para entender em um nível muito mais íntimo quais são as atividades básicas de uma empresa, a fim de ser alertado imediatamente quando algo fora do comum acontecer no que diz respeito à segurança. Cenários futuristas desse tipo dão uma ideia sobre a próxima fronteira da tecnologia da IA e o que isso significa para a segurança.

SISTEMAS DE CONTROLE INDUSTRIAL

Ataques direcionados a ICSs no mundo real irão se tornar uma preocupação crescente

Países que estarão aprendendo e exercitando suas capacidades cibernéticas irão conduzir ataques na infraestrutura crítica de países menores. Eles o farão para obter vantagens políticas ou militares, ou para testar capacidades contra países que ainda não têm aptidão de retaliar, entre outras possíveis motivações. Se os ataques irão se concentrar em sistemas de controle industrial (ICSs) de água, eletricidade ou manufatura, isso dependerá da intenção ou oportunidade do autor da ameaça. No entanto, os incidentes vão destacar pontos fracos como aqueles que deveriam ser restringidos pela diretiva de segurança de rede e de informações da União Europeia (Diretiva NIS) com seus regulamentos para operadores de serviços essenciais.

A conduta desses ataques será a mesma de qualquer outra ameaça direcionada que comece em reconhecimento, até que as metas do atacante sejam cumpridas. Um ataque ICS bem-sucedido impactará na instalação-alvo por meio de paradas operacionais, equipamentos danificados, perdas financeiras indiretas e, na pior das hipóteses, riscos de saúde e segurança dos colaboradores e consumidores.

Os bugs IHM continuarão a ser a fonte primária de vulnerabilidades ICS

Baseado nos dados da ZDI, grande parte das vulnerabilidades relacionadas ao software usado com sistemas de controle de supervisão e aquisição de dados (SCADA) estava nas interfaces homem-máquina (IHMs), 27, 28 que servem como hub principal para gerenciar os diferentes diagnósticos e controladores modulares em uma instalação. Os ICSs, em geral, que incluem sistemas de controle distribuído (DCSs) e diferentes dispositivos de campo, bem como sistemas SCADA, usam alguma forma de HMI. **Em 2019, veremos ainda mais vulnerabilidades de IHM sendo relatadas.**

Por enquanto, esses tipos de software estão mais prontamente disponíveis para os pesquisadores de vulnerabilidade. Também sabe-se que o software IHM não é tão robusto e seguro quanto softwares de empresas como Microsoft e Adobe por vários razões, incluindo a suposição incorreta de que esse tipo de software funcionará apenas em ambientes isolados ou em air-gapped. Além disso, a manutenção e a atualização do software IHM podem ser afetadas ou prejudicadas pelos movimentos de mercado existentes em torno de pequenos fornecedores, que são adquiridos por empresas maiores ou regionais que se fundem com outros.

INFRAESTRUTURA DA NUVEM

Definições de segurança mal configuradas durante a migração para a cloud resultará em mais violações de dados

Migração de dados para a cloud é um esforço em toda a empresa, que deve implicar o mesmo nível de planejamento, comprometimento e envolvimento como em qualquer outra realocação física – talvez ainda mais. Cada migração para a cloud é única em termos de escopo e ritmo, e qualquer melhor prática da indústria ainda precisará ser alinhada com uma circunstância específica da empresa e suas necessidades atuais.

Nossa previsão é que haja mais casos de violações de dados, que serão um resultado direto de definições de segurança mal configuradas durante a migração para a cloud. Substituir a infraestrutura local ou uma nuvem privada por um provedor de serviço cloud pode abrir a empresa a riscos de segurança, a menos que a empresa tenha um bom controle sobre o que está acontecendo com os seus dados. Cloud storage buckets podem ser privados por padrão, mas um bucket existente de fora irá carregar as suas permissões já existentes. Políticas de Acesso devem, portanto, ser muito bem entendidas, bem implementadas e bem preservadas ao longo do uso do bucket.

Instâncias cloud serão usadas para minerar criptomoedas

Mineração em nuvem é uma alternativa para entusiastas na forma legítima de mineração de criptomoedas. Por meio dela, um minerador compra potência de CPU de um provedor ao invés de investir em equipamento. Há diferentes planos de pagamentos para este modelo de negócio, mas o maior apelo da mineração em cloud é que ela é fácil de começar e manter, e por isso faz sentido para alguns mineradores que têm no hardware ou na eletricidade uma barreira.

Com um pouco de imaginação, **mais e mais cibercriminosos irão tentar sequestrar contas na nuvem para minerar criptomoedas ou manter controle através de outras alternativas.** Isto significa que os relatos na mídia sobre cryptojacking – o uso não autorizado dos computadores de minerar criptomoedas – descobertos em ambientes cloud em 2018 é um sinal de uma tendência crescente, e não somente uma tentativa qualquer por parte dos cibercriminosos. Ferramentas de scanner no cloud bucket já estão disponíveis, adicione a isto a dificuldade de obter as múltiplas configurações de segurança para cada implementação correta, e os cibercriminosos irão inevitavelmente encontrar o caminho para a direção certa. Nós também esperamos uma ocorrência mais comum de malwares do tipo de cryptojacking, que irão minimizar o risco de detecção por sufocar o uso do recurso.

Mais vulnerabilidades em softwares relacionados à nuvem serão descobertas

Em termos de preferência de ataque, cibercriminosos continuarão buscando escolhas fáceis; tais como as credenciais das contas e até recursos da cloud motivados a tomar controle dos bancos de dados. De qualquer maneira, a pesquisa sobre a fragilidade da infraestrutura cloud não irá se manter paralisada. À medida em que a escolha pela nuvem aumenta, nós veremos pesquisas sobre vulnerabilidades na infraestrutura cloud começarem a ganhar chão, especialmente enquanto a comunidade open-source encontra mais usos e se aprofunda em softwares como Docker, um programa de containers e Kubernetes, um sistema que orquestra containers.

Ambos Docker e Kubernetes são amplamente adotados para uso em implantações baseadas em cloud. Já houve algumas vulnerabilidades no Kubernetes divulgadas em anos recentes - inclusive uma principal, com classificação "crítica", foi descoberta em dezembro de 2018. Enquanto isso, em um caso notável de pesquisadores investigando vulnerabilidades na infraestrutura cloud, mais de uma dúzia de imagens maliciosas de Docker foram encontradas através da Kromtech por terem sido baixadas pelo menos por cinco milhões de vezes por desenvolvedores desavisados ao longo de um período de um ano, antes que eles fossem retirados.

CASAS INTELIGENTES

Cibercriminosos irão competir pelo domínio na crescente "guerra de worms " em IoT

Quanto mais dispositivos inteligentes estiverem conectados em redes domésticas, roteadores continuarão a ser um atrativo vetor de ataques para cibercriminosos esperando para tomar controle de qualquer quantidade de dispositivos e para qualquer que seja a finalidade. **O ambiente de smart home irá repetir uma era tecnicamente memorável na história da segurança da informação: A tão falada "guerra de worms", no surto de worms do começo dos anos 2000.**

Ataques recentes baseados em roteadores que afetam dispositivos inteligentes, ou ataques em IoT, são na maioria das vezes os mesmos códigos fonte vazados do malware Mirai, que infectou primeiro os dispositivos Linux em agosto de 2016, ou vindos de outros malwares com comportamento similar. Estes pedaços de malware usam uma porção de exploits conhecidos e, na maioria das vezes, senhas e logins fracos para entrar nos dispositivos, isso significa que todos eles estão verificando automaticamente a internet e descobrindo exatamente os mesmos dispositivos. Como há um número finito de dispositivos e apenas uma parte das necessidades de malware estar no controle de um único dispositivo para executar cargas úteis e atividades maliciosas como ataques DDoS para executar os payloads, os cibercriminosos começarão a adicionar códigos para impedir outros atacantes de usar o dispositivo ou expulsar uma infestação já existente de malwares. Desse modo, ele torna-se o dono exclusivo do dispositivo. Especialistas em segurança irão encontrar um comportamento em comum: os desenvolvedores do Netsky começaram uma guerra de worms com outros hackers por trás de outros notáveis worms na época: Mydoom e Bagle.

Surgirão os primeiros casos de idosos tornando-se vítimas fáceis de ataques em dispositivos de saúde inteligente

Vulnerabilidades em dispositivos inteligentes continuarão a ser encontradas por pesquisadores, entusiastas e atacantes. Todavia, os ataques deste tipo permanecerão esporádicos nos anos seguintes enquanto um caminho claro e fácil para o lucro ainda não surgir para os cibercriminosos. Depois de 2019, é fácil de especular como pesquisadores de vulnerabilidades ou até mesmo hackers irão tentar invadir dispositivos inteligentes e sistemas, especialmente os associados com pesquisas importantes e escolha de mercado como, por exemplo, carros autônomos. Por agora, cibercriminosos estão unicamente focados no dinheiro, e como há várias outras maneiras de lucrar, um ataque global a dispositivos inteligentes é improvável de acontecer em 2019.

No limitado domínio de health trackers, de qualquer maneira, nós acreditamos que no mundo real **as primeiras vítimas de ataques em dispositivos de saúde inteligente serão idosas**. Empresas estão explorando clientes idosos como usuários potenciais de smart trackers, ou outro dispositivo de saúde conectado, tais como monitores de batimentos cardíacos ou outras tecnologias que alertam quando um idoso escorrega ou cai. No passado, idosos foram alvos de golpes por telefone que tinham como objetivo o dinheiro de sua aposentadoria. Acreditamos que veremos idosos tornando-se vítimas fáceis de ataques que abusam deste tipo de dispositivo já em 2019. No entanto, usuários idosos do health check não conhecerão o suficiente de computação para checar as configurações de privacidade do dispositivo, resultando em vazamento de dados de informação médica confidencial, permitindo que cibercriminosos acessem dados relacionados a saúde e outros dados pessoais.

Depois de 2019, veremos também mais "voice attacks" afetando usuários de todas as idades, conforme as pesquisas sobre vulnerabilidades em reconhecimento de voz inteligente amadurecem e enquanto assistentes inteligentes começam a ser uma característica mais presentes em casas inteligentes.

PREPARANDO-SE PARA O ANO QUE ESTÁ CHEGANDO

Mais ameaças desconhecidas exigem segurança inteligente em multicamadas para corporações

A realidade da arquitetura dos data centers híbridos modernos e a evolução no acesso e mobilidade de endpoints — incluindo parceiros e terceiros conectados à rede — irão demandar muito mais dos times de Segurança de TI em 2019. A escassez de habilidades nessa área será mais nítida, fazendo com que o aumento do conhecimento existente com tecnologias de segurança inteligentes, eficientes e múltiplas se torne mais crítico e necessário.

Proteger as redes corporativas contra ameaças em constante mudança requer uma percepção inteligente de como os riscos de segurança devem ser gerenciados. A gama completa de ameaças conhecidas e desconhecidas nunca pode ser abordada por uma única tecnologia ultramoderna, pois cada nova geração de ameaças desafia diferentes aspectos da segurança de TI. As empresas não devem procurar por uma "solução mágica", mas sim por uma combinação entre gerações de técnicas de defesa contra ameaças que aplicará a técnica certa no momento certo. Como destacamos nos pontos abaixo:

- Prevenção de Malware (anti-malware, behavioral analysis, machine learning, web reputation).
- Segurança de Rede (intrusion prevention, firewall, vulnerability analysis).
- Segurança de E-mail (anti-spam).
- Segurança do Sistema (application control, integrity monitoring, log inspection).
- Mecanismos de detecção especializados, sandbox customizada e inteligência sobre ameaças globais (para ameaças desconhecidas).
- Segurança de Endpoint.
- Prevenção integrada de perda de dados.

Estas soluções devem ser otimizadas para a realidade de onde e como os usuários realmente se conectam à rede em termos de plataformas e dispositivos. Sendo assim, as equipes de segurança de TI devem ser capacitadas por essas tecnologias para visualizar atividades de rede, avaliar ameaças e tomar as medidas adequadas.

Desenvolvedores devem adotar a cultura DevOps com a segurança como foco.

DevOps combina processos de desenvolvimento de software (Dev) com operações de TI (Ops) para encurtar o ciclo de vida do desenvolvimento de sistemas de uma maneira muito mais eficiente e integrada. DevSecOps — DevOps com foco em segurança — leva a fortes práticas que integram segurança em cada etapa do caminho. Os desenvolvedores de software devem adotar essa mentalidade, juntamente com sua variedade de ferramentas práticas, para colher não apenas os benefícios de segurança, mas também a redução de custos.

Falhas de projeto e outras vulnerabilidades, incluindo aquelas que vazam informações pessoais, são frequentemente descobertas depois que um software é instalado em computadores ou dispositivos

de produção, e tais falhas poderiam diminuir significativamente se a segurança fosse integrada no desenvolvimento logo na fase de planejamento.

Usuários precisam se interessar pelo exercício responsável da cidadania digital e pelas melhores práticas de segurança.

A capacidade dos usuários de distinguir a verdade da mentira, particularmente na internet, se tornará ainda mais importante em 2019. Espalhar a conscientização sobre a mecânica por trás das fake news fará com que o público fique mais resistente à manipulação de opinião. Os governos estaduais e locais farão bem ao incluir treinamento em conscientização sobre segurança cibernética nas escolas e conduzir o mesmo conteúdo para o público em geral.

A engenharia social depende essencialmente das mesmas fraquezas humanas. Portanto, os usuários devem aplicar o mesmo nível de pensamento crítico necessário em seu consumo de mídia social à sua diligência em verificar se um e-mail ou um telefonema está realmente vindo de uma fonte confiável.

Dispositivos de consumo como computadores, tablets e smartphones devem ser protegidos contra ameaças como ransomware, sites perigosos e ladrões de identidade, garantindo principalmente que a proteção completa esteja disponível por meio de soluções antimalware. Essas tecnologias também devem incluir proteção de dados para proteger arquivos valiosos, impedir novas ameaças e garantir que as transações monetárias online sejam realizadas com segurança

Os usuários devem alterar suas senhas regularmente, ter credenciais exclusivas para contas diferentes, aproveitar os recursos de autenticação multifator sempre que possível ou usar uma ferramenta de gerenciamento de senhas para ajudar a armazenar credenciais com segurança.

Os administradores de smart home também devem proteger seus roteadores e dispositivos, verificando as configurações padrão dos produtos e entendendo como configurá-los com segurança, atualizando regularmente o firmware, conectando-se apenas a redes seguras, configurando firewalls para permitir o tráfego somente em portas específicas e configurando "redes convidadas" para minimizar a introdução desnecessária de novos dispositivos na rede. Além disso, sempre que possível, os proprietários devem revisar os históricos de registros dos dispositivos. É claro que senhas únicas e fortes para roteadores e dispositivos também devem ser aplicadas.

O cenário de ameaças promete muitos desafios para quase todos os setores da internet pública em 2019, mesmo que a internet mais rápida, para o bem ou para o mal, surja no horizonte com o lançamento do 5G. No entanto, as ferramentas e tecnologias disponíveis devem capacitar usuários e empresas a se posicionarem de forma mais segura na luta contra os cibercriminosos e outras ameaças emergentes. A compreensão profunda dessas questões é um passo na direção certa.

References

StatCounter. *Statcounter Global Stats.* "Operating System Market Share Worldwide, Jan-Dec 2013." Last accessed on 13 November 2018 at http://gs.statcounter.com/os-market-share/all/worldwide/2013.

StatCounter. *Statcounter Global Stats.* "Operating System Market Share Worldwide, Oct 2017 – Oct 2018." Last accessed on 13 November 2018 at http://gs.statcounter.com/os-market-share.

Lorenzo Franceschi-Bicchierai. (17 July 2018). *Motherboard.* "The SIM Hijackers." Last accessed on 13 November 2018 at https://motherboard.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin.

Ponemon Institute. (June 2018). *Akamai.* "The Cost of Credential Stuffing: Asia-Pacific." Last accessed on 13 November 2018 at https://www.akamai.com/us/en/multimedia/documents/white-paper/the-cost-of-credential-stuffing-asia-pacific.pdf.

Donna Freydkin. (9 February 2018). *Today.* "How online 'sextortion' drove one young man to suicide." Last accessed on 28 November 2018 at https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735.

izzie Dearden. (4 May 2018). *Independent.* "Five British men have killed themselves after falling victim to online 'sextortion', police reveal." Last accessed on 28 November 2018 at https://www.independent.co.uk/news/uk/crime/blackmail-online-sextortion-suicides-videos-photos-sexual-police-advice-a8337016.html.

Gallup. (2017). *Gallup.* "State of the American Workplace." Last accessed on 27 November 2018 at https://news.gallup.com/file/reports/199961/SOAW_Report_GEN_1216_WEB_FINAL_rj.pdf.

Polycom. (2018). *Polycom.* "The Changing World of Work." Last accessed on 13 November 2018 at http://www.polycom.com/content/dam/polycom/common/documents/whitepapers/changing-needs-of-the-workplace-whitepaper-enus.pdf

IDC. (1 October 2018). *IDC.* "All Categories of Smart Home Devices Forecast to Deliver Double-Digit Growth Through 2022, Says IDC." Last accessed on 13 November 2018 at https://www.idc.com/getdoc.jsp?containerId=prUS44361618.

hil Muncaster. (14 September 2018.) *Infosecurity Magazine.* "ICO Swamped with GDPR Breach Over-Reporting." Last accessed on 28 November 2018 at https://www.infosecurity-magazine.com/news/ico-swamped-with-gdpr-breach/.

avid Meyer. (4 December 2018). *Fortune.* "How Email Scammers Are Using Marketeer Methods to Target CFOs." Last accessed on 5 December 2018 at http://fortune.com/2018/12/04/targeted-email-fraud/.

Forrester Research. (14 November 2018). *ZDNet.* "Automation will become central to business strategy and operations." Last accessed on 14 November 2018 at https://www.zdnet.com/article/automation-will-become-central-to-business-strategy-and-operations/.

harles Hymas. (20 September 2018). *The Telegraph.* "Government draws up plans for social media regulator following Telegraph campaign." Last accessed on 13 November 2018 at https://www.telegraph.co.uk/news/2018/09/20/government-draws-plans-social-media-regulator-following-telegraph/.

ebastian Anthony. (7 November 2018). *Ars Technica.* "Adobe demos "photoshop for audio," lets you edit speech as easily as text." Last accessed on 13 November 2018 at https://arstechnica.com/information-technology/2016/11/adobe-voco-photoshop-for-audio-speech-editing/.

Lily Hay Newman. (12 May 2017). *Wired.* "The Ransomware Meltdown Experts Warned About Is Here." Last accessed on 28 November 2018 at https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

Adi Robertson. (28 September 2018). *The Verge.* "California just became the first state with an Internet of Things cybersecurity law." Last accessed on 13 November 2018 at https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.

MITRE ATT&CK. *MITRE.* "Tactic: Execution." Last accessed on 13 November 2018 at https://attack.mitre.org/tactics/TA0002/.

European Union Agency for Network and Information Security. *ENISA.* "NIS Directive." Last accessed on 5 December 2018 at https://www.enisa.europa.eu/topics/nis-directive.

Trend Micro. (23 May 2017). *Trend Micro Security News.* "The State of SCADA HMI Vulnerabilities." Last accessed on 13 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities.

Brian Gorenc. (9 July 2018). *Zero Day Initiative.* "Checking In: A Look Back at the First Half of 2018." Last accessed on 28 November 2018 at https://www.zerodayinitiative.com/blog/2018/7/9/checking-in-a-look-back-at-the-first-half-of-2018.

rend Micro. (23 May 2017). *Trend Micro Security News.* "The State of SCADA HMI Vulnerabilities." Last accessed on 13 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities.

Charlie Osborne. (15 May 2018). *ZDNet.* "Cryptojacking attacks surge against enterprise cloud environments." Last accessed on 28 November 2018 at https://www.zdnet.com/article/cryptojacking-attacks-surge-against-enterprise-cloud-environments/.

Udi Nachmany. (1 November 2018). *Forbes.com.* "Kubernetes: Evolution of an IT Revolution." Last accessed on 28 November 2018 at https://www.forbes.com/sites/udinachmany/2018/11/01/kubernetes-evolution-of-an-it-revolution/#366fcb4554e1.

CVE Details. *CVE Details.* "Kubernetes: List of security vulnerabilities." Last accessed on 28 November 2018 at https://www.cvedetails.com/vulnerability-list/vendor_id-15867/product_id-34016/Kubernetes-Kubernetes.html.

Steven J. Vaughan-Nichols. (3 December 2018). *ZDNet.* "Kubernetes' first major security hole discovered." Last accessed on 3 December 2018 at https://www.zdnet.com/article/kubernetes-first-major-security-hole-discovered/.

Security Center. (12 June 2018). *KromTech Security Center.* "Cryptojacking invades cloud. How modern containerization trend is exploited by attackers." Last accessed on 28 November 2018 at https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers.

Brian Krebs. (1 October 2016). *Krebs on Security.* "Source Code for IoT Botnet 'Mirai' Released." Last accessed on 28 November 2018 at https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

Trend Micro. (13 September 2016). *Trend Micro Security News.* "Linux Security: A Closer Look at the Latest Linux Threats." Last accessed on 28 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-security-a-closer-look-at-the-latest-linux-threats.

Spencer Hsieh. (5 October 2018). *Virus Bulletin.* "Security issues of IoV devices." Last accessed on 28 November 2018 at https://www.virusbulletin.com/conference/vb2018/abstracts/security-issues-iov-devices/.

McCall Robison. (15 November 2018). *MarketWatch.* "These common scams target seniors—how to avoid them." Last accessed on 28 November 2018 at https://www.marketwatch.com/story/these-common-scams-target-the-elderlyhow-to-avoid-them-2018-11-15.

Trend Micro. (11 April 2018). *Trend Micro Security News.* "Threats to Voice-Based IoT and IIoT Devices." Last accessed on 28 November 2018 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-to-voice-based-iot-and-iiot-devices.

on Oltsik. (11 January 2018). *CSO Online.* "Research suggests cybersecurity skills shortage is getting worse." Last accessed on 13 November 2018 at https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html.

For Raimund Genes (1963-2017)

TREND MICRO™ | research

TREND MICRO™ RESEARCH

A Trend Micro, líder mundial em cibersegurança, ajuda a tornar o mundo mais seguro para a troca de informação.

A Trend Micro Research é composta por especialistas apaixonados por investigar e descobrir novas ameaças, compartilhando novos insights e ajudando a combater os cibercriminosos. Nossa equipe global identifica milhões de ameaças todos os dias, publicando pesquisas inovadoras e novas técnicas de defesa, o que faz dela uma líder mundial em revelações de novas vulnerabilidades. Nosso foco é estar sempre à frente das ameaças e publicar pesquisas questionadoras e relevantes.

www.trendmicro.com

©2018, Trend Micro, Inc. Todos os direitos reservados. Trend Micro, o logo Trend Micro t-ball e Trend Micro Protection Network são marcas registradas da Trend Micro Inc. Todos os outros produtos ou nomes podem ser marcas registradas de seus respectivos proprietários.