CENÁRIO DE AMEAÇAS 2018: FORTINET PREVÊ CIBERATAQUES ALTAMENTE DESTRUTIVOS E AUTOAPRENDIZAGEM

O mundo do cibercrime adota avanços em inteligência artificial e automação para usar resgate de serviços comerciais, instalar armas nos dispositivos de IoT e atacar infraestruturas fundamentais

WHITE PAPER

SUNNYVALE, Califórnia – 14 de novembro de 2017

Derek Manky, Estrategista de Segurança Global da Fortinet

"Nossa economia digital é impulsionada por inovações tecnológicas que criam oportunidades para coisas boas ou ruins na cibersegurança. A proliferação de dispositivos online e a hiperconectividade de hoje criou um espaço criminoso cada vez mais difícil de ser controlado. Ao mesmo tempo, os criminosos estão usando cada vez mais automação e inteligência artificial a um ritmo e escala imensuráveis em toda a superfície de ataque em constante expansão. Ataques como WannaCry e NotPetya foram só uma amostra das interrupções e dos impactos econômicos que podem acontecer em breve, resultantes de resgate e destruição de serviços comerciais e propriedade intelectual. As abordagens de segurança baseadas em fabric que usam o poder da automação, integração e segmentação estratégica são fundamentais para combater os futuros ataques altamente inteligentes."

RESUMO DA NOTÍCIA:

A Fortinet® (NASDAQ: FTNT), líder global em cibersoluções de alto desempenho, apresentou hoje as previsões da equipe de pesquisa de ameaças globais do Fortinet FortiGuard Labs sobre o cenário de ameaças para 2018. As tendências mostram os métodos e as estratégias que os cibercriminosos usarão no futuro próximo e o possível impacto dos ciberataques na economia global. Visite nosso blog e veja mais detalhes sobre estas previsões. Abaixo, os destaques:

TRANSFORMAÇÃO DIGITAL USADA PARA O BEM E PARA O MAL

Nos próximos dois anos, a superfície de ataque continuará expandindo, enquanto a ampla visibilidade e controle sobre as infraestruturas atuais diminuirão. A proliferação de dispositivos online com acesso a informações pessoais e financeiras e a crescente conexão de tudo, isto é, exércitos de dispositivos IoT e infraestruturas fundamentais de carros, casas e escritórios, além do aumento de cidades inteligentes, criarão novas oportunidades para os cibercriminosos e outras ameaças. O mercado de cibercriminosos está adotando os últimos avanços em áreas como inteligência artificial para criar ataques mais eficazes. Prevemos que essa tendência será maior em 2018, permitindo as tendências destrutivas mencionadas abaixo.

• Surgimento de Hivenets e Swarmbots de autoaprendizagem: Com base em ataques sofisticados como Hajime e Devil's Ivy, prevemos que os cibercriminosos substituirão os botnets por grupos inteligentes de dispositivos comprometidos chamados hivenets para criar vetores de ataque mais eficazes. Os Hivenets usarão autoaprendizagem para atacar sistemas vulneráveis com eficácia, em uma escala sem precedentes. Eles poderão falar uns com os outros e tomar medidas baseadas na inteligência local compartilhada. Além disso, os zumbis se tornarão inteligentes, realizando comandos sem que o controlador de botnet envie instruções. Como resultado, os hivenets poderão crescer exponencialmente como enxames, ampliando sua capacidade de atacar simultaneamente várias vítimas e impedir a mitigação e respostas aos ataques. Embora esses ataques ainda não estejam usando essa tecnologia swarm (enxame), como eles têm o footprint em seu código, os criminosos podem convertê-lo para atuar com um comportamento de autoaprendizagem. Os criminosos usarão inúmeros dispositivos comprometidos, ou swarmbots, para identificar e direcionar diferentes vetores de ataque ao mesmo tempo, permitindo ataques em alta velocidade e escala, eliminando a previsibilidade necessária para combater o ataque. O FortiGuard Labs registrou 2,9 bilhões de tentativas de comunicação de botnet, todas em um trimestre no início deste ano, acrescentando informações sobre a gravidade do que hivenets e swarmbots podem causar.

• Resgaste de serviços comerciais – um grande negócio: Embora a magnitude da ameaça de ransomware tenha aumentado 35 vezes no último ano com ransomworms e outros tipos de ataques, muito mais está por vir. O próximo grande alvo de ransomware provavelmente serão os provedores de serviços na nuvem e outros serviços comerciais com o objetivo de criar receita. As redes hiperconectadas e complexas que os provedores de serviços na nuvem desenvolveram podem produzir apenas um ponto de falha para centenas de empresas, entidades governamentais, infraestruturas fundamentais e organizações de saúde. Nós prevemos que os cibercriminosos começarão a combinar tecnologias de AI com métodos de ataque de vetores múltiplos para pesquisar, detectar e explorar fraquezas no ambiente de um provedor de serviços na nuvem. O impacto desses ataques pode gerar uma boa receita para a organização criminosa e interromper o serviço para talvez centenas ou milhares de empresas e dezenas de milhares ou milhões de clientes.

• Próxima geração de malware mórfico: Se não no próximo ano, logo veremos malware completamente criado por máquinas baseado na detecção automatizada de vulnerabilidades e análise complexa de dados. Com a evolução natural das ferramentas atuais, os criminosos poderão desenvolver a melhor exploração possível com base nas características de cada fraqueza única. Os tipos de malware usam modelos de aprendizagem para desviar dos sistemas de segurança e podem produzir mais de um milhão de variações de vírus em um dia. Mas até agora, tudo isso é apenas baseado em um algoritmo, com pouca sofisticação ou controle sobre o resultado. Essa abordagem de próxima geração, chamada de malware mórfico, poderá produzir ataques totalmente novos e personalizados que utilizam as variações atuais baseadas em automação e aprendizado automático simples. O FortiGuard Labs registrou 62 milhões de detecções de malware em apenas um trimestre de 2017. Desses, vimos quase 17 mil variantes de malware de mais de 2.500 famílias de malware diferentes. O aumento da automação do malware complicará ainda mais esta situação no próximo ano.

• Infraestruturas fundamentais como principais alvos: Recentemente, os prestadores de serviços de saúde e as infraestruturas fundamentais assumiram o topo da lista de alvos dos avanços do cibercrime. Isso deve continuar em 2018. A expectativa de responder às demandas de funcionários e consumidores nas velocidades digitais está mudando os requisitos dessas redes, aumentando a necessidade de segurança avançada em redes originalmente projetadas para operar isoladamente. Com o alto valor dessas redes e a possibilidade de resultados devastadores, se elas estiverem comprometidas ou desativadas, os prestadores de infraestruturas fundamentais travarão uma batalha com as organizações do cibercrime. Além disso, armar o cibercrime, criando malwares militarizados ou outros tipos de ataques de organizações ciberterroristas, aumentará a urgência de proteger as infraestruturas fundamentais do mundo inteiro.

• Aprendizado de máquina e a darkweb: Com a evolução do mundo do cibercrime, vem a evolução da darkweb. Já vemos serviços avançados oferecidos em mercados da darkweb que utilizam técnicas de aprendizado de máquina. Por exemplo, o serviço conhecido como FUD (do inglês fully undetected, ou totalmente não detectado) agora faz parte de várias ofertas de crime como serviço. Neste sistema, os desenvolvedores criminosos embutem o código de ataque e o malware em um serviço de análise por um valor. Depois, eles recebem um relatório sobre se as ferramentas de segurança de diferentes fornecedores que podem detectá-lo. Para encurtar este ciclo, também é possível usar aprendizado de máquina para modificar o código dependendo de como e o que foi detectado no laboratório, tornando essas ferramentas de invasão e do cibercrime mais indetectáveis. As ferramentas de sandbox avançaram com a aprendizagem de máquina, permitindo identificar rapidamente ameaças não vistas anteriormente e criar proteções de forma dinâmica. Essa mesma abordagem pode ser automatizada e usada na outra direção para mapear redes, encontrar alvos de ataque, determinar onde esses alvos de ataques estão enfraquecidos ou criar um alvo para realizar um teste de ataque virtual e, depois, construir e lançar um ataque personalizado.

TENDÊNCIAS E LIÇÕES PARA SE MANTER À FRENTE DAS AMEAÇAS

Cibercriminosos empreendedores podem usar os avanços da automação e inteligência artificial e as ferramentas certas para comprometer gravemente nossa economia digital. Soluções de segurança devem ser desenvolvidas usando tecnologias de segurança integradas, inteligência de ameaças relevantes e fabric de segurança configurável de forma dinâmica. A segurança deve operar a velocidades digitais, automatizando as respostas e aplicando inteligência e autoaprendizagem para que as redes possam tomar decisões eficazes e autônomas. Isso não só aumentará a visibilidade e centralizará o controle, como também possibilitará a segmentação estratégica, expandindo a segurança na infraestrutura da rede para rapidamente identificar, isolar e corrigir os dispositivos comprometidos e frustrar ataques, mesmo em diferentes ecossistemas da rede, de dispositivos de usuários e recursos na rede local a ambientes na nuvem. Além disso, a higiene de segurança básica precisa fazer parte dos nossos procedimentos de segurança fundamentais, muitas vezes negligenciada, mas indispensável para limitar as consequências negativas que queremos evitar.

Outros recursos

• Veja mais detalhes sobre o Fortinet Security Fabric.

• Veja mais informações sobre nossas previsões para 2018 em nosso blog.

• Veja nossos vídeos que resumem as lições valiosas tiradas do relatório: hivenets, infraestruturas fundamentais e automação.

• Assine os informativos semanais da FortiGuard ou faça parte do beta aberto do FortiGuard Threat Intelligence Service da Fortinet.

• Siga a Fortinet no Twitter, LinkedIn, Facebook e YouTube.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 330,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

.

FTNT-O

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

November 2017