A cada 40 segundos uma empresa sofre um ataque ransomware

bit.pt/40-segundos-empresa-sofre-um-ataque-ransomware/

12/12/2016

Entre janeiro e setembro de 2016, o número de ataques a empresas triplicou. Os valores passaram de um ataque a cada 2 minutos para um a cada 40 segundos. A análise do ano de 2016 comprovou como o modelo de negócio de Ransomware-as-a-Service atrai os cibercriminosos.

Os ataques a utilizadores também foram mais frequente e passaram de um a cada 20 segundos para um a cada 10. Durante o ano analisado pela Kaspersky, apareceram mais de **62 novas famílias de ransomware operacionais**. A ameaça deste tipo de malware cresceu tão rapidamente que a Kaspersky afirma em comunicado que foi **o "protagonista das ameaças virtuais em 2016"**.

No Boletim de Segurança da Kaspersky Lab, o ano de 1016 revelou até que ponto o novo modelo de negócio **Ransomware-as-a-Service** atrai ciberciminosos que não têm as habilidades ou os recursos necessários. Os criadores de códigos oferecem os seus produtos nocivos "on demand" vendendo versões modificadas de forma exclusiva aos seus clientes. De seguida essas versões são distribuídas através de spam ou em sites, e é paga uma comissão aos criadores de códigos.

Segundo a investigação da empresa, o ransomware continuou a crescer, tornando-se mais sofisticado e diversificado e aproximando-se de novos dados, dispositivos, indivíduos e empresas. Uma em cada cinco empresas no mundo sofreu um incidente de segurança de TI como resultado de um ataque de ransomware e uma em cada cinco pequenas empresas não recuperou os seus dados, mesmo depois de pagar.

Alguns setores da indústria sofreram mais ataques que outros. A análise indica que não existe um sector de baixo risco: com a maior taxa, cerca de 23%, está a Educação e com 16%, o sector com menor risco, Comércio e Lazer.

O "ransomware educativo" desenvolvido para dar aos administradores de sistemas uma ferramenta para simular ataques de ransomware foi rapidamente explorado por hackers. Essa exploração deu lugar a Ded_Cryptor e Fantom, entre outros.

Ataques de ransomware, detetados pela primeira vez em 2016, incluíam a encriptação do disco e o bloqueio, de uma vez só, do acesso aos arquivos por parte dos cibercriminosos – Petya é um exemplo. Dcryptor, também conhecido como Mamba, foi um passo além, bloqueando todo o disco rígido.

Ao longo deste ano começaram a aparecer Trojans sofisticados com erros de software e incorreções nas notas de resgate. Com isto a probabilidade de as vítimas não conseguirem voltar a recuperar os seus dados aumenta.

Apesar de todas as preocupações em 2016, surgiram também a primeiras formas de luta contra o ransomware. Exemplo disso é o projeto No More Ransom, lançado em julho, que reúne as forças de segurança e os fabricantes de segurança para localizar e interromper as grandes famílias deste tipo de ameaça. Este projeto ajuda as pessoas a recuperar os seus dados e a reduzir o modelo de negócio lucrativo destes hackers.

O relatório reflete a opinião fundamentada de 31 líderes da **Intel Security,** onde se integra a McAfee Labs. Ele examina as tendências atuais no cibercrime e faz previsões sobre o que o futuro reserva para as organizações que desejam aproveitar as novas tecnologias tanto para expandir os seus negócios como para ter uma segurança mais reforçada.

"Para mudar as regras do jogo entre invasores e defensores, precisamos anular as principais vantagens dos nossos adversários", afirma **Vincent Weafer**, vice-presidente do McAfee Labs na Intel Security. "À medida que

uma nova técnica de defesa é desenvolvida, a sua eficácia vai aumentando até que os invasores são forçados a desenvolver contramedidas para evitá-la", sublinha. Para superar as capacidades dos cibercriminosos, diz o responsável, é preciso ir para lá da simples compreensão do panorama de ameaças para mudar a dinâmica entre invasores e defensores. Aqui, há seis áreas-chave: assimetria de informações, tornar os ataques mais caros, aumentar a visibilidade, identificar melhor a exploração de legitimidade, reforçar a proteção de dados descentralizados, bem como detectar e proteger ambientes sem agente.

Panorama de ameaças de 2017

As previsões são abrangentes, incluindo ameaças associadas a ransomware, ataques de hardware e firmware, ataques em dispositivos de IoT da "casa inteligente", uso da inteligência de máquina para otimizar ataques de engenharia social e maior colaboração entre o setor e a polícia:

1. Os ataques de **ransomware** sofrerão uma queda no segundo semestre de 2017 em termos de volume e eficácia.
2. As explorações de vulnerabilidade do **Windows** continuarão a diminuir; já as ameaças que têm como alvo softwares de infraestrutura e softwares de virtualização irão aumentar.
3. **Hardware e firmware** serão alvos cada vez mais visados por invasores altamente capacitados.
4. Usando softwares em execução em laptops, os hackers farão tentativas de "**sequestro de drones**" para diversas finalidades criminosas ou de hacktivismo.
5. Os **ataques móveis** combinarão bloqueios de dispositivos móveis com o roubo de credenciais, permitindo que os ladrões cibernéticos acedam a informações como contas bancárias e cartões de crédito.
6. Os malwares da **IoT** criarão pontos não autorizados de acesso à casa conectada que poderão ficar anos sem ser detectados.
7. A aprendizagem de máquina acelerará a proliferação e aumentará a sofisticação de ataques de **engenharia social**.
8. Anúncios falsos e "curtidas" compradas continuarão a proliferar e a comprometer a reputação.
9. As guerras de **publicidade** irão ser agravadas e as novas técnicas utilizadas pelos anunciantes para distribuir anúncios serão copiadas por hackers para aumentar a capacidade de distribuição de malware.
10. **Hacktivistas** irão desempenhar um papel importante na exposição de questões de privacidade.
11. Graças à maior colaboração entre o **setor e a polícia**, operações de imobilização realizadas pela polícia reduzirão o cibercrime.
12. A partilha de informações sobre ameaças resultará em grandes progressos em 2017.
13. A **espionagem** ciber tornar-se-à tão comum no setor privado e no submundo do crime como já é entre estados-nação.
14. Empresas do setor de segurança física e ciber irão colaborar para blindar produtos contra ameaças digitais.

Previsões para a segurança da nuvem e a Internet das Coisas

O McAfee Labs também apresentou previsões sobre a IoT e a segurança da nuvem para os próximos dois a quatro anos, incluindo ameaças e tendências económicas, políticas e regionais que provavelmente marcarão cada área. Com base nas considerações feitas pelos investigadores da Intel Security, as seguintes previsões também antecipam as medidas que provavelmente serão tomadas por fornecedores de dispositivos, provedores de serviços em nuvem e fornecedores de segurança.

As previsões para a nuvem englobaram vários tópicos. Tem a questão da confiança na nuvem, armazenamento de propriedade intelectual, autenticação, vetores de ataque no tráfego leste-oeste e norte-sul e lacunas de

cobertura entre camadas de serviço. A McAfee destaca ainda os **hackers de aluguer na nuvem**, ataques de "negação de serviço por resgate", leis e processos judiciais em detrimento da inovação e transferência de dados entre fronteiras; biometria como viabilizadora da nuvem, agentes de segurança de acesso em nuvem (CASBs), aprendizagem de máquina, seguro ciber e os constantes conflitos que colocam a velocidade, a eficiência e o custo na contra-mão do **controlo, da visibilidade e da segurança** das ofertas de nuvem.

As previsões para a IoT concentraram-se nos seguintes tópicos: economia do crime cibernético, ransomware, hacktivismo, ataques de estados-nação à infraestrutura do crime, desafios para os fabricantes de dispositivos, ameaças à privacidade e oportunidades, criptografia, monitoramento comportamental, seguro cibernético e gestão de riscos.

Seis desafios críticos do setor

A seção do relatório sobre problemas difíceis de resolver pressiona o setor a aumentar a eficácia da defesa contra ameaças reduzindo a assimetria de informações entre defensores e invasores, tornando os ataques mais caros ou menos rentáveis, aumentando a visibilidade dos eventos cibernéticos, identificando a exploração da legitimidade com mais eficácia, reforçando a proteção de dados descentralizados, bem como detectando e protegendo ambientes sem agente.

O **Relatório de previsões de ameaças para 2017 do McAfee Labs** está disponível na íntegra.