Em tempos de espionagem, a palavra de ordem de empresas e usuários é a segurança de suas informações. E sem muitas surpresas, um levantamento divulgado pela Intel mostra quais são as principais ameaças cibernéticas esperadas para o ano que vem. Além disso, o estudo prevê o que esperar desse cenário até 2020 e como o mercado de segurança de TI deve se preparar.

O Relatório de Previsões de Ameaças do McAfee Labs apresenta as ideias de 33 líderes de segurança cibernética do McAfee Labs da Intel Security, do Gabinete do CTO, da Foundstone Professional Services e de equipes de Pesquisa Avançada de Ameaças.

No quesito "hardware e firmware", a Intel prevê que os ataques continuarão, assim como o mercado de ferramentas que os tornam possíveis se expandirá e crescerá. As máquinas virtuais serão atacadas com êxito por meio de rootkits no firmware do sistema. Enquanto isso, o ransomware, um tipo de malware que cobra um valor de "resgate" para liberar o acesso, também continuará a ser explorado por cibercriminosos.

Outro ponto destacado na pesquisa é sobre as tecnologias vestíveis e automóveis. Neste caso, aparelhos que não contarem com proteção integrada de segurança serão os alvos preferidos dos crackers, porque eles poderão coletar dados extremamente pessoais. Mais importante ainda, o fato desses gadgets se sincronizarem com os smartphones cria possibilidades de acesso a dados valiosos. Entre as vulnerabilidades estão kernels do sistema operacional, software de rede e Wi-Fi, interfaces de usuário, memória, arquivos locais e sistemas de armazenamento e software de controle de acesso e segurança.

As empresas continuarão melhorando suas posturas de segurança, implementando as mais recentes tecnologias, trabalhando para contratar pessoas talentosas e experientes, criando políticas eficazes e mantendo a vigilância. Assim, os atacantes provavelmente mudarão seu foco e atacarão cada vez mais através dos funcionários, visando, entre outras coisas, os sistemas residenciais deles, que são relativamente desprotegidos, para obter acesso às redes das empresas. Falando no setor corporativo, os cibercriminosos, empresas concorrentes e agentes de Estados nacionais atacarão cada vez mais os serviços de nuvem, os quais gerenciam uma quantidade cada vez maior de informações confidenciais. Esses dados podem ser sobre estratégias de negócios de organizações, inovações de última geração, dados financeiros, planos de aquisição e alienação, dados de funcionários, entre outros documentos.

Ainda nesse aspecto, informações pessoais roubadas estão sendo vinculadas entre si em grandes depósitos de dados, tornando os registros combinados mais valiosos para os criminosos. No próximo ano acontecerá o desenvolvimento de um mercado negro ainda mais robusto para obter dados pessoais, incluindo nomes de usuário e senhas roubadas. Com isso, podem-se desencadear mais casos que envolvam ataques à integridade de sistemas de bancos de dados.

"Para lidar com as realidades desses cenários de negócios, tecnologia e ameaças, precisamos auxiliar as organizações a chegar aonde elas precisam estar, utilizando tecnologias que promovam e não atrapalhem seus negócios, além de compreender que tipos de ameaças podem estar diante delas tanto amanhã como num futuro distante", afirma Vincent Weafer, vice-presidente do McAfee Labs da Intel Security. Previsões até 2020

A perspectiva da Intel tenta prever como mudarão os tipos de autores de ameaças, como mudarão os comportamentos e objetivos dos atacantes e também como o setor enfrentará esses problemas.

Para os próximos cinco anos, são esperados ataques em pontos fracos no firmware e no hardware. Além disso, os criminosos vão adotar métodos mais sofisticados que serão mais difíceis de serem detectados, incluindo ameaças sem arquivo, infiltrações criptografadas, malwares que evitam áreas restritas (sandbox), explorações de remote shell e protocolos de controle remoto.

Como a tecnologia alcançará novos patamares, a Intel acredita que uma guerra cibernética mudará a economia, deslocando o equilíbrio de poder em muitos relacionamentos internacionais. O McAfee Labs prevê que os ataques cibernéticos nas áreas de coleta de informações e de manipulação clandestina de mercados em favor dos agressores se tornarão mais eficazes.

Com tantas ameaças, o setor de segurança desenvolverá instrumentos mais eficazes para identificar e corrigir ataques sofisticados. Será possível desenvolver uma análise comportamental para detectar atividades irregulares de usuários, as quais podem indicar o comprometimento de contas. A segurança integrada à nuvem pode melhorar a visibilidade e o controle.

"Acompanhar, prever e se antecipar aos adversários exige que tenhamos o mesmo nível de troca de informações, computação em nuvem, capacidade de distribuição, agilidade de plataformas e também os mesmos recursos humanos que os criminosos cibernéticos normalmente empregam", completa Weafer. "Para vencer os combates contra as ameaças futuras, as organizações devem ver mais, aprender mais, detectar e reagir com mais agilidade e aproveitar ao máximo todos os recursos técnicos e humanos à sua disposição".

Fonte: CanalTech, em 24.11.2015.