Por que o WannaCry se espalhou tão rapidamente?

Carlos Rodrigues (*)

Desde a primeira vez que o ransomware apareceu, há 20 anos, tornou-se uma das ameaças mais destrutivas para as empresas, afetando organizações de todos os tamanhos e em todas as indústrias. Hoje não conseguimos passar nem mesmo alguns dias sem ler notícias de sobre algum ataque envolvendo alguma variante de ransomware

A sexta-feira de 17 de maio de 2017 ficou marcada como o dia de um dos maiores ataques hackers via ransomware já vistos no mundo. O WannaCry afetou grandes empresas e organismos de 179 países por meio de uma vulnerabilidade presente em todas as versões do Windows desde o Vista. A Telefónica, empresa que controla a Vivo no Brasil e uma das maiores organizações de telecomunicações da Espanha, foi extremamente afetada, tendo mais de 85% de seus computadores infectados e recebendo uma exigência de resgate de mais de 500 mil euros.

No Brasil, os ataques com o ransomware WannaCry afetaram os sistemas do Itamaraty e do Tribunal de Justiça do Estado de São Paulo (TJ-SP), que ficaram fora do ar praticamente o dia todo. Na Inglaterra, uma série de hospitais tiveram seus sistemas bloqueados, afetando até o fluxo de ambulâncias.

Diante de tantas variantes de ransomware atuando no mundo todo, em especial nos últimos três anos, por que o WannaCry conseguiu se espalhar tão rapidamente e causar o estrago que vimos? Sem entrarmos em detalhes técnicos, as técnicas por trás do maior ataque de hacker via ransomware não têm nada de especial.

O que o WannaCry tem de diferente?

O WannaCry é um tipo de cryptoworm, uma forma maliciosa de malware capaz de se propagar sozinha. Isso significa que, uma vez que esteja posicionado dentro da rede, pode espalhar-se automaticamente sem a necessidade de que alguém o controle remotamente. Isso, certamente, influenciou seu poder de espalhar-se pelo mundo.

Porém, existem centenas de cryptoworms que não causaram o mesmo estrago do WannaCry. A diferença é que, ao contrário dos outros ransomwares, que definem como alvo os dados não estruturados hospedados nos sistemas de arquivos, o WannaCry não fazia esse tipo de distinção.

Além disso, em abril, diversas ferramentas hackers criadas pela NSA vazaram online, entre as quais uma ferramenta que explorava vulnerabilidades de hardware e software para que pudesse invadir e mover-se lateralmente nas redes. O WannaCry tirou proveito disso e foi além: uma vez dentro de uma máquina, ele usava sessões de Remote Desktop Protocol (RDP) para criptografar dados em máquinas remotas, buscava outras máquinas com Windows vulneráveis e servidores com vulnerabilidades da Microsoft, e então adotava a abordagem tradicional de buscar arquivos diretamente nos endpoints.

Cryptoworms como o WannaCry podem se replicar e buscar outros computadores vulneráveis em redes ao redor do mundo. A verdade é que a infecção mundial poderia ter sido pior se não fosse pelo pensamento rápido de um especialista em segurança que identificou que o código do malware foi conectado a um domínio que não estava registrado – para que seu autor pudesse parar o ataque, se quisesse, e para evitar técnicas sandboxing de softwares de IDS/IPS. Apostando em um palpite, o especialista registrou o nome do domínio, registrando, assim, milhares de conexões por segundo, parando o que poderia ter sido uma infecção muito maior.

O que aprendemos com isso

A Microsoft lançou um patch para a vulnerabilidade da qual o WannaCry tirou proveito, a SMBv1, em março deste ano. Infelizmente, a verdade é que a presença de bons processos de gestão de patches impediria que a maioria das empresas tivesse sido afetada de maneira tão severa.

É claro que uma boa gestão de patches não é suficiente para proteger-se do ransomware – nem mesmo bons processos de backup são suficientes, pois alguns ransomwares conseguem se esconder até nos backups e atacam novamente quando os arquivos são restaurados.

A verdade é que não existe uma maneira única de parar infecções de ransomware ou qualquer outra ameaça. A segurança da informação serve para reduzir riscos, e isso requer uma abordagem de proteção em camadas, em que cada uma deve contar com os controles de segurança adequados, com o uso de soluções para automatizar processos sempre que possível.

Qualquer organização que diga ser 100% segura contra ransomwares ou qualquer outro tipo de ataque está iludida ou mentindo.

(*) É vice-presidente da Varonis para a América Latina.

Antecipar-se a fraudes é possível? Com analytics sim

Se buscarmos o significado da palavra fraude, descobriremos que em um sentido amplo, remete a um esquema ilícito, de má-fé, realizado com o intuito de lesar alguém ou obter ganhos

Celso Poderoso (*)

Trazendo para o nosso dia a dia, a fraude pode acontecer de diversas maneiras, por inúmeros motivos e em esferas variadas. É um problema recorrente e enfrentado por empresas dos mais diversos segmentos de atuação. Onde houver vulnerabilidades, riscos operacionais, ausência de processos estruturados, de melhores práticas, de segurança da informação, de controles e auditoria interna, lá estarão os fraudadores.

Mas como é possível prever que uma fraude vai ocorrer? Como antecipar-se e evitar o prejuízo antes que o dano ocorra? Isso parece algo meio visionário e meio distante da realidade. Será que métodos e modelos matemáticos são capazes de prever situações futuras? Sim, com certeza. Os esclarecimentos a essas dúvidas podem vir através do analytics, que é uma tendência cada vez mais em uso e que tem trazido resultados extremamente positivos.

Estudos apontam que, no Brasil, empresas perdem cerca de 5% do seu lucro com fraudes. Além disso, 77% das empresas brasileiras foram afetadas por esses golpes entre 2015 e 2016. Perde-se no varejo, perde-se no comércio eletrônico, perde-se na indústria, na construção civil, no segmento de energia e em inúmeras outras áreas. Fraudes que vão desde o CPF falso; um boleto que é emitido, bloqueia a venda do bem que não é pago; mercadorias que são desviadas; até golpes na área de saúde, quando exames médicos que só podem ser prescritos para mulheres – são, por exemplo, equivocadamente solicitados para um homem de 40 anos.

Antes de detalhar como essa tecnologia pode minimizar os prejuízos, é preciso contextualizar: normalmente o fraudador, independente da natureza do ato ilícito que pretende cometer, segue um padrão. Exemplificando com o caso do comércio eletrônico, cujos índices de fraude ficam em torno de 1,4% do valor total das receitas do setor, os consumidores normalmente apresentam um determinado padrão de navegação, como por exemplo, fazem pesquisas em vários sites ou então usam os websites de comparação de preço; pagam sempre com cartão e realizam compras pequenas. Já quem pretende cometer um crime tende a ter outro tipo de comportamento: entra direto no site que foi eleito como a vítima da vez, pois preço não é a questão; vai pagar com boleto e ainda comprar em grande quantidade. Analisando esse cenário é possível identificar padrões comuns de fraude antes mesmo desta efetivamente virar um pedido.

É neste cenário que entra o analytics, que permite a criação de um modelo matemático, que tem a vantagem de poder ser atualizado automaticamente quando se utiliza uma ferramenta. Unindo uma série de variáveis, inseridas dentro de um contexto maior, esse modelo permite que o algoritmo seja modificado sem nenhum tipo de intervenção humana, de acordo com os dados que são recebidos. Isso é na verdade o que o mercado chama de inteligência artificial e/ou aprendizagem de máquina (machine lerarning). A grande vantagem desses sistemas é que eles têm a capacidade de aprender sozinhos: coletam o histórico e modificam-se conforme novos padrões são identificados. Ou seja, a inteligência permite adquirir um conhecimento em cima da base de dados. É com essa lógica que se consegue obter análises de fraude muito fortes, efetivas e preditivas.

E para tudo funcionar bem, é crucial contar com um histórico do que já aconteceu, bem formatado, alimentado com todos os padrões que foram detectados em situações em que as fraudes foram comprovadas. É o Big Data, que dá condições de ampliar ainda mais esse universo de informação, integrando-se a fontes externas de dados, como por exemplo, o Serasa ou outras intuições de proteção ao crédito, Receita Federal, boletins de ocorrências, etc. Onde houver dado disponível, seja ele estruturado ou não estruturado, ele puder ser captado, com certeza ele será agregado e muito útil.

Na prática, o Grupo Energisa, um dos principais conglomerados privados do setor elétrico do país, é um exemplo real de que o apoio da tecnologia analítica pode ser extremamente positivo e rentável para a detecção de fraudes e prevenção de perdas. O projeto DW ENERGISA, que visou a implementação de um ambiente analítico corporativo, fundamentado na arquitetura de Data Warehouse e apoiado no analytics, contribuiu para uma redução de 3,2% nas perdas não técnicas (popularmente conhecidas como gatos), o que equivale a cerca de 365 GWh, montante suficiente para atender 2,4 milhões de consumidores residenciais durante um mês. Isso é possível pois os desvios, graças à análise e cruzamento de informações históricas, são identificados antecipadamente, de maneira rápida, precisa e consistente.

Enfim, é impressionante, mas é difícil imaginar um setor que não apresente fraudes e, ao mesmo tempo, tenha condições de construir um histórico de dados que torne as empresas menos vulneráveis. O maior problema hoje é que ainda associa-se o analytics a algo extremamente complexo, difícil de ser feito e que demanda conhecimentos muito avançados. Não é bem assim e isso precisa ser desmistificado. O importante é começar, por menor que seja o histórico, ele já pode ajudar a alimentar uma base de dados e criar condições para ter respostas, mesmo que o resultado surja um pouco mais adiante.

É preciso enxergar que prever fraudes e evitar prejuízos é um fator de sobrevivência: a empresa que lidar muito bem com essa questão sairá na frente e obterá uma lucratividade bem maior de que seus concorrentes, ainda às voltas com perdas associadas a esses crimes. Acreditar que previsões é uma realidade do mundo corporativo apoiar-se em tecnologias relacionadas ao analytics é sem dúvida um grande passo para incrementar os negócios.

(*) É Diretor América Latina da área de Professional Services da MicroStrategy empresa líder mundial no fornecimento de plataformas analíticas e software de mobilidade.

Qual nota você daria para a postura de segurança da sua empresa?

O mercado de segurança da informação muda com velocidade assustadora, constantemente são desenvolvidas novas ameaças e, consequentemente, novos produtos são criados para combatê-las. Muitas vezes as empresas fazem investimentos em novas ferramentas de segurança sem entender se é realmente aquilo que precisam para estarem protegidas.

Em busca de mais segurança as empresas compram e instalam diferentes soluções e acabam perdendo a visibilidade do ambiente como um todo, não sabem onde estão as suas vulnerabilidades, quais são os dados críticos para o andamento do negócio, onde estão alocados ou quem tem acesso a eles. A complexidade do ambiente torna cada vez mais difícil gerenciar tantos sistemas e filtrar tantos alertas. Mesmo com altos investimentos em soluções de segurança a empresa pode apresentar diversas vulnerabilidades e sofrer enorme prejuízo no caso de um ataque.

Fazendo uma comparação com o nosso cotidiano, quando estamos doentes, não compramos todos os remédios disponíveis na farmácia. É preciso saber qual é a doença e qual é o remédio ideal para tratá-la. Na segurança da informação funciona da mesma forma, apenas acumular produtos não vai resolve o problema, é preciso entender quais são os pontos críticos e tratá-los da melhor forma.

A segurança corporativa envolve mais do que produtos, ela depende de tecnologias, processos e pessoas. Se os processos não estiverem bem alinhados e as pessoas não forem capacitadas, a tecnologia não irá funcionar. Se a equipe não estiver bem treinada, os riscos serão maiores. Na prevenção de vazamento de informações, por exemplo, o processo conta mais do que produto, é o processo que irá definir as normas de como a ferramenta vai trabalhar. Se o processo estiver errado, a ferramenta não irá corresponder.

Antes de adquirir mais soluções é preciso parar e avaliar: Qual é a real postura de segurança da sua empresa? Qual nota você daria para esta postura? Quais são as suas vulnerabilidades e como elas são tratadas? Os processos de segurança estão bem definidos? As soluções estão integradas ou existem brechas entre elas?

Para esta avaliação, analise o alcance das ferramentas de rede e endpoint, os procedimentos e as políticas aplicadas na empresa. Uma análise que englobe tanto a tecnologia quanto a governança aumentará a visibilidade do ambiente para os executivos e técnicos responsáveis pela segurança.

O próximo passo é definir um plano para aprimorar a segurança. Se houver diversos pontos a serem corrigidos, determinar quais são os mais críticos e quais ainda dependem de outros processos anteriores para serem corrigidos, em médio e longo prazo. Além de conhecer a sua real postura de segurança, a análise permite apontar onde estão as vulnerabilidades da corporação, traçar metas para endereçar os problemas mais urgentes e direcionar investimentos de forma mais assertiva.

(Fonte: Jeferson Propheta é diretor de serviços de segurança da McAfee para a América Latina).

News @TI

Solução livre no combate a ataques virtuais ganha força

@A Internet é uma estrutura complexa e em constante desenvolvimento. A todo momento sua resistência é colocada a prova, seja por conta de inovações que forçam empresas, usuários e sistemas a se atualizarem ou mesmo por ataques que, conforme o crescimento da Internet, vão se tornando mais frequentes e complexos. O cenário pede mudanças constantes e ações assertivas para segurança de todos na grande rede e nada mais colaborativo e robusto para ajudar nesse quesito que o Software Livre. Com pesquisas e investimento, a Hostnet liderada pelo seu diretor Michel Machado engenheiro PhD em Ciência da Computação e membro do grupo de pesquisa da Universidade de Boston está a frente de um projeto open source inovador (www.hostnet.com.br).

serviço ajuda empresas a prever e prevenir ciberataques

@A ESET, líder em detecção proativa de ameaças, lança na América Latina o ESET Threat Intelligence, um serviço voltado a empresas, que ajuda a prever e prevenir ataques cibernéticos. A ferramenta notifica praticamente os usuários de ameaças em tempo real que podem afetar seus negócios. Ao mesmo tempo, a solução permite que os departamentos de segurança das organizações analisem códigos maliciosos específicos e recebam informações sobre funcionalidade e impacto. Esse serviço foi construído a partir de uma mistura de conhecimento estruturado da ESET e as mais recentes tecnologias. Na prática, o Threat Intelligence permite que as empresas entendam e gerenciem os riscos para o negócio, mitigando ameaças e melhorando a eficiência dos sistemas de defesa (www.eset.com.br).