TENDÊNCIAS 2019:

privacidade e intrusão na aldeia global

ÍNDICE

INTRODUÇÃO

Há vários anos, os especialistas da ESET de todo o mundo participam do Relatório de Tendências, no qual analisam os principais acontecimentos de segurança e consideram quais podem ser os cenários futuros de ataques e as medidas para combatê-los.

Mas, além disso, o fundo da questão não varia muito: se trata de garantir a disponibilidade, integridade e confidencialidade dos dados de usuários e empresas contra os ataques de cibercriminosos que tentam acessá-los, manipulá-los e/ou roubá-los. Portanto, nesta edição você poderá conferir uma seção dedicada à privacidade dos dados e a preponderância que terá a nível de negócio para realizar uma gestão adequada do mesmo, principalmente considerando todas as consequências do caso que envolveu o Facebook e a Cambridge Analytica, assim como a brecha de segurança do Google e sua decisão de fechar sua rede social Google+.

Esse tipo de incidente começa a atingir as grandes empresas do setor e abre uma questão sobre qual pode ser o impacto para outras empresas menores que não podem ou não sabem como proteger adequadamente a privacidade de seus usuários.

Em resposta a essa situação, em que há uma enorme quantidade de informações pessoais e privadas dos usuários que esses serviços administram, esse questionamento solicita que as instituições governamentais tomem nota de como estão processando e protegendo os dados e passem a exercer controles, como ocorreu na União Europeia através do GDPR, que entrou em vigor em 25 de maio de 2018. Na seção correspondente a esta questão, não apenas serão analisadas situações a respeito deste regulamento, mas também quais serão as implicações futuras em torno do controle governamental da proteção da informação dos usuários em seu caráter de cidadãos.

E embora o restante das seções lide com questões que parecem ser mais circunstanciais e "atuais", os problemas subjacentes giram em torno da proteção de dados e da privacidade. Acontece que, dado que a tecnologia está constantemente avançando, o impacto sobre as práticas e usos por parte dos usuários também vai passando por mudanças e transformações, o que faz com que os cibercriminosos busquem novas maneiras de tirar proveito disso. Por isso, neste relatório apresentamos uma seção sobre assistentes domésticos e as precauções que devem ser tomadas em torno da tendência da Internet das Coisas e suas implicações para a segurança de usuários e empresas. Outra questão relacionada é uma ameaça que tem atraído muita atenção este ano e que se aproveita de uma tecnologia legítima como a blockchain: estamos falando dos coinminers, uma ameaça que tenta se aproveitar dos recursos de processamento das vítimas para minerar criptomoedas e gerar um retorno econômico ao cibercriminoso.

É claro que todos esses avanços tecnológicos e suas consequentes tentativas de aproveitamento por parte do cibercrime também têm como contrapartida o uso da tecnologia para proteger aos usuários e empresas. Um exemplo desse avanço é o machine learning, que possibilita aproveitar ao máximo a enorme quantidade de informações geradas a partir da interação entre usuários e sistemas, sendo capaz de processá-las e fazendo com que os sistemas se aperfeiçoem. Mas a história nos mostrou que toda a tecnologia pode ser explorada com qualquer tipo de propósito, portanto, na seção sobre machine learning, surge a seguinte pergunta: essa tecnologia pode ser explorada com intenções maliciosas?

Parte da tarefa de proteger as informações dos usuários e empresas passa por conhecer o panorama e os desafios da segurança da informação, por isso, convidamos você a ler todas as seções deste relatório para saber quais serão as tendências em segurança para o ano de 2019 e também para os próximos anos.

1

COINMINERS: A NOVA TURMA DO BAIRRO?

- Lembra o que é ransomware?
- Enriquecer com a mineração de criptomoedas
- Protegendo seu sistema

AUTOR

David Harley
ESET Senior Security Researcher

Coinminers: a nova turma do bairro?

Para muitas pessoas, seu primeiro encontro com *moedas digitais* ou *criptomoedas* deve ter sido quando elas, ou alguém que conhecem, foram alvo de um ransomware, que geralmente demanda um pagamento para suas vítimas por meio de criptomoedas, como o *Bitcoin*, para a recuperação dos dados criptografados.

O uso desse método de pagamento é vantajoso para criminosos porque as transações não são fáceis de vincular a uma identidade do mundo real, especialmente se convertidas em outras criptomoedas antes de serem finalmente trocadas por dinheiro, ou itens com valor real. Como consequência, muitas vítimas de ransomware tiveram de seguir as instruções de algum criminoso sobre como criar uma carteira de Bitcoin ou outros meios para realizar um pagamento de resgate.

Isso não significa, é claro, que as vítimas de ransomware estejam bem familiarizadas com o esoterismo da criptomoeda ou entendam o que se define por mineração de criptomoedas (às vezes conhecida como criptomineração), mesmo que as tenham usado para pagar um resgate. Uma descrição detalhada de como a *blockchain*, *as criptomoedas e a mineração de moedas* funcionam não corresponde ao escopo deste artigo. Embora a 'mineração' de moedas virtuais não ocorra exatamente da mesma forma pela qual os Sete Anões buscavam por pedras preciosas, envolve investir trabalho em termos de processamento informático e energia elétrica para 'encontrar' algo. De maneira um pouco simplista, a *mineração de criptomoedas* consiste em dedicar o poder de processamento a um processo matemático que cria e distribui moedas virtuais.

A mineração de criptomoedas ou as criptomoedas em si, não são necessariamente *ilegais*, embora existam muitos provedores de aplicativos e especialistas que poderiam ser acusados de deturpar o potencial de lucro desse movimento acerca da mineração. Parte do entusiasmo dos fornecedores e especialistas de aplicativos, chamando todos aqueles que desejem se envolver com o assunto, foi comparado ao *esquema de Ponzi* e à *Bolha do Mar do Sul*.

Ainda que o Bitcoin seja a moeda de que todos já ouvimos falar, há muitas outras criptomoedas. O *Monero*, por exemplo, é popular entre os cibercriminosos porque é projetada com foco em privacidade, oferecendo vantagens óbvias para criminosos – mais benefícios para eles do que para o resto de nós.

Na verdade, a mineração de Bitcoins é *um processo caro*. Hoje, praticamente não gera lucros, com exceção àquelas operações de maior escala e que exigem demais de PCs e dispositivos individuais, embora algumas moedas alternativas sejam menos exigentes. A carga de processamento pode, no entanto, ser compartilhada entre várias máquinas e dispositivos, e é por isso que existem aplicativos confiáveis (muitos deles pagos) que possuem interface de 'pool de mineração'. Isso não significa que os proprietários de máquinas participantes estejam sempre cientes de seu papel e tampouco que o lucro também seja compartilhado. Cada vez mais, vemos instâncias de *serviços legítimos* sendo fornecidos em troca do 'empréstimo' de poder de processamento de um dispositivo individual para fins de mineração, mas

quando um dispositivo é sequestrado de forma ilegítima (criptojacking) não há nenhuma troca justa. O mais notório é que parte do poder de processamento do sistema das vítimas é sequestrado por um malware em disco ou sem arquivo (frequentemente chamado de coinminer), ou por scripts *em um site* (criptojacking no navegador).

Eu vou, eu vou...

Sistemas individuais dedicados à mineração de criptomoeda tendem a não confiar exclusivamente nos *ciclos de* Unidade Central de processamento (CPU), mas também no processamento de dispositivos auxiliares, tais como Unidades de Processamento Gráfico (GPUs) e chips dedicados a circuitos integrados de aplicação específica (ASIC). Será que veremos mais malwares de mineração que pretendem tirar proveito desse hardware? É provável que indivíduos ou empresas que incursionam conscientemente no ramo da mineração, com hardwares dedicados relativamente caros, estarão em busca de quaisquer ciclos roubados (inclusive utilizando softwares de segurança!), mas usuários de máquinas de alto desempenho para jogos, por exemplo, podem ser menos cautelosos.

Não obstante, uma queda no desempenho seria provavelmente visível caso os sistemas utilizados para aplicações recurso-intensivas fossem recrutados secretamente para a mineração de criptomoeda, especialmente no caso de sistemas relativamente ultrapassados, como consoles mais antigos e dispositivos móveis desatualizados. Isso significa que os mineradores de criptomoedas vão evitar esses sistemas? Não necessariamente. Os cibercriminosos geralmente não se importam com a conservação dos recursos, a menos que desejem desviar de seu objetivo para continuarem incógnitos, em vez de terem seus esforços "prejudicados". Além disso, conforme o uso frequente de mineração através do navegador sugere, um determinado dispositivo pode ser útil mesmo se não for de alta potência ou estiver disponível a longo prazo.

O uso de ciclos de CPU e GPU visivelmente alto pode muito bem sugerir a presença de um malware de mineração de criptomoeda. Outros possíveis sintomas incluem o superaquecimento (resultando em atividade persistente dos resfriadores, ou em dispositivos muito quentes, no caso de telefones e tablets), falhas inexplicáveis ou reinicializações e volumes de tráfego de rede incrivelmente elevados. Sem dúvidas, também podem ser sintomas de outras questões relacionadas ou não com o malware ou di-

> *Quando um dispositivo é sequestrado de forma ilegítima (criptojacking) não há nenhuma troca justa.*

ferentes problemas de segurança.

O que aconteceu com o ransomware?

Nos últimos anos, ransomware tem sido descrito como o *succès fou* no campo do cibercrime. As opiniões e estimativas quanto à 'fatia de mercado' e o impacto financeiro de tipos específicos de ameaça a qualquer momento variam tão amplamente que seu valor mal pode ser discutido. Ainda assim, existem poucas dúvidas de que até recentemente a mídia e o público pareciam estar mais conscientes sobre ransomwares do que de qualquer outra ameaça cibernética atual.

Entretanto, no início de 2018, pôde-se observar os malwares para mineração de criptomoeda sendo descritos como "o novo ransomware", ao passo que os ataques de ransomware atraíram muito menos atenção da mídia. Isso não significa, naturalmente, que a epidemia do ransomware chegou ao fim, mas vemos poucas histórias sobre indivíduos que perdem dados ou que acabam tendo que pagar para resgatá-los. Não é possível afirmar se isso ocorre devido à uma mudança no interesse da mídia para assuntos sobre ataques de malware mais romantizados, mais "glamourosos", ou a um declínio significativo de ataques de ransomware a indivíduos.

Entretanto, ainda encontramos histórias de grandes empresas que são atacadas por ransomware. É possível que isso indique menos interesse em epidemiologia de 'mosaico', em que campanhas de spam de malwares resultam em muitas vítimas, cada uma gerando um lucro pequeno, na esperança de que todas as peças do mosaico irão totalizar um lucro substancial. Em vez disso, parece haver uma tendência para um número pequeno de vítimas altamente rentáveis. Por exemplo, *estima-se* que aqueles por trás do ransomware SamSam têm lucrado em torno de 330.000 dólares por mês, focando em empresas e organizações do setor público. Além disso, tem ocorrido uma diversificação nos ransomware circles, como a *sextorsão*.

Males convergentes

Certamente, não há nenhuma lei da natureza que diga que um malware não possa caber em mais de uma categoria. O XBash é um exemplo recente de funcionalidade convergente, *relatado como* uma combinação de um número surpreendente de características:

- Pode ser descrito como um ransomware, embora pseudo-ransomware talvez seja uma descrição melhor, já que parece não haver nenhuma maneira pela qual o grupo de cibercriminosose por trás do Xbash consiga restaurar os dados das vítimas que escolhem pagar. Isso o torna funcionalmente mais próximo da classe destrutiva de malware que chamamos de wiper, apesar da demanda por resgate.
- É ainda descrito como uma combinação dessa funcionalidade com funcionalidades de botnet, de mineradores de criptomoeda e de autopropagação.
- É multiplataforma, capaz de variar sua carga conforme for executado no Linux ou Windows, e de acordo com quais serviços estiverem disponíveis. Além disso, há vários add-ons de terceiros para Kodi *que são utilizados* para distribuir mineradores de criptomoedas para Linux e Windows, por exemplo. E sim, há tipos de malware para mineração de criptomoeda que visam macOS ou Android, também.

Trinta anos no ramo de segurança me ensinaram que sofisticação e versatilidade funcional não são necessariamente indicadores de uma tendência maior; podem simplesmente denotar uma transição entre classes de ameaça, da mesma maneira que Melissa era tanto um sinal de alta para vírus de macro quanto um

No início de 2018, pôde-se observar os malwares para mineração de criptomoeda sendo descritos como "o novo ransomware"

aviso sobre a chegada de uma onda de remetentes em massa. Ainda é provável que – a curto prazo pelo menos – os cibercriminosos continuarão cobrindo as apostas com malwares experimentais que encontrem lucro, em qualquer lugar e de qualquer maneira. Provavelmente também veremos mais softwares de mineração de criptomoeda *tentando remover* mineradores concorrentes em sistemas comprometidos a fim de obter uma fatia maior do processamento.

Quanto lucro pode-se conseguir com a criptomineração?

Uma pesquisa do Instituto da Universidade Técnica de Braunschweig para Segurança de Aplicativos *sugere* que criptojacking baseados na web são comuns, mas moderadamente rentáveis. Em geral, no entanto, a tendência acerca de criptojacking não mostra sinais de desaceleração por enquanto. Tomáš Foltýn relatou recentemente que *uma em cada três empresas no Reino Unido foi atingida por criptojacking em abril de 2018*, e quase dois a cada três executivos de TI acreditam que seus sistemas tenham sofrido criptojacking em algum momento.

Um artigo de Phil Muncaster cita relatórios constatando que a criptomineração aumentou 956% em um ano, e que o número de empresas afetadas dobrou no primeiro semestre de 2018. Os cibercriminosos obtiveram lucros de aproximadamente 2,5 bilhões de dólares nesses seis meses. *Um outro relatório* demonstra que a mineração ilegal de criptomoedas aumentou, até o momento em que foi publicado, 459% em 2018, atribuindo o aumento ao uso do *EternalBlue*. Pode-se prever que essa tendência crescente continuará por um tempo ainda, embora não se saiba até que ponto a NSA deva ser responsabilizada.

O minerador Coinhive tem sido amplamente utilizado como um add-on a sites da web, porque permite que peguem "emprestado" os ciclos do sistema do visitante a fim de minerar Monero. No entanto, *rapidamente ficou popular* entre os cibercriminosos, que usaram o minerador para hackear sites confiáveis e executar scripts Coinhive, configurados para minerar Monero em benefício do hacker. Mais recentemente, o Crypto-Loot também foi escolhido para propósitos similares, *notoriamente*, pelo Pirate Bay.

Conclusão: para manter seu sistema seguro

Nem todas as sugestões aqui são específicas para malwares de mineração de criptomoedas (ou ransomwares), mas podem ajudá-lo a reduzir o impacto de outras ameaças também.

- Softwares de segurança ajudam na proteção contra malwares de mineração de criptomoedas e outras "maçãs envenenadas". Não apenas como um meio de evitar todos os tipos de outros malwares, mas especificamente como meio de detecção de malware para mineração de criptomoedas sob a forma de arquivos executáveis, que podem comprometer seus sistemas e detectar ou bloquear scripts de mineração de criptomoeda no navegador.
- Esse malware é frequentemente detectado como 'Possivelmente indesejado' ou 'Possivelmente Inseguro' (consulte *https://support.eset.com/kb2629/* e *https://www.welivesecurity.com/media_files/white-papers/Problematic-Unloved-Argumentative.pdf*), para se certificar de que seu software de segurança está configurado para sinalizar esses aplicativos.

Os cibercriminosos obtiveram lucros de aproximadamente 2,5 bilhões de dólares nesses seis meses aproximadamente 2,5 bilhões de dólares nesses seis meses.

- Apesar das reivindicações de alguns concorrentes fornecedores de tecnologia, softwares de segurança convencionais são capazes de detectar muitos processos maliciosos na memória principal ou de scripts executados no servidor.
- Outra maneira recomendada para a redução de riscos relacionados ao navegador é a instalação de um *ad-block*, que possui muitas outras vantagens... Ou o uso de um bloqueador de script confiável.
- Lembre-se que os coinminers com frequência encontram seu caminho através de vulnerabilidades como o EternalBlue, *já consertado* em março de 2017. Instale patches com as atualizações o mais breve possível, independentemente do sistema operacional que esteja utilizando.
- Há sempre o risco de cibercriminosos causarem prejuízos, portanto, assegure-se de que haja backups (off-line) salvos de forma segura.
- Nenhum produto é capaz de detectar tudo que acontece. Às vezes, bom senso e prudência podem protegê-lo quando a tecnologia falha.

2

AS MÁQUINAS APRENDEM, OS HUMANOS NÃO TANTO

- Sistema de machine learning
- Tecnologia usada para propagar malware
- Limitações práticas do machine learning

AUTORA

Lysa Myers
ESET Senior Security Researcher

As máquinas aprendem, os humanos não tanto

Há um *ditado* de que as três virtudes de um grande programador são a preguiça, a impaciência e a arrogância. É especialmente importante ter isso em mente ao discutir o futuro do cenário acerca de malwares. Também é uma boa regra, ao fazer previsões de segurança cibernética, lembrar que (sem importar de qual lado da lei se está) as pessoas estão tentando obter um retorno razoável de seu investimento em tempo e esforço. O que essas regras podem nos ensinar sobre o futuro da segurança cibernética quando se trata de adotar o machine learning?

Em relação à previsão de como os criminosos podem agir, podemos dizer com segurança que, em todos os casos, exceto os mais excepcionais, estão tentando roubar dinheiro ou mercadorias valiosas com o mínimo de esforço. Para a maioria dos tipos de invasores, não vale a pena o tempo ou o esforço para desenvolver ou implantar as tecnologias mais avançadas se os ataques básicos e automatizados estiverem fornecendo o que procuram. Esse é certamente o cenário mais frequente e um problema significativo para a maioria das pessoas que protegem suas casas ou empresas.

Já os ataques aos estados-nação quase certamente empregarão ferramentas mais complexas para alcançar seus objetivos. Com um orçamento muito mais generoso, essa possibilidade certamente não deve ser descartada ou ignorada. Grandes organizações, especialmente aquelas que estão protegendo pesquisas líderes no setor ou as informações pessoais de milhões de clientes, precisam ser ainda mais cautelosas com os invasores que possuem bons recursos. E em algum momento essas ferramentas mais complexas irão inevitavelmente ter seu uso difundido para o mainstream dos operadores de malware.

Para os profissionais da área de segurança, obter o melhor retorno sobre o investimento significa tentar proteger o máximo possível e da maneira mais eficiente um determinado orçamento, tanto em termos de dinheiro quanto de pessoal. Para fornecedores de produtos de segurança, embora certamente existam preocupações orçamentárias, o fator mais importante é a necessidade de otimizar as soluções que fornecemos aos nossos clientes para que os produtos detectem tudo que puderem, com o menor custo a eles, em termos de capacidade de processamento e qualquer manutenção que precise ser feita por operadores humanos.

Neste capítulo, discutiremos como o machine learning é usado – e continuará a ser adotado – por pessoas de ambos os lados nessa equação; aqueles que estão atacando sistemas e aqueles que os defendem. Também discutiremos algumas das limitações práticas do machine learning, e onde os humanos ainda serão cruciais no processo de criação de novas ferramentas não somente para atacar, como também defender sistemas.

A aplicação do machine learning para defender

A base de qualquer bom sistema de machine learning traduz-se em uma grande

Os sistemas utilizados para identificar arquivos suspeitos e comportamentos agora possuem um contexto e vocabulário muito mais profundos para descrever comportamentos indesejados.

quantidade de dados úteis. Sem informações para aprender, as máquinas não têm as matérias-primas necessárias à criação de regras efetivas para a tomada de decisões.

Leitores frequentes do WeLiveSecurity já conhecem o fato de que os produtos de segurança têm usado a automação e o machine learning *há algum tempo*. Essa tem sido uma parte importante de nossa caixa de ferramentas por mais de vinte anos, e sua proeminência, sem dúvida, aumentará com o passar do tempo.

Pesquisadores da indústria de antimalware recolhem e trocam dados sobre ameaças há várias décadas para que nós possamos maximizar a nossa capacidade de proteger os clientes contra comportamentos maliciosos. Concomitantemente, também estivemos em diálogo com uma grande variedade de fornecedores de software para coletar dados sobre o estado atual acerca dos arquivos limpos. Isso nos dá uma grande quantidade de informações históricas e atuais com as quais treinamos sistemas de machine learning sobre quais arquivos e comportamentos são considerados suspeitos, e quais características são mais prováveis de indicar uma intenção benigna. Esse processo nos ajuda a identificar arquivos e comportamentos problemáticos e a manter falsos positivos ao mínimo.

Quando a indústria antimalware começou, grande parte do trabalho de análise de ameaças era feito manualmente, e a quantidade de informações armazenadas era bastante básica. Os primeiros sistemas de machine learning usavam traços de arquivos maliciosos conhecidos, bem como arquivos limpos, para inferir se as amostras futuras eram suspeitas.

À medida que a enxurrada de novos malwares cresce, muito mais do trabalho de análise inicial é feito pela automação para que os pesquisadores gastem menos tempo executando tarefas repetitivas e mais tempo aplicando suas percepções de especialistas para analisar e entender padrões em amostras individuais, bem como entre variantes e campanhas inteiras de malware. Esse trabalho automatizado aumentou drasticamente a quantidade e os tipos de dados armazenados sobre o comportamento de amostras individuais e melhorou nossa compreensão de padrões mais amplos no cenário de ameaças. Dessa forma,

os sistemas utilizados para identificar arquivos suspeitos e comportamentos agora possuem um contexto e vocabulário muito mais profundos para descrever comportamentos indesejados.

A funcionalidade de produtos de segurança continua em expansão, e o números e tipos de especialistas em segurança que participam nas trocas de informação continuam aumentando. Toda essa informação adicional têm melhorado a profundidade e a amplitude dos dados que os defensores estão capturando sobre a evolução no cenário de malwares.

O machine learning tem uma longa história na defesa contra malwares e outras ameaças de segurança. O futuro promete um aumento constante de maneiras para identificar o comportamento problemático ou anômalo, não apenas nos níveis de arquivo, sistema ou rede, mas também através da internet como um todo.

O uso do machine learning para atacar

Conforme discutido anteriormente, a maioria dos ataques de malware são implementados da maneira mais simples possível; não há sentido em encontrar novas tecnologias ou técnicas se as antigas estão trazendo um fluxo constante de renda ilegítima. Esse provavelmente continuará sendo o caso, já que o baixo custo de entrada no cibercrime não para de atrair mais participantes "com problemas éticos". Sem uma mudança radical na forma como as pessoas entendem e implementam a segurança, nunca podemos ignorar o impacto dos ataques contra os frutos fracos das antigas vulnerabilidades e lacunas na higiene básica de segurança.

Mas a medida que o mercado de crimes cibernéticos se torna mais disputado, e mais estados-nação entram na briga, é provável que isso leve alguns criminosos a usar mais automação para tornar suas criações mais eficientes. Os cibercriminosos já estão utilizando pesquisas automatizadas para ajudar a encontrar máquinas e contas on-line vulneráveis, além de coletar enormes quantidades de dados diferentes para um reconhecimento direcionado subsequente. Essa automação, sem dúvida, aumentará, buscando tornar os esforços existentes mais econômicos e melhores para os ataques de engenharia social.

E ao passo que as organizações criminosas criam bancos de dados mais abrangentes, podem ser usadas para informar o machine learning, de modo que regras de ataque possam ser criadas para tornar suas campanhas mais eficazes. Há três áreas que parecem mais receptivas à assistência por machine learning: a de aquisição de alvos, de exploração de vítimas e de proteção de seus recursos contra interrupções.

Atualmente, a automação de reconhecimento parece se concentrar amplamente na busca de alvos vulneráveis. Ao adicionar melhores informações a um banco de dados de alvos vulneráveis, os criminosos podem criar uma imagem mais detalhada que lhes permitirá obter mais valor de cada alvo. Em vez de pedir o equivalente em moeda criptografada de algumas centenas ou alguns milhares de dólares em resgate de um alvo cujo banco de dados vale milhões – em que os criminosos estão efetivamente deixando uma quantia significativa de dinheiro na mesa – estariam mais aptos a avaliar o máximo que um alvo se dispusesse a pagar. Além disso, com um reconhecimento melhor, poderiam ser mais cuidadosos ao removerem todos os bens valiosos localizados na organização vitimada, em vez de apenas pegar a primeira coisa que parecesse interessante.

A engenharia social sempre foi uma área

Os cibercriminosos podem empregar rastreadores web que acompanham as vítimas nos sites por elas acessados ou obter informações de intermediários de dados para criar perfis.

bastante problemática para criminosos que buscam explorar um alvo escolhido, dada a natureza internacional de seus esforços. Podemos pensar em casos de phishing ou tentativas de golpe que recebemos em que a ortografia e gramática ridiculamente ruins ou que a mensagem difere significativamente do que alguém esperaria de alguém se não tivesse sido tão mal falsificada. Embora alguns ataques de phishing e outras fraudes tenham certamente melhorado sua capacidade de imitar fontes legítimas, muitas situações ainda são falsificações dolorosamente óbvias. O machine learning pode ajudar a aumentar a eficácia nessa área.

No exemplo de publicidade direcionada, os criminosos têm um modelo de como melhorar a eficiência de suas comunicações. Embora seja improvável que tenham a riqueza de dados armazenados pelos fornecedores que rastreiam as compras regulares das pessoas, os cibercriminosos podem empregar rastreadores web que acompanham as vítimas nos sites por elas acessados ou obter informações de intermediários de dados para criar perfis. Isso poderia tornar as tentativas de phishing e fraudes muito mais pessoais e, portanto, mais atraentes.

A abordagem mais tecnicamente complicada – e, portanto, menos provável de se tornar comum a curto prazo – seria o machine learning auxiliando cibercriminosos na proteção de sua infraestrutura e evitando a detecção de maneira mais eficaz. Isso implicaria principalmente tornar sua estrutura de comando e controle mais resiliente e criar novas variantes de malware.

De que forma o machine learning afetaria a "corrida armamentista"

Desde a descoberta dos primeiros arquivos criados com intenção maliciosa, houve uma corrida armamentista entre os criadores e detectores de malware. O machine learning não acabará com esse impasse. Existem – e sempre existirão – limites às maneiras pelas quais os computadores podem ser úteis na substituição de seres humanos como os tomadores de decisão. Deve sempre haver uma relação de assistência mútua, em vez de uma delegação total de nossa responsabilidade.

A criatividade dos desenvolvedores humanos (benevolentes e malevolentes) sempre exigirá a presença de especialistas humanos que enxerguem quando algo está bem fora dos padrões anteriores. Isso permitiria a esses indivíduos maliciosos ganharem vantagem se omitíssemos completamente as pessoas do processo de análise para defesa.

Muitos cibercriminosos com motivações financeiras têm, hoje, um processo de aquisição de dados que favorece a rápida rotatividade de informações, uma vez que detalhes de pagamentos em cartões e credenciais de acesso a sites tendem a se tornar obsoletos rapidamente. Contudo, esses criminosos estão mudando seu foco para tipos de dados mais estáveis, como seguros e dados médicos, que mantêm seu valor por mais tempo. É provável que os bancos de dados com presença mais permanente passem a ter mais detalhes e, portanto, de maior utilidade para fins ilícitos. Como seus próprios recursos ganham mais estabilidade e valor, podem necessitar de métodos de proteção mais avançados.

Ironicamente, isso faria com que a corrida armamentista existente se tornasse menos uma batalha de um lado majoritariamente atacando e todos os demais se defendendo, e mais um combate de ataque e contra-ataque.

No fim das contas, o que provavelmente veremos será um aumento gradual nas tendências já existentes; o machine learning mais difundido e mais bem preparado para defender máquinas; e um aumento de invasores muito bem financiados passando suas ferramentas e técnicas para o mainstream do malware. Enquanto o poder e a importância dos sistemas de machine learning não devem ser ignorados pela defesa, e provavelmente não o serão pelos atacantes, o fato é que não se trata de um trunfo para nenhum dos lados.

O crime cibernético é extremamente lucrativo para a maioria dos seus perpetradores, sem que estes tenham de desenvolver ferramentas da última moda, embora devêssemo-nos preparar como se os criminosos estivessem implantando suas armas mais formidáveis. Não obstante, a segurança defensiva é suficientemente complexa para que os seres humanos não apenas necessitem de computadores no auxílio da identificação de arquivos e comportamentos suspeitos, como os computadores sempre precisarão de seres humanos para ajudar na identificação de novos tipos de armas.

3

O GDPR NA UE: O PRIMEIRO PASSO PARA UMA LEI GLOBAL DE PRIVACIDADE?

- O valor da privacidade de dados
- UE vs. EUA
- Regulamentos de privacidade em ascensão

AUTOR

Stephen Cobb
ESET Senior Security Researcher

O GDPR na UE: o primeiro passo para uma lei global de privacidade?

Para qualquer empresa ou consumidor preocupado com a privacidade de informações pessoais na era digital, 2018 será lembrado como o ano em que o Regulamento Geral de Proteção de Dados (GDPR, sigla em inglês) entrou em vigor na União Europeia (UE). Esse regulamento já causa grandes impactos na privacidade digital, não apenas na UE como também nos EUA, assim como em outros países, uma tendência que influenciará a conjuntura da cibersegurança em 2019 e no futuro.

O anúncio da inevitabilidade?

A maioria dos funcionários de empresas de privacidade já conhecia o GDPR muito antes de entrar em vigor. A linguagem do regulamento foi promulgada em 2015 e adotada em 2016, com um período de graça de dois anos pós-adoção. A "data de início" do GDPR da qual as pessoas se recordam – 25 de maio de 2018 – foi o fim desse período de graça e o início de sua plena aplicação pela UE.

Nessa época, a maioria das empresas americanas já havia ao menos considerado o GDPR. Se você esteve em qualquer seminário ou conferência relacionados ao GDPR nos EUA durante 2017, é provável que tenha notado que a pergunta mais amplamente feita por empresas americanas foi: O GDPR nos afeta? "Sim" era quase sempre a resposta, pelas razões resumidas em um *artigo de 2016 da WeLiveSecurity*. As empresas devem cumprir com o GDPR se:

- monitoram o comportamento dos titulares de dados que estejam localizados na UE, ou
- têm escritórios fora da UE mas fornecem bens ou serviços à UE (incluindo serviços gratuitos), ou
- possuem um "estabelecimento" na UE, independentemente do local em que processam seus dados pessoais (por exemplo, um processamento baseado em nuvem realizado fora da UE para uma empresa sediada na UE está sujeito ao GDPR).

E a segunda pergunta mais comumente feita nas discussões sobre o GDPR nos EUA foi: Como podemos evitá-lo? As respostas de especialistas de empresas como a Deloitte, PwC e KPMG podem ser resumidas da seguinte maneira: não percam tempo com manobras técnicas para evitar o GDPR – em vez disso, planejem o alinhamento das estratégias de dados da sua empresa com o GDPR, pois algum nível desse regulamento é inevitável onde quer que estejam suas operações.

A privacidade de dados ganha importância

A previsão do regulamento de privacidade "estilo GDPR universal" foi inicialmente vista com ceticismo até que o *California Consumer Privacy Act* de 2018 entrou em jogo. Aliás, o CCPA foi assinado menos de 40 dias após o GDPR ter entrado em vigor e reitera que, ao se tratar de empresas cuidando de suas informações pessoais, os californianos têm o direito de:

- saber quais informações pessoais uma

Planejem o alinhamento das estratégias de dados da sua empresa com o GDPR, pois algum nível desse regulamento é inevitável onde quer que estejam suas operações.

empresa coletou, adquiriu ou calculou sobre eles
- acessar, transferir ou deletar informações pessoais em posse de uma empresa
- saber se suas informações pessoais são ou não vendidas ou divulgadas pela empresa; em caso afirmativo, quem as recebe
- proibir a venda de suas informações pessoais pela empresa
- receber os mesmos serviços e preços da empresa, mesmo que exerçam seus direitos de privacidade

Embora a maneira pela qual esses direitos são explicitados *no CCPA* inclua inúmeras exceções e limitações, não há dúvida de que isso marca uma grande mudança no cenário da privacidade nas Américas. Ainda que a Califórnia seja apenas um dos Estados Unidos da América, seria a *quinta maior economia do mundo* se fosse um país independente (logo atrás da Alemanha, do Japão, da China e do restante dos EUA). Isso faz com que tenha grande influência, em termos de práticas jurídicas e comerciais.

A privacidade divide

Para entender como a adoção de proteções no estilo GDPR da Califórnia para dados pessoais pode impactar o cenário da privacidade em 2019, é preciso analisar como a UE e os EUA lidaram com o assunto até o momento. A Carta dos Direitos Fundamentais da União Europeia contém um direito explícito relativo à proteção de dados pessoais e proíbe a coleta ou uso de informações pessoais sobre os residentes da UE sem o seu conhecimento e permissão.

Nos EUA, não há nenhum direito constitucional explícito a respeito da privacidade. Portanto, informações sensíveis sobre as pessoas podem ser coletadas e usadas por empresas a menos que uma lei ou um processo determinem o contrário. Aqui está um exemplo do que isso significa:
Imagine que você abra uma empresa que ofereça um serviço de "compartilhamento de carona" por aplicativo como a Uber. Para isso, sua empresa coleta dados sobre as pessoas que usam o serviço, incluindo nomes e detalhes de suas viagens. Se estiver localizada na UE, há leis que restringem o que poderá fazer com esses dados, ainda

que não existam leis específicas de privacidade para serviços dessa natureza.

Nos EUA, a resposta a "O que a minha empresa de compartilhamento de carona pode fazer com as informações pessoais que coleta?" normalmente é "depende". As variáveis incluem em que lugar a empresa está instituída e onde opera, mas a resposta pode ser resumida a... "O que você quiser e puder fazer com isso". Isso pode continuar sendo a praxe até que se instaure um processo ou uma *lei de privacidade* seja aprovada para regulamentar o uso de dados pessoais coletados por empresas de compartilhamento de carona.

Posto de outra forma, os EUA têm diferentes proteções para diferentes tipos de dados pessoais, criados de maneiras diferentes, em momentos diferentes. Por exemplo, o Video Privacy Protection Act de 1988 foi redigida e promulgada poucos dias após os registros de locação de vídeos de alguém nomeado ao Supremo Tribunal serem vazados a um jornal.

As proteções de privacidade existentes nos EUA originam-se em leis federais, legislações estaduais ou decisões de tribunais a nível estadual ou federal. (Para mais detalhes sobre a lei de privacidade dos EUA leia o artigo técnico da ESET: *https://www.welivesecurity.com/wp-content/uploads/2018/01/US-data-privacy-legislation-white-paper.pdf*.)

Na UE, dados pertencentes a você enquanto indivíduo identificável são protegidos, por padrão, desde o início. Esse é o significado prático do termo "proteção de dados" no uso europeu. Qualquer pessoa que deseje coletar dados relativos a você precisa da sua permissão legal para fazê-lo, e quando tiver seus dados, deve exercer um controle rígido sobre quem pode acessá-los e com que finalidade. Isso se aplica a novas formas de dados pessoais assim que surgirem, para que você não precise passar por um processo ou um incidente político vergonhoso.

Uma crescente onda de regulamentos de privacidade

De que forma um único estado pode fazer a diferença na proteção da privacidade sem a existência de uma lei fundamental de privacidade de dados nos EUA? Trata-se de riqueza, influência e inveja. A Califórnia é o estado mais rico dos EUA e pode arcar com os custos de introduzir direitos que podem ser mais difíceis de estabelecer em outros estados. Isso abre o caminho para outros estados, cujos habitantes provavelmente invejarão os californianos se tiverem melhores proteções de privacidade do que seu próprio estado, assim como muitos americanos têm cada vez mais inveja dos direitos dos europeus sob o GDPR.

A história também tem seu papel: o primeiro passo para o CCPA de 2018 foi dado ainda em 1972. Foi quando os eleitores da Califórnia emendaram a constituição do estado para incluir a privacidade nos direitos "inalienáveis" de todas as pessoas (cada estado dos EUA pode ter sua própria constituição, além da constituição federal). Apenas cinco anos depois, a Califórnia aprovou o Information Practices Act de 1977 para limitar a coleta, gerenciamento e disseminação de informações pessoais por órgãos estatais, um movimento motivado pelo aumento do processamento de dados nas divisões governamentais.

Vinte e cinco anos após o ato, em 2002, quando os modelos de negócios baseados na Internet começaram a expandir a coleta de informações pessoais e aumentaram o risco de divulgação não autorizada, a Califórnia implementou a primeira lei estadual exigindo notificações de violação de dados. Avance 16 anos e encontre, em 2018, todos os 50 estados dos EUA com uma lei de notifica-

Ignorar os direitos à privacidade e a proteção de dados como "apenas uma anomalia europeia" é difícil quando essa anomalia está prestes a se tornar lei no estado americano que abriga gigantes digitais como Google, Facebook, Apple, HP e Oracle.

ção de violação, sugerindo fortemente que outras proteções, como os direitos de privacidade de dados no estilo GDPR consagrados no CCPA, também se espalhem pelos EUA. Há contra-argumentos para essa previsão, entre os quais a luta em curso para alterar o CCPA antes de sua entrada em vigor em 2020. Para combater isso, os defensores da privacidade continuam pressionando os legisladores (o *movimento pró-CCPA* tem site próprio, uma estratégia que poderia ser facilmente adotada em outros estados).

O desafio para as empresas que acham que o CCPA prejudicará seus negócios é o seguinte: como convencer os consumidores/eleitores de que precisam de menos proteção da sua privacidade do que as pessoas de outros países? Ignorar os direitos à privacidade e a proteção de dados como "apenas uma anomalia europeia" é difícil quando essa anomalia está prestes a se tornar lei no estado americano que abriga gigantes digitais como Google, Facebook, Apple, HP e Oracle. Essas empresas operam globalmente, e a tendência global é claramente voltada para a privacidade no estilo GDPR, e não distante dela.

O maior país da América Latina – o Brasil ¬¬– adotou uma nova Lei Geral de Proteção de Dados (LGDP) em 2018 para substituir uma estrutura de privacidade setorial semelhante à dos EUA hoje. De acordo com *analistas jurídicos globais*, "a LGPD do Brasil ecoa muitos dos componentes do GDPR". Além disso, a LGPD ajudará o Brasil a alcançar "uma descoberta de adequação recíproca da Comissão Europeia semelhante à que o *Japão recebeu*". Então, sim, outra grande economia – o Japão – está se aproximando dos níveis da UE de proteção de privacidade. E a China não ficou para trás, embora o controle interno da Internet *no país seja um fator que dificulta o processo*, o fato de um dos maiores processadores de dados do mundo estão desenvolvendo habilidades e tecnologia para manipular dados de maneira compatível com o GDPR é claramente significativo.

Resumo

Um objetivo básico da cibersegurança é controlar o acesso à informação para que ela não seja exposta sem autorização. Um dos objetivos da regulamentação da privacidade é influenciar a maneira como a "exposição não autorizada" é definida com relação às informações pessoais e, em seguida, explicitar as consequências para as empresas quando permitem que essa exposição ocorra. Consequentemente, uma violação de dados pode fazer mais do que prejudicar a confiança que as pessoas depositam em uma empresa - conforme discutido em "Tendências 2019: Privacidade Recarregada" – também pode ser dispendioso se sua violação, e/ou seu manuseio violar regulamentações de privacidade.

Em outubro de 2018, o *Supervisor Europeu de Proteção de Dados anunciou* que o mundo poderia esperar as primeiras multas de GDPR "de alguns casos até o final do ano". Mais ou menos na mesma época, a Comissão Irlandesa de Proteção de Dados (Irish Data Protection Commission) começou a investigar o Facebook por uma violação que "*poderia resultar em uma multa de até 1,63 bilhão de dólares*". À medida que o impacto do GDPR se torna mais evidente – e mais real – prevemos que muitas empresas estarão ocupadas com os preparos para obedecer ao CCPA e qualquer legislação semelhante em todo o mundo em 2019.

4

PRIVACIDADE RECARREGADA: ELA DECIDIRÁ QUEM CONTINUA NO JOGO?

- Vulnerabilidades e falhas expuseram a milhões
- O teste do Facebook
- Novos modelos de privacidade

AUTORES

Lysa Myers & Stephen Cobb

ESET Senior Security Researcher

Privacidade recarregada: Ela decidirá quem continua no jogo?

O número de pessoas cuja privacidade digital foi colocada em risco por algum tipo de problema de segurança de dados em 2018 provavelmente ultrapassou a marca de dois bilhões antes do final do terceiro trimestre. Se esse número parecer exagerado, lembre-se de que apenas cinco organizações expuseram quase 1.8 bilhão de registros antes da metade do ano: *Aadhaar*, *Exactis*, *Under Armour*, *MyHeritage*, e *facebook*. Claro, 2018 pode ficar aquém dos 7,8 bilhões de registros expostos em 2017, ou até mesmo do recorde anterior de 6,3 bilhões em 2016.

O que pode ser ainda mais interessante sobre 2018 é que muitas das gafes de privacidade deste ano não se encaixam perfeitamente na percepção comum de "violação". Enquanto a maioria de nós imagina uma violação na forma de agressores invadindo um sistema na esperança de roubar informações, não se pode afirmar que muitos dos problemas de privacidade de 2018 foram de autoria de um agressor. Alguns desses problemas foram resultado de vulnerabilidades ou bugs que permitiam acesso não intencional, como os problemas do Facebook que colocavam em risco as *contas de 90 milhões de usuários*, ou o bug no *Google+* que expôs as contas de mais de meio milhão de usuários (e contribuiu para o desaparecimento dessa plataforma).

Às vezes, os problemas de privacidade são produzidos por produtos ou serviços que se comportam como planejados e descritos em Contratos de Licença, mas de maneiras que se revelam pesadelos horríveis à privacidade. Dois exemplos desse tipo de problema são *o escândalo de dados da Cambridge Analytica* no Facebook e sua *VPN Onavo* de detecção de dados. As consequências não intencionais do compartilhamento de dados agregados lideraram manchetes desde o início de 2018, com a *confusão do mapa de calor do Strava*.

E quais são as implicações para 2019? Muito dependerá de dois grandes players: Facebook e Google. Entre eles, essas empresas acumularam gigantescas bases de usuários, juntamente com uma quantidade verdadeiramente impressionante de dados pessoais sobre eles, e isso deve ser protegido contra o acesso não autorizado. As pessoas agora se perguntam se essas empresas se tornaram, em um âmbito social, "*grandes demais para falhar*".

O Facebook e a Google desenvolveram plataformas muito poderosas. Possuem o potencial de conectar muitas pessoas com o objetivo de compartilhar e disseminar informações, tanto para o bem quanto para o mal. Como resultado, muitas pessoas passaram a depender do uso de produtos do Facebook e da Google. Para qualquer coisa que essas plataformas façam que seja muito arriscado ou perigoso para indivíduos específicos as usarem, há uma maneira de efetivamente alienã-los.

Isto é, do ponto de vista social, esperar que as pessoas escolham não participar de qualquer funcionalidade oferecida pelo Facebook ou pela Google seria o mesmo que escolher evitar a participação na vida moderna. Embora na teoria seja possível

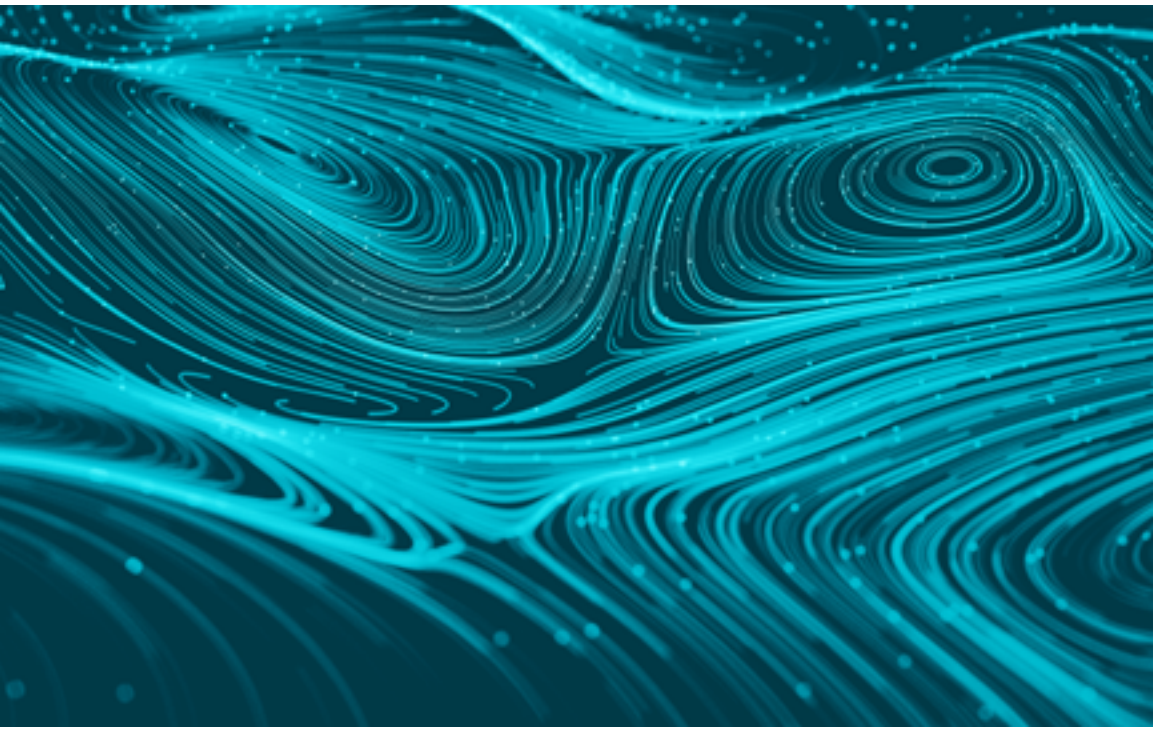
fugir de ambos, fazê-lo nos dias de hoje seria um obstáculo para realizar coisas comuns nos negócios ou na vida pessoal que a maioria das pessoas consideraria muito difícil sem as redes.

Elevando o nível ou ultrapassando-o?

As pessoas ainda estão usando o Facebook em massa, apesar de dois grandes erros de privacidade de dados em 2018, mas os sentimentos de muitos usuários azedaram de maneiras difíceis de serem capturadas com estatísticas. Em vez de o Facebook ser um lugar onde as pessoas esperam se conectar e compartilhar histórias com sua família e amigos, para alguns isso se tornou um lugar em que as pessoas perdem o contato com a família e os amigos se abandonarem a rede.

Vários estudos recentes mostraram um declínio no uso do Facebook, no engajamento e na receita publicitária, que vem se acelerando nos últimos anos. Olhando com mais atenção para essa informação, percebe-se que existem algumas advertências bastante amplas. Por exemplo, embora menos pessoas estejam usando o serviço por meio de um navegador da Web para computadores, outras o fazem por meio do aplicativo para dispositivos móveis. Menos pessoas gastam tempo e dinheiro no Facebook, mas gastam mais em redes pertencentes ao Facebook, como o Instagram e o WhatsApp. Embora as pessoas possam deixar o site do Facebook a contragosto, não estão abandonando completamente seu ecossistema.

Menos pessoas gastam tempo e dinheiro no Facebook, mas gastam mais em redes pertencentes ao Facebook, como o Instagram e o WhatsApp.



Considere o dispositivo do Facebook Portal para fazer chamadas de vídeo, programado para estrear no final de 2018. Isso pode ser um teste interessante do sentimento público em relação à empresa em 2019. No que se refere à privacidade, os dispositivos de assistente virtual podem ser descritos como, da melhor maneira possível, uma bênção mista para a privacidade, o que é de se esperar toda vez que colocarmos um dispositivo com um microfone sempre ligado em nossas casas.

Os assistentes virtuais que fornecem energia aos mais populares "alto-falantes inteligentes" – Alexa, Google Assistant, Siri e Cortana – estão disponíveis há vários anos. Isso significa que eles são muito bem testados, populares e provavelmente bastante confiáveis. O desafio que o Portal enfrentará em 2019 é que as gafes de privacidade recentes do Facebook podem dificultar a obtenção de um nível similar de confiança para esse dispositivo. Diversos analistas observaram que o lançamento de um dispositivo de vigilância poucos dias depois de expor muitos milhões de contas de usuários sugere que o Facebook está fechando os olhos para as preocupações de privacidade de seus usuários.

Se o Facebook realmente começa a tropeçar, pode ser porque continua colocando recursos para tirar proveito da dependência das pessoas em sua plataforma, sem aparentemente perceber que estão perdendo a confiança de seus usuários.

Há muito tempo se sabe que as violações e outros problemas de privacidade podem ter impactos financeiros severos, mesmo em empresas muito grandes. Basta dar uma olhada no que acontece com o preço das ações em uma empresa de capital aberto quando uma violação de privacidade é divulgada. O estoque da empresa de relatórios de crédito Equifax – outro grande repositório de informações pessoais – caiu 30% na sequência do desastre de seus dados em 2017 e, mesmo 12 meses depois, não se recuperou totalmente. O Facebook está em uma posição ligeiramente diferente porque seus clientes não são seus usuários, mas seus anunciantes. Dito isso, a desconfiança do usuário pode ter um efeito indireto se os anunciantes do Facebook veem menos valor na plataforma como meio de alavancar o produto.

Diversidade defensiva e novos modelos de privacidade

As empresas que são tão presentes em nossas vidas diárias têm um público cativo. Será 2019 o ano em que as grandes empresas finalmente demonstrarão que levaram a privacidade a sério o suficiente para que não haja violações significativas de privacidade? Isso não está claro, mas não há dúvida de que 2018 foi um ano em que muitas pessoas foram forçadas a considerar os perigos de ter uma grande empresa como o portal para toda a sua existência na Internet.

Uma possível tendência em 2019 é encontrar mais pessoas buscando alternativas para as plataformas atualmente dominantes, em um esforço para diversificar seu próprio mundo digital. Essa diversificação tem dois benefícios principais: a "biodiversidade" digital e a manutenção de "zonas" digitais segregadas. Alcançar um fluxo de informações sem atritos entre cada pessoa e entidade conectada parece ótimo, assim como a ideia de usar as credenciais de uma plataforma para acessar todas as suas contas on-line em qualquer lugar. No entanto, as desvantagens podem ser difíceis de prever e são potencialmente enormes.

Considere a banana como um exemplo biológico. A banana Cavendish é tão onipresente que, se você disser "banana", a imagem que vem imediatamente à mente da maioria das pessoas é esse clone padrão, o amarelo. As bananas compradas na Finlândia ou na Flórida serão geneticamente idênticas entre si. Mas por quanto tempo?

As bananas Cavendish estão à beira do desastre fúngico que condenou sua antecessora, a Gros Michel. Muito da razão pela qual as bananas compradas em supermercados são de safras tão precárias é porque não há diversidade genética para ajudar sua população de plantas a suportar doenças e outros desastres. Uma vez que uma área é infectada com o fungo patogênico, ela permanece no solo por mais de três décadas, de modo que as bananas suscetíveis não podem mais

Uma possível tendência em 2019 é encontrar mais pessoas buscando alternativas para as plataformas atualmente dominantes, em um esforço para diversificar seu próprio mundo digital.

ser cultivadas nesse local. A única coisa que nos permitiu manter a banana Cavendish como uma cultura viável foi a criação de procedimentos de biossegurança que mantenham diferentes plantações separadas – não apenas geograficamente, mas em nível microbiano.

Em comparação, considere a situação das rãs e dos sapos que foram afetados pelo *fungo quitrídio*; diferentes populações de anfíbios ao redor do globo foram similarmente afetadas por um fungo que era frequentemente transportado por seres humanos. Havia preocupações semelhantes de que esse patógeno destruiria espécies em todo o mundo se o avanço da ameaça não fosse interrompido. Como esses sapos não são clones, mas geneticamente diferentes, eles têm uma variedade de genes para ajudá-los a se adaptar às ameaças. As populações de rãs e sapos começaram a desenvolver resistência a essa ameaça; os indivíduos agora sobrevivem apesar de estarem infectados.

Uma população ou ecossistema homogêneo – no mundo das moléculas e dos micróbios ou no reino dos dígitos e dados – cria o potencial de risco generalizado quando uma ameaça aparece. Se diversificarmos nosso ecossistema digital, tanto como indivíduos quanto como população, diminuiremos os riscos e facilitaremos a recuperação quando houver problemas. Por exemplo, ter um único login que vincula muitas de nossas contas on-line significa que, quando uma ameaça é encontrada em qualquer lugar desse ambiente, isso representa um risco para todas essas contas. Embora seja potencialmente menos conveniente ter que colocar nossos ovos metafóricos em diferentes cestas, também poderemos perder menos se uma dessas cestas for derrubada.

Resumo

Em 2019, poderemos ver uma maior diversidade de plataformas, pois as pessoas evitam lugares que se mostraram inseguros, além de uma diminuição contínua de confiança e envolvimento com plataformas existentes. Podemos até ver algumas empresas e/ou ofertas de produtos desaparecerem devido a preocupações com confiança e privacidade. Além disso, à medida que o ano se desenrola, lembre-se que os medos do consumidor não são os únicos motivadores de privacidade no trabalho. Considere os cenários de risco regulatório descritos nas "Tendências 2019: GDPR". O GDPR pode não ser a única fonte de sanções que atingem as empresas em 2019 se elas não lidarem com a questão da privacidade. Já temos outras localidades – mais recentemente *o Brasil* e *a Califórnia* – que aprovaram legislação semelhante e é improvável que sejam as últimas.

5

COMANDOS DE VOZ PARA CASA: QUANDO OS SEUS DISPOSITIVOS NUNCA SÃO DESLIGADOS

- Ataques que continuarão
- Usabilidade e segurança alinhadas
- Avanço da segurança de dados

AUTOR

Camilo Gutiérrez Amaya

ESET Head of Awareness & Research

Comandos de voz para casa: quando os seus dispositivos nunca são desligados

Se você pensar nos dispositivos eletrônicos que são usados diariamente, quais são os mais importantes? Pensou no roteador? Este dispositivo, que geralmente não é mais do que uma caixa preta em um canto da casa, tornou-se crucial - ainda mais do que o computador ou o dispositivo móvel.

Isso porque, além de dar acesso à Internet aos usuários, esse dispositivo transmite todas as informações confidenciais dos usuários e, se não for atualizado corretamente, pode ser explorado por um cibercriminoso para comprometer todos os dispositivos conectados. Portanto, um roteador que esteja vulnerável pode se tornar uma plataforma de ataque que serve como uma ponte para acessar outros dispositivos na mesma rede.

Mas no momento não é o único dispositivo que agrupa informações de outros dispositivos. De fato, nos últimos tempos, os assistentes de voz começaram a se popularizar. Além de estarem conectados a vários dispositivos, tem a capacidade de controlá-los, como é o caso de luzes inteligentes, sensores, câmeras e até mesmo eletrodomésticos. E com esse aumento na variedade de dispositivos interconectados, a superfície de ataque também cresce.

Com o crescente número de dispositivos inteligentes conectados, que de acordo com um relatório da IDC estimam que em *2020 serão 80000 milhões*, veremos no próximo ano um aumento no número de ataques, nos quais serão utilizados desde scripts automatizados de vulnerabilidades em dispositivos IoT até ataques direcionados usando exploits projetados para assumir o controle dos mesmos. Além disso, tendo em conta que os roteadores e os assistentes de voz são os que mais interagem com outros dispositivos inteligentes, estes serão os pontos preferidos pelos cibercriminosos.

Crescimento de ataques

Infelizmente, determinar o quanto os ataques aumentarão durante o próximo ano não é possível, mas sem dúvida veremos com mais frequência casos de ameaças desenvolvidas especificamente para esses dispositivos. Também podemos esperar mais diversidade de ameaças direcionadas a dispositivos que funcionam como concentradores, como roteadores ou assistentes, já que esses são os que podem fornecer a um cibercriminoso o acesso a uma rede inteira junto com dispositivos conectados e, o mais importante: as informações administradas.

Não podemos perder de vista o fato de que durante os últimos anos temos testemunhado diferentes tipos de ataques a roteadores, como o caso da "botnet Carna" e seu "Censo da Internet em 2012", bem como outros eventos de menor escala que ocorreram antes de Mirai. De fato, pode-se dizer que Carna foi a precursora da botnet Mirai e, embora não tivesse a intenção maliciosa da última, Carna conseguiu comprometer varios dispositivos, como os roteadores SOHO. O caso da botnet Mirai foi um dos mais populares. Composta principalmente por dispositivos IoT comprometidos (infectou 600.000 dispositivos em todo o mundo), e foi usada para

realizar dezenas de milhares de ataques DDoS - incluindo um dos maiores da história, quando em outubro de 2016 atacou os servidores da Dyn e derrubado serviços populares como Netflix, Twitter, Spotify, PayPal, bem como vários meios de comunicação nos EUA e Europa. Além disso, também foram realizadas pesquisas com assistentes de voz, em que uma das mais recentes mostrou que é possível *enviar comandos ocultos, que não são detectáveis ao ouvido humano*, para assistentes como Siri da Apple, Alexa da Amazon e o Assistente do Google, ativando os sistemas dos dispositivos, sem que o usuário possa perceber.

E, embora muitas dessas pesquisas tenham sido baseadas em provas de conceitos, elas mostram que é possível que um invasor desbloqueie dispositivos, faça transferências bancárias ou realize compras on-line simplesmente encobrindo mensagens maliciosas em uma reprodução de áudio normal.

Portanto, há um desafio para o futuro, já que proteger esses pontos concentrados em todo o nosso mundo conectado não será fácil. Por exemplo, um mau funcionamento desses componentes ou um ataque que os use como uma plataforma pode comprometer as informações de uma grande variedade de dispositivos.
Embora a usabilidade e a facilidade que os dispositivos inteligentes oferecem ao usuário sejam muito bem avaliadas, eles também podem representar uma porta aberta para a entrada de ameaças. A realidade é que, à medida que avançamos em direção a uma maior adoção no uso de dispositivos IoT agrupados sob um assistente doméstico, aumentam os riscos para segurança e privacidade. Não se pode esquecer que, com a evolução da tecnologia, a forma como os cibercriminosos pensam e agem também evolui.

O equilíbrio entre usabilidade e segurança

Se você já conta com dispositivos inteligentes em sua casa ou está pensando em um novo, deve levar em consideração a segurança que ele pode oferecer. No início deste ano, os pesquisadores da ESET publicaram um *relatório sobre a análise de doze dispositivos populares de IoT no mercado* e, além de encontrar várias vulnerabilidades (em alguns casos até graves), cada um dos dispositivos analisados apresentou algum problema em termos de privacidade, sendo o desempenho dos assistentes de voz inteligentes o que gerou maior preocupação. Portanto, é importante investigar os recursos que o dispositivo, como o fabricante, oferece e, a partir dessa informação, determinar se existe um equilíbrio entre conforto e segurança.

Embora a usabilidade e a facilidade que os dispositivos inteligentes oferecem ao usuário sejam muito bem avaliadas, eles também podem representar uma porta aberta para a entrada de ameaças

Então, se no ano que vem você planeja comprar um Alexa, Google Home, Amazon Echo, Apple HomePod ou outro assistente similar, antes de tudo é necessário estar ciente de quais dados pessoais eles captam e compartilham e assim determinar qual é o mais conveniente e aquele que melhor se adapte às suas necessidades de segurança e à sua expectativa de privacidade.

Os mesmos ataques que vimos até agora na Internet vão migrar para dispositivos com menos recursos de segurança. Por isso, é necessário considerar desde o local físico em que esses dispositivos estão localizados até pensar em adquirir os dispositivos que oferecem melhores características de criptografia ou com uma autenticação robusta. Essas são medidas que devem ser levadas em conta porque ainda estamos longe dos padrões de segurança para IoT.

Portanto, 2019 apresenta um panorama complexo sobre as ameaças que podemos ver para essas tecnologias e, embora as preocupações com segurança e privacidade possam ser muitas, é hora dos usuários tomarem medidas de proteção e não deixarem essas decisões apenas nas mãos dos fabricantes.

Prioridade para a segurança de dados

Então, até onde a segurança deve ser prioridade para o próximo ano quando falamos sobre dispositivos como assistentes de voz? O mais importante sobre segurança nesse caso é precisamente saber quais dados circulam e são coletados por esses dispositivos: informações de identificação, dados que permitem o acesso a perfis on-line, informações financeiras e, em geral, dados que podem ser sensíveis. A grande variedade de dispositivos, tecnologias, protocolos e fornecedores torna difícil chegar facilmente a uma padronização que permita definir as medidas de segurança que podem ser adotadas. Este é um processo que leva tempo e não veremos esses padrões implementados no próximo ano.

Então, enquanto chegamos a esse ponto, os fabricantes devem cuidar de estabelecer políticas de segurança na camada de aplicação de seus produtos que permitam proteger a integridade e a confidencialidade dos dados. Caso contrário, nos encontraremos diante de ataques nos quais, após a injeção de código, explorem vulnerabilidades que permitam o acesso às informações armazenadas nos servidores.

O que esperar do futuro?

Atualmente, temos visto um aumento na superfície de ataque, com casos em que chegamos a sistemas que usam uma ampla gama de tecnologias e protocolos de comunicação. E, ao lado desse crescimento, veremos como, durante o próximo ano, as ameaças terão diferentes vetores de ataque que aproveitarão a ampla variedade de opções.
Já vimos como os cibercriminosos utilizaram dispositivos IoT para realizar amplos ataques de negação de serviço, mas à medida que mais dispositivos são conectados e integrados à vida de todos, os invasores continuarão explorando seus recursos para detectar outras vulnerabilidades (eles já fizeram isso com termóstatos, sistemas de câmaras de segurança, brinquedos para crianças, veículos, etc.) e, dessa forma, transportam ameaças, tais como fraudes, ransomwares ou a mineração de criptomoedas, para esses dispositivos de forma generalizada. Com o crescimento do uso de criptomoedas e o grande número de dispo-

Os mesmos ataques que vimos até agora na Internet vão migrar para dispositivos com menos recursos de segurança.

sitivos conectados à Internet, os dispositivos inteligentes podem se tornar o ponto de entrada para um cibercriminoso obter grandes fazendas de criptomineração.

Há quem se preocupe com essa realidade e já esteja tomando medidas. Um exemplo é a aprovação de *uma nova lei no estado da Califórnia, Estados Unidos*, que até o ano 2020 exigirá que todos os dispositivos IoT comercializados no mercado sejam configurados com senhas exclusivas.

Portanto, dado este cenário que não parece muito encorajador, como usuário, é necessário que você conheça os dispositivos adquiridos, os recursos oferecidos pelos fabricantes e, acima de tudo, faça um uso seguro da tecnologia. A realidade é que a grande variedade de fabricantes em sua corrida desenfreada para vender seus produtos pode deixar muitos deles com vulnerabilidades que os deixam mais expostos, portanto, estar ciente de que há riscos é a melhor maneira de estar preparado para garantir a segurança de seus dispositivos e informações.

CONCLUSÃO

2018 foi um ano em que os dados e a privacidade tiveram um protagonismo especial. Casos específicos como o incidente com o Facebook e a Cambridge Analytica ou a entrada em vigor do Regulamento Geral de Proteção de Dados (GDPR, sigla em inglês) foram os principais responsáveis para que a privacidade e a segurança dos dados ganhassem tanto destaque.

Os capítulos deste relatório mostram a importância dos dados, tanto para as empresas quanto para os usuários. Para aqueles que são responsáveis por fornecer proteção e também para os cibercriminosos.

Como vimos, a evolução das ameaças está relacionada com a evolução da tecnologia ou ao comportamento dos usuários. Assim como os mercados procuram aprender mais sobre o comportamento dos usuários na Internet para estabelecerem uma comunicação personalizada, o mesmo acontece no caso de invasores, que certamente começarão a adotar o uso de tecnologias como o Machine Learning com o propósito de coletar dados que podem ser usados para realizar campanhas de engenharia social personalizadas e mais convincentes.

Portanto, neste contexto em que todas as atividades que realizamos na era digital deixam uma marca, e que continuarão existindo incidentes que afetarão empresas e usuários, a entrada em vigor do GDPR representa um farol para o mundo que certamente começará a se replicar em diferentes países e regiões por meio de diversas iniciativas de proteção de dados. Apesar da GDPR ter despertado muitas interrogações no setor empresarial, principalmente nos países que não estavam localizados na União Européia, os fatos que ocorreram este ano parecem ter provocado uma mudança de consciência que até agora não havia sido alcançada. Isso será o suficiente? Provavelmente não.

Este cenário marcado pelo surgimento de regulamentações para a proteção de dados representa um desafio: como as novas regulamentações que surgem em cada região ou país serão complementadas e articuladas com o resto dos países, já que a própria natureza da Internet é o desconhecimento das fronteiras geográficas. Também levanta outros tipos de perguntas, como saber o que acontecerá quando duas normas forem contraditas ou lacunas legais forem detectadas em casos que não foram previstos. Porque além do estabelecimento de normas, é necessário um sistema que acompanhe as necessidades que surjam e que contemple os avanços naturais para atualizar as normas a cada momento. Nesse sentido, é o momento em que as empresas e os governos devem demonstrar seu compromisso e não deixar tudo para as empresas de segurança ou usuários.

À medida que os avanços tecnológicos são desenvolvidos, a superfície dos ataques está se expandindo cada vez mais e é por isso que o desafio está em levar a cabo a educação em vários níveis e públicos. Em um mundo atual atravessado pela interconectividade, onde todos os serviços estão interligados na nuvem, nos quais assistentes virtuais, roteadores e outros dispositivos inteligentes podem ser a porta de entrada para o roubo de informações ou em que um site pode ter sido infectado por um código malicioso para minerar criptomoedas, torna-se cada vez mais necessário um perfil de usuário mais atento, com mais ferramentas para fazer uso responsável e consciente da tecnologia, que

saiba não apenas como se proteger, mas também conheça a responsabilidade e os riscos envolvidos no upload de informações pessoais para a nuvem, além de estar ciente do tipo de informação que está sendo carregada e compartilhada com serviços de Internet legítimos.

E organizações, empresas e fabricantes devem fazer sua parte se não quiserem ser afetados por usuários que perderam a confiança como resultado de terem sido prejudicados por um incidente de segurança. Mesmo empresas como o Facebook, cujo principal valor é o serviço oferecido pelo gerenciamento de grandes volumes de informações pessoais, já não têm mais a mesma percepção que antes por parte dos usuários. Mas a realidade é que nem todas as empresas têm uma segunda chance de demonstrar que consideram a proteção de tais informações uma prioridade, e um único incidente em que os dados pessoais dos usuários são comprometidos pode ser suficiente para que se perda definitivamente a confiança e que isso leve ao desaparecimento de um serviço ou a quebra de uma empresa.

O ano de 2019 começará e continuará havendo casos de vazamentos de informações, dispositivos que saem da fábrica sem ter controles de segurança suficientes e campanhas sofisticadas que afetam intituições críticas. Em paralelo, continuarão chegando na caixa de entrada dos usuários campanhas de phishing que tentam se aproveitar de indivíduos sem as habilidades suficientes para usar a tecnologia. Considerando essa diversidade e complexidade dos ataques, há várias responsabilidades dos diversos atores da sociedade (empresas, usuários, fabricantes, governos, organizações da sociedade civil) para garantir que a privacidade e a confidencialidade dos dados sejam mantidas.

Esperamos que este relatório seja útil para aqueles que podem interferir na tomada de decisões e que juntos possamos colaborar para tornar a tecnologia um ambiente mais seguro.

www.eset.com