TENDÊNCIAS EM CIBERSEGURANÇA 2018: O CUSTO DO NOSSO MUNDO CONECTADO

ENJOY SAFER TECHNOLOGY™

ÍNDICE

INTRODUÇÃO

O ano em que a segurança virou manchete

2017 será um ano (infelizmente) memorável para o nosso setor: o ano em que a (in)segurança virou manchete dos grandes veículos de comunicação. Se analisarmos os principais acontecimentos e notícias, veremos muitos casos que conquistaram grande notoriedade não somente por ter afetado milhões de usuários ao redor do mundo, mas também por ter atingido importantes empresas multinacionais e entidades governamentais.

Dois dos fatos de maior repercussão deste ano foram, sem dúvida, as infecções em massa do ransomware WannaCryptor primeiro e, em seguida, do Petya/NotPetya. A capacidade que essas ameaças têm de autorreplicar-se permitiu que milhares de equipamentos e servidores ao redor do mundo fossem tomados como reféns a uma escala e a uma velocidade sem precedentes até esse momento. No entanto, também fez com que cada vez mais pessoas começassem a preocupar-se com questões de segurança.

Essas infecções em massa não foram os únicos acontecimentos que chegaram aos meios de comunicação em massa. Recordemos a brecha na Equifax, que poderia ter afetado mais da metade da população adulta dos Estados Unidos, ou o ataque à HBO, no qual foram filtradas informações privadas de seus atores e materiais relacionados a suas produções, como roteiros ou capítulos da série "Game of Thrones". Este ano, inclusive, a Yahoo! admitiu que, durante a brecha de 2013, todo o seu banco de dados havia ficado vulnerável, ou seja, os dados de 3 bilhões de contas, que incluíam nomes, endereços de e-mail, datas de nascimento, senhas e, em alguns casos, preguntas e respostas de segurança, foram comprometidos.

E isso não é tudo: durante este ano, falou-se também das acusações de interferência russa durante as eleições presidenciais dos Estados Unidos em 2016, do descobrimento do KRACK, uma vulnerabilidade no sistema de criptografia WPA2 que torna as conexões Wi-Fi inseguras, e do Industroyer, a maior ameaça aos sistemas de controle industrial desde o Stuxnet, que pode se adaptar para afetar diversos tipos de infraestruturas essenciais, como fornecimento de água, eletricidade e gás.

Como podemos ver, este foi um ano repleto de acontecimentos em termos de segurança e no qual vimos a concretização de várias das preocupações que viemos apresentando ao longo dos últimos anos nos documentos de Tendências, escritos pelos especialistas em segurança da ESET. As notícias sobre segurança abrangem cada vez mais aspectos de nossa vida cotidiana e afetam públicos cada vez maiores e mais diversificados.

O avanço da tecnologia e sua rápida adoção fazem com que vários cenários que alguns anos atrás pareceriam impensáveis entrem no campo das possibilidades hoje em dia. Principalmente agora, quando começam a aflorar evidências de que muitos dos sistemas e protocolos que usamos não foram projetados levando-se em consideração a segurança, porque não foram projetados

para ser conectados à Internet. Como solucionar isso sem ter que voltar atrás nas nossas capacidades tecnológicas?

Neste relatório, os especialistas em segurança da ESET apresentarão os principais eixos de segurança que acreditamos que serão fundamentais para o próximo ano e analisarão as formas de enfrentá-los. Esperamos que esse exercício de olhar para o futuro permita que todos os atores envolvidos e preocupados com a segurança da informação reflitam, debatam e prepararem-se para os desafios de hoje e de amanhã.

1

A revolução do ransomware

- Ransomware com características de worm
- Surtos globais
- Resgate sem .ware
- Outros tipos de ransomware
- RaaS: Ransomware como um serviço

AUTOR

David Harley
ESET Senior Research Fellow

A revolução do ransomware

Foi assim que entrei nessa área, há quase 30 anos. O primeiro surto de malware para o qual prestei consultoria foi o extraordinário Trojan AIDS do Dr. Popp, que tornava os dados da vítima inacessíveis até que fosse feito um pagamento de "renovação de uso de software". Depois disso e por um longo período, não houve nada significativo que pudesse ser chamado de ransomware, a menos que sejam levadas em consideração as ameaças de ataques persistentes do tipo DDoS (ataque de negação de serviço) feitas contra organizações.

Negação plausível demais

Embora os ataques de negação de serviço ampliados por meio de redes de computadores infectados por bots estivessem virando um problema considerável na virada do século, as ameaças de extorsão por DDoS cresceram no mesmo ritmo (ainda que de forma menos dramática) com a ascensão dos ransomware nos últimos anos. No entanto, as estatísticas foram ofuscadas pela relutância de algumas organizações vítimas em falar e por um aumento simultâneo de ataques DDoS no âmbito político em vez de por motivos meramente financeiros. Apesar disso, há outras interações complexas entre os tipos de malware. Já houve casos de variantes de ransomware que incorporavam um bot para DDoS e, mais recentemente, os responsáveis pela botnet Mirai optaram por forçar via DDoS o "kill switch" Wannacryptor (também conhecido como Wannacry) para permitir que cópias inativas do malware fossem reativadas.

As voltas dos worms

Naturalmente, há muito mais que apenas o fator Mirai no malware que a ESET chama de Win32/Filecoder.WannaCryptor. A combinação de ransomware e worms acelerou a disseminação do malware, embora de forma não tão dramática em termos de volume bruto quanto alguns dos ataques de worms vistos na primeira década do milênio, em parte porque a sua disseminação dependia de uma vulnerabilidade já amplamente corrigida. No entanto, seu impacto financeiro em algumas organizações de grande porte chamou a atenção dos meios de comunicação no mundo todo.

Pague agora! E jogue o *nosso* jogo*

Uma das peculiaridades do Wannacryptor era a baixa probabilidade de que alguém recuperasse todos os seus dados, mesmo que pagasse. Esse não é o único caso, é claro. Há diversos exemplos de ransomware nos quais os cibercriminosos foram incapazes de recuperar uma parte ou até qualquer um dos dados devido a imperícias no código, ou eles nunca tiveram a intenção de realmente possibilitar sua recuperação. O Ranscam e o Hitler, por exemplo, simplesmente excluíam os arquivos, sem criptografia e sem nenhuma possibilidade de que os criminosos fossem capazes de ajudar a recuperá-los. Felizmente, esse tipo não parece ter tido muita difusão. Talvez o exemplo mais notável seja o clone parcial do Petya, que o ESET detecta como Diskcoder.C e que de fato criptografa os dados. Dada a competência com que o malware é executado, a ausência de um mecanismo de recuperação não parece ser acidental. Em vez disso, trata-se de um caso de "pegar o dinheiro e fugir".

Febre dos limpadores

Embora o malware por vezes chamado de NotPetya não tenha nenhum problema em obter lucro fazendo-se passar por um ransomware, outros "limpadores" claramente têm um objetivo diferente, como o malware Shamoon reavivado recentemente. Trata-se de um malware com funcionalidade de exclusão de dados que visa à Ucrânia e inclui o Killdisk (associado ao BlackEnergy) e, mais recentemente, ao Industroyer.

O que é possível aprender com essas tendências?

Sequestrar os seus dados em troca de resgate é uma maneira fácil que o cibercriminoso encontra para obter lucro ilicitamente. Além disso, destruir os dados por outras razões, que incluem motivos políticos, parece estar em alta na atualidade. Em vez de especular sobre todas as possíveis variações do tema de destruição de dados, vamos observar algumas das medidas que reduzem os riscos em todos os casos.

1. Entendemos que as pessoas optam por pagar na esperança de receber seus dados em troca, apesar de saber que isso incentiva os cibercriminosos. Antes de pagar, no entanto, consulte o seu fornecedor de software de segurança: a) caso seja possível fazer a recuperação sem pagar o resgate, e b) caso seja de conhecimento geral que, apesar de pagar o resgate, os dados jamais serão recuperados para essa variante específica do ransomware.

2. Proteger os dados de forma proativa é mais seguro que confiar na competência e boa-fé de um criminoso. Faça back-ups de tudo o que for importante, com frequência, mantendo pelo menos alguns back-ups off-line em dispositivos que não sejam expostos com frequência a formas de corrupção por ransomware ou outros malwares e em um local seguro (de preferência, em mais de um local). Obviamente, os back-ups protegem os dados de riscos que vão além de ransomwares e outros malwares.

3. Muitas pessoas e organizações hoje em dia não pensam muito nos back-ups em termos de dispositivo de armazenamento, como discos ópticos e armazenamento em memória Flash, mas em termos de alguma variante de armazenamento na nuvem. Este último tipo, muito provavelmente, estará hospedado em um local remoto. No entanto, devemos recordar que, se esse armazenamento estiver sempre disponível, seu conteúdo pode ficar vulnerável a ataques por ransomware da mesma forma que uma cópia local. É importante que o armazenamento em local remoto:
   a. Não esteja on-line de forma sistemática ou permanente.
   b. Proteja os dados dos back-ups contra modificações automáticas e silenciosas ou substituições feitas por malwares quando a instalação remota estiver on-line.
   c. Proteja as versões anteriores de dados dos back-ups contra exposição para que, caso as cópias posteriores sejam comprometidas, ainda seja possível recuperar uma parte dos dados, inclusive as versões anteriores de dados atuais.
   d. Proteja o consumidor por meio da definição das responsabilidades legais e contratuais do fornecedor do serviço, o que acontece se esse fornecedor cessar suas atividades, e assim por diante.

4. Não subestime a utilidade de dispositivos de back-up que não são regraváveis ou reutilizáveis. Se você não conseguir modificar o que foi escrito nelas, o

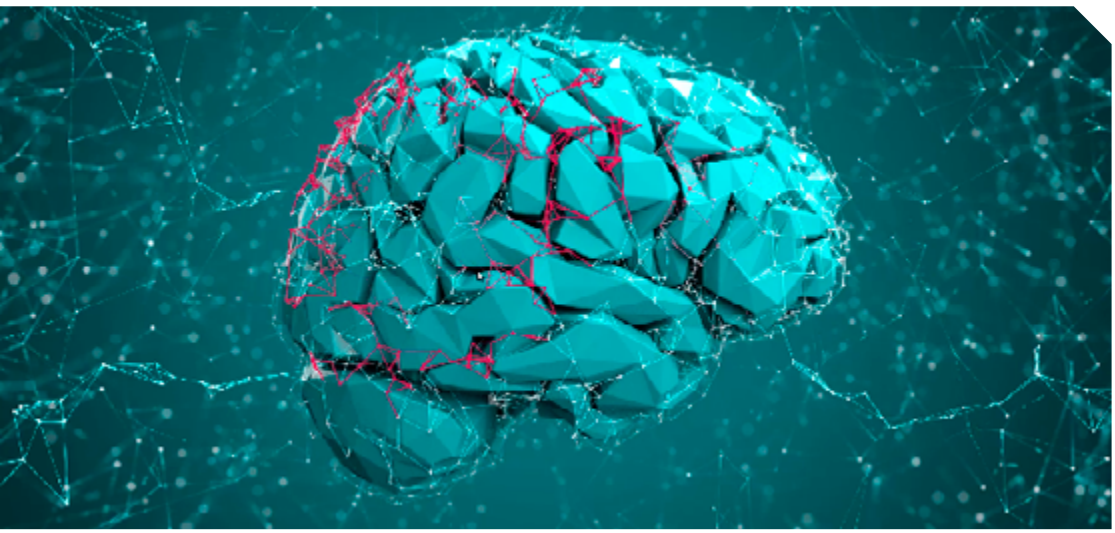
Faça backups de tudo o que for importante, com frequência, mantendo pelo menos alguns backups off-line em dispositivos que não sejam expostos com frequência a formas de corrupção por ransomware ou outros malwares e em um local seguro (de preferência, em mais de um local)..

ransomware também não conseguirá. Verifique com frequência razoável se a sua operação de back-up/recuperação está funcionando adequadamente e se os seus dispositivos (somente leitura, com gravação desativada ou com possibilidade de gravação) ainda podem ser lidos (e também se a gravação não está sendo habilitada com frequência no caso de dispositivos com possibilidade de gravação). Faça back-ups dos seus back-ups.

ransomware ainda está ativo. Felizmente, os back-ups podem salvar os seus dados quando (e se) algum código malicioso conseguir passar pelo seu software de segurança.

E quanto ao futuro?

"Não faça previsões na área de informática que você possa comprovar ainda em vida", sábias palavras de Daniel Delbert McCracken. Apesar disso, podemos arriscar alguma extrapolação a partir da evolução recente dos ransomware para oferecer algumas considerações ponderadas sobre sua evolução futura.



5. É claro que não vou dizer que você deveria confiar somente nos back-ups em vez de usar um software de segurança, mas tenha em mente que *remover* um ransomware ativo por meio de um software de segurança que o detecte não é nenhuma garantia de conseguir recuperar os dados. Remover um ransomware e, em seguida, optar por pagar o resgate pode significar que os dados nem sequer poderão ser recuperados, mesmo com a cooperação dos criminosos, porque o mecanismo de remoção da criptografia é parte integrante do próprio malware. Por outro lado, não é uma boa ideia restaurar os seus dados em um sistema no qual o

Direcionamento

O Trojan AIDs era bastante específico quanto ao seu direcionamento. Mesmo nesse caso, poucas pessoas estavam interessadas nos detalhes das pesquisas sobre o AIDS. A distribuição do Trojan por meio de disquetes era razoavelmente onerosa e o mecanismo de pagamento do resgate não estava a favor do cibercriminoso. (É claro que o Dr. Popp não tinha a facilidade do usar criptomoedas, a Dark Web ou maneiras fáceis de usar o Western Union, o esquema favorito dos golpistas do 419 ou

golpe nigeriano, ou de monetizar fotografias íntimas.)

O ataque em si era um ransomware "clássico", no sentido de que privava a vítima de seus próprios dados. Posteriormente, os ataques DoS e DDoS privaram as empresas da possibilidade de beneficiarem-se dos serviços que forneciam: embora fossem os clientes que estavam impossibilitados de usar esses serviços, eram seus prestadores que deveriam pagar o resgate. No entanto, à medida que o uso não corporativo da Internet se expandiu, a superfície de ataque e o espectro de possíveis alvos também aumentou. Isso deve desempenhar um papel na atual disseminação dos ransomwares mais modernos.

Falta de direcionamento

Embora a imprensa e os departamentos de marketing dos produtos de segurança fiquem entusiasmados sempre que um alvo de grande valor é revelado (como locais que prestam serviços de saúde, instituições acadêmicas, operadoras de telefonia, ISPs etc.), é incorreto presumir que esses tipos de instituição são sempre alvejados especificamente. Uma vez que nem sempre sabemos que vetor de comprometimento foi utilizado para uma campanha específica, não podemos dizer que nunca acontece. Porém, parece que as quadrilhas de ransomware estão tendo bastante sucesso com os pagamentos feitos pelas instituições de grande porte, comprometidas por ataques laterais provenientes de funcionários que foram atacados com sucesso enquanto usavam suas contas corporativas. A NHS Digital, por exemplo, nega que os cuidados com a saúde sejam alvos específicos, uma opinião que compartilho de forma geral, mas sem deixar de concordar que os locais que prestam serviços de saúde "têm sido vítimas frequentes".

Isso pode mudar?

Até este momento, parece que ainda há organizações preparadas para gastar quantias relativamente grandes com o pagamento de resgates. Em alguns casos, essa é uma "estratégia de back-up" razoável, reconhecendo que é sensato manter o baú cheio para o caso de suas defesas técnicas contra ransomware falharem. Em outros casos, as empresas talvez esperem que pagar o resgate seja menos oneroso que erguer novas defesas complexas que nem sempre podem ser eficazes. Só isso já pode atrair ataques a empresas percebidas como alvos fáceis. O aumento do volume dos ataques de exclusão de arquivos e de ataques de ransomware nos quais o pagamento não resulta na recuperação dos dados pode mitigar essa tendência pouco saudável, mas as empresas percebidas como tendo uma baixa probabilidade de reforçar suas defesas com todos os seus esforços podem ser mais especificamente afetadas nesse caso. Afinal, é mais provável que um ataque bem-sucedido a uma organização de grande porte pague um valor maior e em tempo mais hábil que os ataques disseminados a usuários de computadores e endereços de e-mail aleatórios.

Dados versus dispositivos*

Analisando-se os ataques a smartphones e outros dispositivos móveis, eles parecem estar menos focados nos dados e mais em negar o uso do dispositivo e dos serviços que ele proporciona. Isso é suficientemente grave quando a alternativa a pagar o resgate é ter as configurações e os dados apagados, principalmente à medida que mais pessoas preferem usar os dispositivos móveis em detrimento de computadores e até notebooks, de forma que uma ampla faixa de dados parece estar ameaçada. À medida que a Internet das Coisas Desnecessariamente Conectadas fica cada vez mais difícil de evitar, a superfície de ata-

ques aumenta, com dispositivos em rede e sensores incorporados a itens e contextos inesperados: de roteadores a geladeiras, passando por medidores inteligentes, TVs, brinquedos, centrais elétricas, postos de combustível e até marca-passos. À medida que tudo se torna mais "inteligente", também cresce o número de serviços que podem ser interrompidos por malware (com ou sem pedido de resgate). Nos anos anteriores, discutimos as possibilidades daquilo que o meu colega Stephen Cobb chama de Ransomware das Coisas. Até hoje, ainda há menos exemplos reais dessas ameaças que o esperado, considerando-se a atenção que elas atraem. Isso, no entanto, pode mudar com facilidade, caso o ransomware mais convencional fique menos efetivo como forma de obtenção de dinheiro fácil. Embora eu ache que isso não vá acontecer tão cedo...

Por outro lado, não há muitas indicações de que a segurança da Internet das Coisas esteja acompanhando o ritmo de crescimento desses dispositivos. Já estamos vendo muito interesse por parte dos cibercriminosos em obter lucro com essa falta de segurança. Escrever e distribuir malware que afete uma grande parcela de dispositivos da IoT não é tão simples quanto a imprensa às vezes presume e, portanto, não há motivos para entrar em pânico, mas não deveríamos subestimar a tenacidade e capacidade do submundo digital de criar surpreendentes reviravoltas.

**Minhas desculpas a Henry Newbolt, autor de Vitai Lampada, de onde tirei a citação adaptada: https://en.wikipedia.org/wiki/Henry_Newbolt.*

2

Ataques às infraestruturas críticas em ascensão

- Os ataques às infraestruturas críticas continuam crescendo
- Estudo de caso da ESET: Industroyer & Black Energy
- Ataques à cadeia de suprimentos
- Por que isso também pode acontecer no seu país?

AUTOR

Stephen Cobb
ESET Senior Security Researcher

Ataques às infraestruturas críticas em ascensão

As ameaças cibernéticas a infraestruturas essenciais viraram manchetes em 2017, começando com um relatório da Reuters publicado em janeiro que afirmou que um recente apagão na Ucrânia foi causado por um "ataque cibernético". No relatório de tendências do ano passado, nós dissemos que era esperado que os ataques a infraestruturas "continuassem a ser notícia e a afetar vidas em 2017". Infelizmente, estávamos certos, e devo dizer que a mesma tendência deve se repetir em 2018, pelas razões mencionadas nesta atualização. É importante lembrar que as infraestruturas essenciais englobam mais que a rede elétrica e incluem os setores de defesa e saúde, produção de manufatura e alimentos essenciais, água e transporte.

Desligar e ligar de novo

Vamos analisar como as coisas evoluíram com o passar do tempo. No fim de dezembro de 2015, os ataques cibernéticos às companhias elétricas da Ucrânia resultaram na interrupção do fornecimento de eletricidade a centenas de milhares de lares naquela parte do planeta durante várias horas. O primeiro artigo publicado por pesquisadores da ESET em 2016 foi o artigo escrito por Anton Cherepanov, Análise do BlackEnergy, o código malicioso usado durante o ataque. Esse malware não manipulou diretamente dispositivos do Industrial Control System (ICS - Sistema de Controle Industrial), mas permitiu que os cibercriminosos penetrassem as redes de companhias de distribuição de eletricidade e interrompessem os softwares usados pelo equipamento do ICS. Relatórios publicados pela imprensa à época, alguns com manchetes chamativas, como "Malware apaga as luzes", não esclareceram essa diferença.

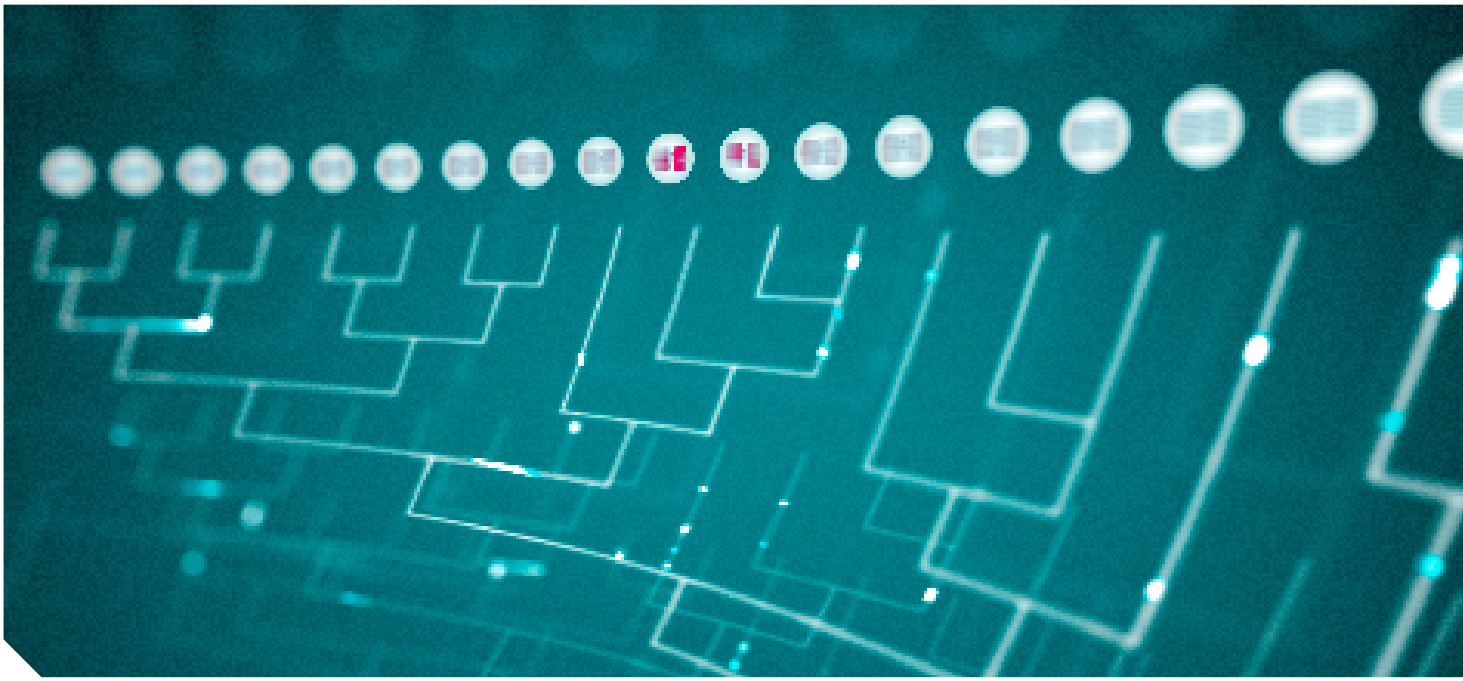
O ataque perpetrado no fim de 2016, reportado pela primeira vez em janeiro de 2017, foi bastante diferente, como alegaram os pesquisadores da ESET Anton Cherepanov e Robert Lipovsky no We Live Security. Suas análises encontraram um novo malware capaz de controlar diretamente os interruptores e disjuntores das subestações elétricas, em alguns casos literalmente desligando e religando-os repetidas vezes (o que pode, em grande escala, causar graves interrupções do fornecimento). Eles apelidaram esse malware de Industroyer e indicaram claramente que se tratava da maior ameaça aos sistemas de controle industrial desde o Stuxnet. Quando apresentaram sua análise do malware no evento Black Hat USA de 2017, apesar da enorme quantidade de participantes, não se ouvia sequer um ruído.

As implicações do Industroyer para o futuro das ameaças a infraestruturas essenciais são no mínimo preocupantes, como é possível perceber pelo tom desta entrevista com Robert. O equipamento industrial visado pelo Industroyer é usado no mundo todo (muito além da Ucrânia, como no Reino Unido, na Europa e nos Estados Unidos, e em diversos setores essenciais). Além disso, muitos dos equipamentos do ICS ainda em uso na atualidade não foram projetados levando-se em consideração a conectividade com a Internet, gerando um grande desafio para a implementação de medidas adequadas de proteção.

Naturalmente, muitas das organizações que atualmente operam infraestruturas essenciais estão trabalhando arduamente para protegê-las. A pesquisa da ESET sugere que os ataques que utilizam o Industroyer teriam que ser direcionados a alvos específicos. Isso pode limitar os ataques aos cibercriminosos bem financiados e impedir campanhas generalizadas com o objetivo de apagar as luzes, causar perturbações de transportes ou interromper a fabricação de produtos essenciais. No entanto, não é raro que esses parâmetros mudem com o tempo, à medida que o código malicioso é aperfeiçoado e mais informações são coletadas. Em outras palavras, a capacidade de realizar ataques à rede elétrica tende a aumentar em 2018, a menos que eles sejam impedidos por medidas preventivas, como atualizações de sistemas, detecção preventiva de sondagens de redes e uma melhoria drástica nas taxas de detecção e prevenção de "phishing".

Infraestrutura e cadeia de suprimentos

Infelizmente, a atualização de equipamentos antigos do ICS com mecanismos não projetados para operar levando-se em consideração a conectividade com a Internet não aumenta a segurança automaticamente. Segundo Stephen Ridley, fundador e CTO da Senrio, empresa focada na segurança de dispositivos conectados, isso se deve ao fato de que os dispositivos industriais estão deixando de ser circuitos integrados de aplicação específica (ASIC) e tornando-se arquiteturas SoC (System-on--Chip), para as quais existem bibliotecas de código amplamente disponíveis.



Apesar de gerar uma economia de custos, a nova abordagem cria pontos fracos na cadeia de suprimentos, como chips com vulnerabilidades de difícil correção e reutilização de códigos com vulnerabilidades de software inerentes. Exemplos em 2018 são a falha Devil's Ivy em mais de 200 modelos

diferentes de câmera de segurança produzidos pela Axis Communications, bem como as vulnerabilidades BlueBorne, que afetaram vários bilhões de dispositivos nas plataformas Windows, Linux, iOS e Android. Mais exemplos a serem descobertos em 2018.

Um tipo diferente de problema na cadeia de suprimentos apareceu nas manchetes em 2017, em parte porque afetou a indústria do entretenimento. Embora alguns argumentem que não seja uma infraestrutura crítica, esse setor aprendeu algumas lições em 2017 que são de grande importância para os setores verdadeiramente essenciais da economia. A tentativa de pedir resgate ao Netflix pela série "Orange Is the New Black" e o roubo digital do mais recente episódio de Piratas do Caribe revelaram aspectos preocupantes da segurança da cadeia de suprimentos.

Embora aparentemente muitas empresas de grande porte estejam levando a segurança cibernética a sério nos últimos tempos, com equipes de segurança obtendo o orçamento e o apoio das áreas executivas para que possam fazer um bom trabalho, muitas das pequenas empresas que fornecem produtos e serviços às grandes organizações ainda enfrentam desafios de segurança cibernética. Isso as torna alvos atraentes de ataques se, por exemplo, elas possuírem um filme multimilionário em seus sistemas de processamento de áudio de pós-produção, que, por sua vez, estão conectados à sua rede corporativa, cujos usuários não foram treinados para reconhecer e-mails de "phishing".

Em 2017, ficou evidente que os pontos fracos desses pequenos fornecedores na área de segurança cibernética são uma forma de comprometer grandes alvos, como os principais estúdios cinematográficos. Após vários casos de destaque terem sido relatados pela imprensa, eu fiz um apanhado de alguns conselhos sobre segurança na cadeia de suprimentos, que também são relevantes para as organizações envolvidas com infraestruturas essenciais. Afinal, os cibercriminosos podem deparar-se com dificuldades para penetrar diretamente a rede de uma empresa de serviços públicos de grande porte, mas e as empresas que lhe prestam serviços de limpeza e zeladoria?

Em tempos passados, nós nos preocupávamos com "ataques de zeladores mal-intencionados", nos quais um indivíduo de ética duvidosa e alguma experiência tecnológica obtinha acesso não autorizado durante seu intervalo descanso no horário noturno. Além de não ter sido possível eliminar essa ameaça completamente, surgiram outras, como a de uma empresa de fornecimento de serviços de limpeza e zeladoria que esteja conectada aos sistemas de uma usina elétrica através de um portal de serviços de fornecedores que tenha sido mal isolado da rede do ICS.

O que isso significa? As organizações com infraestruturas essenciais devem continuar a melhorar sua segurança em 2018, reduzindo a eficácia dos ataques de "phishing" (que ainda constituem um dos vetores de ataque preferidos), isolar e controlar os acessos à rede, revisar e testar hardwares e softwares antigos e modernos, além de tomar as devidas providências digitais em relação aos fornecedores. Também devem observar e reagir aos diversos tipos de sondagem e vigilância de rede que possam indicar a iminência de um ataque cibernético de grande escala.

os cibercriminosos podem deparar-se com dificuldades para penetrar diretamente a rede de uma empresa de serviços públicos de grande porte, mas e as empresas que lhe prestam serviços de limpeza e zeladoria?

3

Ataques à democracia: pode haver processos eleitorais seguros?

- Votação eletrônica e votação na Internet
- Hacktivismo e ataques durante campanhas eleitorais
- Como a segurança pode mudar a direção de um país

AUTOR

Camilo Guttierrez
ESET Head of Awareness and Research

Ataques à democracia: pode haver processos eleitorais seguros?

Nos últimos dois anos, houve disputas eleitorais em muitos dos países mais influentes do mundo. Após essas eleições, surgiram muitas perguntas, mas a principal é a possibilidade de um ataque cibernético influenciar uma fraude eleitoral a ponto de mudar o rumo político de uma nação.

Qualquer resposta à pregunta seria imprudente, mas, sem dúvida, estamos diante de um panorama que traz desafios. Há evidências suficientes para afirmar que o voto eletrônico ainda está longe de ter uma implementação segura nos países que o testaram, como veremos mais adiante.

Além disso, há outros dois eixos aos quais precisamos voltar a atenção. Em primeiro lugar, a influência das redes sociais na opinião pública e seu uso como ferramenta de hacktivismo; em segundo lugar, a necessidade de incluir assuntos de segurança cibernética nacional dentro da gestão política.

Sistemas de voto eletrônico inseguros

A inclusão da tecnologia nos processos eleitorais era questão de tempo, principalmente quando consideramos as razões pelas quais alguns países (como Argentina, Brasil, Alemanha ou Estados Unidos) decidiram implementar em alguma medida o voto eletrônico: acabar com a fraude, regularizar e acelerar a contagem, e complementar os registros em papel.

O problema começa quando eles não são complementados, mas substituídos. É verdade que não se pode frear o avanço da tecnologia, mas talvez seja necessário reorientar todos os esforços na direção de mecanismos adicionais de controle, não rumo a um modelo que, na realidade, só agrega novos pontos de falha sem eliminar os riscos: da mesma forma que os chefes de campanha, militantes e outros atores têm encontrado maneiras de fraudar eleições ao longo dos anos por meio da exploração do sistema eleitoral físico, os cibercriminosos também encontrarão uma forma de explorar o sistema digital, principalmente se contarem com algum tipo de patrocínio.

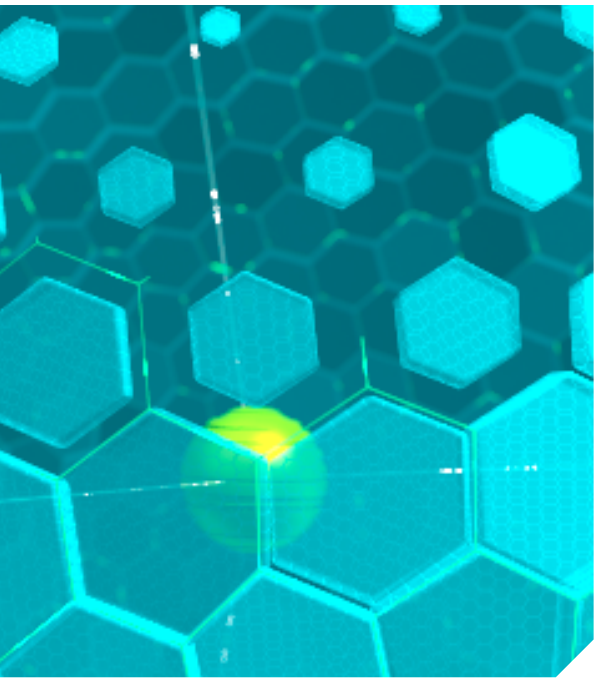
Em 2006, Harri Hursti já havia demonstrado, no célebre documentário "Hacking Democracy", que poderia comprometer por completo o sistema de voto Diebold no Condado de Leon, na Flórida, usando um cartão de memória. Dessa forma, ele conseguiu mudar todos os votos sem ser detectado, mas o software, com algumas variações, um novo nome e um novo dono, continua sendo usado nos Estados Unidos para contar votos.

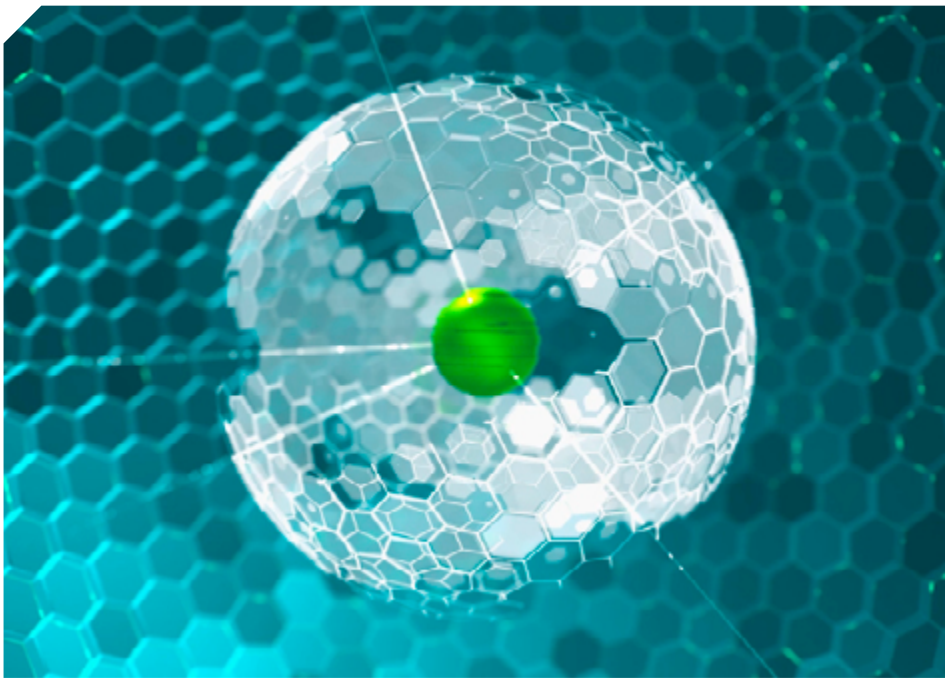
Passaram-se mais de 10 anos e pouco mudou, exceto pelo surgimento de mais evidências. A urna eletrônica no Brasil está rodeada de polêmica desde 2012, quando se descobriu que era possível quebrar completamente o caráter sigiloso dos votos. Após anos exibindo suas vulnerabilidades, nas eleições de 2018, o Tribunal Superior Eleitoral voltará a adotar (de maneira híbrida) o registro em papel dos votos em 5% das urnas. Entretanto, na Argentina e na Alemanha, também foram demostradas vulnerabilidades na transmissão de votos.

Então, a tendência indica que não podemos depender da tecnologia para algo tão delicado quanto um processo eleitoral: devemos usá-la como ferramenta complementar. Se a ideia é mitigar fraudes em qualquer uma de suas formas, consideremos sistemas híbridos, com registro de votos tanto eletrônico quanto em papel.

Hacktivismo para mudar a opinião pública

As interações de carácter político não escaparam ao alcance do fenômeno das





redes sociais. Estas são usadas como plataformas de campanha para atingir um número maior de pessoas, e também fomos testemunhas de seu uso para desestabilizar campanhas eleitorais por meio da disseminação de rumores, da criação de notícias falsas e, é claro, dos ataques em massa e dirigidos a figuras públicas.

O detalhe é que muitos desses ataques são feitos por meio de bots, ameaças informáticas ou outros tipos de ferramenta maliciosa que, com uma adequada gestão da segurança nas campanhas eleitorais, poderiam passar despercebidas. De forma inversa, o que seria uma expressão popular acaba sendo a manifestação de um grupo de atacantes.

O fato de isso permitir manipular ou desviar a opinião pública não significa o apocalipse da democracia, mas representa desafios de segurança para garantir uma participação política saudável.
No último mês de julho, foi anunciado o programa "Defending Digital Democracy", que conta com a participação e o financiamento de empresas como Facebook e Google. Isso é um reflexo da importância de levar em consideração a proteção desses tipos de mecanismo.

Enquanto as partes envolvidas não tomarem decisões sobre o assunto, continuaremos vendo esses incidentes no futuro.

Segurança cibernética nacional

A tecnologia faz parte das nossas vidas e, portanto, uma das responsabilidades de um Governo é garantir que os usuários possam interagir com ela da maneira mais segura possível, por meio de um programa de segurança cibernética de alcance nacional e da incorporação de personagens como CISOs e auditores.

E, uma vez que os funcionários, como, por exemplo, as autoridades de tribunais ou comissões eleitorais, precisam tomar decisões sobre a implementação de tecnologias, eles devem ter uma formação em segurança cibernética à altura das circunstâncias para saber escolher de forma correta.

É necessário considerar que novos avanços geram novos riscos e, se quisermos usar a tecnologia para melhorar as nossas vidas, não devemos deixar que novos problemas sejam criados. Tudo o que está relacionado ao sistema eleitoral deve começar a ser considerado como parte da infraestrutura crítica de cada país (e ser cuidado como tal).

Os desafios já se apresentaram. Chegou a hora de executar as ações de prevenção pensando na segurança digital da informação e de todos os atores envolvidos contribuírem com soluções para garantir a correta execução dos processos democráticos.

As redes sociais são usadas como plataformas de campanha para atingir um número maior de pessoas, e também fomos testemunhas de seu uso para desestabilizar campanhas eleitorais por meio da disseminação de rumores, da criação de notícias falsas e, é claro, dos ataques em massa e dirigidos a figuras públicas.

4

Cumprir pena por cibercrime: polícia e pesquisadores de malware se unem

- Interrupções, prisão e como a ESET luta contra a atividade cibercriminal
- Caso de sucesso: como a Windigo ajudou a prender um cibercriminoso?
- Por que devemos nos importar?

AUTOR

Alexis Dorais-Joncas
ESET Senior Security Researcher

Cumprir pena por cibercrime: polícia e pesquisadores de malware se unem

O principal papel da análise de malware é determinar como certo malware funciona, extrair IoCs (Indicadores de Comprometimento) e definir possíveis contra-ataques. Esse trabalho é quase que inteiramente técnico: seu foco são arquivos binários e suas propriedades. Os resultados da análise de malware são cruciais para as organizações, permitindo se defender contra surtos ou agir mediante uma infecção em tempo real. Eles também são cruciais para os vendedores de softwares de segurança, fazendo com que eles possam criar melhores detecções e medidas de proteção para seus consumidores.

Outros tipos de questões precisam ser respondidas. Esse arquivo está relacionado com aquele outro? Como a estrutura C&C (Comando e Controle) é construída e como o protocolo de comunicação funciona? Como a botnet monetiza suas atividades: *pay-per-install*, spam, redirecionamento de tráfego?

Responder perguntas como essas é o que a pesquisa de malware faz. Ela permite um melhor entendimento sobre o que há por trás de uma simples amostra de malware, para conectar os pontos e conhecer melhor o que acontece.

É claro que isso também ajuda os desenvolvedores de softwares de segurança – também conhecidos como vendedores de soluções antivírus – para que eles criem proteções melhores. No entanto, as informações decorrentes da pesquisa de malware podem ser úteis para a luta contra o cibercrime e o cumprimento das leis. Como isso acontece? Com alguns exemplos do trabalho feito pela ESET, podemos ver como isso ajudou a interromper operações maliciosas.

Campanha disruptiva contra Dorkbot

Em 2015 a ESET foi convidada pela Microsoft para uma campanha contra a família de malware do Win32/Dorkbot, em uma campanha CME (*Coordinated Malware Eradication*). Dorkbot era um kit que estava disponível para compra em fóruns clandestinos, que infectou mais de um milhão de computadores cruzando diversas botnets independentes. O objetivo dessa campanha era interromper totalmente o maior número de botnets possíveis, derrubando suas estruturas C&C simultaneamente.

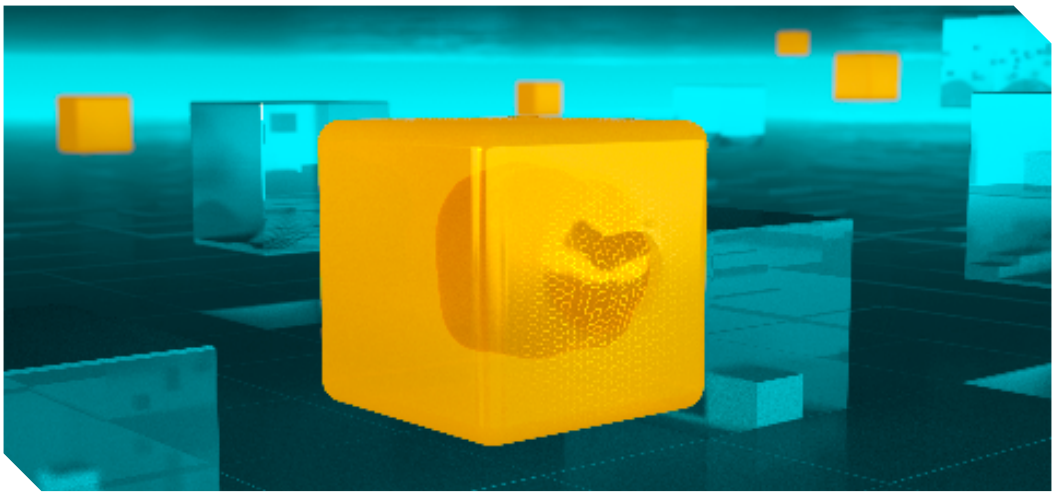
Para ajudar nessa operação, os pesquisadores de malware da ESET automatizaram o processo de extração dos dados binários da C&C do Dorkbot. Nós aplicamos esse processo para as assinaturas já existentes e as amostras novas do Dorkbot. Após isso, sanitizamos manualmente os resultados, removendo os sinkholes conhecidos e limpando os domains/IPs para mitigar o risco de perda de recursos legítimos. A Microsoft juntou nossas informações com as dela e criou uma lista imensa de todos os nodos C&C que estavam ativos para serem localizados. Essa lista completa foi depois entregue para agências de forças de segurança em todo o mundo, como a *Canadian Radio-television and Telecommunications Comission* (CRTC), o *Department of Homeland Security's United States Computer Emergency Readiness Team* (DHS/US CERT), *Europol*, o *Federal Bureau of Investigation* (FBI), *Interpol*,

e o *Royal Canadian Mounted Police* (RCMP). No dia do interrompimento, mandados de retirada foram executados em uma ação coordenada.

Desde então, vimos um grande declínio das atividades relacionadas ao Dorkbot no mundo todo, indicando que a campanha CME obteve sucesso.

informações relevantes que estavam disponíveis para o público.

Com esses dados em mãos, o FBI foi capaz de fazer sua parte, de maneira devagar, porém com garantindo que daria certo. Em meados de 2015 um cidadão russo chamado Maxim Senakh foi identificado como um dos colaboradores por trás da Operação



Windigo e a Ebury botnet

Em 2014 a ESET publicou pela primeira vez uma grande análise técnica que chamamos de Operação Windigo. Resumidamente, Windigo foi sustenado por um roubo de credenciais que infectou dez mil servidores Linux, em que foram instalados componentes maliciosos, usados para monetizar a botnet para redirecionar o tráfego da web e enviar spam. Após a publicação, iniciamos uma colaboração com o FBI em sua investigação frente o cibercrime por trás da Operação Windigo.

Nossa contribuição foi compartilhar informações técnicas decorrentes das nossas pesquisas de malware, como IPs infectados, dados retirados das mensagens de spam enviadas pela botnet, entre outras

Windigo e formalmente indiciado nos Estados Unidos.
Senakh foi preso pelas autoridades finlandesas ao passar pela fronteira, enquanto voltava de férias para a Rússia, e depois foi extraditado para os EUA em fevereiro de 2016. Senakh foi julgado como culpado por conspiração e crime por fraude na rede, violando a Lei de Fraude e Abuso de Computador. Ele foi sentenciado por 46 meses de prisão.

Mais detalhes sobre essa história estão disponíveis nesse post https://www.welivesecurity.com/br/2017/10/30/eset-ajudou-o-fbi-caso-windigo/

Por que devemos nos importar?

Gastar tempo e energia para fazer com que a vida dos cibercriminosos seja bem mais complicada vale a pena. Acreditamos que seja a melhor maneira de ajudar a previnir as atividades do cibercrime e assim tornar a Internet um lugar mais seguro. Também acreditamos que é a coisa certa a se fazer.

Existem diversas teorias por trás da clássica prevenção de crimes e nós com certeza não iremos fingir que somos criminologistas. No entanto, há uma linha tênue entre o que fazemos para combater o cibercrime e a teoria de "*situational crime prevention*", que é definida por:

Uma *situational crime prevention* é baseada na premissa de que o crime é geralmente oportunista, e essa teoria visa modificar os fatores contextuais para limitar as oportunidades dos infratores para engajamento de comportamentos criminosos.

As técnicas para isso podem ser divididas em diversas categorias e três delas são relacionadas ao que fazemos.

1. Aumentar os esforços envolvidos nas ações ilegais. Executar campanhas disruptivas como a que foi realizada contra Dorkbot, força os cibercriminosos a se organizar de maneira diferente e faz com que eles busquem por novas estratégias ou técnicas, como criar um novo malware ou mudar os protocolos de comunicação, claramente aumentando os esforços necessários para manter uma operação criminosa ativa.

2. Reduzir os prêmios decorrentes de um crime. Concluindo a categoria acima, quando se torna a operação criminosa mais complicada, isso necessariamente aumenta os esforços para cometer um crime, o que reduz o lucro proporcionalmente.

3. Aumentar o risco relacionado aos atos ilegais.

Disponibilizando informações técnicas para agentes de forças de segurança os ajuda a guiar suas investigações para a direção certa e assim construir casos mais sólidos. Quanto mais as investigações cibercriminais forem apoiadas por pesquisadores de malware, isso irá gerar mais prisões, consquentemente aumentando o risco dos infratores serem pegos.

Algumas pessoas acham que somente alguns são punidos ao realizar um cibercrime, sendo fácil cometer delitos na Internet de forma anônima, sem muitas chances de serem rastreados. É praticamente o contrário: manter uma operação de segurança (OPSEC) perfeita e de maneira consistente é bem difícil. Pense em tudo que deve ser feito para realizar uma operação criminosa: lançar campanhas de infecção, monitorar o status da botnet, atualizar os componentes maliciosos, registrar nomes de domínio ou serviços de hospedagem, monetizar a operação em si, e muito mais. Para realizar um cibercrime perfeito, cada etapa deve ser executada com excelência a todo o tempo. Cibercriminosos são humanos e humanos cometem erros. Basta um dia ruim em que o atacante se conecta ao servidor errado antes de ativar a VPN ou a conexão TOR e uma flecha gigante estará apontada para ele ou ela em um arquivo qualquer, somente esperando alguém para achá-lo.

Algumas pessoas também desistem de ir atrás de cibercriminosos porque quando são identificados, eles ainda permanecem fora de alcance. Talvez eles vivem em um país em que não existem leis efetivas contra o esse tipo de crime, ou que não possui extradição para outros países os investigarem, porém os humanos cometem erros. Para eles serem pegos, basta que eles saiam de seu país para aproveitar suas férias em outro lugar.

Para realizar um cibercrime perfeito, cada etapa deve ser executada com excelência a todo o tempo. Cibercriminosos são humanos e humanos cometem erros.

2017 foi marcado por um enorme número de prisões em diversas operações cibercriminosas, como foi destacado no excelente sumário feito pelo Stephen Cobb. As grandes forças de segurança ao trabalhar com instituições privadas como a ESET, tendem a ganhar bastante experiência para atingir o objetivo de rastrear infratores. Essa união trará mais e mais sucesso para as investigações e contribuirá para fazer com que a Internet seja um lugar mais seguro para todos. Com exceção dos cibercriminosos.

Para realizar um cibercrime perfeito, cada etapa deve ser executada com excelência durante todo o tempo. Cibercriminosos são humanos e humanos cometem erros.

5

A informação pessoal na nova era da tecnologia e a legislação

- Como a IoT está nos levando a um mundo "público" em termos de informações pessoais
- Perfis montados nas redes sociais
- Comportamento dos usuários usados na indústria AV (Microsoft, Kaspersky) em relação aos antivírus gratuitos

AUTOR

Tony Anscombe
ESET Global Security Evangelist and Industry Partnerships Ambassador

A informação pessoal na nova era da tecnologia e a legislação

A privacidade é, ou pelo menos deveria ser, um direito fundamental do ser humano. No entanto, tem se tornado cada vez mais complexo para qualquer consumidor ou empresa manter uma atitude neutra em relação ao tratamento dos dados. Pode haver adeptos da privacidade extremamente motivados no mundo tecnológico que não deixam marcas em lugar algum, mas a realidade é que a maioria de nós deixa marcas por todo o lado, como na areia de uma praia em um dia ensolarado.

Os dados conduzem à próxima revolução tecnológica, e alimentam os imensos sistemas de inteligência artificial que estão sendo construídos. Quando os nossos dados entrarem no processo de decisões tomadas por máquinas, será que poderemos algum dia remover, de fato, as nossas informações e ser esquecidos? Será que as empresas que coletam dados sequer compreendem onde e como eles são usados pelos sistemas de IA?

Embora a maioria de nós saiba que está entregando as informações para as redes sociais ou para outras empresas por meio de formulários e registros, há muitas outros serviços de coleta de dados que podem não ser tão evidentes.

Software e serviços gratuitos

Como muitos dos consumidores esperam usufruir de softwares sem pagar por eles, ou pagando muito pouco, alguns fornecedores optaram por entrar no mercado de coleta e compartilhamento de dados. Há apenas algumas poucas maneiras de rentabilizar os produtos de software gratuitos, e mesmo os menos intrusivos, pelo menos do ponto de vista do usuário, podem estar coletando e vendendo os dados para terceiros.

No ano passado, vimos fornecedores de segurança confiáveis optarem por oferecer produtos antivírus gratuitamente. Embora não tenham declarado abertamente as suas intenções de rentabilizar os seus novos produtos gratuitos, devemos contar com métodos de rentabilização indireta, como a coleta de dados.

A oferta de produtos gratuitos com rentabilização indireta pode ter sido acelerada pela Microsoft, quando passou a oferecer o Windows Defender AntiVirus como opção gratuita padrão. À medida que uma porcentagem dos usuários aderiu à opção padrão da Microsoft, passou a haver menos oportunidades para os fornecedores existentes venderem softwares, e daí surgiu a necessidade de procurar formas de rentabilização alternativas e de competir com os seus próprios softwares gratuitos.

A tendência de softwares gratuitos ou de baixo custo aumentará ao longo do próximo ano. O risco para a privacidade resulta da falta de métodos tradicionais de rentabilização, e a divulgação complexa projetada para ocultar o intuito de quais dados estão sendo coletados e se estes poderão ser vendidos. Muitas empresas oferecem políticas de privacidade extenuantes e ilegíveis, compreensíveis apenas para os advogados.

Com qualquer produto gratuito, é importante que o usuário compreenda como é que a empresa está ganhando dinheiro.

No caso de um jogo para dispositivos móveis, por exemplo, pode ser através da exibição de anúncios, ou oferecer a compra de níveis adicionais do jogo. Se não é evidente a forma como a empresa está ganhando dinheiro, é grande a probabilidade de que o método de rentabilidade venha dos seus dados e da sua privacidade.

Internet das Coisas (IoT)

Embora os produtos e aplicativos gratuitos já conheçam os nossos hábitos online, a adoção da IoT pelos consumidores e empresas significa que os dados sobre a forma como vivemos está agora disponível para coleta e exploração.

Ao voltar de carro para casa, o seu celular está transmitindo as condições do tráfego para compartilhá-las com outros motoristas, na esperança de que isso lhe permita fazer os desvios corretos ou boas decisões de condução para chegar em casa mais cedo. O termostato conectado na sua casa está se comunicando com o seu celular, já que a sua localização e a hora do dia indicam quando você está a caminho de casa. Ao chegar na rua da sua casa, a porta da garagem abre automaticamente, utilizando a sua proximidade para decidir quando deve fazê-lo. As luzes se acendem e a música passa automaticamente do carro para a casa. Os dispositivos IoT são projetados para trabalhar em conjunto e simplificar a nossa existência.

E cada dispositivo tem muito para contar graças aos dados que coleta. A combinação desses dados dará o panorama completo da nossa vida, onde trabalhamos, onde comemos, quando vamos à academia, que cinema nos agrada, onde fazemos compras, e assim por diante. Os dados combinados e a inteligência artificial podem significar que começaremos a ser marionetes da tecnologia, que começará a tomar decisões por nós.

A companhia de análises Gartner previu que em 2018 haverá 11,2 bilhões de dispositivos conectados no planeta, aumentado para 20,4 bilhões em 2020. A revolta dos dispositivos está a caminho, fique atento.
Cada vez que um dispositivo pede para ser conectado devemos instruir o consumidor ou a empresa a ler a política de privacidade e tomar decisões conscientes sobre aceitar ou não os termos de coleta de dados definidos na política de privacidade.

Legislação

Em 2018, a Regulação de Proteção de Dados Pessoais aprovada na Comissão Europeia dará poder aos cidadãos sobre a forma como as suas informações são processadas e usadas. A legislação tem efeito sobre qualquer empresa que processar ou coletar os dados de um cidadão da União Europeia, independentemente da região em que estiver localizada.

A não conformidade pode resultar em multas substanciais, mas ainda não há uma resposta clara sobre como essas multas serão aplicadas para empresas fora da UE. A Comissão precisará criar um exemplo com uma empresa localizada fora de seus limites territoriais, e potencialmente pouco tempo depois da data de implementação em maio. Sem um exemplo de sua aplicação, muitas empresas internacionais podem arriscar o não cumprimento, portanto, poderemos ver a Comissão Europeia avançar e tomar medidas contra uma empresa internacional em 2018.

A privacidade nos EUA teve um retrocesso em 2017, quando a nova administração revogou a legislação pendente que limitava a coleta sem consentimento de dados pessoais por parte dos ISPs. Embora alguns ISPs tenham feito um compromisso vo-

E cada dispositivo tem muito para contar graças aos dados que coleta. A combinação desses dados dará o panorama completo da nossa vida.

luntário de não permitir marketing de terceiros, isso não significa que não o usarão para o seu próprio benefício comercial.

A abrangência dos dados coletados sobre os nossos hábitos online poderia facilmente permitir a criação de perfis que exponham interesses extremamente pessoais que sequer percebemos que estão sendo coletados.

O ecossistema dos Big Data faz com que muito mais empresas tenham agora a capacidade de coletar e vender dados.

Com a facilidade com que as empresas podem coletar e vender os dados e com a nossa propensão a evitar ler uma política de privacidade e aceitar automaticamente as definições padrão, a nossa identidade, estilo de vida e dados pessoais passarão a ser um ativo corporativo.

Os perfis dos clientes poderiam se tornar o alvo de hackers. Já assistimos ao vazamento de dados pessoais de sites que armazenam dados, de lojas, entre outros, mas o roubo dos dados que são gerados ao observarem tudo o que fazemos online poderia ser o objetivo final de um cibercriminoso. A oportunidade de chantagear os usuários com base nos seus hábitos online.

A capacidade de manipular enormes quantidades de dados, conforme descrevemos acima, e usá-los para algo significativo é um conceito relativamente novo para muitos fornecedores de software, desde que se tornou uma tarefa menos onerosa.

Espero que 2018 traga uma maior conscientização dos usuários, mas, sendo mais realista, suspeito que veremos uma maior quantidade de dados coletados e pouca conscientização dos usuários. Com cada dispositivo que é conectado sem haver uma decisão ou opção consciente, a nossa privacidade é prejudicada mais um pouco, até que, em algum momento, a privacidade será algo que apenas os nossos antepassados desfrutaram.

CONCLUSÃO

Conclusão

O espectro dos ataques cibernéticos continuará avançando, como ficou claro após analisar a evolução do ransomware e dos ataques à infraestrutura crítica, por exemplo. No entanto, devemos ter presente que estes cenários complexos são apenas uma parte do panorama de crimes cibernéticos, e não é sequer a parte mais evidente: os ataques avançados chamam mais a atenção, mas representam apenas uma pequena porcentagem daquilo que vemos diariamente em um laboratório de análises de malware.

O certo é que a grande maioria das ameaças que atingem os seus objetivos diariamente são aquelas mais simples, as que se distribuem por campanhas maliciosas de e-mails indesejados, phishing e downloads diretos, e, portanto, as que poderiam ser neutralizadas com pouco esforço. O problema é que ainda não se destinam recursos suficientes para fazê-lo, e que falta maior conscientização do público para estar mais preparado.

Os acontecimentos que envolveram falta de segurança informática de 2017 demostraram que, devido ao avanço da tecnologia e de sua rápida adoção por parte de usuários e empresas, vários dos cenários que alguns anos atrás pareceriam impensáveis encontram-se hoje no âmbito das possibilidades.

Mais além das particularidades de cada caso, o denominador comum de todas estas situações é sempre o mesmo: a informação. Não importa se se trata de informações de uma empresa, de um governo ou de um usuário particular que acredite não possuir nenhum dado de interesse. Hoje em dia, a informação é compartilhada por vários participantes. Ela é usada como moeda para acessar aplicativos e conteúdos gratuitos, é usada por entidades governamentais para manter os seus registros e ordenar as suas operações, e é usada pelas empresas que operam na Internet para gerar rentabilidade à custa dos perfis dos usuários.

Na maior parte dos casos, trata-se de uma atividade legítima e transparente, frequentemente descrita nos termos e condições que poucos se dão ao trabalho de ler. Mas o que acontece quando estas informações passam por tantas mãos? Multiplicam-se as possibilidades de que algo dê errado, o que aumenta proporcionalmente o risco.

A informação pessoal de um usuário pode ser comprometida por um incidente particular, como uma infecção por malware ou uma campanha de phishing, ou através de uma brecha nos sistemas de uma empresa de confiança do cliente, ou mesmo devido a um ataque cibernético que afete uma entidade governamental ou financeira, por exemplo.

Portanto, se há tantas frentes a serem protegidas, o que estamos esperando para instar todos os participantes envolvidos a fazer a sua parte? Não se trata de uma missão que diz respeito apenas às empresas de segurança cibernética, nem se pode exigir que elas acabem com o problema. Seria o mesmo que exigir que o remédio erradique a enfermidade, ou que a polícia erradique a criminalidade.
As fraudes digitais e as ameaças informáticas continuarão a existir enquanto

houver na nossa sociedade pessoas dispostas a prejudicar os outros pelo simples fato de que podem fazê-lo.

É hora de todos os níveis de usuários e, especialmente, os cidadãos, compreenderem que a sua segurança depende tanto dos fornecedores de sua preferência como de si mesmos, e que há ainda muito por fazer. O primeiro passo é compreender o valor da informação nestes tempos, e os motivos pelos quais cada participante precisa dela para atingir os seus objetivos. Não se pode proteger alguma coisa sem saber primeiro do quê e porquê a estamos protegendo.

O conhecimento das ameaças e as medidas para evitá-las são hoje indispensáveis para proteger a disponibilidade, a confidencialidade e a integridade da informação dos diferentes elementos da sociedade, informação que se converteu na base de muitas atividades, tanto lícitas quanto ilícitas.

O panorama parecer ser alentador: desde que o WannaCryptor tomou por surpresa o mundo inteiro, a segurança tem começado a estar presente em mais aspectos e para um maior número de participantes. Os ataques às contas de redes sociais de celebridades e clubes de futebol, como o Real Madrid e o Barcelona, assim como aos sistemas internos de empresas de alto perfil como a HBO, Disney e Equifax, também causaram um impacto no público geral, que começa a compreender o que está ocorrendo.

Esperamos que este relatório ajude a evidenciar os temas-chave que faltam abordar para avançarmos rumo a um ambiente mais seguro.

ENJOY SAFER TECHNOLOGY™