esquerda.net

Published on *Esquerda* (http://www.esquerda.net)

Relatório secreto da NSA mostra hacking russo dias antes da eleição americana

2017/06/11 - 4:12pm

A espionagem russa lançou um ataque cibernético aponta um relatório da NSA obtido por The Intercept. Este é o relato mais detalhado até agora de um órgão do governo norte-americano sobre a interferência russa nas eleições de 2016. Por Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim

A espionagem russa lançou um ataque cibernético em pelo menos um fornecedor de software de votação dos EUA e enviou e-mails de phishing a mais de 100 funcionários de secções eleitorais poucos dias antes da eleição presidencial norte-americana, em novembro do ano passado. É o que aponta um relatório de segurança secreto obtido por The Intercept.

O relatório da Agência Nacional de Segurança (NSA, na sigla em inglês) foi fornecido anonimamente a The Intercept e autenticado de forma autónoma. O documento, datado de 5 de maio de 2017, analisa informações levantadas pela NSA sobre meses de esforços por parte da espionagem russa para promover ataques cibernéticos contra funcionários e contra a infraestrutura de votação dos EUA. É o relato mais detalhado até agora de um órgão do governo norte-americano sobre a interferência russa nas eleições de 2016.

O documento mostra como a NSA estuda a mecânica dos ataques russos, mas não entra em detalhes sobre a segurança ?crua? subjacente sobre a qual se baseia a análise. Um oficial de informações dos Estados Unidos, que não quis se identificar, alertou para o risco de se tirar conclusões definitivas baseadas na análise de apenas um documento.

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

[redacted] DIRNSA [redacted]

National Security Agency

Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any

Relatório da NSA [1]

O relatório indica que a ação russa nos sistemas de votação dos EUA pode ter sido mais profunda do que se imaginava até agora. Já na introdução, a NSA deixa claro que a responsável pelos ataques cibernéticos em questão foi a espionagem militar russa, mais especificamente a Diretoria-Geral de Segurança do Estado-Maior da Rússia (GRU, na sigla em inglês):

> ?Os agentes da Diretoria-Geral de Segurança do Estado-Maior Russo? executaram operações de ciberespionagem contra uma empresa norte-americana em agosto de 2016 para obter informações sobre soluções de software e de hardware eleitorais? Os autores provavelmente usaram os dados obtidos nessa operação para? lançar uma ação de *spear-phishing* (N.T.: e-mail malicioso direcionado a um alvo específico) voltada para servidores eleitorais dos Estados Unidos, tendo por alvo registros de eleitores?.

O texto vai na contramão da declaração [2] do presidente russo. Na semana passada, Vladimir Putin afirmou que a Rússia não havia interferido em eleições estrangeiras: ?Nós não nos envolvemos nisso num âmbito estatal, nem tivemos intenção de fazê-lo?. Até então, Putin vinha negando veementemente qualquer envolvimento russo. Mas, pela primeira vez, deixou em aberto a possibilidade de que hackers russos com ?tendências patrióticas? tenham sido responsáveis pelo ataque. Já o relatório da NSA é inequívoco: o ataque cibernético foi realizado pelo GRU.

A NSA não chega a uma conclusão sobre a interferência do ataque no resultado da eleição e admite que ainda há muito por descobrir sobre a extensão da ação dos hackers. No entanto, o relatório levanta a hipótese de ter havido violação de alguns elementos do sistema de votação, com consequências ainda incertas.

Entrámos em contacto com a NSA e com o Diretor de Segurança dos EUA, que não quiseram comentar. A NSA pediu que não publicássemos o relatório secreto. Quando informados de que iríamos prosseguir com a matéria, pediram para ocultarmos trechos dos documentos obtidos. Concordamos em não divulgar partes que julgamos não serem de claro interesse público.

O relatório acrescenta novos e significativos detalhes à análise que já havia sido feita pelo governo Obama, em janeiro. A avaliação chegou a apresentar algumas conclusões dos órgãos de segurança dos EUA, mas omitiu muitos pormenores, alegando que não seria prudente divulgar informações sobre fontes e métodos estratégicos. O estudo havia concluído que o Kremlin ordenara um extenso e diversificado esforço de propaganda ?para minar a confiança dos eleitores no processo democrático dos EUA, afetar Hillary Clinton, prejudicar sua eleição e potencial presidência?.

Nessa ocasião, o impacto das ações russas no resultado das eleições não chegou a ser investigado, muito embora já reconhecessem que ?a segurança russa havia obtido e mantido o acesso a funcionários de vários conselhos eleitorais municipais e estaduais dos EUA?. Segundo o Departamento de Segurança Nacional, a avaliação concluiu, em tom tranquilizador, que ?os sistemas atacados pelos agentes russos não estavam envolvidos na contagem de votos?.

Só que agora a NSA descobriu que hackers do governo russo, integrantes de uma equipa

cuja missão é ?realizar espionagem cibernética de eleições norte-americanas e estrangeiras?, se concentraram em partes do sistema diretamente ligadas ao processo de registo de eleitores, incluindo um fabricante de aparelhos para manter registos eleitorais. Os dispositivos produzidos por essa empresa contam com internet sem fio e Bluetooth, o que pode ter criado um ponto de partida ideal para os ataques.

Spear-Phishing Campaig

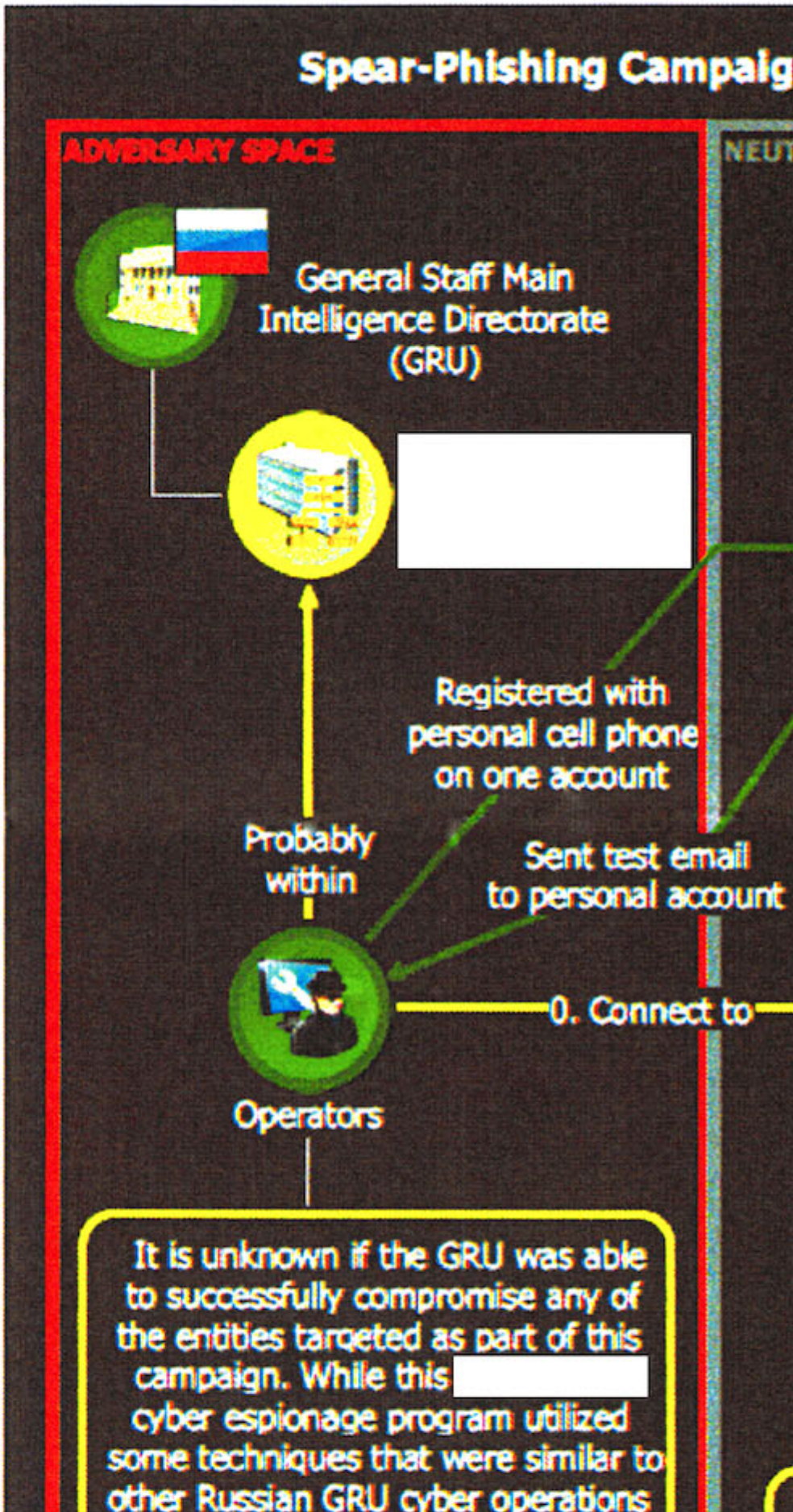


Tabela anexada ao relatório secreto da NSA dá um panorama detalhado do ataque de spear-phishing realizado pelo governo russo. The Intercept não teve acesso à segunda página do documento. Imagem: NSA

O ataque por e-mails de *spear-phishing*

Conforme descreve o relatório da NSA, o plano russo era simples: passar por um fornecedor de urnas eletrónicas para fazer com que funcionários de secções eleitorais abrissem documentos do Word com vírus ? dando aos hackers controle total sobre os computadores infetados.

Mas para conseguir enganar as autoridades locais, os hackers precisavam de um disfarce convincente. Para isso, invadiram sistemas internos de um fornecedor de software eleitoral. Em 24 de agosto de 2016, mandaram e-mails falsos para uma empresa do ramo, fingindo ser a Google. Embora não identifique claramente a empresa, o relatório da NSA faz referência a um produto fabricado pela VR Systems, da Florida, que fornece serviços e equipamentos para votações eletrónicas em oito estados.

O e-mail de *spear-phishing* continha um link que direcionava os funcionários para um site falso do Google que, por sua vez, pedia dados de login e mandava tudo para os hackers. A NSA identificou sete ?potenciais vítimas? na empresa. O servidor conseguiu bloquear os e-mails mandados para três delas. Mas a NSA concluiu que pelo menos uma das sete contas foi invadida. No relatório, a agência de segurança dos EUA observa que ?não se sabe se a ação de *phishing* acima mencionada atingiu com sucesso todas as vítimas pretendidas nem quais dados podem ter sido extraídos?.

A VR Systems não quis comentar o *hacking* descrito no relatório da NSA. O Diretor de Operações, Ben Martin, respondeu por e-mail a The Intercept:

> ?*Phishing* e *spear-phishing* não são incomuns em nosso segmento. Para combater esse tipo de ameaça, participamos regularmente de acordos entre empresas, governo e agências regulatórias. Temos políticas e procedimentos em vigor para proteger nossos clientes e nossa empresa.?

O relatório da NSA indica que a VR Systems sofreu apenas roubo de dados de login e não invasão do sistema. Mas isso não é necessariamente um bom sinal. Jake Williams, fundador da empresa de segurança cibernética Rendition Infosec e ex-membro da equipa de Acesso Personalizado da NSA, diz que roubo de logins pode ser ainda mais perigoso do que ter um computador infetado.

Para ele, ?na maioria das vezes, o roubo de login é mais danoso? uma vez que as informações do funcionário podem ser usadas para entrar em ?VPNs corporativas, e-mail ou serviços na nuvem?, permitindo o acesso a dados internos. O risco é ainda maior porque é comum o funcionário usar a mesma senha para vários serviços. Como a palavra em inglês sugere, o *phishing* não precisa que todos mordam a isca para ser bem-sucedido. Williams ressalta, no entanto, que os hackers ?nunca querem só um? conjunto de logins.

Campaign Against U.S. Company 1 and Voter Registration-Themed Phishing
Officials (S//SI//REL TO USA, FVEY/FISA)

Russian Cyber Threat Actors Target U.S. Company 1 (S//REL TO USA, FVEY/F

(TS//SI//OC/REL TO USA, FVEY/FISA) Cyber threat actors [redacted]

phishing campaign from the email address noreplyautomaticservice@gmail.com on
victims that included employees of U.S. Company 1, according to information that b
2017.[1] This campaign appeared to be designed to obtain the end users' email cred
victims to click on an embedded link within a spoofed Google Alert email, which wo
malicious domain [redacted].[2] The following potential victims w

- **U.S. email address 1 associated with U.S. Company 1,**
- **U.S. email address 2 associated with U.S. Company 1,**
- **U.S. email address 3 associated with U.S. Company 1,**
- **U.S. email address 4 associated with U.S. Company 1,**
- **U.S. email address 5 associated with U.S. Company 1,**
- **U.S. email address 6 associated with U.S. Company 1, and**
- **U.S. email address 7 associated with U.S. Company 1.**

(TS//SI//OC/REL TO USA, FVEY/FISA) Three of the malicious emails were rejected
the response message that the victim addresses did not exist. The three rejected e
email address 1 to 3 associated with U.S. Company 1.

Trecho do relatório ultrassecreto da NSA sobre uma operação da agência de segurança russa para atacar a estrutura eleitoral americana. Imagem: NSA

Tradução: Ataques a empresa norte-americana 1 e ação de phishing de registro eleitoral tendo por alvo servidores municipais
Agentes russos atacam empresa norte-americana 1 com ameaças cibernéticas
Agentes[redigido] lançaram ação de spear-phishing a partir do e-mail noreplyautomaticservices@gmail.com [3] no dia 4 de agosto de 2016, tendo por alvo funcionários da empresa norte-americana 1, de acordo com informações que se tornaram disponíveis em abril de 2017. A ação parece ter sido pensada com o objetivo de colher os dados de login de usuários. Os recipientes da mensagem eram levados a clicar em um link anexado no corpo do e-mail, que imitava uma mensagem do Google Alert. Ao clicar, eram redirecionados para o domínio falso [redigido]. Foram identificadas as seguintes vítimas potenciais:
? E-mail dos EUA 1 associado com empresa dos EUA 1
? [?]
Três dos e-mails contendo o malware foram bloqueados pelo servidor da companhia, que

mandou uma resposta automática dizendo que o endereço da vítima não existia.

Em todo o caso, os hackers aparentemente conseguiram o que precisavam. Dois meses depois, no dia 27 de outubro, criaram uma conta no Gmail, projetada para parecer a de um funcionário da VR Systems, e usaram documentos obtidos na operação anterior para lançar uma segunda ação de *phishing*, dessa vez contra funcionários das secções eleitorais do governo dos EUA. Esses e-mails continham um documento do Word que havia sido ?troianizado?. Quando aberto, enviaria um sinal para a ?infraestrutura maliciosa? criada pelos hackers.

A NSA concluiu que essa fase da operação de *spear-phishing* foi provavelmente lançada entre 31 de outubro e 1º de novembro. Os e-mails com o vírus foram enviados para 122 endereços ?de organizações municipais?, provavelmente para servidores ?envolvidos na gestão de sistemas de registo de eleitores?. Os e-mails continham anexos do Microsoft Word ? aparentemente, informações sobre a linha de produtos de banco de dados EViD, da VR Systems. Na verdade, eram comandos maliciosos que se ativavam quando o usuário abria o documento. Esses arquivos, que funcionam como armas cibernéticas, usavam o PowerShell, uma linguagem de script da Microsoft, projetada para administradores de sistemas e instalada automaticamente em computadores com Windows, permitindo um amplo controle sobre as configurações e funções de um sistema. Caso fossem abertos, os arquivos ?muito provavelmente? teriam instruído o computador infetado a baixar um segundo pacote de malware de um servidor remoto, também controlado pelos hackers. Ainda de acordo com o relatório, isso levaria os invasores a ter ?acesso permanente? aos computadores e permitiria que eles procurassem arquivos de seu interesse. Basicamente, esse documento do Word adulterado desbloqueia e abre uma ?porta? no sistema, permitindo que qualquer software malicioso seja automaticamente baixado.

Segundo Williams, quando esse tipo de ataque é bem-sucedido, o hacker passar a ter uma capacidade ?ilimitada? de buscar arquivos de seu interesse. ?Assim que o usuário abre o [anexo do e-mail]?, explica Williams, ?o invasor pode fazer as mesmas coisas que o usuário local?. Vikram Thakur, gerente sénior de investigação da equipa de segurança da Symantec, diz que, em casos como esse, ?a quantidade de dados roubados é limitada apenas pelas proteções instaladas pelos administradores de sistema?. Williams ressalta que esse tipo de roubo de dados geralmente é criptografado, ou seja, quem observa uma rede sendo infetada não consegue ver o que estava sendo roubado, só percebe que algo de errado está acontecendo. Williams define esse método como de ?sofisticação mediana?, que ?praticamente qualquer hacker consegue fazer?.

A NSA, no entanto, não tem certeza sobre os resultados do ataque. ?Não se sabe se a ação de *spear-phishing* acima mencionada atingiu com sucesso todas as vítimas pretendidas nem quais dados podem ter sido acessados pelo invasor?.

O FBI não nos informou se vai realizar uma investigação criminal sobre o ataque cibernético sofrido pela VR Systems.

Durante uma conferência de imprensa realizada em dezembro, o ex-presidente Barack Obama afirmou ter pedido ao presidente russo, Vladimir Putin, para não hackear a infraestrutura eleitoral dos EUA. ?Eu estava preocupado em garantir que [a invasão aos e-mails do partido Democrata] não fosse agravada por outros potenciais ataques que poderiam

dificultar a contagem de votos e afetar o próprio processo eleitoral?, disse Obama. ?Então, no início de setembro, quando encontrei o presidente Putin na China, achei que a maneira mais eficaz de garantir que isso não aconteceria fosse falar diretamente com ele e dizer para parar com isso. Que haveria consequências graves se ele não tomasse providências. E, de facto, não notámos mais nenhuma violação de nosso processo eleitoral?.

No entanto, a NSA descobriu que a interferência de facto continuou. ?É preocupante que isso tenha acontecido em outubro?, diz um alto funcionário de uma agência reguladora, especialista em ataques cibernéticos. ?Em agosto de 2016, o FBI e o Departamento de Segurança Interna deram alertas. Então, não foi uma surpresa. Não era difícil se defender dessas ameaças, mas era preciso verba orçamentária e atenção para o problema?, disse ele.

O documento da NSA descreve brevemente duas outras operações de *hacking* russo relacionadas com as eleições. Em uma delas, hackers militares criaram uma conta de e-mail para fingir ser mais uma empresa eleitoral (citada no documento como ?empresa norte-americana 2?). Assim, enviaram falsos e-mails de teste, oferecendo ?produtos e serviços relacionados com as eleições?. A agência não conseguiu descobrir se houve roubo de dados usando essa outra conta de e-mail.

Numa terceira operação, o mesmo grupo de hackers enviou e-mails de teste para endereços do Escritório Eleitoral da Samoa Americana, provavelmente para saber se essas contas existiam antes de lançar outro ataque de *phishing*. Não está claro se a iniciativa foi bem-sucedida, mas a NSA avaliou que os russos tinham intenção de ?passar por um fornecedor de serviços de voto em trânsito?. O relatório não indica por que os russos visaram as pequenas ilhas do Pacífico, um território dos EUA que não participa na eleição.

Um alvo atraente

Para conseguir atenção e verba para um problema de segurança eleitoral, é preciso primeiro resolver um impasse político. ?O problema é que ninguém pensa na questão da segurança até algo dar errado. E depois que acontece, um dos lados não vai querer resolver, pois a falha o favoreceu?, diz Bruce Schneier, especialista em segurança cibernética no Berkman Center [4], de Harvard, que escreveu várias vezes sobre as vulnerabilidades dos sistemas eleitorais dos EUA. ?Torna-se um problema de segurança muito difícil de ser resolvido, contrariamente à segurança da conta bancária, por exemplo?.

Schneier considera que o ataque descrito pela NSA é um procedimento padrão de *hacking*. ?Roubo de login, *spear-phishing* ? é assim que funciona. Uma vez que você consegue uma base, você começa a explorar outras possibilidades de ataque?.

Isso tudo significa que é imprescindível entender o papel da VR Systems no sistema eleitoral norte-americano e as consequências dessa invasão na integridade do resultado da eleição.

A VR Systems não vende as urnas *touchscreen*, mas sim o software e os dispositivos que verificam e catalogam os que estão aptos votar no dia da eleição ou na votação antecipada. Empresas como a VR são ?muito importantes? porque ?um sistema de registo funcional é central para as eleições americanas?, explica Lawrence Norden, vice-diretor do Centro de Justiça Brennan, da Faculdade de Direito da Universidade de Nova York. De acordo com ele, empresas como a VR também são estratégicas porque as secções eleitorais contam com poucos especialistas em tecnologia da informação (às vezes, não têm nenhum). Isso significa que ?o fabricante também fornece boa parte da assistência em TI, incluindo a programação e

a segurança cibernética? ? ou seja, não é exatamente o tipo de gente que você quer ver prejudicada por um país hostil.

De acordo com o site da VR Systems, a empresa possui contratos em oito estados: Califórnia, Flórida, Illinois, Indiana, Nova York, Carolina do Norte, Virgínia e Virgínia Ocidental.

Pamela Smith, presidente da Verified Voting, ONG que monitora as eleições, concorda que, mesmo que a VR Systems não seja responsável por computar os votos, é um alvo sedutor para quem almeja interferir na votação.

?Tendo acesso a um banco de dados de eleitores de um Estado, eles podem mudar ou remover dados. Isso pode ser decisivo na hora de o eleitor votar. Ele pode ter que usar uma cédula ?provisória?, por exemplo. Nesse caso, o voto precisa ser verificado antes de ser contabilizado. Isso cria obstáculos ao eleitor, que precisa comprovar sua identidade para seu voto valer?.

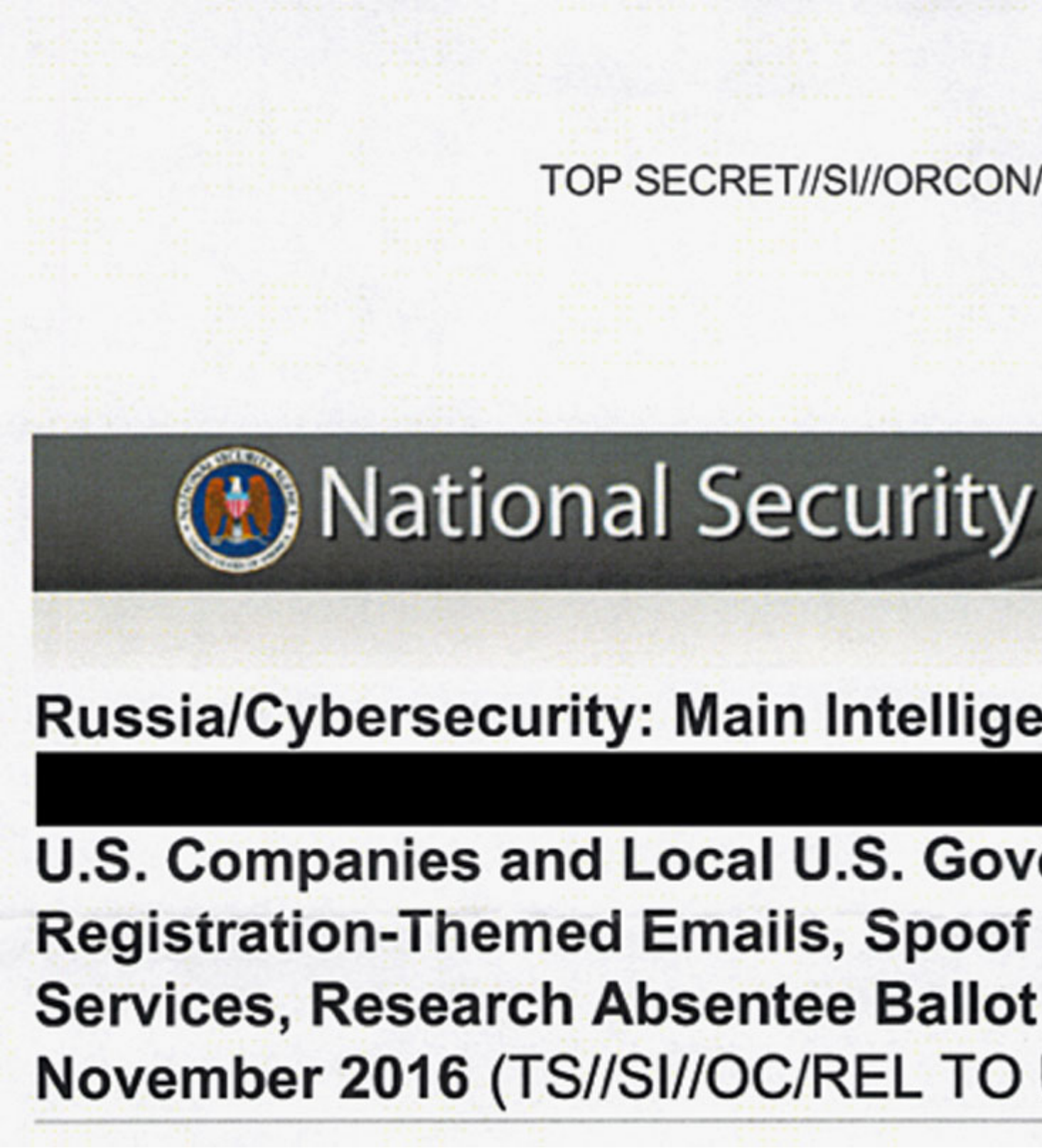
Mark Graff, consultor em segurança digital e ex-diretor de segurança cibernética do Lawrence Livermore National Lab, descreveu essa tática como um ?ataque de negação de serviço eleitoral?, similar ao que acontece quando um site é derrubado por milhares de pedidos de acesso falsos. Para Graff, mais preocupante ainda seria se os hackers passassem a visar uma empresa como a VR Systems com o objetivo de se aproximar da contagem dos votos. Invadir diretamente ou alterar as máquinas de votação seria muito óbvio e, por isso mesmo, mais arriscado do que atacar um setor adjacente e menos visível do sistema de votação, como os bancos de dados de registo eleitoral. A esperança dos hackers é de mirar em um e acertar no outro. No caso da VR Systems, a empresa propagandeia o facto de seus equipamentos estarem conetados à Internet, permitindo que ?o histórico de votação do eleitor seja transmitido imediatamente ao banco de dados eleitoral do condado?, de forma contínua. Ou seja, um ataque cibernético nos moldes acima descritos poderia se espalhar por equipamentos interligados da mesma maneira que germes se espalham através de um aperto de mão.

Para Alex Halderman, diretor do Center for Computer Security and Society, da Universidade de Michigan, especialista em eleições eletrónicas, uma das principais preocupações em relação ao cenário descrito no documento da NSA é a probabilidade de os funcionários responsáveis pelos registos de votação fazerem também a pré-programação das máquinas de votação. As urnas eletrónicas não estão conetadas a programas como o EViD da VR Systems, mas recebem configurações e atualizações manuais de servidores municipais ou estaduais, que podem ser responsáveis por ambas as etapas. Se o malware do GRU tiver essas pessoas como alvo, as consequências são preocupantes.

?Normalmente, uma empresa fica responsável pela programação pré-eleitoral das máquinas de votação de um condado?, conta Halderman a The Intercept. ?Eu ficaria bem preocupado se um invasor capaz de comprometer o bom funcionamento do fornecedor do registo de votação conseguisse usar atualizações de software distribuídas por esse mesmo fornecedor para infetar também o sistema de gerenciamento de eleições das próprias máquinas eleitorais?, acrescenta. ?Se ele conseguir fazer isso, pode fazer com que a urna crie contagens fraudulentas?.

De acordo com Schneier, para um hacker, a vantagem de invadir o sistema da VR é reunir informações para preparar e executar ataques contra os funcionários que trabalham nas eleições. De facto, com o logotipo do fornecedor principal da secção eleitoral, um e-mail falso

parece muito mais autêntico.



Tradução: Agência Nacional de Segurança ? Rússia/Cibersegurança: Agentes da Diretoria-Geral de Segurança do Estado-Maior [redigido] atacaram empresas e servidores municipais norte-americanos através: de e-mails fraudulentos que levavam o destinatário a inserir seus dados de login; de anúncio de produtos e serviços inexistentes ligados à eleição; de ferramentas de busca de e-mails de cadastrados para voto em trânsito. Agosto a novembro de 2016. Imagem: NSA

Uma brecha como essa poderia levar até mesmo a suspender a votação. Um funcionário da segurança norte-americana admitiu que a operação russa que visou o software de registo de eleitores poderia ter interrompido a votação nas zonas eleitorais onde os produtos da VR Systems estavam sendo usados. Halderman explica que um registo de votação comprometido não causa só caos no dia da eleição. ?Você poderia interferir em áreas que votam predominantemente em determinado candidato e, assim, criar um efeito partidário?.

Esse método para prejudicar a eleição presidencial tem seus desafios. Como se trata de um sistema descentralizado, os processos mudam não só de estado para estado, mas de condado para condado. Além disso, como a eleição é por Colégio Eleitoral, fica difícil prever onde o hacker deve concentrar seus esforços.

?Hackear uma eleição é difícil, mas não por causa da tecnologia ? essa é a parte mais fácil. Difícil é saber o que vai dar resultado?, explica Schneier. ?Se considerarmos as últimas eleições: 2000 foi decidido na Flórida; 2004, em Ohio; as eleições mais recentes, em alguns condados de Michigan e Pensilvânia, então é difícil saber exatamente onde hackear?.

Ao mesmo tempo, a descentralização do sistema também é uma vulnerabilidade. Não há uma fiscalização rígida do governo federal sobre o processo eleitoral ou sobre a compra de hardware ou software de votação. Do mesmo modo, o registo de eleitores, o recenseamento eleitoral e a contagem de votos não têm uma supervisão nacional efetiva. Não existe uma autoridade única responsável por garantir e proteger as eleições. Christian Hilland, porta-voz da Comissão Eleitoral Federal (FEC, na sigla em inglês) disse a The Intercept que ?a FEC não tem jurisdição sobre questões de votação ou de software e hardware de contagem de votos. Você pode falar sobre esses assuntos com a Comissão de Assistência Eleitoral (EAC)?.

Mas apurar informações com a EAC inspira menos confiança ainda. A comissão foi criada pelo Congresso em 2002, na esteira do polémico processo eleitoral de 2000. Em seu site, a EAC afirma que ?serve de centro nacional [5] de informações sobre processos eleitorais. A EAC também certifica laboratórios de testes e sistemas de votação [6]?, mas é uma comissão remota, sem autoridade efetiva. O link para a certificação dos sistemas de votação dá numa página inexistente.

Se houvesse uma autoridade eleitoral federal nos EUA, poderia ter sido aberta uma investigação sobre o que aconteceu em Durham, na Carolina do Norte, no dia da eleição. O sistema de registo não funcionou direito em vários locais de votação, causando confusão e longas filas. Cédulas de papel tiveram de ser usadas e a votação foi até tarde da noite.

O recenseamento eleitoral de Durham foi gerenciado pela VR Systems, justamente a empresa que foi alvo do *hacking* russo, de acordo com o relatório da NSA.

As autoridades locais negaram que a interrupção tenha sido causada por um ataque hacker. ?O Conselho eleitoral da Carolina do Norte não percebeu nenhuma atividade suspeita ou fora do normal durante as eleições de 2016. Todos os potenciais riscos ou vulnerabilidades estão sendo monitorados. A agência trabalha em conjunto com o Departamento de Segurança Interna dos EUA e com o Departamento de Tecnologia da Informação da Carolina do Norte para ajudar a mitigar quaisquer potenciais riscos?, disse Patrick Gannon, porta-voz do conselho eleitoral do estado.

George McCue, vice-diretor do conselho eleitoral do condado de Durham, disse que o software da VR Systems não era o problema. ?A investigação não encontrou nenhum indício de problema com o software?, disse ele. ?Parece que ocorreram erros em diferentes pontos do processo, seja na configuração dos computadores ou com os funcionários eleitorais que os utilizam?.

Toda essa história só faz aumentar as expectativas em relação às investigações sobre uma suposta colaboração entre a campanha de Trump e as operações russas. Essa semana, James Comey, diretor do FBI demitido por Trump, deverá depor ao Congresso[1]. Se o conluio ficar comprovado ? uma possibilidade remota, ao menos por enquanto ?, significa que a ajuda da Rússia foi muito além de hackear e-mails dos Democratas para servir à propaganda do candidato republicano. Significa que a própria infraestrutura eleitoral dos EUA foi atacada.

Seja qual for a conclusão final sobre a campanha de Trump, não será nada comparado à ameaça à legitimidade das eleições que a desconfiança na infraestrutura do processo eleitoral representa. A conclusão da NSA indica ?que países estão buscando táticas cada vez mais específicas de manipulação eleitoral, e precisamos estar vigilantes em defesa da legitimidade das eleições?, diz Schneier. ?As eleições fazem duas coisas: a primeira delas é escolher um vencedor; a segunda é convencer o perdedor da lisura do processo. Havendo suspeita de ataque hacker às eleições, estamos pondo em risco a legitimidade da votação, mesmo que o ataque não tenha realmente acontecido?.

Ao longo da história, a transferência de poder sempre foi o momento de maior fraqueza para as sociedades, tendo levado a enormes derramamentos de sangue. A transferência pacífica de poder é uma das maiores inovações da democracia.

?[Uma eleição] não precisa somente ser justa. Tem que ser comprovadamente justa, de modo que o perdedor possa dizer: ?Sim, perdi sem sombra de dúvidas??. Se não conseguirmos garantir isso, estamos ferrados?, diz Schneier. ?Uma sociedade pode se despedaçar se estiver convencida de que uma eleição não foi justa?.

Artigo de Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim, publicado em theintercept.com [7]. Tradução: Charles Nisz e Carla Camargo Fanha.

---

1 O testemunho de James Comey no Congresso dos EUA sustentou tese de ?obstrução de justiça? por Trump [8]. *Nota de esquerda.net.*

Sobre o/a autor(a):

Source URL: http://www.esquerda.net/en/artigo/relatorio-secreto-da-nsa-mostra-hacking-russo-dias-antes-da-eleicao-americana/49174

Links:
[1] https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1
[2] http://www.politico.com/story/2017/06/01/putin-russian-state-has-never-been-involved-in-hacking-239014
[3] mailto:noreplyautomaticservices@gmail.com
[4] http://berkman.harvard.edu/
[5] https://www.eac.gov/search/
[6] https://www.eac.gov/testing_and_certification/default.aspx
[7] https://theintercept.com/2017/06/06/exclusivo-relatorio-secreto-da-nsa-mostra-hacking-russo-dias-antes-da-eleicao-americana/
[8] http://www.esquerda.net/artigo/testemunho-de-ex-diretor-do-fbi-sustenta-tese-de-obstrucao-de-justica-por-trump/49167