Uma greve cheia

Sobre Crowdstrike e eu vou deixar análises de TI

#CrowdStrike #DNC #Clinton #FBI

As águias são caçadoras incrivelmente graciosas. Suas habilidades para identificar até mesmo o menor animal lá do alto nos céus são lendárias. Qualquer pessoa que já teve a chance de observar um interruptor de águia em modo de ataque, acendendo seu mergulho veloz mas determinado ao solo, dificilmente esquecerá essa visão. Coincidência, essa águia faz parte do logotipo da Crowdstrike, uma empresa que fornece software e serviços de TI em segurança de rede. A empresa foi fundada em 2011 por George Kurtz, um ex-CTO do provedor de segurança de computadores pessoais McAfee, e Dimitri Alperovich, um especialista em segurança de TI nascido na Rússia e ex-VP da McAfee. Em 2012, um ex-funcionário do FBI chamado Shawn Henry se juntou à empresa, outros 12 meses depois, a empresa lançou seu primeiro produto chamado Crowdstrike Falcon.

Semelhante aos falcões reais, o software foi criado para vigiar constantemente as redes de computadores e seu imenso tráfego de dados em busca de invasores que pretendiam roubar informações confidenciais, endereços IP e muito mais nessa rede. Depois que a empresa conseguiu identificar uma série de ataques a várias redes corporativas e industriais, supostamente da China, Coreia do Norte e Rússia em 2014 e 2015, Crowdstrike recebeu financiamento em grande escala do Google, totalizando mais de US $ 480 milhões em 2019. A empresa também recebeu uma avaliação de mais de US $ 3 bilhões em 2018 com receitas de vendas anuais de apenas US $ 100 milhões e foi listada na NASDAQ em 2019.

Os três principais acionistas atuais da Crowdstrike listam dois grandes investimentos do Vale do Silício empresas e - estranhamente - Allianz Asset Management GmbH, sediada em Munique, Alemanha. A empresa tem atualmente uma capitalização de mercado de mais de US $ 15 bilhões com pouco mais de 2.000 funcionários, não tem dívidas e tinha mais de US $800 milhões em caixa em outubro de 2019 - nada mal por ser "apenas" uma empresa de software.

Em meio a todo esse sucesso estrondoso indiscutível, apareceu um incidente bastante estranho em 2016, quando Crowdstrike emitiu um relatório chique e colorido sobre como um grupo russochamado "Fancy Bear" supostamente hackeou um aplicativo militar ucraniano chamado "ArtOS", um software que pode ser instalado em Tablet PC e que é usado para controle de fogo "para fazer ajustes nas condições de disparo de sistemas balísticos e meteorológicos", de modo que o desenvolvedor do aplicativo, Yaroslav Sherstuk. Crowdstrike fez uma série de avaliações políticas de alto nível e afirmou que os militares ucranianos sofreram "pesadas perdas" na artilharia, principalmente por causa do ataque russo.

> Durante esse prazo de desenvolvimento proposto, uma série de eventos significativos ocorreram entre a Ucrânia, a Rússia e a comunidade internacional. Mais notavelmente, as tentativas russas de influenciar as relações ucraniano-UE resultaram no movimento de protesto em larga escala Maidan, resultando na derrubada do então presidente Victor Yanukovich, na invasão e anexação da Península da Crimeia pela Rússia e no conflito armado prolongado no leste da Ucrânia. Portanto, a criação de um aplicativo [App] que vise algumas das forças da linha de frente essenciais na defesa ucraniana na frente oriental provavelmente seria uma alta prioridade para os desenvolvedores de malware adversários russos que buscam virar o conflito a seu favor. . Para as tropas ucranianas, as forças de artilharia também suportaram um alto custo ... (Relatório Crowdstrike 'Uso de malware Fancy Bear e Android no

> rastreamento de unidades de artilharia de campanha ucranianas')

Estranhamente, as principais conclusões de Crowdstrike foram rapidamente descartadas. Por exemplo, pelo Instituto Internacional de Estudos Estratégicos (IISS), que emitiu a seguinte declaração :

> O relatório Crowdstrike usa nossos dados, mas as inferências e análises extraídas desses dados pertencem exclusivamente aos autores do relatório. A inferência que eles fazem de que as reduções nas reservas de artilharia D-30 ucraniana entre 2013 e 2016 foram principalmente o resultado de perdas em combate não é uma conclusão que jamais sugerimos, nem que acreditamos ser precisa. (Declaração do IISS de 2017)

Outro pesquisador do IISS afirmou que a redução de unidades militares foi atribuída principalmente a uma realocação de suas unidades para outros comandos militares. Os militares ucranianos relataram que as perdas de artilharia na luta inicial com os separatistas foram "várias vezes menores do que o número relatado por Crowdstrike e não estão associadas à causa específica" do hackeamento. O desenvolvedor do aplicativo emitiu uma declaração sobre as descobertas de Crowdstrike na Ucrânia no Facebook , chamando-as de "delirantes". Ele admitiu que seus e-mails foram comprometidos, no entanto.

Curiosamente também que um alto funcionário dos EUA explicou em uma conferência na Dinamarca em 2018 sobre como os EUA continuaram a apoiar explicitamente os esforços de segurança cibernética da Ucrânia com um total de US $ 10 milhões - somos quase tentados a considerar para limpar a bagunça do Crowdstrike:

> Durante essa viagem - acho que foi em setembro do ano passado [2017] - anunciamos que estávamos aumentando nosso financiamento de assistência à Ucrânia em US $ 5 milhões, com foco específico na segurança cibernética. E então, quando o secretário assistente Mitchell viajou para a Ucrânia nesta primavera [2018], ele anunciou um adicional de US $ 5 milhões em assistência de segurança cibernética dos EUA para a Ucrânia. (Jorgan K. Andrews, Subsecretário Adjunto, Escritório de Assuntos Internacionais de Entorpecentes e Polícia, junho de 2018 em Kopenhagen, Dinamarca)

Apenas alguns meses antes do desastre do Crowdstrike na Ucrânia, a empresa recebeu permissão do Comitê Nacional Democrata (DNC) em 2016 para investigar seus servidores de computador supostamente hackeados pela Rússia. A campanha de Hillary Clinton alegou que não apenas milhares de seus e-mails foram roubados - publicados pelo Wikileaks alguns meses antes das eleições presidenciais de 2016 nos EUA - mas também toda a sua presidência.

Existem declarações e eventos ainda mais contraditórios em torno das investigações subsequentes do Servidor DNC de Crowdstrike - não se limitando a algumas alegações confusas de Crowdstrike sobre datas de atribuição, pessoal e métodos - do que na distorcida história de hacking militar na Ucrânia. O DNC descobriu oficialmente em 28 de abril de 2016 que seus servidores foram 'hackeados'. Apesar do primeiro pagamento da DNC ao Crowdstrike em 5 de maio de 2016, ambos falharam em evitar que os e-mails de Clinton fossem obtidos primeiro pelo hacker "Guccifer 2" e até mesmo publicados no Wikileaks quase dois meses depois, com 75% dessas mensagens de e-mail indicando uma data de criação posterior do que na primeira semana de maio de 2016.

Alperovitch, CEO da Crowdstrike, afirmaque os grupos vinculados à Rússia usaram um comando de software chamado 'Powershell.exe' ou 'X-Agent' com parâmetros enigmáticos que se transformavam em código de programa quando executados, capazes de controlar o software de gerenciamento do Windows. A evidência de que tais comandos foram realmente implantados por hackers russos é difícil, senão quase impossível, de provar e poderia muito bem ter sido inserida por alguns dos muitos membros do governo ocidental que vimos no passado, para 'destruir Trump'.

> Alperovitch tem experiência significativa de trabalho como especialista no assunto com todos os níveis de aplicação da lei dos EUA e internacional em análise, investigações e perfis de atividades do crime organizado transnacional e ameaças cibernéticas de terroristas e adversários de estados nacionais. Ele é frequentemente citado como uma fonte especializada em publicações nacionais, incluindo a Associated Press, NBC, New York Times, USA Today e o Washington Post. (Dmitri Alperovitch, membro sênior do Conselho do Atlântico)

Uma análise forense independente do arquivo Zip contendo um aparente subconjunto de todos os e-mails de Clinton obtidos pelo hacker 'Guccifer 2' chegou à conclusão de que os arquivos individuais obtidos por ele - não o Wikileaks - foram salvos pela última vez em 2015, principalmente, exfiltrados em 16 de abril , 2016 usando uma conexão lenta - provavelmente por satélite - com a Internet, depois salvo em um pen drive, copiado deste pen drive para um computador com fuso horário do leste dos EUA e, finalmente, compactado neste computador em um único arquivo Zip em 20 de junho de 2016, se as informações de data de todos os arquivos individuais não foram alteradas pelo 'hack'. Além disso, o próprio presidente e CSO da CrowdStrike, Shawn Henry, declarou na frente do Comitê de Inteligência em 5 de dezembro de 2017 (na página 32) que "não tínhamos evidências concretas de que os dados foram exfiltrados do DNC, mas temos indicadores de que eles foram exfiltrados".

> **Sr. Henry**: "O advogado acabou de me lembrar que, no que se refere ao DNC, temos indicadores de que os dados foram exfiltrados. Não tínhamos evidências concretas de que os dados foram exfiltrados do DNC, mas temos indicadores de que foram exfiltrados." (p. 32)
> ...
> **Sr. Henry**: "Sim, senhor. Então, novamente, encenado para, o que, quero dizer, não há - a analogia que usei com o Sr. Stewart anteriormente foi que não temos vídeo de está acontecendo, mas há indicadores de que isso aconteceu. Há momentos em que podemos ver os dados exfiltrados, e podemos dizer de forma conclusiva. Mas, neste caso, parece que foi configurado para ser exfiltrado, mas simplesmente não temos o evidências que dizem que ele realmente saiu." (p. 32)
> ...
> **Sr. Henry**: "Então, alguns dos dados que vimos foram encenados, mas não tínhamos indicação de que foram exfilados, mas foram encenados - pareciam ser encenados para exfil, que estavam associados a pesquisas que haviam sido conduzidas pelo DNC sobre os candidatos da oposição." (p. 49)
> ...

> **Sr. Stewart, de Utah**: "Ok. Você disse algo, e eu quero reafirmar - e me diga se estou errado - se eu pudesse. Você disse, eu acredito, falando sobre o Computador DNC, você tinha indicações de que os dados estavam preparados para serem exfiltrados, mas nenhuma evidência de que realmente foram deixados. Eu anotei isso corretamente ?"
> **Sr. Henry**: "Sim"
> **Sr. Stewart de Utah**: "E, neste caso, os dados que estou supondo que você 'está falando é do e-mail, bem como de tudo o mais que eles possam estar tentando receber."
> **Sr. Henry**: "Havia arquivos relacionados a pesquisas de oposição que foram conduzidas."
> **Sr. Stewart, de Utah**: "Tudo bem. E quanto aos e-mails que todos conhecem? Também houve indicadores de que foram preparados, mas não evidências de que realmente foram exfiltrados ?"
> **Sr. Henry**: "Não há evidências de que eles foram realmente exfiltrados. Há evidências circunstanciais -"
> **Sr. Stewart de Utah**: "Ok"
> **Sr. Henry**: "- mas nenhuma evidência de que eles foram realmente exfiltrados. Mas deixe-me também afirmar que se alguém estiver monitorando um servidor de e-mail, poderá ler todos os e-mails." (p.74/75)
>
> Transcrições de entrevistas de Shawn Henry no House Committee on Intelligence em 5 de dezembro de 2017

Além disso, Hillary Clinton usou um servidor de e-mail privado em seu escritório particular em Chappaqua, Nova York para assuntos oficiais do Departamento de Estado e até convidou o Google em 2012 - cobrindo o cronograma de ataques da embaixada dos Estados Unidos em Benghazi - para gerenciar sua conta de e-mail oficial pessoalmente, muito provavelmente para contornar a obrigação de ter suas conversas oficiais com o governo respaldadas e disponíveis ao público. Seu servidor privado em Chappaqua estava executando um software de gerenciamento de e-mail do Windows.

Além de tudo isso, não é preciso ter olhos de águia para ver as palavras claramente questionáveis do ex-diretor do FBI James Comey quando questionado em janeiro de 2017 no Senado dos EUA sobre os servidores DNC e o Crowdstrike:

> **Comey**: "Preferimos obter acesso ao dispositivo ou servidor original envolvido, é a melhor evidência."
> **Senador**: "Você teve acesso para fazer perícias nesses servidores ?"
> **Comey**: "Não éramos, uma empresa privada altamente respeitada [Crowdstrike] eventualmente teve

> acesso e compartilhou conosco o que viu lá."
> **Senador**: "Normalmente é assim que o FBI prefere fazer a perícia ou você prefere sentir e ver o servidor você mesmo ?"
> **Comey**: "Sempre preferimos ter acesso a nós mesmos, se isso for possível."
> **Senador**: "Você sabe por que foi negado o acesso aos servidores ?"
> **Comey**: "Não sei ao certo.Não sei ao certo."
> **Senador**: "Houve um pedido ou vários pedidos ?"
> **Comey**: "Múltiplos pedidos em diferentes níveis e, em última análise, o que foi combinado é que a empresa privada compartilharia conosco o que viu."
>
> (Ex-diretor do FBI James Comey em uma audiência no Senado dos EUA em 10 de janeiro de 2017)

Parece que o DNC estava no comando do FBI em 2016, não o Departamento de Justiça ou o Congresso dos EUA e / ou o Senado dos EUA. Toda a saga DNC poderia ser arquivada sob a pasta 'Corrupção massiva', se não houvesse o famoso telefonema do presidente dos EUA Donald Trump com o recém-eleito presidente ucraniano Zelensky em 25 de julho de 2019, no qual o presidente dos EUA mencionou Crowdstrike em particular:

> Gostaria que nos fizesse um favor, porque nosso país passou por muitas coisas e a Ucrânia sabe muito sobre isso. Eu gostaria que você descobrisse o que aconteceu com toda essa situação com a Ucrânia, **dizem Crowdstrike**... Acho que você tem um de seus ricos ... **O servidor, dizem que a Ucrânia tem**. Aconteceu muita coisa, toda a situação ... Gostaria que o Procurador-Geral telefonasse para você ou seu pessoal e gostaria que você descobrisse o que está acontecendo. Como você viu ontem, toda aquela bobagem terminou com uma atuação muito ruim de um homem chamado Robert Mueller, uma atuação incompetente, mas dizem que muito disso começou com a Ucrânia. (Präsident Donald Trump dos EUA em uma conversa por telefone em 25 de julho de 2019 com o Presidente da Ucrânia, Zelensky)

Logo depois, o inferno estourou entre a maioria dos políticos democratas dos EUA no Congresso dos EUA e que pretendiam seriamente acusar o presidente dos EUA por causa dessas palavras picantes - e em relação a algumas relacionadas à corrupção de Joe Biden na Ucrânia - em seu telefonema normal e apropriado com Zelensky. O teatro do impeachment não durou muito, foi finalmente rejeitado no Senado dos EUA no início de 2020 e rendeu um esforço suprapartidário quando todos os republicanos no Congresso dos EUA também o rejeitaram.

Pode não haver outra explicação além de que a Ucrânia de fato tem uma cópia digitalmente espelhada desse servidor DNC em algum lugar. Com materiais possivelmente contagiosos.

As águias podem ver isso claramente de cima e de longe.

https://www.sun24.news/pt/uma-greve-cheia-sobre-crowdstrike-e-eu-vou-deixar-analises-de-ti.html