Trabalho de Engenharia de Software

Curso de Tecnologia em
Análise e Desenvolvimento de Sistemas

Instituto Federal de Educação,
Ciência e Tecnologia de São Paulo
(IFSP)
Câmpus Campinas

O vírus "Stuxnet"

Antonio Leonel CP300371X

Entre 2009 e 2011, foram noticiadas informações sobre o “Stuxnet”, que foi considerado a “praga” digital mais sofisticada já criada, que foi o mesmo período que o governo do IRÃ começou a enriquecer urânio.

O propósito deste vírus, era de impedir ou atrasar o processo de enriquecimento dos IRANIANOS e ele foi desenvolvido pelo EUA com ajuda de ISRAEL.
Este vírus usa PCs e a Internet para chegar e atacar PLC ou CLP (Controladores Lógicos Programáveis) da marca Siemens, eles (PLC) são um dos equipamentos Industriais mais usados em Fábricas, Usinas e etc. Ele provocou falhas mecânicas em uma parcela das centrífugas de enriquecimento, atrasando assim o processo em anos.
As mencionadas usinas não estava “ligadas” a internet, então a estratégia foi de “infectar” a maior parte possível do computadores Iranianos (somente os Iranianos), esperando que algum funcionário fosse infectado e que ele usando um pendrive, acaba-se levando o vírus para a usina. E foi o que aconteceu.

Nações estavam preocupadas com a segurança, pois nem todos os países investem e segurança. Como a RÚSSIA estava preocupada pois se uma usina nuclear elétrica, fosse afetada, poderia provocar uma outra “CHERNOBYL”.
Houve uma “ocorrência” nos EUA, em que uma usina de energia ficou parada 15 dias, e ninguém soube o motivo ….VIRUS?

Para prevenir este problema de ataque de um vírus, deve-se manter todos os equipamentos atualizados, serem feitos testes de segurança de rede, deixar equipamento “vitais” desconectados da internet (quando possível) quando não, instalar sistema de segurança eficientes como por exemplo um FIREWALL, controlar muito bem o uso de pen drives e instalar sistemas de verificação independentes para monitorar funcionamentos.

http://g1.globo.com/tecnologia/noticia/2011/01/virus-stuxnet-foi-criado-pelos-eua-e-por-israel-diz-jornal.html

https://super.abril.com.br/tecnologia/virus-entra-em-programa-nuclear-e-salva-o-mundo/

http://g1.globo.com/tecnologia/noticia/2011/01/virus-stuxnet-foi-criado-pelos-eua-e-por-israel-diz-jornal.html

Vírus que atrasou programa nuclear do Irã foi criado pelos EUA e por Israel

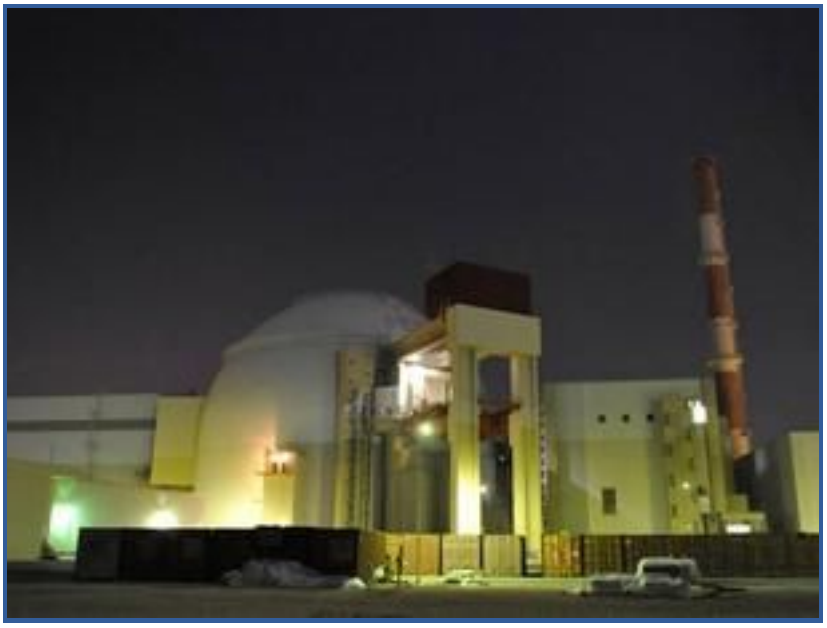
Segundo jornal 'New York Times', 'missão' do vírus foi bem-sucedida.

'Stuxnet' é considerada a praga digital mais sofisticada já criada.

Altieres Rohr

Especial para o G1

FACEBOOK



Usina nucleares do Irã teria sido

alvo do vírus"Stuxnet". (Foto: AP)

O vírus "Stuxnet", considerado por especialistas a praga digital mais sofisticada já criada, teria sido resultado de uma operação conjunta dos Estados Unidos com Israel, segundo reportagem do jornal “New York Times”. O periódico afirma que a missão do vírus era causar danos às centrífugas da usina nuclear iraniana de Natanz, e que esse objetivo foi alcançado, atrasando o programa nuclear iraniano em pelo menos cinco anos.

O "Stuxnet" atacava controladores lógicos industriais da Siemens, alterando suas configurações para sabotar as centrífugas das usinas. De acordo com o jornal, a companhia teria auxiliado a criação do vírus, embora sem ter intenção, quando

compartilhou dados de vulnerabilidades em seus produtos com um programa do governo dos Estados Unidos que buscava aumentar a segurança de sistemas industriais.

Israel teria testado o código do vírus em instalações de Dimona, usando centrífugas e controladores idênticos aos iranianos.

O jornal observa que nenhum especialista norte-americano ou israelense consultado confirmou a origem do vírus, mas que, ao mesmo tempo, “nenhum deles conseguiu esconder um sorriso de orgulho” ao comentar sobre as dificuldades impostas no avanço do programa nuclear iraniano.

Russos temem 'Chernobyl iraniano'

O jornal “The Daily Telegraph” diz ter obtido um relatório escrito por cientistas russo preocupados com os estragos causados pelo vírus "Stuxnet". Segundo eles, não há dados suficientes para determinar se as usinas nucleares estão em condições seguras de operação.

A usina de Bushehr começou a ser preparada em outubro e deveria fornecer energia elétrica para os iranianos a partir da metade deste ano. Relatos afirmam que a usina também teria sido atacada pelo "Stuxnet", gerando as preocupações dos russos que estão auxiliando o programa nuclear do Irã.

No documento, os cientistas se dizem preocupados com a possibilidade de um “Chernobyl iraniano”, em referência ao acidente ocorrido na usina nuclear de Chernobyl, na Ucrânia, que na época estava sob responsabilidade russa como parte da União Soviética. O acidente, ocorrido em 1986, causou 56 mortes diretas e até 4 mil mortes indiretas, segundo estimativas, além de ter deixado a região inabitável.

Os cientistas pedem ajuda ao Kremlin e afirmam que o governo do Irã não pretende permitir que novos testes de segurança sejam realizados, porque o programa nuclear já está com uma década de atraso.

https://super.abril.com.br/tecnologia/virus-entra-em-programa-nuclear-e-salva-o-mundo/

Vírus entra em programa nuclear e salva o mundo

Conheça a misteriosa história do Stuxnet: o programa que salvou o planeta. Ou que acabou de dar início à 3ª Guerra Mundial

Por Da Redação

access_time31 out 2016, 18h46 - Publicado em 21 fev 2011,

Marcos Ricardo dos Santos e Alexandre Versignassi

Os engenheiros se preparam para encerrar o expediente e ir para casa. A semana de trabalho tinha sido intensa, mas eles estavam satisfeitos. Tinham cumprido uma antiga promessa feita ao presidente Mahmoud Ahmadinejad: colocar em operação total mais de 8 mil centrífugas de enriquecimento de urânio em Natanz, na região central do Irã. Era o início de 2010 e agora o país estava prestes a produzir suas primeiras bombas atômicas. Foi aí que os engenheiros viram algo estranho: centenas de centrífugas tinham parado de funcionar. De uma vez. O que podia ter acontecido? Qualquer problema que desse em uma única das centrífugas, um alarme soaria a tempo de os engenheiros salvarem a máquina. Mas não. Não teve alarme.

Sabotagem, então? Quase impossível. O governo conhecia o passado de todos os funcionários com acesso à usina. E, mesmo se houvesse um alto

traidor ali, ele não conseguiria fazer nada sozinho. E agora? Agora a única certeza era que a bomba iraniana iria atrasar. Talvez alguns anos.

PUBLICIDADE

Alguns meses depois, na Bielo-Rússia, outros engenheiros veem algo paralisante. São os técnicos da VirusBlokAda, uma empresa de programas antivírus. Eles estavam examinando o computador de um cliente iraniano em busca de ameaças à segurança da máquina. Encontraram um vírus ali.

Como qualquer outro vírus, esse se espalhava via internet. E como qualquer outro vírus ele tinha um nome de batismo escrito em seu códgo-fonte. No caso, Stuxnet. Mas não era qualquer vírus. Eles estavam frente a frente com o maior demônio digital da história. O vírus mais complexo, inteligente e destrutivo que alguém havia criado.

Seu computador talvez esteja contaminado por ele agora mesmo. Mas ok. Não tem problema. O bichinho é inofensivo para Windows, Mac OS ou qualquer sistema operacional que você conheça. Esse vírus não foi feito para danificar computadores, mas para destruir centrífugas de urânio. Mais precisamente, as centrífugas do Irã. O Stuxnet é uma arma de guerra.

Ele só atua em um sistema operacional chamado Scada, desenvolvido pela empresa alemã Siemens. Esse sistema controla centrífugas de urânio.

Mais: ele não invade qualquer sistema Scada. Cada tipo de usina de enriquecimento de urânio usa esse sistema numa configuração particular. E o vírus foi programado para atacar só a configuração que as usinas do Irã usam. Para completar, ele tem uma especialidade: caça computadores localizados no Irã. Apesar de ter se espalhado pelo planeta em 2010, atingindo pelo menos 100 mil computadores, a distribuição geográfica dele não foi uniforme: 60% das infecções aconteceram em território iraniano. Entrar em micros do Irã (ou de qualquer outro lugar) é fácil. Mas penetrar as instalações nucleares são outros quinhentos. Elas não têm conexão com a internet, justamente para evitar ataques desse tipo. A estratégia do vírus, porém, era clara: contaminar em massa os computadores pessoais do país contando com que algum funcionário tivesse seu pen drive infectado em casa e acabasse levando o vírus para as instalações nucleares. Pelo jeito, foi o que aconteceu. Genial.

O que o vírus fez

O Stuxnet mostrou que um vírus de computador pode destruir máquinas fisicamente, causando mais danos do que se um grupo de vândalos entrasse nas instalações e quebrasse tudo no porrete. O primeiro passo para entender como ele consiguiu isso é visualizar como funciona o enriquecimento de urânio. Para construir uma bomba atômica, você precisa desse elemento – é a explosão dele que gera as energias atômicas

de uma bomba nuclear. Mas o urânio que as mineradoras extraem é inútil, pelo menos logo que sai da Terra. É que existem dois tipos: o Urânio 238 e o 235. A espécie mais energética, que serve para usinas nucleares e bombas, é o 235. O 238 é praticamente lixo. Só que eles existem grudados na natureza. Uma pedra de urânio é sempre formada por essas duas variedades. E a quantidade de urânio ruim é sempre bem maior: em cada tonelada de urânio, existem só 7 quilos do 235.

Então alguém precisa separar o joio do trigo. Aí é que entram as centrífugas. São cilindros que giram a mais de 1 000 rotações por segundo. O movimento lança os átomos de U238 (mais pesados) contra a parede do equipamento. E lá no meio o que sobra é um urânio cada vez mais rico em U235.

Se você quiser uma bomba atômica, vai precisar de U235 praticamente puro. Para conseguir isso, milhares de centrífugas processam urânio bruto o tempo todo.

É aí que o Stuxnet age. As centrífugas de Natanz rodam a 1 064 giros por segundo. Quando o vírus invade o sistema, ele manda a rotação aumentar em 40%. Mas só por 15 minutos, para não levantar suspeitas. Enquanto faz isso, ele ainda manda o sistema de segurança das instalações dizer que está tudo bem. E os engenheiros não veem nada de errado. Aí passam mais algumas semanas e tome 40% a mais outra vez. O alumínio dos

rotores não aguenta o esforço e racha. E tchau centrífugas. Foi o que aconteceu no Irã.

O vírus não chegou a destruir todas: foram cerca de 1 000 das 8 692 centrífugas. Provavelmente ele só conseguiu invadir parte do sistema.

Mesmo assim foi algo inédito. Acreditava-se que só uma ação militar que bombardeasse o Irã pra frear o enriquecimento de urânio no país poderia causar um estrago tão grande.

Operação abafa

Tão grande o estrago, aliás, que o próprio Irã não quis assumir a existência do ataque num primeiro momento. Nenhum engenheiro veio a público dizer o que aconteceu exatamente na usina (o parágrafo que abre este texto é baseado numa suposição sobre como os funcionários teriam reagido à quebra das centrífugas). Só sabemos o modus operandi do Stuxnet graças aos técnicos que analisaram cópias do vírus encontradas em computadores comuns – estava tudo escrito no código do programa.

O governo iraniano só se manisfestou em junho de 2010, quando o vírus foi descoberto na Bielo-Rússia. Na ocasião, Ahmadinejad disse que o Stuxnet só tinha atingido computadores pessoais dentro das usinas. Apenas em novembro o presidente do Irã finalmente admitiu: sim, o vírus tinha danificado “uma quantidade limitada de centrífugas”.

Mas o Instituto para a Ciência e a Segurança Internacional (uma organização que monitora instalações nucleares mundo afora – usando inclusive funcionários delas como informantes), sabe que o Irã desativou por volta de 1 000 centrífugas entre novembro de 2009 e fevereiro de 2010, bem na época em que o vírus estava agindo. Aí foi só juntar A com B. Quando Ahmadinejad assumiu o problema, não restaram dúvidas. Um vírus tinha vencido uma batalha contra um país. Mas quem estava por trás do ataque?

Quando alguém pergunta quem criou este ou aquele vírus, a imagem que vem à mente é a do nerd no quarto invadindo sistemas de segurança em busca de notoriedade entre seus pares. Mas não foi daí que surgiu o Stuxnet. Ele é bem mais do que um vírus comum. Especialistas calculam que seria necessária uma equipe de 6 a 10 pessoas trabalhando por 6 meses para criar um vírus tão esperto. Sem falar no aparato de espionagem: o Stuxnet sabia como as centrífugas iranianas funcionavam. Conseguir informações assim não é para pessoas comuns. É coisa para governos.

Suspeito número 1: Israel. Suspeito número 2: EUA. Suspeito número zero: Israel e EUA, em conjunto. Fontes ligadas ao governo americano disseram ao New York Times, sob anonimato, que o serviço de inteligência dos EUA estudou como invadir os sistemas da Siemens usados nas instalações iranianas. Essas informações, segundo eles, foram passadas para Israel, que teria testado a eficácia do Stuxnet nas centrífugas em que faz seu próprio urânio enriquecido. Também há uma evidência mais pitoresca. Um dos arquivos do Stuxnet se chama Myrtus ("Esther", em hebraico). Seria uma referência ao Livro de Esther, do Antigo Testamento. Ele relata um complô persa para destruir os judeus – e os persas foram o povo que deu origem ao Irã. Seja como for, ninguém tinha assumido a autoria até o fechamento desta edição.

Note que essa não é uma história de mocinhos e bandidos. Dessa vez, o interesse contra a proliferação de armas atômicas contou contra o Irã. E não é exagero dizer que o vírus "salvou o mundo" ao atrapalhar Ahmadinejad. Quanto mais tempo se ganha antes de ele entrar para o clube atômico, maior a chance de uma saída diplomática para as rusgas entre o Irã e o Ocidente. Mas o feitiço também pode ir contra o feiticeiro.

Para o engenheiro americano John Weiss, um dos primeiros a estudar o Stuxnet, a ameaça de ciberataques vale para todos. Recentemente, ele reuniu evidências de 180 casos de grandes sistemas de infraestrutura danificados em diferentes partes do mundo. E considera que boa parte aconteceu de propósito. "Houve um caso em que uma usina de energia americana ficou duas semanas parada e ninguém sabia o que era. Ninguém avisou as autoridades, nem o FBI, porque acreditavam, como

sempre, que era só um problema técnico. Mas quem garante que não foi um ataque de vírus?", diz.

Para deixar o cenário ainda mais preocupante, os especialistas no assunto são unânimes: preparar um ciberataque massivo – capaz de parar um país inteiro – seria relativamente simples. E barato, pelo menos do ponto de vista dos orçamentos militares, sempre na casa dos bilhões de dólares.

Em um congresso de hackers em Las Vegas, em julho de 2010, o especialista em espionagem informática Charlie Miller calculou que seriam necessários não mais que US$ 100 milhões para realizar um ataque cibernético eficaz contra os EUA. "Trabalhei em condições reais, como se a Coreia do Norte tivesse me contratado para orquestrar a ofensiva", explicou Miller na época.

Cientes dos riscos, alguns países estão estudando formas de se proteger contra vírus e hackers. Em setembro do ano passado, o Departamento de Segurança Interna dos EUA realizou, junto com outros 11 países, o exercício de um plano de defesa. Batizada de Cyber Storm III, a operação examinou como uma nação reagiria se serviços essenciais, como o sistema financeiro, fossem tirados do ar do dia para a noite. "Existe uma probabilidade real de que, no futuro, o país seja alvo de um ataque destrutivo. Precisamos estar preparados", disse à época o general Keith Alexander, comandante de uma nova unidade militar americana voltada

especificamente para ameaças eletrônicas. Pois é. Uma 3a Guerra Mundial pode estar longe. Mas a 1a Guerra Digital não. Essa já começou.

1ª guerra digital

As maiores batalhas

Estônia fora do ar

Orgulhosa de ter quase todos seus serviços estatais online e de ter feito as primeiras eleições nacionais pela internet, a Estônia chegou a ter o apelido de “e-stônia”. Em 2007, o país sofreu um ciberataque que tirou do ar todos os sites do governo, além das páginas de jornais, TVs e bancos. O motivo? Uma polêmica sobre a remoção de uma estátua que causava discussões entre adeptos e opositores do antigo sistema comunista do país. Os russos foram acusados, mas até hoje não sabem a origem do ataque.

Vingando Assange

Em dezembro de 2010, a prisão de Julian Assange, criador do Wiki-Leaks, despertou um onda de ciberataques. Em nome da liberdade na internet, a Operação Vingar Assange conseguiu derrubar sites de instituições financeiras que deixaram de intermediar doações ao Wiki-Leaks – Visa,

Mastercard, PayPal e PostFinance. Também atacou o site do Ministério Público da Suécia, autor do pedido de prisão contra Assange por assédio sexual, e a página do senador americano Joe Lieberman, que acusou o WikiLeaks de espionagem contra os EUA. Em um dos banners deixados na internet por participantes do ataque, podia-se ler: “A primeira guerra de informação foi deflagrada. A campo de batalha é o WikiLeaks. Os combatentes são vocês”. Foram ataques simples, facilmente resolvidos pelas empresas, mas que demonstraram o poder de mobilização e a ameaça que uma horda de hackers amadores pode representar.

China x Google

Em janeiro de 2010, hackers chineses foram acusados de invadir sistemas de 20 empresas americanas, entre elas o Google. Segundo a empresa, os hackers estariam acessando, a pedido do governo chinês, as contas de e-mails de ativistas contrários ao regime. Em represália, o Google anunciou que encerraria suas operações na China. Mas não chegou a tanto: só passou a redirecionar sua página chinesa para seus servidores em Hong Kong. Nisso, conseguiu escapar das leis de censura de lá, que impedem a busca com expressões como “direitos humanos”, por exemplo. Seja como for, não fez muita diferença para os chineses. Lá o monopólio sempre foi de um buscador local: o Baidu.

Pequim sequestra a rede

Os casos de ações cibernéticas não se limitam apenas aos rebeldes atacando o sistema. O império também contra-ataca. Em abril de 2010, a Comissão de Revisão de Economia e Segurança China-EUA trouxe a público o fato de que a China teria “capturado” 15% de toda a internet por 18 minutos, desviando dados por meio da China Telecom. Sim, o país estaria interferindo não apenas na internet chinesa (toda controlada, como se sabe), mas na de todos os países. O governo americano admitiu o fato, mas, oficialmente, não chegou a considerá-lo como um caso de ciberataque. O episódio serviu como um alerta global para a facilidade de um país interferir na estrutura de comunicações de outro e, mais ainda, que ninguém está imune à ciberguerra.

Para saber mais

The Virus Creation Labs: A Journey into the Underground

George Smith, Create Space, 2009