



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



Cyberⁱ War – A Nova Guerra

Parte I – Os Agentes

Por Leonardo SANTOS Silva (022/2007)

1 Introdução

Já não é mais novidade. A novidade, agora, são os alvos. Nestes dias do mês de Junho, notícias de sites que são invadidos e se tornaram indisponíveis são cada vez mais frequentes. Mas quem são esses hackers, o que eles querem, como eles atacam e como se proteger deles? São perguntas encadeadas que, na maioria das vezes, não possuem respostas simples e lineares. Apesar desta dificuldade, a ameaça é presente e real e não há mais como ignorá-la.

Este é o primeiro texto de uma série de três. Aqui mostraremos a cultura do hacker: quais são as suas ações e seu comportamento. O segundo texto mostrará algumas técnicas usadas nos ataques e como são realizadas. No terceiro texto, será mostrado como o Brasil se prepara para enfrentar estas novas ameaças.

2 Hackers, crackers e outros vilões da era digital

O termo Hacker está universalmente difundido entre o público geral como o vilão das histórias de ciber ataques. Qualquer crime, invasão ou quebra de programa secreto, por exemplo, está associado a este nome. Porém, no universo técnico, costumamos segregar essas duas personalidades.

Hacker é uma palavra de origem inglesa. Significa “aquele profissional que, com o uso de suas ferramentas, tiram o excesso de pedra ou madeira para criar a escultura que todos irão admirar”. É um trabalho de refinamento, de profundo conhecimento em sua área de atuação. Fazendo uma analogia com a área de tecnologia, podemos dizer que os hackers são profundos conhecedores de como as diversas áreas da informática se comportam. Pessoas com conhecimentos avançados no funcionamento dos sistemas operacionais, da internet, ou do desenvolvimento de programas, geralmente são considerados hackers modernos, pois possuem um conhecimento em sua área de atuação, muito maior do que seus pares.

No outro lado da moeda, existem aqueles que obtêm esse conhecimento acima da média, acabam usando-o para obter vantagens de maneira ilícita. Invasão de sistemas, destruição de sites da internet, quebra ou maneiras de burlar os direitos autorais de programas são alguns



exemplos básicos de ciber crimes que são cometidos. Pessoas envolvidas nestes crimes foram designadas, pelos profissionais de segurança, por crackers, ou seja, aqueles que quebram.

E finalmente, temos aqueles que, apesar de mostrar interesse no assunto, não possuem conhecimento técnico tão elevado. Para sanar esta deficiência em pouco tempo, estas pessoas recorrem a programas prontos, que realizam ataques de maneira automatizada. A única dificuldade, neste caso, é procurar um programa específico na Internet, instalá-lo e direcionar seu ataque a um alvo específico. Estes, tecnicamente são chamamos de ScriptKids. Um exemplo disto acontece no filme "Matrix Reloaded" (2003), onde a personagem Trinity utiliza um aplicativo chamado NMap para invadir um sistema de segurança.

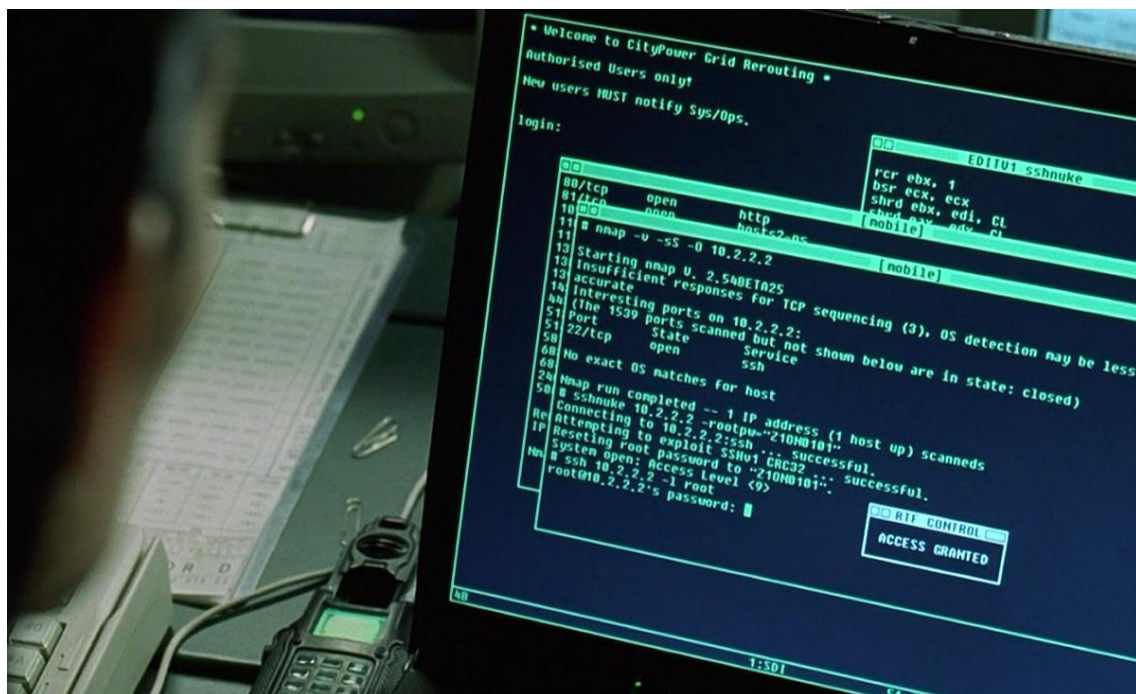


Imagem 1: Trinity usa o NMap para invadir o sistema de controle de uma empresa de energia

Para quem não sabe, este aplicativo existe. No filme, os comandos usados para executar a invasão são exatos e precisos. Trinity, em menos de 5 minutos, consegue invadir a rede de segurança da empresa de energia. Há várias ferramentas deste tipo e suas funções vão, desde identificar redes vulneráveis, até alterar as informações de um banco de dados corporativo.

No entanto, hacker é o termo mais difundido na mídia, como o único vilão no ambiente virtual. Por este motivo, assim será usado neste artigo.

Com a massificação do uso das redes sociais, tornou-se mais fácil encontrar grupos organizados em torno de um objetivo comum. Isto não foi diferente para os hackers, que se



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



uniram em vários grupos de atuações. Com o passar do tempo, esses grupos foram crescendo e se tornando cada vez mais ativos, sejam por suas ideologias ou pela sua forma de ação. Atualmente, os dois grupos de hackers mais famosos são o Anonymous e o LulzSec.

3 Anonymous



O termo Anonymous, como um grupo, foi criado na internet em 2003 para representar um conjunto de usuários online e sincronizados, como uma consciência coletiva. No início, foi concebido como uma coletividade descentralizada, atuando de maneira coordenada e agindo anonimamente. Seu símbolo e suas fantasias foram inspirados em Guido Fawkes (Ativista Espanhol - 1570-1606) e no personagem protagonista do filme "V de Vendetta" (2006).

O grupo não possui uma estrutura hierárquica, lista de participantes, porta vozes e ritos de entrada ou saída do grupo. No começo, o Anonymous parecia não ter uma causa fixa, atacando, principalmente, sites de entretenimento. Qualquer pessoa poderia fazer parte deste grupo, ou não. Qualquer um que se dizer parte do Anonymous, efetivamente o é. Porém o grupo esteve ligado a uma série de ataques DDoS (na qual veremos na próxima parte), o que chamou a atenção dos noticiários.

Algumas das ações realizadas pelos Anonymous que foram expostas na mídia estão listadas a seguir.

- *A prisão de Chris Forcand*ⁱⁱ

Em dezembro de 2007, Chris Forcand (53) foi preso pela polícia Canadense. Ele é acusado dos crimes de assédio sexual de um menor de 14 anos, pela posse de arma ilegal e pelo trânsito com arma sem a devida autorização. A polícia chegou até o condenado por meio de uma série de denúncias de um grupo de "ciber-vigilantes" que estavam descontentes com o comportamento de Forcand.

- *Invasão do Fórum da Fundação de Epilepsia*ⁱⁱⁱ

Em março de 2008 o fórum da Fundação de Epilepsia (EUA e UK) foi invadido e imagens animadas foram colocadas neste fórum. Essas imagens serviram como gatilhos causadores de dores de cabeça e ataques epiléticos em pessoas fotossensíveis.

- *YouTube Porn day*^{iv}



Em 20 de março de 2009, internautas, que alegaram pertencer ao grupo Anonymous, postaram centenas de milhares de vídeos pornográficos no YouTube.com, como se fossem vídeos caseiros.

- *Eleições Iranianas em 2009^v*

Após as eleições presidenciais Iranianas em 2009, vários cidadãos daquele país se levantaram contra a reeleição de Mahmoud Ahmadinejad. Imediatamente, forças do governo romperam as comunicações do país com o resto do mundo, numa tentativa de controle. O Anonymous e o site ThePirateBay.com, auxiliaram na difusão de informações para os manifestantes, chegando a concentrar cerca de 22 mil participantes, provendo recursos e suporte aos iranianos protestavam naquele momento.

- *Avenge Assange (Vingança Assange)^{vi}*

Em dezembro de 2010, o site que mantinha a documentação do WikiLeaks acabou saindo do ar, pressionados pela retirada dos documentos secretos da diplomacia norte americana. Em resposta a esta ação, o Anonymous anunciou seu apoio ao WikiLeaks, dando início a uma série de ataques DDoS contra a Amazon, PayPal, MasterCard, Visa e ao Banco Suíço PostFinance.

- *Operação Payback (troco)^{vii}*

O Anonymous lança um ataque gigante à PSN (PlayStation Network) da Sony, como uma forma de protesto pelo fato da grande corporação japonesa processar George Hotz (por quebrar o código do PS3) e Alexandre Egorenkov (que com o código do PS3 quebrado, restaurou o sistema operacional Linux dentro do dispositivo). Várias informações dos empregados da PSN foram divulgados, incluindo fotos, nomes, endereços e familiares.

- *Bank of America^{ix}*

Em março de 2011, o grupo Anonymous começou a liberação de e-mails internos do Bank of America que documentavam "fraude e corrupção".

- *Polícia Espanhola^x*

Em 12 de Junho de 2011, um ataque de DDoS tirou do ar o site da Polícia Espanhola por cerca de uma hora. O ataque foi uma resposta do grupo Anonymous para a prisão de três indivíduos associados a atos de desobediência civil e atribuídos ao grupo.

- *Anti Corrupção na Malásia^{xi}*



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

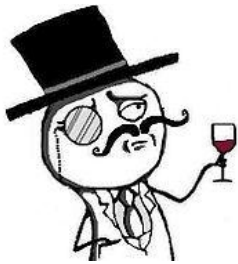
“Conhecer o Brasil para melhor servi-lo”



No dia 15 de Junho de 2011 o grupo lançou um ataque contra 91 sites do governo Malaio em resposta à decisão da corte daquele país em bloquear sites do Wikileaks e ThePirateBay.com, o que o grupo classificou com censura ao direito humano à informação.

Essas não são todas as atividades do grupo Anonymous. Várias outras estão bem documentadas. Mas por estes exemplos, pode-se ter uma ideia dos comportamentos que lhe são atribuídos.

4 LulzSec



LulzSec é um grupo recente, tendo sido fundado no início de maio de 2011. O nome tem origem no termo LOL (risada) e Sec de Security. Seu objetivo, ao que tudo indica, é a realização de ataques em alvos considerados “High Profiles”, isto é, agências governamentais e grandes empresas presentes na mídia. Os dois principais tipos de ataques utilizados pelo grupo são os DDoS e o ataque em troncos telefônicos, algumas vezes por divertimento, outras como um protesto político. A seguir, algumas ações deste grupo:

- Maio de 2011

O grupo invadiu o site da Fox.com^{xii} e divulgou vários usuários e senhas, de funcionários e clientes. Cerca de 73.000 usuários foram afetados.

O grupo também invadiu o site da PBS^{xiii}, uma rede de TV Pública Norte Americana, onde divulgaram a falsa notícia de que o cantor de Rap 2Pac (falecido em 1996) estava vivo e morando na Nova Zelândia.

- Junho de 2011

No dia 8, a empresa Black & Berg Cybersecurity Consulting lançou um desafio.

Ofereceu US\$ 10.000 para quem invadisse seu próprio site e alterasse a imagem da primeira página. Em menos de 15 minutos, o grupo LulzSec conseguiu o feito, mas recusou o prêmio.^{xiv}

No dia 9, o grupo enviou um e-mail para o Serviço Nacional de Saúde do Reino Unido alertando sobre diversas falhas em seus sites e solicitando que as correções fossem feitas. O grupo não invadiu o site da NHS.^{xv}

No dia 11, o grupo invade o site de pornografia pron.com, de onde obtém diversos cadastros de usuários. Entre esses cadastros, o grupo divulga os cadastros com e-mails da administração pública americana (.gov e .mil)^{xvi}.

No dia 13, o grupo invade o site do Senado Norte Americano, em resposta a declaração do Pentágono de que um ciber ataque poderia ser considerado um “ato de



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



Guerra^{xvii}.

No dia 14, o grupo realizou uma série de ataques aos sites de jogos on-line como Minecraft, League of Legends, The Escapist, EVE Online, League of Legends, Heroes of Newerth além de realizar um ataque de negação aos telefones da Blizzard^{xviii}.

No dia 15, o site www.cia.com é atacado e fica fora do ar por algumas horas^{xix}.

- Operação ANTISec^{xx}

No dia 20 de junho, com a ajuda de alguns membros do grupo Anonymous, o Lulzsec inicia uma série de ataques a entidades governamentais e importantes corporações, com o objetivo de roubar e expor informações sobre corrupção. Os alvos foram:

- Serious Organised Crime Agency (SOCA), Uma agência da Lei no Reino Unido.
- Site da Agência Central de Inteligência.
- Site do governo chinês jhq.gov.cn.
- Sites brasileiros como brasil.gov.br, receita.fazenda.gov.br, presidencia.gov.br.
- Companhia de energia Petrobras.
- Divulgação de informações pessoais de hackers de outros grupos, como endereço, nome real, família, etc, para o FBI.
- Roubo da base de dados do Senso britânico de 2011.

5 Conclusão

Um movimento bem organizado ou uma atitude anárquica. O fato é que, não importa qual o grupo, houve, há e certamente haverá discórdia, brigas, demonstração de força e muita troca de informação entre eles. Alguns integrantes do grupo estão bem maduros, outros, estão no início de sua carreira. A constatação é de que a guerra já começou e está longe de terminar. Ao contrário das guerras que aconteciam no passado, onde exércitos se movimentavam e era possível traçar estratégias para um confronto simétrico, esse novo campo de batalha é invisível e o inimigo assimétrico. Por enquanto, a maioria dos ataques são de negação de serviço (DDoS). Porém, estes ataques têm um prazo de vida curta e a restauração para um padrão considerado normal pode ser realizado de forma rápida. Quando os ataques forem mais sérios, com a apropriação de informações, destruição de bancos de dados e exposição de pessoas, aí sim, estaremos vivenciando uma ciber guerra.



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



Sobre o Autor



Leonardo Santos Silva (LeoSantos@LeonardoSantos.com.br) é Administrador, com MBA em Gestão Executiva e Adesguiano da turma de 2007. Já atuou em diversas empresas como especialista em Segurança da Informação, possuindo vários certificados na área e realizando análises de risco, criando Plano de Continuidade de Negócios, Política de Segurança da Informação, Infraestrutura de Chaves Públicas, Análises Criptográficas e Defesa em Perímetro.

<http://www.LeonardoSantos.com.br>

ⁱ O termo em inglês grafado com Y. Entretanto, alguns órgãos (como o EB) ao descrever seu centro de combate de guerra tecnológica, utiliza a letra “i” (Ciber) indicando uma tropicanização da palavra.

ⁱⁱ <http://cnews.canoe.ca/CNEWS/Crime/2007/12/07/4712680-sun.html>

ⁱⁱⁱ <http://www.wired.com/politics/security/news/2008/03/epilepsy>

^{iv} <http://news.bbc.co.uk/1/hi/uk/8061979.stm>

^v <http://iran.whyweprotest.net/>

^{vi} <https://uloadr.com/u/4.png>

^{vii} <http://www.thetechherald.com/article.php/201114/7017/Anonymous-Operation-Sony-is-a-double-edged-sword>

^{viii} <http://arstechnica.com/tech-policy/news/2011/04/anonymous-goes-after-sony-makes-it-personal-very-personal.ars>

^{ix} <http://www.heraldsun.com.au/news/breaking-news/hacker-group-anonymous-says-it-will-release-bank-of-america-emails/story-e6frf7jx-1226020941770>

^x <http://www.bbc.co.uk/news/technology-13749181>

^{xi} <http://www.pcmag.com/article2/0,2817,2387108,00.asp>

^{xii} <http://www.foxnews.com/scitech/2011/06/21/brief-history-lulzsec-hackers/>

^{xiii} http://articles.cnn.com/2011-05-30/tech/pbs.hackers_1_pbs-tupac-shakur-tupac-story?_s=PM:TECH

^{xiv} <http://www.ibtimes.com/articles/159446/20110608/lulzsec-hacking-competition-black-berg-cybersecurity.htm>

^{xv} <http://www.bbc.co.uk/news/technology-13712377>

^{xvi}

http://www.pcworld.com/article/230122/porn_site_users_beware_lulzsec_posts_your_email_address.html

^{xvii} <http://online.wsj.com/article/BT-CO-20110613-710201.html>

^{xviii} <http://arstechnica.com/tech-policy/news/2011/06/titanic-takeover-tuesday-lulzsecs-busy-day-of-hacking-escapades.ars> e <http://techland.time.com/2011/06/14/lulzsec-knocks-minecraft-eve-online-league-of-legends-and-the-escapist-offline/>

^{xix} <http://news.consumerreports.org/electronics/2011/06/cia-website-hacked-lulzsec-takes-credit-again.html>

^{xx} <http://content.usatoday.com/communities/technologylive/post/2011/06/lulzsec-anonymous-declare-war-against-governments-corporations/1>