Cyber Crimes – a trilha do dinheiro

Pedro Bueno, *McAfee AvertLabs / SANS Internet Storm Center*

There was a time when major crimes committed via the Internet were done mostly by teenage pranksters, and major crimes committed in real life were largely done by adult criminals. Unfortunately these days are gone. Criminal organizations have discovered that online illegal activity can be as profitable as running a real-life scam or an illegal business. Organized crime, mafia groups, and terrorist groups are now using the Internet for illegal fund raising, fraud schemes, and money laundering. This paper will "follow the money" to show how the Internet is being used to finance terrorist groups and support organized criminal activity. We will also demonstrate why Cyber-Terrorism is not only acts of targeting other nation's cyber infrastructure, but also a means to funnel cyber cash to real-life terrorist groups.

I. Introdução

Desde os atentados de 11 de Setembro, os grupos terroristas têm estado sob uma maior vigilância por parte das autoridades. No mundo cibernético não foi diferente, com o aparecimento cada vez maior do chamado cyber terrorismo, e já é possível dizer que os soldados perderam o monopólio da guerra como era conhecida [1]. Apesar da definição de cyber terrorismo caracterizar dano e destruição através do comprometimento de sistemas, neste artigo iremos ver uma outra visão, a de como técnicas de crimes cibernéticos têm sido utilizadas para financiar organizações criminosas, incluindo o terrorismo no mundo real.

II. MOTIVAÇÃO

A. *Financiamento Ilegal*

Como qualquer grupo criminoso, seja o crime organizado ou o terrorismo, as ações precisam ser financiadas, para qualquer que seja o objetivo, como a compra de armamentos, planos estratégicos, operações e treinamento.

B. *Terrorismo*

O terrorismo, devido aos fatos ocorridos nos últimos anos, vem oferecendo uma série de exemplos desta interligação entre o real e o virtual:

1) Em 1999, um hacker com nickname NeOh, foi procurado um grupo do oriente médio para conseguir os planos estruturais de um AirBus A300, com a promessa de receber 10000 USD. Os planos foram conseguidos, mas ele nunca recebeu o prometido. Acredita-se que alguns destes planos foram fundamentais para o seqüestro de um avião da Indian Airlines no Afeganistão em dezembro de 1999. [2]

2) Em fevereiro de 2001, o hacker Ne0h foi novamente abordado pelo mesmo grupo que prometeu o dobro do pagamento por alguns outros planos de aeronaves, mas o hacker, como não havia recebido na primeira vez, desistiu. Descobriu-se que os planos eram para aeronaves idênticas as utilizadas no atentado de 11 de setembro. [2]

3) Acredita-se que o atentado a bombas em uma boate em Bali em 2002 foi parcialmente financiado graças a fraudes online com cartões de crédito. O autor destes atentados, Imam Samudra, possui um livro publicado cujo titulo é "Aku Mekawan Terroris!", cuja tradução para o inglês é "Me Against the Terrorist!", que possui um capitulo chamado "Hacking, why not".[3]

4) Em Abril de 2006, 5 parentes de um jordaniano com cidadania americana acusado de ser um contato da Al Qeada foram presos na Califórnia (EUA) acusados fraudar bancos em centenas de milhares de dólares, com financiamentos e empréstimos. Investigações mostraram que parte do dinheiro foi transferido para uma conta em Amman, na Jordânia. [11]

C. *O modelo Máfia*

Com os altos lucros obtidos com as ações criminosas, um outro modelo real de crime organizado está migrando para o mundo virtual, a Máfia. Um exemplo recente apontado pelo FBI é o CardPlanet [4]. Esse grupo de crime organizado possui a mesma estrutura que a Máfia italiana, e possuía vários outros grupos 'afiliados', como o grupo hacker russo chamado Mazafaka (cujo site web possui o sugestivo titulo "Network Terrorism" [5]), ShadowCrew e IAACA cuja sigla em inglês significa International Association for the Advancement of Criminal Activity.

III . MÉTODOS UTILIZADOS PARA OBTENÇÃO ILEGAL DE RECURSOS FINANCEIROS

A. Roubo de Identidade

O crescimento da internet permitiu que os esquemas tradicionais de fraude tivessem um significativo aumento, graças a utilização e a facilidade que a mesma oferece. Os comprometimentos e invasões de bases de dados de cartões de credito e instituições financeiras para obtenção de informações sensíveis como números de identificação de cartões de crédito fez com que os crimes de roubo de identidade subissem.

O impacto dessas ações é maior que apenas a perda de dinheiro, e é ainda mais grave se pensarmos que terroristas tem utilizado essas técnicas para obtenção de financiamentos e empréstimos. Um exemplo é o de células da Al Qaeda que utilizavam cartões de credito roubados em compras de celulares que eram utilizados para comunicação com outras células terroristas no Paquistão, Afeganistão, Líbano, etc...[6]

B. Phishing (1.0 e 2.0)

1) Phishing 1.0 é o phishing tradicional, que funciona da seguinte maneira:

I. UMA REPLICA DA PAGINA DE UM BANCO É HOSPEDADO EM UM SERVIDOR (PREFERENCIALMENTE UM SERVIDOR DE HOSPEDAGEM GRATUITA).

II. O USUÁRIO RECEBE UM E-MAIL OU DE ALGUMA OUTRA MANEIRA É LEVADO A CLICAR NESTE LINK FALSO, ACHANDO QUE É O LINK DO SEU BANCO.

III. COMO A PÁGINA É UMA RÉPLICA DO SITE DO SEU BANCO, O USUÁRIO IRÁ INSERIR SUAS CREDENCIAIS NESTE SITE, E ASSIM QUE CONFIRMAR ESSES DADOS SERÁ REDIRECIONADO AO WEBSITE VERDADEIRO DE SEU BANCO.

IV. COM BASE NOS DADOS CAPTURADOS O HACKER PODE UTILIZAR PARA REALIZAR TRANSAÇÕES FINANCEIRAS ILEGAIS.

A figura abaixo ilustra o caso típico de Phishing 1.0, com uma página falsa do Banco Santander, hospedada em um servidor no Reino Unido.

Figura 1 – Phishing Santander

2) Phishing 2.0

Com o passar dos anos, as instituições financeiras passaram a implementar novas técnicas de segurança para seus clientes. O Phishing 2.0[12], a segunda geração dos phishings, tem como objetivo principal tentar *bypassar* essas novas proteções, como:

I. - OTP – one time password. Um exemplo desse tipo de proteção são os Token que geram novos números a cada 30/60 segundos, sendo esta a senha da pessoa.

II. - IP Geolocation – o banco associa a conta da pessoal com a localidade dela, assim uma pessoal na Rússia não pode acessar a conta de um banco brasileiro.

O Phishing 2.0 funciona da seguinte maneira:

1. O usuário é levado a clicar em um link de seu banco
2. O site com o phishing na verdade não é um site com uma replica do site do seu banco, mas um servidor proxy que conecta ao site real do banco.
3. O hacker toma conta da sessão assim que o usuário se 'loga' no banco
4. Quando o usuário sai, o proxy continua ativo, fazendo 'refreshes' para evitar um timeout
5. O hacker pode alterar a sessão de acordo com suas necessidades.

Um exemplo:
- O cliente fala para o proxy: Transfira 1000 reais para conta XXX / Ag YYY
- O proxy fala para o banco: Transfira 1000 reais para conta AAA / Ag BBB
- O banco para o proxy: Confirma transferência de 1000 reais para conta AAA / Ag BBB
- O proxy fala para o cliente: Confirma transferência de 1000 reais para conta XXX / Ag YYY
- O cliente fala para o Proxy: Confirmo transferência para XXX / YYY e o numero do meu token é 123456
- O proxy fala para o banco: Confirmo transferência para AAA / BBB e o numero do meu token é 123456.

Figura 2 – Funcionamento do Phishing 2.0

Para *bypassar* a proteção do IP Geolocation, o Phishing 2.0 utiliza uma botnet para escolher um proxy que esteja em uma

região do banco.

3) *Bankers 1.0*

Os trojans bancários, também chamados de Pws-Banker são malwares cujo objetivo é o de se instalar na máquina da pessoa e monitorar seu trafego. Quando o usuário for entrar em uma pagina do seu banco, o trojan irá carregar uma aplicação que irá simular a pagina do seu banco e capturar as informações do cliente. Normalmente esses trojans são constituídos de 2 componentes:

I. DOWNLOADER – os downloaders normalmente são baixados ao clicar em links de e-mails falsos, como Cartões Virtuais, Orkut, Comunicados (SERASA, SPC, TSE).

É importante notar que muitas vezes os e-mails são criados e distribuídos com tanta pressa e sem "controle de qualidade", que as vezes é possível ver um e-mail cujo remetente é "Americanas.com" e o assunto "Justiça Eleitoral".

Ao clicar nesses links para baixar um "formulário", "cartão", etc... o downloader irá fazer, em background, o download do componente principal, o Pws-Banker.

A razão de se ter 2 componentes é que o downloader tem em média 10 a 20kb de tamanho, ou seja, extremamente rápido de ser baixado, enquanto o Pws-Banker pode variar de 500kb a 2Mb, o que seria muito lento e poderia levantar suspeitas do usuário.

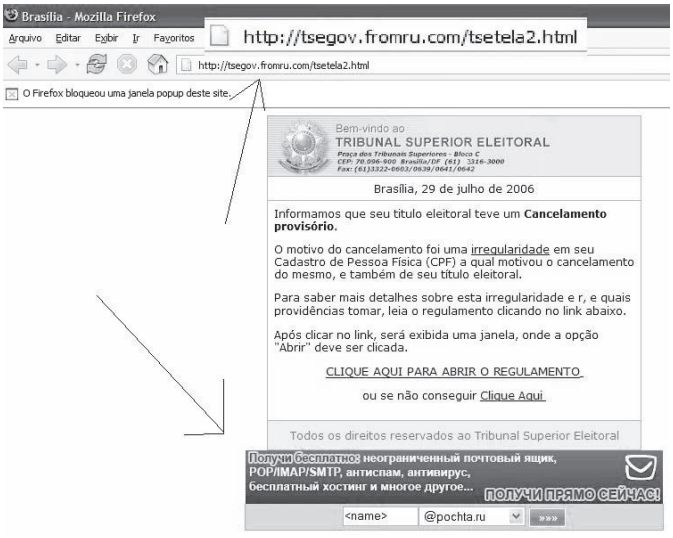

Figura 3 - Exemplo de Phishing para Downloader

A figura acima mostra um exemplo real de um falso aviso do Tribunal Superior Eleitoral, hospedado em um site na Russia, que inclusive contem banners em russo.

II. Pws-Banker – o pws-banker é o software que irá monitorar as urls dos principais bancos e simular a pagina do banco quando o usuário tentar acessá-la. Assim que obtiver as informações, ele envia um email para o hacker, para que o mesmo possa acessar o banco com as credenciais do cliente, e assim poder realizar transferências ilegais.

As informações são transmitidas no seguinte formato:

```
>>B.a.c.o.d.o=B.r.a.s.i.l<<<
=-=-=-=CAIXA ECONOMICA FEDERAL=-=-=-=
=-=-=-=BANCO REAL=-=-=-=
=-=-=-=UNIBANCO=-=-=-=
![Titu].....:
![Age].....:
![Cont].....:
![SeAA].....:
![SeCart]....:
=-=Tabela=-=
=-=Chave20:
=-=Chave25:
=-=Chave33:
=-=Chave35:
=-=Chave11:
=-=Chave17:
=-=Chave52:
```

Figura 4 – Exemplo dos dados transmitidos

4) *Bankers 2.0*

A segunda geração dos Bankers, chamada de Bankers 2.0[8] apresenta duas modificações em relação a sua versão anterior:

I. Targeted Bank – o contrario do antigo trojan bancário que tinha a capacidade de simular paginas de vários bancos diferentes, o novo Pws-banker é direcionado a algum banco especifico que tenha um método de proteção especifico. Um exemplo é o PWS-Banker.gen.t[9], que era direcionado ao Banco Bradesco, e que realizava um harvesting no HD do cliente, em busca de arquivos do tipo *.crt e *.key, utilizados para certificação digital, um outro método de prover maior segurança ao acesso a internet banking.

II. Modular – a segunda modificação é que a arquitetura desses trojans agora é modular. Ou seja:

a) Usuário é levado a baixar o downloader
b) Downloader busca o arquivo links.jpg do site www.free.ru (na Rússia)
c) Arquivo links.jpg na verdade é um arquivo texto que contem links para o downloader baixar arquivos específicos do site www.free.cn (na China).

d) Downloader baixa do site www.free.cn, pws-bankers direcionados para alguns bancos específicos.

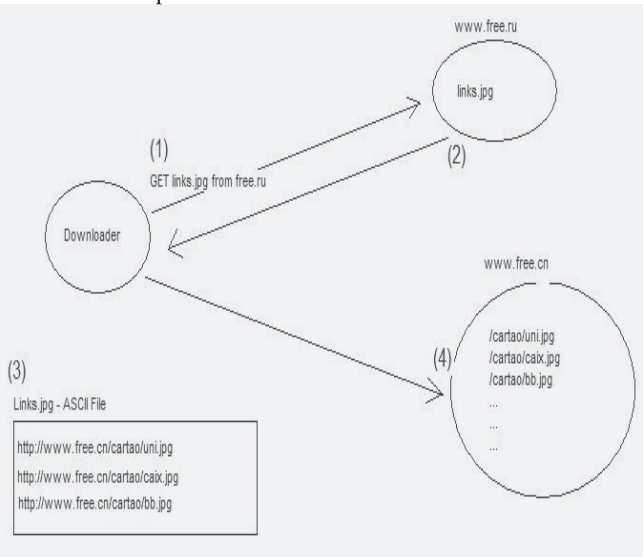

Figura 5 – Fucionamento do Banker 2.0

Neste exemplo, a escolha dos domínios .ru e .cn não foram aleatórias. A escolha dos lugares para hospedagem dos trojans geralmente também não é aleatória, pois a intenção é manter esses trojans disponíveis pelo maior tempo possível. E a ação de remoção de trojans em sites de hospedagens (gratuitas ou não) nestes paises é extremamente complicada devido a barreira da língua, ficando assim um maior tempo disponível.

5) Botnets

- Uma outra forma de obter ganhos financeiros é através da utilização das botnets. Em resumo, uma botnet é o conjunto de bots, que caracterizam um computador sob o domínio remoto de um hacker (máquinas zombies).

As botnets podem variar de tamanho, com poucas máquinas à até milhões de maquinas[10]. Elas já tem sido utilizadas a alguns anos para os mais variados propósitos, como:

A. Armazenamento de conteúdo copyrighted – esses conteúdos podem variar de sofwares, livros e videos piratas

B. Envio de spams – esses spams podem conter links para phishings e downloads de Pws-bankers

C. Ataques DDoS – esses ataques podem servir como duas fontes diferentes de ganhos financeiros:

✓ Venda de ataques a algum site de competidor.

Em 2004, Saad Echouafni, CEO da empresa Orbit Telecomunications, foi condenado por contratar um ataque de DDoS a sites de competidores, provocando perdas de cerca de 1 milhão de dólares.

✓ Extorsão de um site, no qual ele paga uma quantia para ter a 'proteção' que não irá receber um ataque de DDoS e ficar indisponível e perder milhares de dólares pelo tempo do ataque, no qual os clientes não terão acesso ao site.

Em outubro de 2005, uma botnet com mais de 1.5 milhões de máquinas foi descoberta na Holanda, e a prisão de 3 homens indicava que os mesmos trabalhavam para o crime organizado russo, chamada "Russian Internet Máfia".

IV CONCLUSÃO

A utilização da internet pelos grupos que promovem atividades ilegais, como grupos extremistas armados, Máfia e crime organizado é cada vez mais perceptível, assim como a interação entre os mesmos e os métodos utilizados. Com tamanha interação e a clara motivação financeira entre estes grupos, fica claro como o contra-ataque das autoridades está um passo atrás. Um possível caminho para se chegar ao estagio atual dos criminosos é o compartilhamento de informações entre a comunidade de segurança de informações e as autoridades responsáveis por combater os mesmos. Fabricantes de Anti-Virus, IDSs, Listas de segurança fechadas são apenas alguns exemplos por onde esse fluxo de informações poderia passar.

Finalmente, o importante a ser notado é que se atitudes como essa não foram tomadas, estaremos sempre fadados a estarmos em modo reativo, ao invés de estamos tomando ações pró-ativas visando a proteção do usuário final.

REFERENCIAS

[1] Liang Quiao. 1999. Unrestricted Warfare
[2] Sachs, Marcus. et all. 2004 Cyber Adversary Characterization – Auditing the hacker mind. Syngress
[3] Emerging Terrorist Capabilities for Cyber Conflict against the U.S. Homeland. Disponível em http://www.cyberconflict.org/pdf/WilsonNov012005.pdf
[4] FBI: Cybercriminals taking cues fromMafia –Disponíveç em http://www.infoworld.com/article/06/08/07/HNcybercriminals_1.html
[5] Mazafaka Network Terrorism Group. Disponível em http://www1.mazafaka.ru/
[6] FBI Congressional Testimony. Disponível em http://www.fbi.gov/congress/congress02/idtheft.htm
[7] Botnets – f-secure blog
[8] Bankers 2.0. Disponível em http://isc.sans.org/diary.php?storyid=1543
[9] McAfee Vil Description. Disponível em: http://vil.nai.com/vil/content/v_140334.htm
[10] Dutch Botnet Trio Reportedly Connected to Russian Mob. Disponível em http://www.techweb.com/wire/security/173600331
[11] Five Relatives of Terrorism suspect arrested. Disponível em: http://www.msnbc.msn.com/id/12523560/from/RSS/
[12] Phishing 2.0 - http://biz.yahoo.com/prnews/060712/sfw062.html?.v=67

Pedro Bueno was the coordinator of the CSIRT at one of the Brazil's largest Telecom companies and is currently a Anti-Virus Research Engineer at McAfee AvertLabs. He is one of the handlers at the SANS Institute's Internet Storm Center, where he deals daily with cutting edge security issues and authored a series of the Malware Analysis Quizes. He is also a member of The SANS Top 20 Internet Security Vulnerabilities expert's Team for about 5 years.