INTELIGÊNCIA COMPUTACIONAL

NO COMBATE ÀS FRAUDES, CRIMES E LAVAGEM DE DINHEIRO

Agenda

- Deep Web – Além da Internet que conhecemos
- Moeda virtual – o Bitcoin
- Uso ilegal de moeda virtual: o caso silk road

Agenda

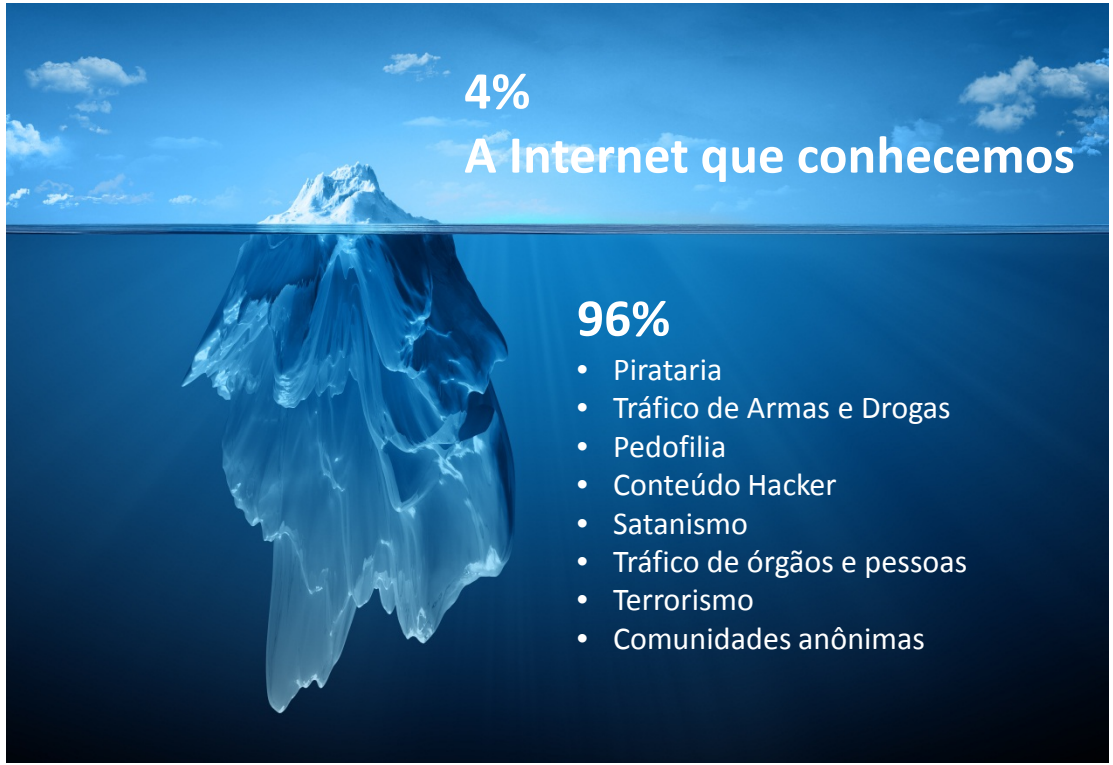
- Deep Web – Além da Internet que conhecemos
- Moeda virtual – o Bitcoin
- Uso ilegal de moeda virtual: o caso silk road

Deep Web

ALÉM DA INTERNET QUE CONHECEMOS

Deep Web

- Informações “invisíveis” aos sistemas de busca da Web



Fonte: BERGMAN, M.K. The Deep Web: Surfacing Hidden Value. Journal of Electronic Publishing, v.7, n.1, aug. 2001.

Camadas da Deep Web

Camada 0 – Common Web

- A internet "normal", que todos nós acessamos diariamente

Camada 1 – Surface Web

- Um lado mais "escuro" da web, onde ficam sites incomuns, mas que ainda sim pode ser acessado facilmente

Camada 2 – Bergie Web

- Último level de classe "baixa", aqui encontram-se sites de grupos fechados e que utilizam proxy, Tor ou alguma ferramenta para permitir o acesso;

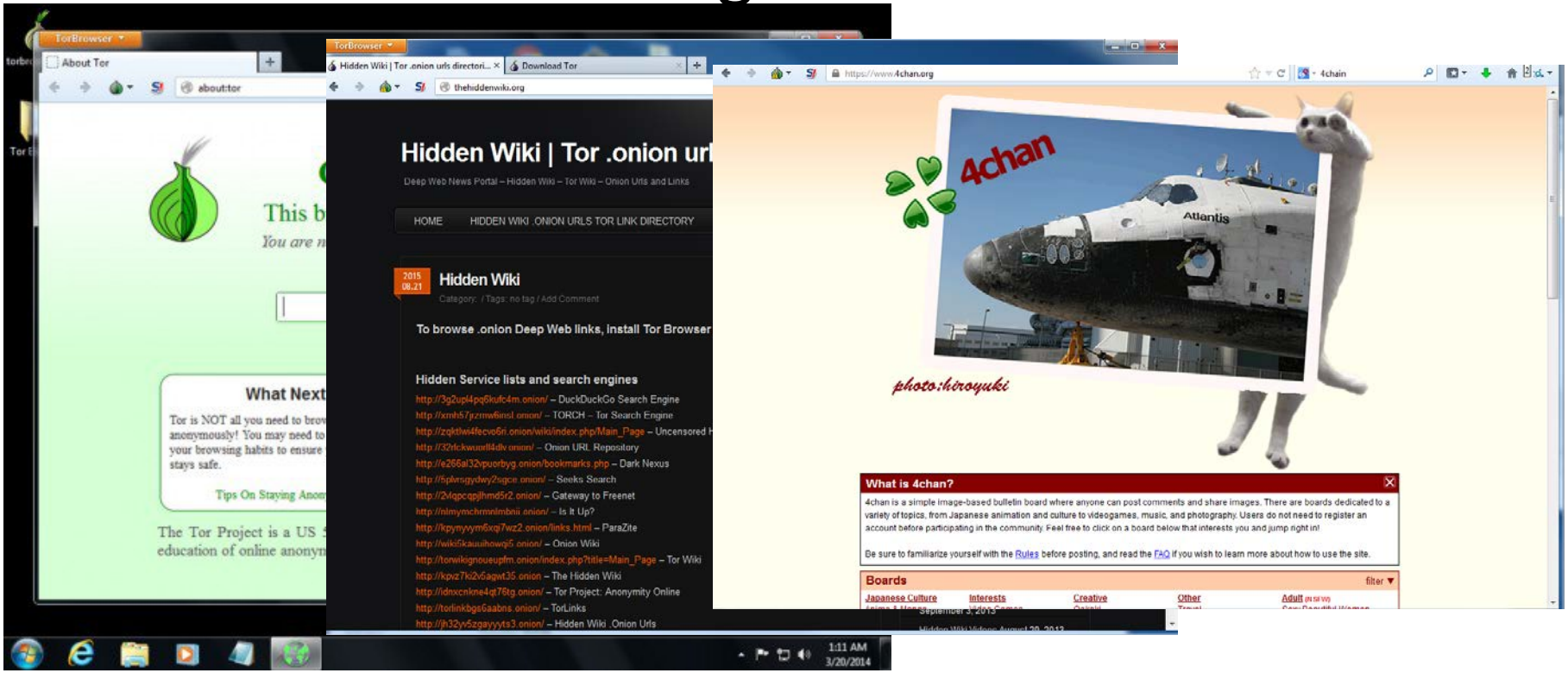
Camada 4 - Charter web

- Início da Deep Web
- Utiliza o Tor para ter acesso,
- Duas partes:
  - Sites comuns como Hidden Wiki e HackBB,
  - Sites restritos e de grupos fechados

Camada 5-Marianas web

- Divisor de águas entra a Deep web "falsa" e a legítima web oculta, aqui se encontram pessoas com um conhecimento mais avançado em computação
- 3 Subcamadas:
  - 1: vídeos e documentos governamentais, sendo uma rede fortemente criptografada e segura;
  - 2: aqui se encontram pessoas que disputam o controle sobre o nível 8. Bilhões de dólares são negociados e tratados.
  - 3: Basicamente onde há o controle tecnológico global, há documentos relacionados com computação quântica, grandes elite hackers, que obviamente não são nem comentados nas mídias andam por aqui, o foco é poder e dinheiro

Navegador Tor



Deep Web - formato dos links

- http://kpvz7ki2v5agwt35.onion (The Hidden Wiki - Contém toneladas de informações sobre sites Tor)
- http://xmh57jrzrnw6insl.onion (Motor de busca para sites Deep Web)
- http://eqt5g4fuenphqinx.onion (Pesquisa em diretório dentro da Internet profunda)
- http://jhiwjjlqpyawmpjx.onion (Tormail, gratuito para envio de mensagens anônimas)
- http://4eiruntyxxbgfv7o.onion (Mensagens instantâneas anônimas)
- http://eqt5g4fuenphqinx.onion (Core .onion, pesquisa em diretório)

Agenda

- Deep Web – Além da Internet que conhecemos
- Moeda virtual – o Bitcoin
- Uso ilegal de moeda virtual: o caso silk road

MOEDA VIRTUAL: O BITCOIN

O que é o Bitcoin funciona?

Moeda virtual

- Modelo econômico sem governos ou instituições financeiras
- Transações P2
- Funcionamento baseado em conjunto de regras
  - Usuários são responsáveis pela regulação do dinheiro

Como o Bitcoin funciona?

Carteiras virtuais

- Gera endereços bitcoin aleatórios
- Endereço único para cada transação

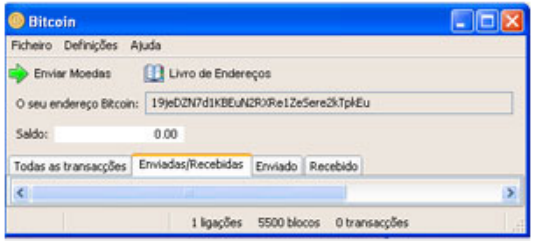


Foto do programa Bitcoin. Protocolo aberto permite criação de diferentes clientes de Bitcoin (Foto: Reprodução)

Saldos – cadeia de blocos

- Livro de registro de contabilidade público compartilhado
- Toda transação confirmadas são incluídas na cadeia de blocos
- Protegido por criptografia

Como o Bitcoin funciona?

Transações

- Transferência de valor entre carteiras Bitcoin
- Incluída na cadeia de blocos
- Uso de chave privada, para assinar transações

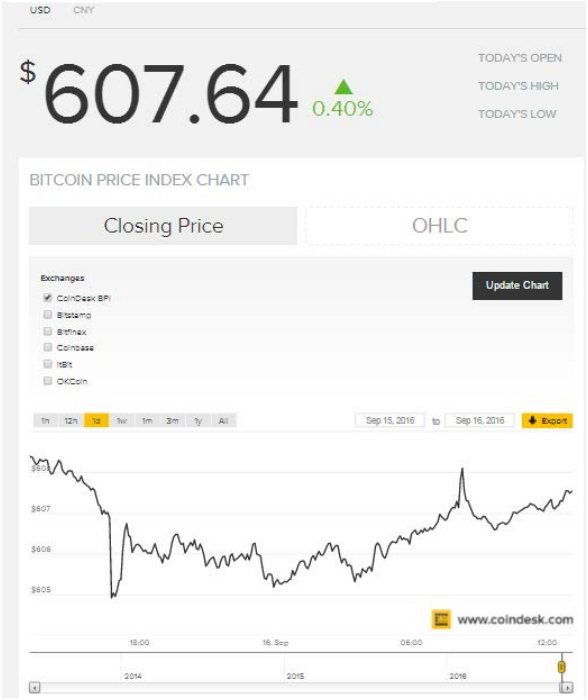
Mineração de Bitcoin

Mineração – processamento das transações

- Similar à mineração do ouro
- bitcoin deve ser “descoberto”
- Combinação de dois fatores definem seu valor:
  - Escassez: controlada pelo software que controla a cadência da mineração
    - Dificuldade: quebrar um hash, para receber bitcoins (descobrir, minerar)
    - Limitado em 21 milhões, com mineração até 2040.
  - Custo ($) de mineração: computadores especializados (1.2 a 30 K US$), gasto de energia

Cotação do Bitcoin 16Set16

http://www.coindesk.com/price/



https://www.mercadobitcoin.net

Bitcoin no mundo

http://www.infomoney.com.br/mercados/bitcoin/noticia/3185905/regular-

http://olhardigital.uol.com.br/pro/noticia/bitcoin-e-proibida-na-tailandia/36275

Bitcoin é proibida na Tailândia

REDAÇÃO OLHAR DIGITAL 30/07/2013 12H17 DINHEIRO

A Bitcoin sofreu um duro golpe nesta s
tailandês de proibir as operações da m

POR FELIPE MORENO - EM MERCADOS - 28 mar, 2014 14h36

? Governo brasileiro não deve
ecer bitcoin como "moeda"

o tal - e sim como um

https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country

Legality of bitcoin by country

From Wikipedia, the free encyclopedia

The legal status of bitcoin varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed its use and trade, others have banned or restricted it. Likewise, various government agencies, departments, and courts have classified bitcoins differently. While this article provides the legal status of bitcoin, regulations and bans that apply to this cryptocurrency likely extend to similar systems as well.

Infográfico: como funciona o Bitcoin

Quanto vale 1 bitcoin?

A moeda é instável e segue as leis de mercado (quanto maior a procura, maior sua cotação)

Preço em 15Set16

R$ 1.968.99

12 milhões

em circulação em março de 2014

A criação de bitcoin tem limite

O protocolo gerador de bitcoins está previsto para gerar 21 milhões de unidades da moeda até 2140. Depois disso, a recompensa da mineração virá apenas das taxas de operação

Estabelecimentos que usam bitcoin

O bitcoin pode ser usado para comprar via internet produtos ou serviços. Quem aceita (ex.):

WordPress | reddit

Silk Road

anonymous marketplace

Infográfico: Filipe Campoi Texto: Guilherme Tagiaroli e Fernando Couri

UOL

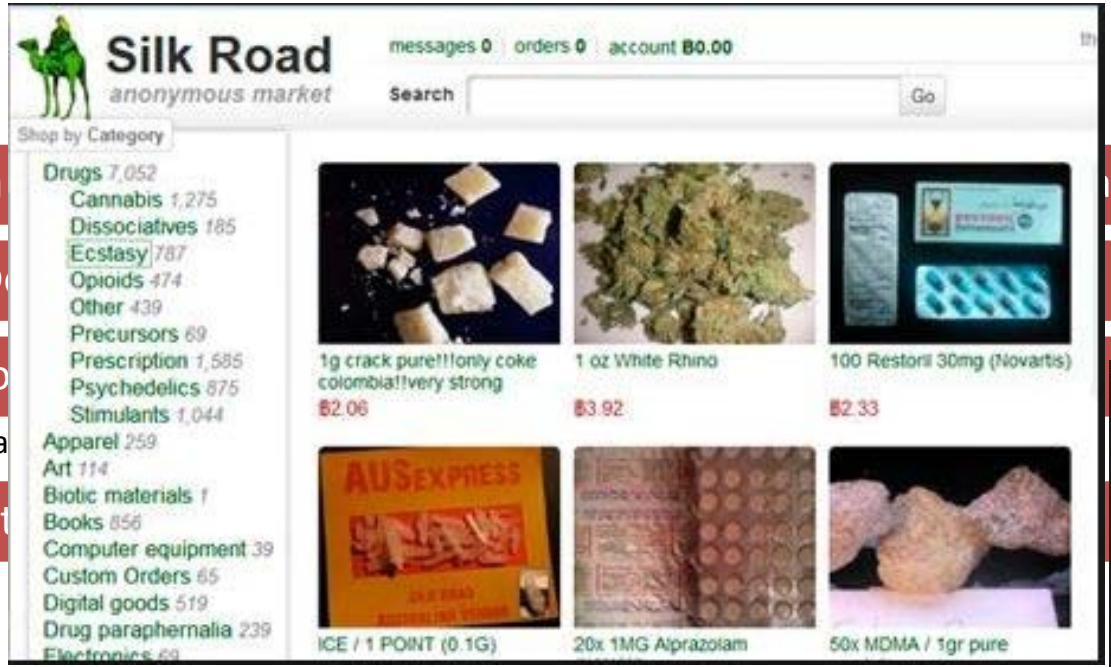
Agenda

- Deep Web – Além da Internet que conhecemos
- Moeda virtual – o Bitcoin
- Uso ilegal de moeda virtual: o caso silk road

USO ILEGAL DE MOEDA VIRTUAL: O CASO SILK ROAD

O que era o Silk Road

- Site de venda
- Operava na D
- Transações co
  - anonimato pa
- Criado e mant



ado em 2001

Tribunal de Contas do Estado de São Paulo

Como foi a investigação do FBI

Jan/2011

- Usuário **altoid** posta mensagens em dois fóruns, perguntando se alguém havia comprado no **Silk Road** e outra em um fórum do Bitcoin (Bitcoin Talk) falando da nova "loja virtual".

Mar/2011

- Silk Road está **operacional** e que já completou 28 transações
- **Tópico** no Bitcoin talk sobre o site
- 1ª **reclamação** de cliente

Abr/2011

- 1.000 usuários

Jun/2011

- 1º fórum oficial no Tor
- DPR faz 1º post, sob o nome “Silk Road”

Ago/2011

- Início do mercado de falsificação de documentos emitidos pelo governo
- Documentos emitidos por empresas (diplomas, ingressos, etc.) não podem ser falsificados

Tribunal de Contas do Estado de São Paulo

Como foi a investigação do FBI

Out/2011

- Usuário **altoid** posta anúncio de emprego para profissional de TI no Bitcoin Talk. A vaga é para uma startup Bitcoin.
- FBI suspeita que altoid é **Ross Ulbricht**

Nov/2011

- Agentes começam a fazer compra de drogas no Silk Road

Dez/2011

- Silk Road muda o endereço na rede Tor: **silkroadvb5piz3r.onion**

Jan/2012

- Silk Road muda o sistema de comissão, aumentando os ganhos do site

Fev/2012

- Nasce Dread Pirate Roberts - DPR

Tribunal de Contas do Estado de São Paulo

Como foi a investigação do FBI

Mar/2012

- É criado uma conta no site de alertas StackOverflow.com com o nome e e-mail de **Ross Ulbricht**, com 2 posts:
- (1) Destruindo uma sessão específica em CodeIgniter [1]
- (2) Como conectar um serviço oculto Tor usando cURL [2] em PHP?
- Em menos de 1 min, o nome e e-mail são mudados para **frosty**.

Abr/2012

- **Agente federal** disfarçado se apresenta como um **contrabandista** com uma grande quantidade de drogas, e pede ajuda para encontrar alguém que queira comprar em grandes quantidades. Esta comunicação continua durante o resto do ano e em Janeiro de 2013.

Out/2012

- DPR posta a estratégia de marketing: comecei um discussão no Bicoin Talk e o resto foi boca a boca.

[1] CodeIgniter é um framework PHP

[2] cURL é uma library e ferramentas para transferir arquivos por meio de diversos protocolos

Como foi a investigação do FBI

Dez/2012

- **Ross Ulbricht** e Rene Pinnel gravam uma entrevista entre eles para o site Story Corps, sobre a mudança para São Francisco, a "**meca das startups**" (https://www.youtube.com/watch?v=HYShi9dhhJY)

Jan/2013

- O agente secreto transporta um quilo de mistura com "**quantidades detectáveis de cocaína**" a um vendedor Silk Road, por US$ 27,000. Uma semana depois, DPR informa que o vendedor foi preso e roubou bitcoins de outros vendedores. **DPR contrata o assassinato** do vendedor por US$ 80,000.

Jan/2013

- **Black Market Reloaded**, concorrente do Silk Road, ganha 16 mil novos usuários e atua em "mercados" proibidos no Silk Road: armas, assassinatos, etc.

Tribunal de Contas do Estado de São Paulo

Como foi a investigação do FBI

Fev/2013

- DPR e o agente falam sobre **a tortura e assassinato** do vendedor.
- DPR solicita um **vídeo ou uma foto** como prova e o agente responde com fotos encenadas , dizendo o corpo da vítima foi " completamente destruído para eliminar evidências.

Mar/2013

- **FriendlyChemist** envia ameças à DPR, dizendo que ele tem uma lista de nomes e endereços de vendedores e clientes do Silk Road.
- FriendlyChemist ameaça de publicar a lista a menos que DPR pague **US$ 500,000** para ele pagar o seu fornecedor de drogas

Mar/2013

- **DPR** pede que o fornecedor de drogas entre em contato diretamente com ele. **Redanwhite** entra em contato.
- **DPR** faz uma oferta para Redanwhite vender no Silk Road, que diz que só se FriendlyChemist se encontrar com ele ou pagar a dívida.

Como foi a investigação do FBI

Mar/2013

- DPR envia os dados pessoais e endereço de FriendlyChemist.
- FriendlyChemist exige o pagamento em 72 horas, para não divulgar 5.000 nomes
- DPR comenta com redanwhite que "gostaria de colocar uma recompensa pela cabeça de FriendlyChemist", que aceita o trabalho por 150,000.
- Agente Tardell do FBI não encontra registro do crime no endereço fornecido por DPR

Jun/2013

- Ross Ulbricht aluga um quarto em **São Franciso** sob o nome Joshua Terrey.

Jul/2013

- FBI consegue uma **imagem** do servidor Silk Road
- Há mais de **950 mil usuários** registrados no Silk Road
- Mais de **US$ 1.2 bilhões** em negócios

Como foi a investigação do FBI

Mar/2013

- DPR envia os dados pessoais e endereço de FriendlyChemist.
- FriendlyChemist exige o pagamento em 72 horas, para não divulgar 5.000 nomes
- DPR comenta com redanwhite que "gostaria de colocar uma recompensa pela cabeça de FriendlyChemist", que aceita o trabalho por 150,000.
- Agente Tardell do FBI não encontra registro do crime no endereço fornecido por DPR

Jun/2013

- Ross Ulbricht aluga um quarto em **São Franciso** sob o nome Joshua Terrey.

Jul/2013

- FBI consegue uma **imagem** do servidor Silk Road
- Há mais de **950 mil usuários** registrados no Silk Road
- Mais de **US$ 1.2 bilhões** em negócios

Tribunal de Contas do Estado de São Paulo

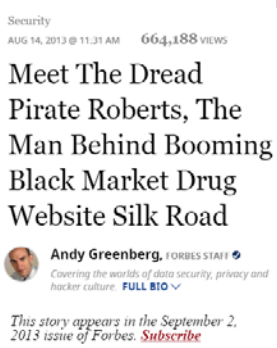
Como foi a investigação do FBI

Jul/2013

- Ulbricht é interrogado por oficiais do Departamento de Segurança Interna após a apreensão de vários IDs falsos com a foto dele.
- Ulbricht diz que é possível para qualquer um comprar documentos no Silk Road

Ago/2013

- Andy Greenberg, repórter Forbes , publica artigos detalhando sua comunicação com DPR e da ideologia libertária que sustenta o projeto Silk Road.
- DPR reconhece que “os mais altos níveis de governo” estão atrás dele


Security
AUG 14, 2013 @ 11:31 AM 664,188 VIEWS

Meet The Dread Pirate Roberts, The Man Behind Booming Black Market Drug Website Silk Road

Andy Greenberg, FORBES STAFF
Covering the worlds of data security, privacy and hacker culture. FULL BIO

This story appears in the September 2, 2013 issue of Forbes. Subscribe

Set/2013

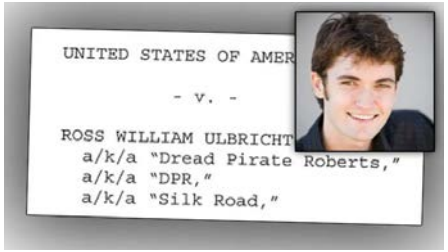
- Atlantis concorrente do Silk Road, é desligado abruptamente por "razões de segurança" e fica com todos os recursos dos seus usuários.

Tribunal de Contas do Estado de São Paulo

Como foi a investigação do FBI

Out/2013

- Ulbricht é acusado pelo assassinato do vendedor Silk Road em Feb/2012
- Preso e acusado por tráfico de drogas, computer hacking e lavagem de dinheiro
- Transferido para o Estado de NY



Out/2013

- FBI revela que atuava no Silk Road desde sua criação, usando sua característica de anonimicidade como arma e fazendo apreensões de drogas
- FBI apreende 144.000 BTC do computador de Ulbricht

Out/2013

- Silk Road é desligado e substituído por uma página inicial do FBI.
- O valor do Bitcoin cai mais de 20% no dia 2 (100 dólares), mas recupera-se e vale mais de 200 no dia 23.
- FBI prende um dos maiores traficantes do Silk Road
- 4 suspeitos presos no Reino Unido

NO FIM...

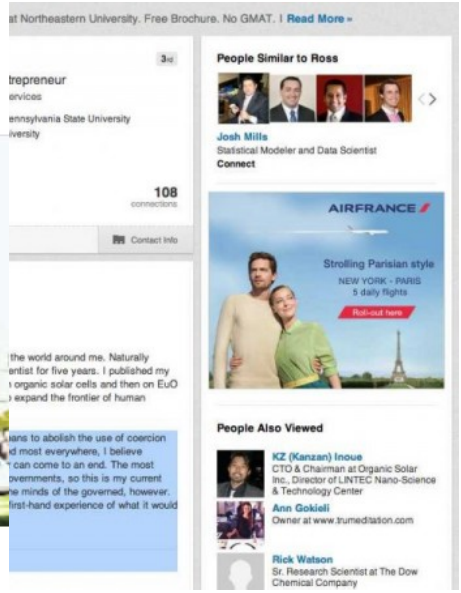
Ross Ulbricht, fundador do site ilegal Silk Road, é condenado à prisão perpétua nos EUA

Site de venda de drogas da internet profunda teria movimentado cerca de US$ 200 milhões até ser fechado, em outubro de 2013

Ross Ulbricht, de 31 anos: prisão perpétua por operar o Silk Road - HANDOUT / REUTERS

POR O GLOBO

29/05/2016 17:46 / atualizado 29/05/2016 20:34



NO FIM...

http://www.coindesk.com/silk-road-agent-stolen-bitcoin/

CRIME • NEWS

Silk Road Agent May Have Stolen More Bitcoin After Guilty Plea

Stan Higgins (@mpmcsweeney) | Published on July 1, 2016 at 18:16 BST

NEWS

Monitoração de fóruns e da própria Deep Web e Silk Road

- Mensagens nos fóruns Bitcoin Talk e Silk Road (altoid, rossulbritch@gmail.com, DPR, etc.)

Infiltração, mesmo que virtual

- Agentes se passando por vendedores e compradores

Tecnologia x 4ª emenda (direito à privacidade)

Tecnologias utilizadas

Descoberta do servidor Silk Road

- O FBI (e não NSA) descobriu o endereço IP do servidor por **falha de configuração** na interface de login do site, monitorando a troca de mensagens IP entre o site e usuários que tentavam se logar. Ao examinar essas mensagens, descobriu-se um **endereço IP da Internet comum** e ao se digitar esse IP em um browser, o Silk Road carregou. Com base em informação pública (whois.icann.org) chegou-se ao servidor na Islândia.

Computação Forense

- Foi solicitada uma imagem do servidor e realizada uma análise forense para confirmação de que o servidor era usado pelo Silk Road.
- Foram identificados outros Ips de servidores de backup, incluindo um localizado em um datacenter na Pensilvânia.

Monitoração dos dados de conexão da Internet do suspeito

- Endereços IPs, datas, hora, duração.
- Com esses dados, foi possível concluir que Ulbricht e DPR eram a mesma pessoa

Tecnologias utilizadas

Descoberta do servidor Silk Road

- O FBI (e não NSA) descobriu o endereço IP do servidor por **falha de configuração** na interface de login do site, monitorando a troca de mensagens IP entre o site e usuários que tentavam se logar. Ao examinar essas mensagens, descobriu-se um **endereço IP da Internet comum** e ao se digitar esse IP em um browser, o Silk Road carregou. Com base em informação pública (whois.icann.org) chegou-se ao servidor na Islândia.

Computação Forense

- Foi solicitada uma imagem do servidor e realizada uma análise forense para confirmação de que o servidor era usado pelo Silk Road.
- Foram identificados outros Ips de servidores de backup, incluindo um localizado em um datacenter na Pensilvânia.

Mandados judiciais para monitorar os dados de conexão da Internet do suspeito

- Endereços IPs, datas, hora, duração. FBI alegou que não foram capturados conteúdos das mensagens.
- Com esses dados, foi possível concluir que Ulbricht e DPR eram a mesma pessoa


In God we trust
All others we monitor
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Obrigado

FABIO XAVIER
FABIO@TCE.SP.GOV.BR