Cibersegurança e seus impactos na sociedade da era digital

Rogerio Bastos

https://certbahia.pop-ba.rnp.br

Quem somos

É responsável pela conexão das instituições baianas à rede acadêmica Brasileira (Rede Ipê) e operação da Rede Metropolitana de Salvador (Remessa).

Coordenação de Segurança da Informação e Comunicações da STI/UFBA, responsável pelas questões de segurança digital na Universidade.

É um CSIRT de coordenação para as instituições clientes do PoP-BA/RNP e parceiras da Remessa.

O que é Segurança da Informação?

O que é Segurança da Informação?

- Segurança da Informação engloba tudo que está relacionado com a proteção da informação. Não se restringe a informação digital.

- Tenta preservar a confidencialidade, integridade, disponibilidade, autenticidade, responsabilidade, não repúdio e confiabilidade da informação.

- Procura prevenir o acesso, uso, divulgação, interrupção, modificação ou destruição não autorizada.

O que é Segurança da Informação?

- Segurança da Informação no contexto dos sistemas computacionais é conhecida como cibersegurança ou segurança de computadores.

- E se aplica ao hardware, software, sistemas e informações digitais.

Qual a importância da Segurança da Informação?

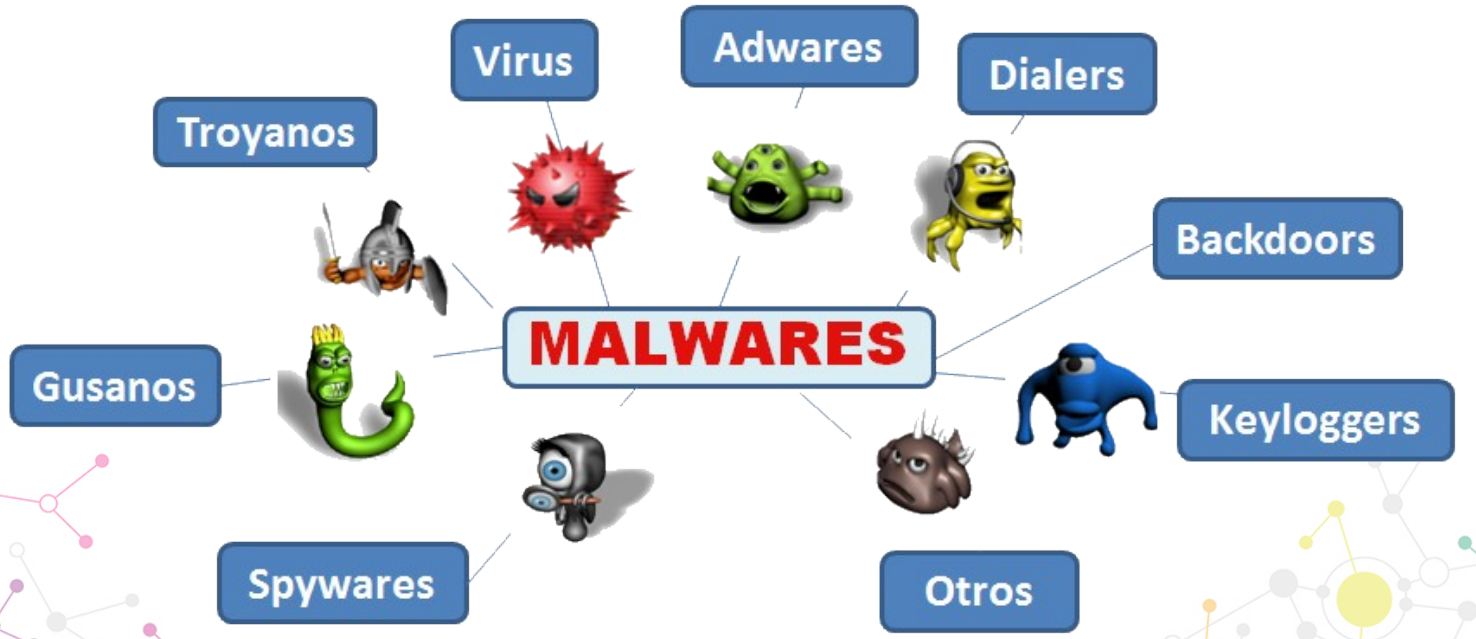
Qual a importância da Segurança da Informação?

- A importância da segurança cibernética cresce com a nossa dependência aos sistemas computacionais, tais como a Internet, computadores, smartphones e a Internet das Coisas.

Como a Segurança da Informação influencia nossas vidas?

Malware

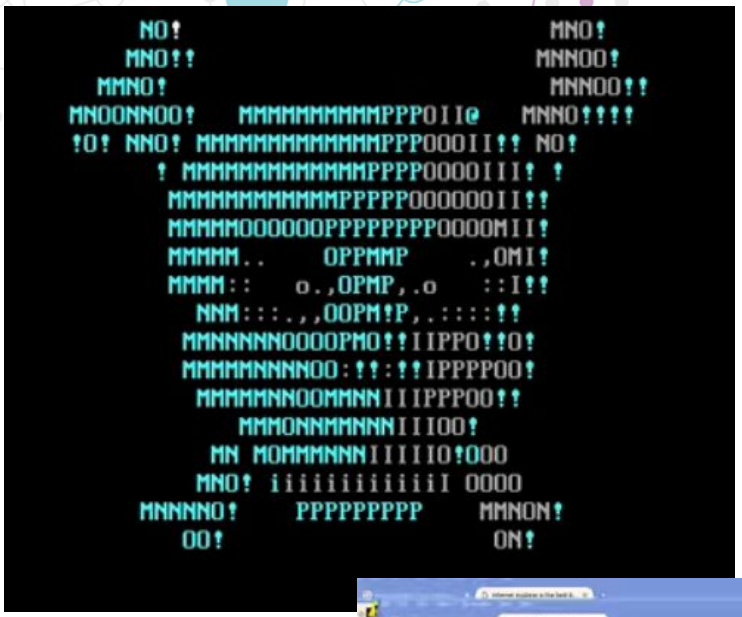
- É um software destinado a infiltrar-se em sistema de computador alheio de forma ilícita, com o intuito de causar danos, roubar de informações, dentre outras atividades maliciosas.

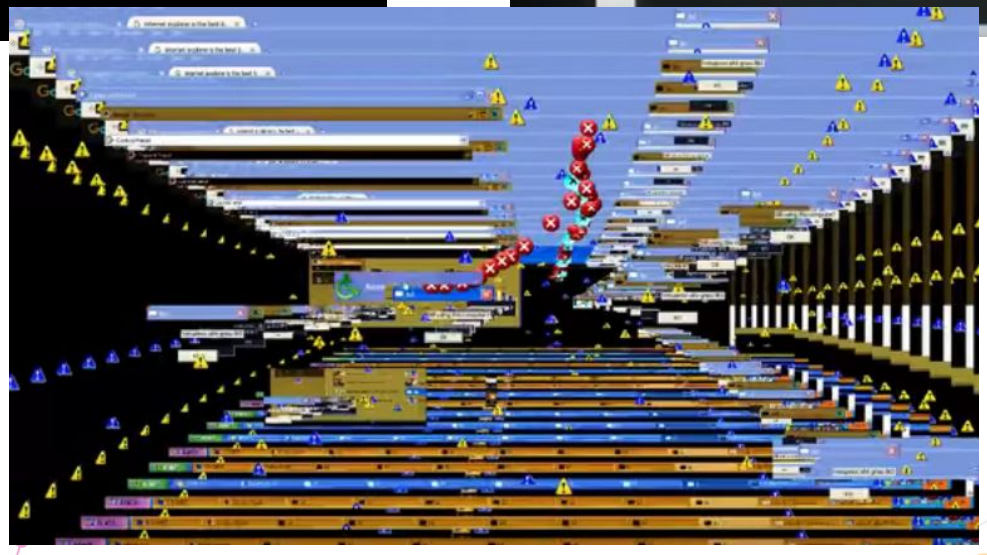


Malware

- Motivação
  - Aprendizado
  - Diversão
  - https://www.youtube.com/user/danooct1

Malware





Malware

- Motivação
  - Retorno Financeiro
  - Espionagem
  - CyberWar
- Ransomware
  - Sequestra o dispositivo ou os dados do usuário
  - Exige pagamento (resgate) para desbloqueá-los
  - https://sti.ufba.br/cosic-mantem-campanha-em-seguranca-da-informacao

Malware

- WannaCry (Maio/2017)
  - Ransomware que explora uma vulnerabilidade do Windows (EternalBlue) para infectar as máquinas via rede.
  - Se espalhou rapidamente, infectando computadores em mais de 150 só no primeiro dia.
  - Até julho/2017 as carteiras de bitcoin associadas ao malware receberam mais de 50 BTC (~ $120.000).

Malware

- Empresas e órgãos públicos brasileiros afetados pelo WannaCry:
  - Petrobras
  - Instituto Nacional do Seguro Social (INSS) em todo o Brasil
  - Tribunais da Justiça de São Paulo, Sergipe, Roraima, Amapá, Mato Grosso do Sul, Minas Gerais, Rio Grande do Norte, Piauí, Bahia e Santa Catarina
  - Ministério Público de São Paulo
  - Itamaraty
  - Instituto Brasileiro de Geografia e Estatística (IBGE)

http://g1.globo.com/tecnologia/noticia/veja-empresas-e-orgaos-publicos-que-tiraram-sites-do-ar-apos-ciberataque-mundial.ghtml

Malware

- Petya (Junho/2017)
  - Ransomware que utiliza a mesma vulnerabilidade usada pelo WannaCry para infectar máquinas Windows.
  - Especula-se que o principal objetivo tenha sido destruir dados.
  - Afetou principalmente a Ucrânia.

Phishing

- Phishing é um ataque que utiliza artifícios tecnológicos e psicológicos para enganar as vítimas se passando por uma entidade confiável para obter dados sensíveis ou instalar softwares maliciosos.

Phishing

- Tecnologia
  - Falso remetente
  - Sites e URLs semelhantes
  - Redirecionamento e encurtadores de URLs
  - BGP e DNS attacks

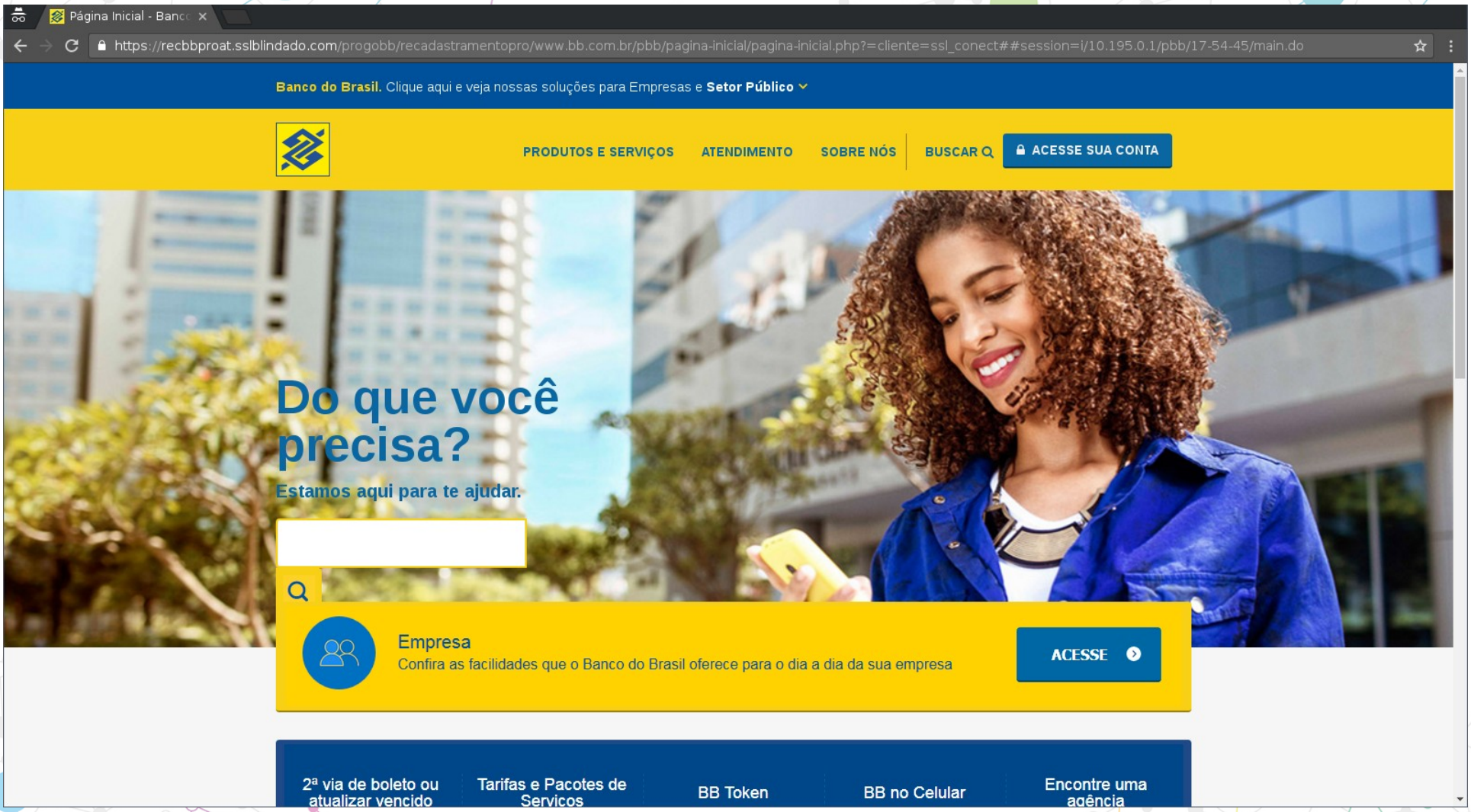
Phishing

- Psicologia
  - Entidade confiável
  - Sentimento de urgência, medo ou preocupação
  - Sentimento de curiosidade
  - Vantagem financeira

Phishing


PRODUTOS E SERVIÇOS
ATENDIMENTO
SOBRE NÓS
Atenção! Comunicado importante do Banco do Brasil.
Prezado (a) cliente,
Informamos que desde o dia 25 de outubro de 2016 nosso sistema de identificação mudou, e para garantir o acesso a sua conta através do Internet Banking é necessário realizar o recadastramento.
Se o recadastramento não for realizado até o dia 20/outubro/2016, acarretará no bloqueio do seu acesso para sua segurança.
Clique no botão abaixo para acessar sua conta e realizar o processo de atualização
ACESSAR
Caso não veja o botão clique aqui.
SAC - 0800 729 0722 | Ouvidoria - 0800 729 5678.
Mais de 5 mil agências para facilitar seu dia a dia.
ENCONTRE UMA AGÊNCIA

Phishing


Página Inicial - Banco
https://recbbproat.sslblindado.com/progobb/recadastramentopro/www.bb.com.br/pbb/pagina-inicial/pagina-inicial.php?=cliente=ssl_conect##session=i/10.195.0.1/pbb/17-54-45/main.do
Banco do Brasil. Clique aqui e veja nossas soluções para Empresas e Setor Público
PRODUTOS E SERVIÇOS
ATENDIMENTO
SOBRE NÓS
BUSCAR
ACESSE SUA CONTA
Do que você precisa?
Estamos aqui para te ajudar.
Empresa
Confira as facilidades que o Banco do Brasil oferece para o dia a dia da sua empresa
ACESSE
2ª via de boleto ou atualizar vencido
Tarifas e Pacotes de Serviços
BB Token
BB no Celular
Encontre uma agência

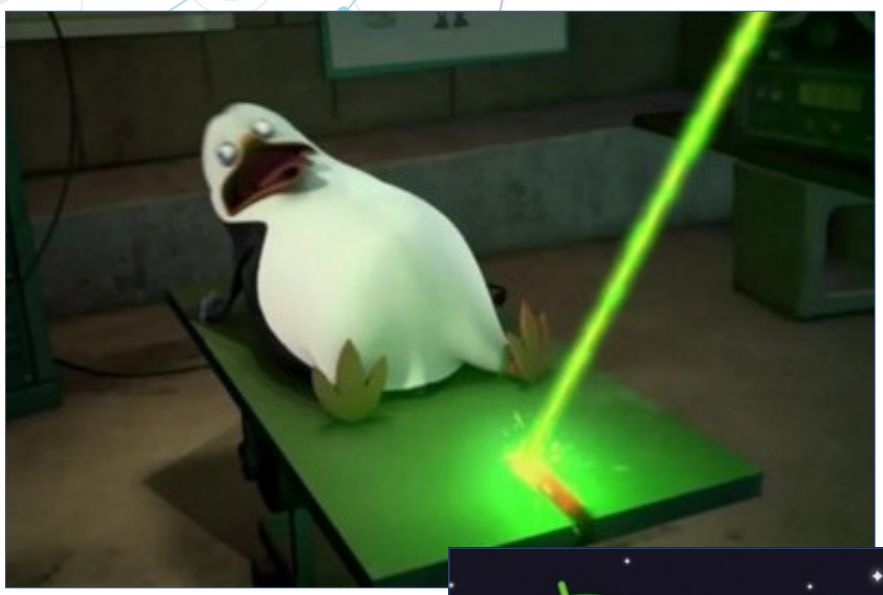
Phishing

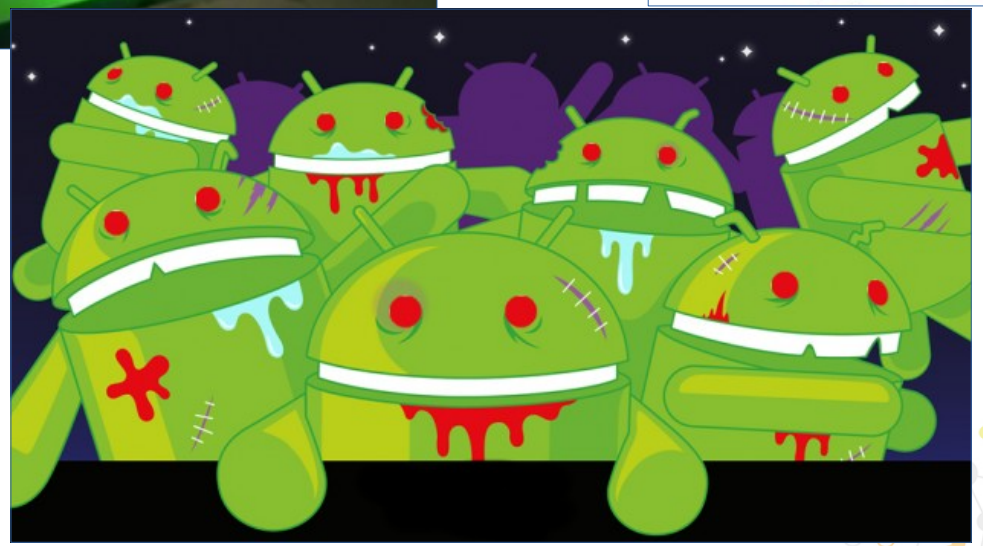
- Catálogo de Fraudes do CAIS/RNP
  - https://www.rnp.br/servicos/seguranca/catalogo-fraudes
- Catálogo de URLs Maliciosas (CaUMa)
  - https://cauma.pop-ba.rnp.br

Vulnerabilidades

- É uma fraqueza que permite ao atacante afetar as propriedades de segurança (e.g. confidencialidade, integridade, disponibilidade, autenticidade, etc).

Vulnerabilidades





Vulnerabilidades

- Heartbleed (Abril/2014)
  - Permite ler áreas de memória que não deveriam ser públicas (e.g. chave privada do certificado SSL).
  - Afetou 70% dos websites, além de outros serviços que utilizam SSL.
  - http://heartbleed.com/

Vulnerabilidades

- Shellshock (Setembro/2014)
  - Várias vulnerabilidades no Shell Bash que permitem a execução de comandos no host afetado (RCE).
  - Afeta Linux, BSD, Mac OS e outros sistemas baseados em UNIX como o da Cisco.

Vulnerabilidades

- Stagefright (Julho/2015)
  - Conjunto de vulnerabilidade no serviço de mídia do Android que permitem a execução de comandos no host afetado (RCE).
  - Afetou o Android da verão 2.2 (Froyo) até 5.1.1_r9 (Lollipop), correspondendo a 95% dos dispositivos na época.
  - http://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/

Vulnerabilidades

- DROWN (Março/2016)
  - Vulnerabilidade no protocolo SSLv2 que permite descriptografar outras conexões que utilizam a mesma chave privada, inclusive as que usam TLS.
  - Exemplos de sites que estava vulneráveis: yahoo.com, alibaba.com, samsung.com, 4shared.com, apache.org.
  - Estima-se que o problema afetou 22% dos servidores na época.
  - https://drownattack.com/

Vulnerabilidades

- ImageTragick (Abril/2016)
  - Conjunto de vulnerabilidades no software ImageMagick que permitem a execução de comandos no host afetado (RCE), dentre outras coisas.
  - Afetou inúmeros plugins e sistemas que processam imagens, como Drupal, Joomla, Wordpress e Facebook.
  - http://4lemon.ru/2017-01-17_facebook_imagetragick_remote_code_execution.html
  - https://imagetragick.com/

Vulnerabilidades

- DirtyCow (Outubro/2016)
  - Vulnerabilidade no kernel do Linux que permite elevação de privilégio.
  - Estava no código do Linux desde a versão 2.6.22, disponibilizada em Setembro de 2007.
  - https://dirtycow.ninja/

Vulnerabilidades

- Stack Clash (Junho/2017)
  - É uma vulnerabilidade em diversos sistemas operacionais que permite corromper regiões de memória e executar código com privilégio do kernel.
  - Afetou Linux, OpenBSD, NetBSD, FreeBSD e Solaris.
  - https://blog.qualys.com/securitylabs/2017/06/19/the-stack-clash

Vulnerabilidades

- Broadpwn (Julho/2017)
  - Vulnerabilidade no chipset Wi-Fi da Broadcom que permite a execução de código no chip
  - A vulnerabilidade pode ser explorada remotamente e sem a interação do usuário.
  - Afeta milhões de dispositivos que utilizam a família chips Wi-Fi Broadcom BCM43xx, com por exemplo dispositivos Android e iOS.
  - https://www.blackhat.com/us-17/briefings/schedule/#broadpwn-remotely-compromising-android-and-ios-via-a-bug-in-broadcoms-wi-fi-chipsets-7603
  - Em abril/2017 o pessoal do Project Zero publicou uma vulnerabilidade semelhante:
  - https://googleprojectzero.blogspot.com.br/2017/04/over-air-exploiting-broadcoms-wi-fi_4.html

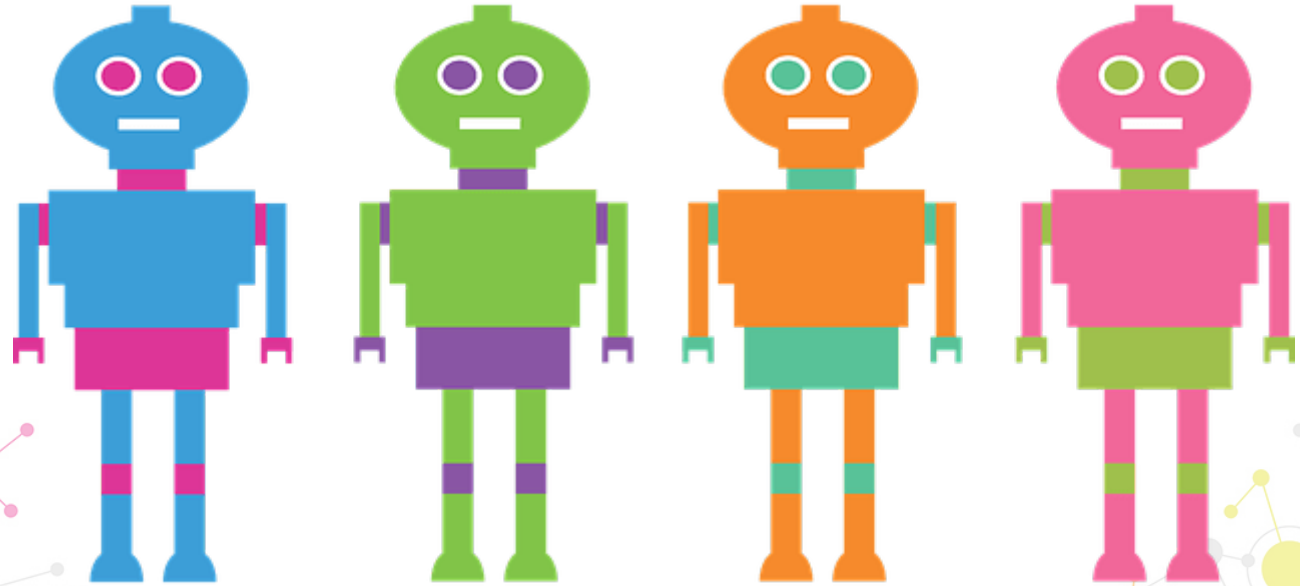
Vulnerabilidades

- Vulnerabilidade no protocolo SS7 (2008)
  - SS7 é um conjunto de protocolos desenvolvidos na década de 1970 utilizado na comunicação entre telefones de diferentes operadoras.
  - Permite redirecionar ligações e SMS para outros dispositivos, o que torna a autenticação com dois fatores (2FA) usando celular insegura.
  - https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls

Qual o motivo de tantas vulnerabilidades?

Social Bot

- Softwares que simula o comportamento humano de forma automática nas redes sociais (e.g. Facebook e Twitter).



Social Bot

- Utilização
  - Aumentar a visibilidade de uma conta.
  - Fazer propaganda (spamming).
  - Diminuir a credibilidade de outra conta através de contas falsas.
  - Ofuscar mensagens/notícias importantes através de uma grande quantidade de publicações sobre outros assuntos.
  - Influenciar a opinião pública, manipulando os trends topics ou repetindo publicações sobre o mesmo assunto.

Social Bot

- Casos reais:
  - Processo de Impeachment da presidente Dilma (2015)
  - Eleição de Trump nos EUA
- Computational Propaganda in Brazil: Social Bots during Elections

http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Brazil-1.pdf

Como detectar publicações manipuladas?

Data Leak

- É a divulgação de dados privados ou confidenciais.
- Pode ocorrer devido ao roubo de um dispositivo, invasão de sistemas computacionais, divulgação proposital, etc.

Data Leak

- PlayStation Network – serviço de mídia e entretenimento da Sony, bastante utilizado pelo usuários do console PlayStation.
- Dados de 77Mi de usuários foram comprometidos por invasores em Abril/2011.
- https://en.wikipedia.org/wiki/2011_PlayStation_Network_outage

PLAYSTATION®
Network

Data Leak

- LinkedIn – rede social com o objetivo de conectar profissionais.
- 117Mi de contas comprometidas em 2012 foram divulgadas online em Maio/2016.
- https://techcrunch.com/2016/05/18/117-million-linkedin-emails-and-passwords-from-a-2012-hack-just-got-posted-online/

Data Leak

- Dropbox – serviço de hospedagem de arquivos.
- 68Mi de contas (email e hash da senha) comprometidas em 2013, mas só foi divulgado em Agosto/2016.
- https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

Data Leak

- Tumblr – serviço de blog e rede social.
- 65Mi de contas (email e senha) comprometidas em 2013.
- https://nakedsecurity.sophos.com/2016/05/31/65-million-tumblr-passwords-stolen-and-up-for-sale/

Data Leak

- Yahoo – provedor de serviços web, tais como e-mail e messageiro.
- 1B de contas comprometidas em Agosto/2013, mas só foi divulgado em Dezembro/2016.
- https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached

Data Leak

- Slack – serviço em nuvem para colaboração entre equipes de desenvolvimento.
- Invasores tiveram acesso à base de usuários em Março/2015.
- https://techcrunch.com/2015/03/27/slack-got-hacked/

Data Leak

- Minecraft – jogo de ação em 2D.
- 7Mi de contas vazadas de um servidor em Abril/2016.
- https://motherboard.vice.com/en_us/article/bmvj9m/another-day-another-hack-7-million-emails-and-hashed-passwords-for-minecraft

Data Leak

- AdultFriendFinder – rede social para encontros.
- Invasores tiveram acesso aos dados de 73Mi de usuários.
- https://nakedsecurity.sophos.com/2016/10/21/millions-of-adultfriendfinder-user-accounts-hacked-again/

Data Leak

- Snapchat – aplicativo de mensagens através de imagens e videos.
- 1.7Mi de contas vazadas em Abril/2017.
- http://www.bgr.in/news/indian-hacker-group-leaks-data-of-1-7-million-snapchat-users-after-ceos-poor-country-comments-report/

Data Leak

- Verizon – uma das maiores empreses de telecomunicações dos EUA.
- Dados de 14Mi de clientes vazados em Julho/2017 (número do telefone, nome e PIN).
- http://money.cnn.com/2017/07/12/technology/verizon-data-leaked-online/index.html

Data Leak

- Rainbow Table Attack
- https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

Data Leak

- Como saber se tive meus dados vazados?
  - https://haveibeenpwned.com/
  - https://leakbase.pw/
  - https://leakedsource.ru/

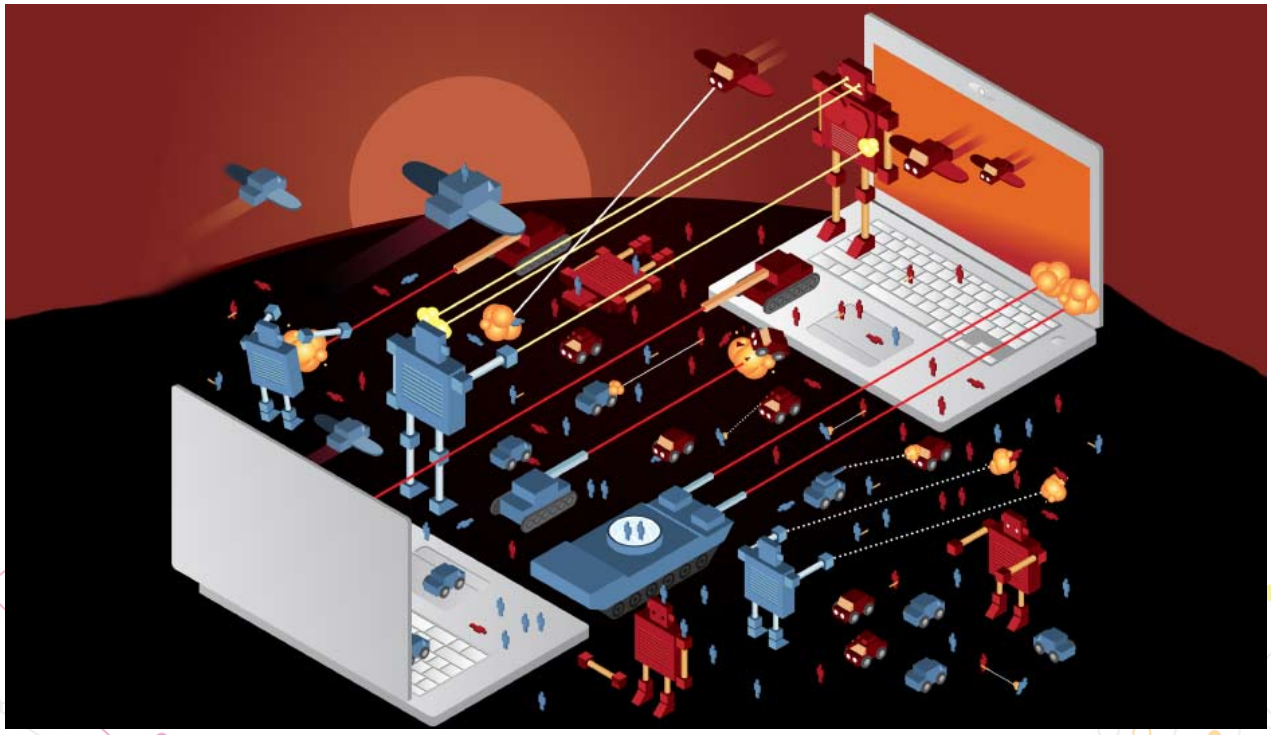
Qual a responsabilidade dos usuários e provedores de serviços sobre os dados que são vazados na internet?

Espionagem, Guerra e Vigilância Cibernética

- Espionagem é prática de obter informações de caráter sigiloso, sem a autorização dos donos, para obter alguma vantagem.

Espionagem, Guerra e Vigilância Cibernética

- Ciberguerra é a guerra onde a batalha ocorre através de meios eletrônicos e informáticos e não com armas físicas.



Espionagem, Guerra e Vigilância Cibernética

- Vigilância é a atividade de monitoramento e acompanhamento de comportamento e atividades.
- Atinge profundamente o direito à privacidade, sendo usada também para limitar direitos políticos e liberdades individuais.

Espionagem, Guerra e Vigilância Cibernética

- Stuxnet (2010)
  - Malware identificado em 2010 criado para sabotar o programa nuclear do Irã.
  - Documentary Zero Days
  - To Kill a Centrifuge

    https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
  - Adventures in Analysing Stuxnet

    https://media.ccc.de/v/27c3-4245-en-adventures_in_analyzing_stuxnet

Espionagem, Guerra e Vigilância Cibernética

- Duqu (2011)
  - Conjunto de malwares identificados em 2011 que tinham o propósito de coletar informações. O Duqu está relacionado ao caso Stuxnet.
  - Duqu: A Stuxnet-like malware found in the wild

    http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf
  - W32.Duqu: The precursor to the next Stuxnet

    http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Espionagem, Guerra e Vigilância Cibernética

- Flame (2012)
  - Malware descoberto em 2012, utilizado para espionar países do oriente médio.
  - sKyWIper: A complex malware for targeted attacks

    http://www.crysys.hu/skywiper/skywiper.pdf

Espionagem, Guerra e Vigilância Cibernética

- Bundestrojaner
  - Malware descoberto em 2011, utilizado pela polícia alemã para espionar civis suspeitos.
  - https://ccc.de/en/updates/2011/staatstrojaner
  - https://nakedsecurity.sophos.com/2016/02/24/german-police-given-go-ahead-to-use-home-brewed-spying-trojan/

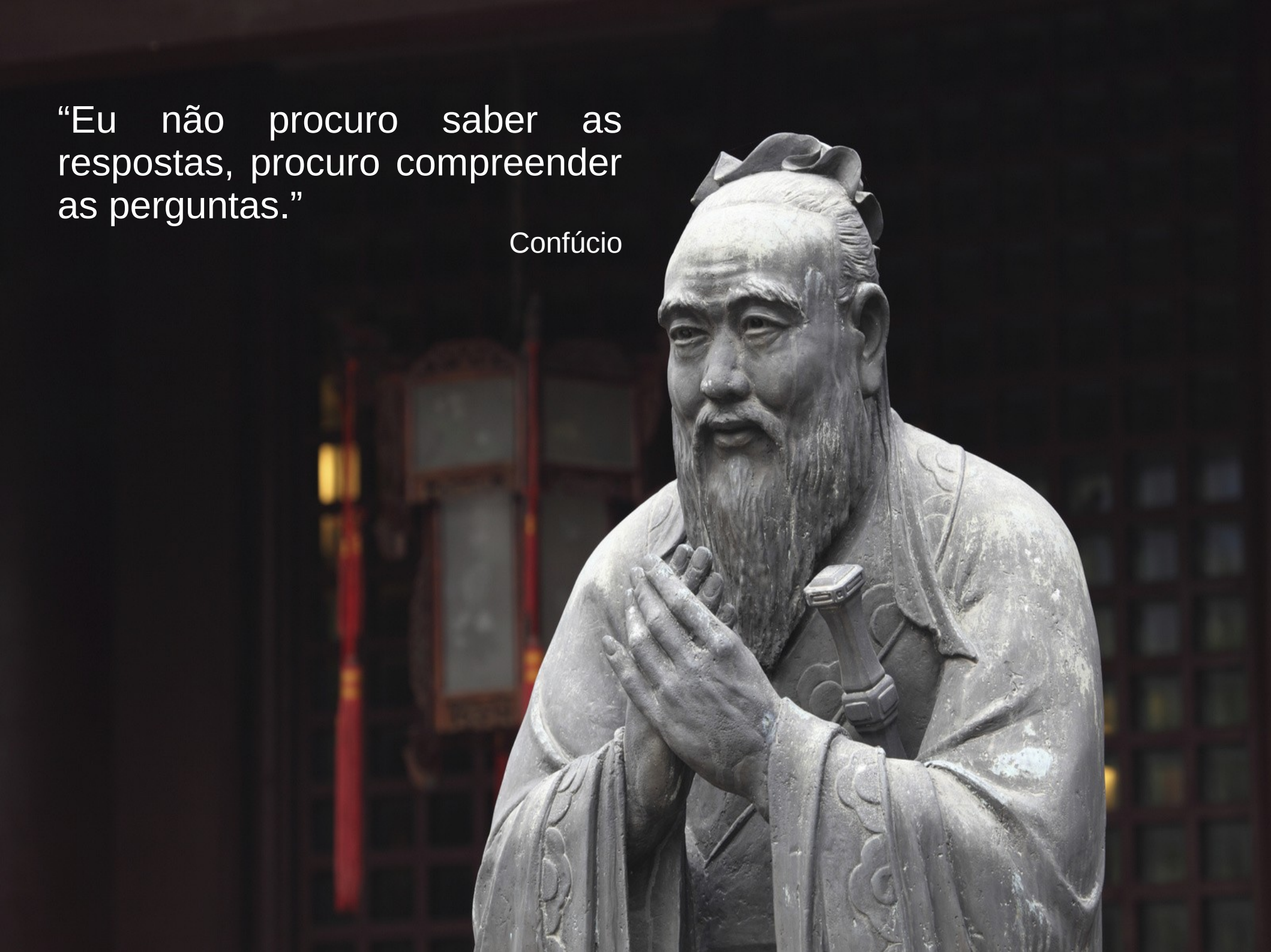
Espionagem, Guerra e Vigilância Cibernética

- Edward Snowden
  - Vazou informações da NSA em 2013, revelando vários programas de espionagem e vigilância cibernética.
  - https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet

Espionagem, Guerra e Vigilância Cibernética

- Vault 7 (2017)
  - Série de documentos que começaram a ser divulgado em Março/2017 no Wikileaks com informações sobre projetos de ciber espionagem da CIA.
  - Quantidade de dados muito maior que o vazamento causado por Snowden.
  - Novos malwares: Fulcrum, AfterMidnight, Assassin, HighRise, Grasshopper, Athena, Hera, etc.
  - https://wikileaks.org/vault7/

Quais as consequências de uma guerra cibernética?


“Eu não procuro saber as respostas, procuro compreender as perguntas.”
Confúcio