Introdução aos Sistemas de Informação

Segurança

Autores:

Carolina Silva Figueiredo
Ellen Christina Amaral Santana
João Vítor da Silva
Ricardo Mendes Paduan
Israel Lúcio De Lima Vaz
Wellington Marcio da Silva
Nathan Estevão Santos

Temas

- ➔ *Criptografia*
- ➔ *HASH*
- ➔ *Certificação Digital*
- ➔ *Malware*
- ➔ *Phishing*
- ➔ *Ransomware*
- ➔ *DDoS*

Criptografia

O que é?

- Criptografia é a prática de codificar e decodificar dados.
- Trata-se de um conjunto de regras que visa codificar a informação de forma que só o emissor e/ou receptor consiga decifrá-la.

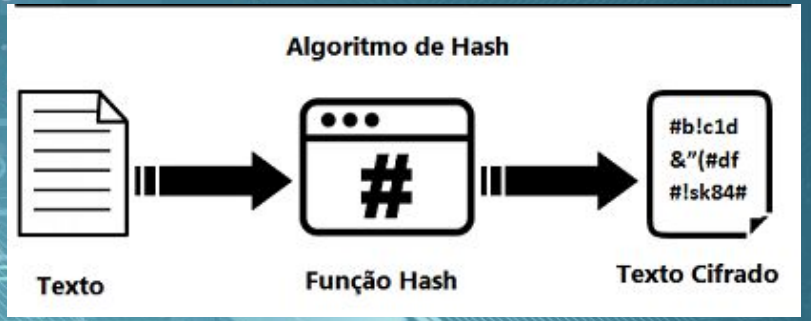
Quando deve ser usada?

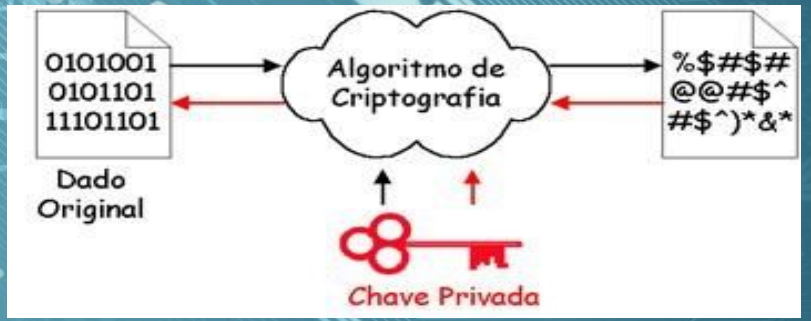
- Esse recurso é amplamente utilizado com o intuito de evitar invasões de pessoas mal-intencionadas às mensagens e arquivos salvos em diferentes formatos.

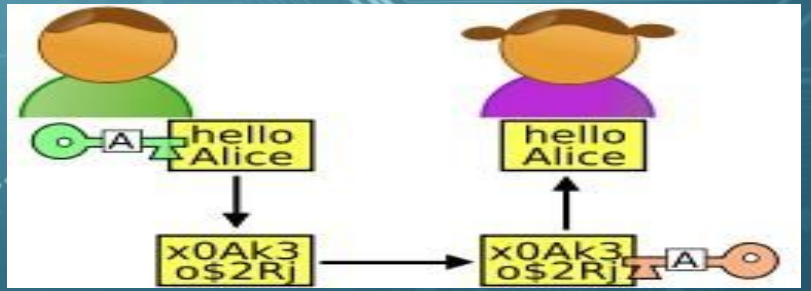
- Atualmente, a criptografia é amplamente utilizada na Web, em segurança a fim de autenticar os usuários para lhes fornecer acesso, na proteção de transações financeiras e em redes de comunicação.

Tipos de Criptografia

- Algoritmo de Hash
- Chaves Simétricas
- Chaves Assimétricas



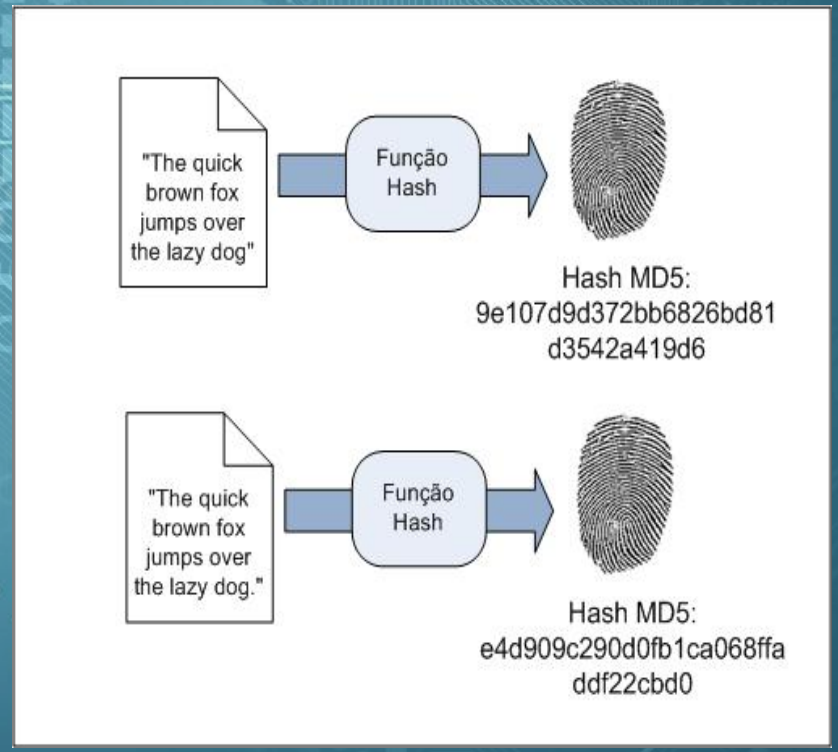





Hash

Oque é?

- Uma função hash é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. Os valores retornados por uma função hash são chamados valores hash, códigos hash, somas hash, checksums ou simplesmente hashes.
- Dessa forma, as funções Hash são largamente utilizadas para buscar elementos em bases de dados, verificar a integridade de arquivos baixados ou armazenar e transmitir senhas de usuários.



Como é utilizado?

- Através de um arquivo suspeito de vírus, o Hash tem função de extrair o código genético do arquivo e descobrir se foi ou não alterado.
-

Exemplos de aplicações com Hash:

A criptografia hash é utilizada para:

- Resumir dados.
- Verificar integridade de arquivos.
- Garantir a segurança de senhas dentro de um servidor.

Usando método Hash:

- Na verificação de integridade, aplica-se a função Hash diretamente sobre o dado e salva-se o resumo gerado. Após o dado ser transmitido para o receptor, este calcula o resumo sobre o dado recebido e obtém um novo resumo. Se os resumos forem iguais, assume-se que o dado é igual. Se forem diferentes, recomenda-se um novo download do arquivo.
- Já para o armazenamento da senha de forma segura, usa-se um procedimento semelhante. No servidor, apenas o resumo da senha do usuário é armazenado. Quando o usuário insere a senha, calcula-se a função Hash da senha e o servidor compara com o resumo armazenado. Se os resumos forem iguais, o usuário é autenticado.

Certificação digital

Oque é?

- A Certificação Digital é a tecnologia que, por meio da criptografia de dados, garante autenticidade, confidencialidade, integridade e não repúdio às informações eletrônicas.
- Trata-se de um documento digital utilizado para identificar pessoas e empresas no mundo virtual.

Exemplos

- e-CPF
- e-CNPJ
- NF-e
- CRM Digital
- Certificado Digital OAB
- Certificado Digital de Atributo
- CT-e
- E-mail seguro pessoal

Como são utilizados?

- Assinar e enviar documentos pela internet, por meio da Assinatura Digital;
- Fazer transações bancárias;
- Enviar as declarações da sua empresa, como ECF de pessoa jurídica;
- Fazer login em ambientes seguros;
- Assinar NF-e, escriturações contábeis e fiscais;
- Acessar os serviços do CNES (Cadastro Nacional de Entidades Sindicais);
- Fiscalizar e registrar os serviços de transporte de carga entre duas empresas;
- Acessar o Portal da Receita Federal e-CAC;
- Habilitar a e-CNH em seu celular;
- Participar de leilões eletrônicos;
- Criar procurações eletrônicas.

Como é feita a segurança das informações

- Todo Certificado Digital tem uma Chave Pública ou Privada, isto é, um nome e um número exclusivo que garante segurança ao usuário. Essa chave compõe um sistema de criptografia assimétrica, onde os dados só conseguirão ser acessados se o receptor tiver a chave correta para decodificá-los.

- Essas duas chaves são geradas aleatoriamente por funções matemáticas e trabalham em conjunto. Tudo que uma assina, somente a outra é capaz de autenticar. Essas características trazem maior segurança ao documento.

Tipos de certificados digitais

- Tipo A (certificado de assinatura digital)
- Tipo S (certificado de sigilo/ confidencialidade)
- Tipo T (certificado de tempo)

Como é feito o armazenamento das informações?

- Armazenado no computador
- Em mídias criptográficas Token ou Cartão
- No servidor (Certificado Digital SSL)
- HSM (Hardware Secure Module)
- Certificado Digital na nuvem
- No dispositivo móvel


Malware

Oque é?

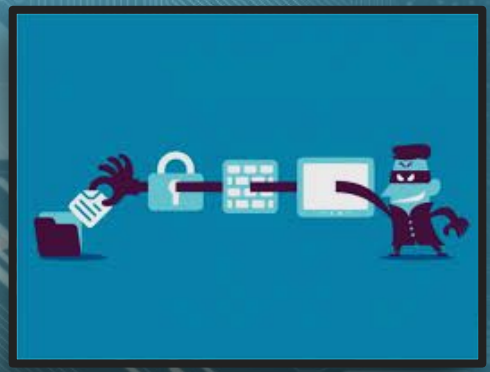
- Malware vem do inglês ***Mal****iciuos* *Soft****ware*** (Software Malicioso);
- Trata-se de um software codificado com a intenção de danificar dispositivos, roubar dados e causar danos às pessoas, embora não tenha a capacidade de interferir no hardware.
- Qualquer tipo de dispositivo pode ser alvo de um malware, sejam elas, Android, Windows, Mac, Apple, etc.

Exemplos

- Vírus
- Cavalos de Tróia
- Spywares
- Ransomwares
- Worms
- Adware
- Botnets

Como são utilizados?

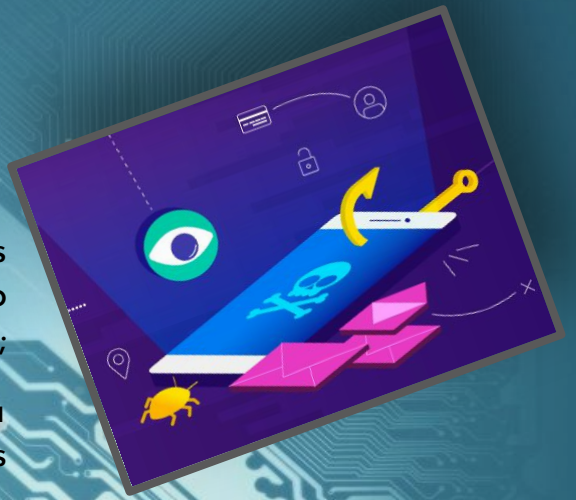
- Frequentemente desenvolvido por times de hackers;
- Usados em sua maioria como forma de fazer dinheiro, seja:
- Pela proliferação do malware;
- Por meio de leilão na Dark Web;
- Algumas vezes são usados como ferramentas de protesto;
- Para testes de segurança de rede;
- Ou até, como armas de guerra entre governos.



Como são implementados?

- As duas maneiras mais comuns de se infectar com um malware é através da internet e do email;
- Eles podem vir juntamente com algum arquivo (video, musica, jogo) que foi baixado em sites duvidosos da internet;
- Ou mesmo se esconder em arquivos em anexos recebidos pelo email, vindos de fontes desconhecidas;
- Além de poderem estar ocultos em aplicativos legítimos que foram baixados por fontes não confiáveis.

O que faz um malware?



- Cada tipo de malware tem uma funcionalidade diferente.
  - Vírus: prendem-se a arquivos limpos e infectam outros arquivos, pode se espalhar incontrolavelmente infectando funções centrais. Normalmente são arquivos executáveis (.exe);
  - Cavalo de Tróia: finge ser um software legítimo, ou se infiltra em um corrompido e discretamente cria entradas para outros malwares;
  - Spyware: se esconde em segundo plano e grava suas atividades online, incluindo usuários e senhas;
  - Worms: Infectam redes inteiras de dispositivos;
  - Adware: softwares agressivos de publicidade, que pode vir a abrir brechas na sua segurança permitindo a entrada de outros malwares;
  - Botnets: Redes de computadores infectados forçados a trabalharem juntos sob o controle de um invasor;

Como detectar e remover um Malware?

- Alguns malwares são mais fáceis de serem detectados, como por exemplo o adware. Possíveis sinais de que há um malware em seu dispositivo:
  - Computador lento;
  - Mensagens de pop-up;
  - Programas desconhecidos que se executam por conta própria;
  - Som do disco rígido em constante ação;
  - Perda de espaço em disco;
- Mas a melhor forma de detectá-los é com um anti-malware (ou antivírus), que escaneia o dispositivo em busca dos malwares antes que eles prejudiquem sua máquina;
- Como cada tipo de malware se executa de uma maneira, cada um deles tem uma forma diferente de ser removido, por isso é tão importante o uso de anti-malwares.

Phishing

Oque é?

Phishing é um termo originado do inglês (fishing) que em computação se trata de um tipo de roubo de identidade online. Essa ação fraudulenta é caracterizada por tentativas de adquirir ilicitamente dados pessoais de outra pessoa, sejam senhas, dados financeiros, dados bancários, números de cartões de crédito ou simplesmente dados pessoais.

Como são utilizados?

- Falsos e-mails ou mensagens
- Ataque aos arquivos do Google Docs
- Peixe grande
- Phishing por ransomware
- Vishing

Como pode ser evitado?

- Desconfie de todos os e-mails que receber
- Mantenha seu sitema atualizado
- Mantenha antivirus e firewall atualizados
- Crie uma politica de rejeição de dominios
- Blinde os executivos de maior poder de decisão
- Avalie sua interação com clientes

evite os arquivos:
.exe, .src, .pif, .cmd, .com, .cpl, .bat, .vir

Ransomware

Oque é?

- Ransomware é um tipo de software malicioso projetado para bloquear o acesso a um sistema de computador ou arquivos de computador até que uma quantia em dinheiro seja paga.
- O ransomware geralmente é instalado quando você abre um anexo mal-intecionado em uma mensagem de e-mail ou quando clica em um link mal-intecionado.

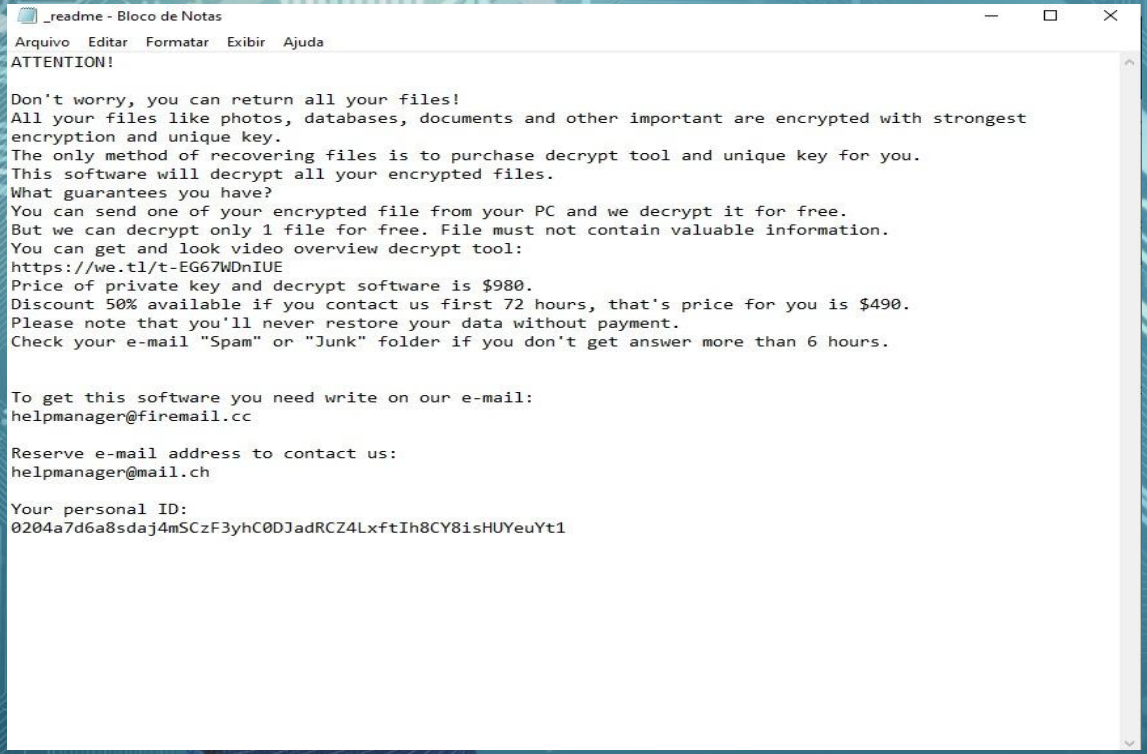
A economia do Ransomware

- De acordo com o DOJ(Departamento De Justiça dos Estados Unidos), uma média de 4.000 ataques de ransomware ocorreram por dia em 2016 nos EUA, um aumento de 4x em relação a 2015. O FBI relata que mais de $ 1 bilhão em resgates foram pagos em 2016, contra 240 milhões em 2015.
- O ransomware é simples de criar e distribuir, entre os cibercriminosos é um negócio muito rentável com plano de ação muito claro e ganho direto.

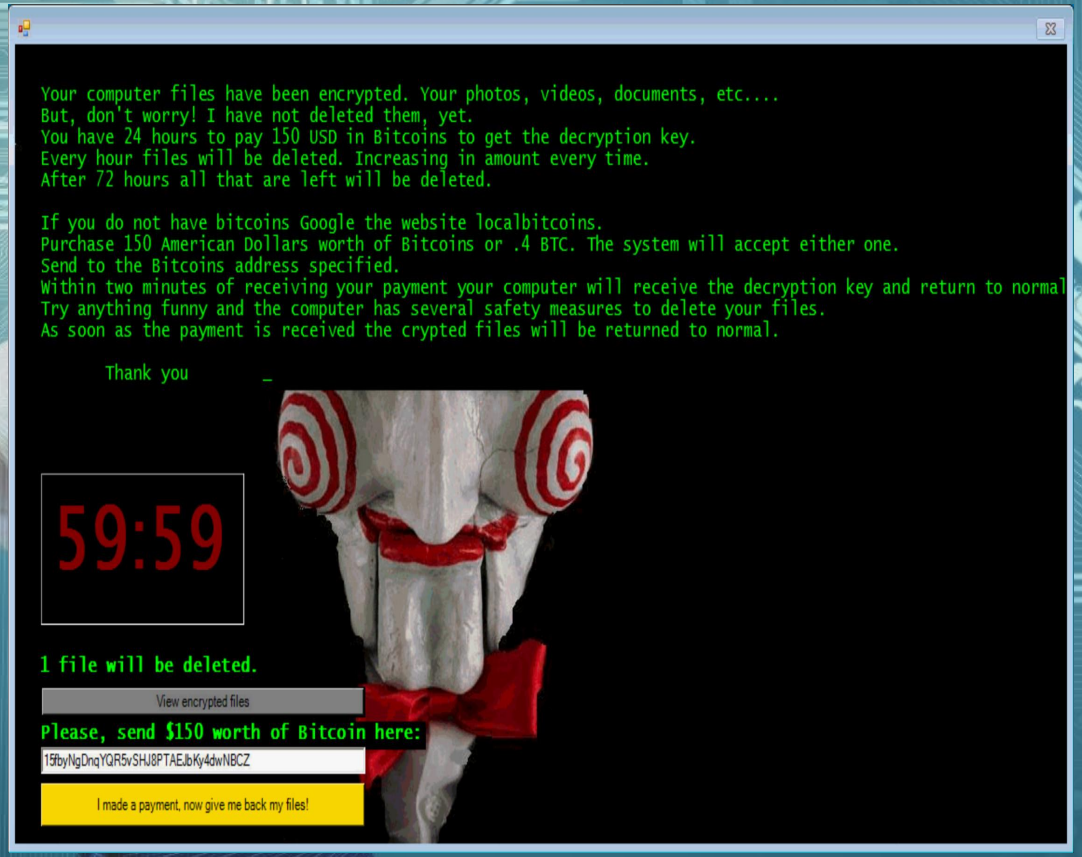
Por que é tão eficaz ?

- Os fornecedores de ransomware costumam ser especialistas em marketing eletrônico. Ransomware exibe mensagens intimidantes semelhantes às seguintes:
- "Seu computador foi usado para visitar sites com conteúdo ilegal. Para desbloquear o computador, você deve pagar uma multa de $100."
- "Todos os arquivos em seu computador foram criptografados. Você deve pagar este resgate dentro de 72 horas para recuperar o acesso aos seus dados."

Exemplos


_readme - Bloco de Notas
Arquivo Editar Formatar Exibir Ajuda
ATTENTION!
Don't worry, you can return all your files!
All your files like photos, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-EG67WDnIUE
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.
To get this software you need write on our e-mail:
helpmanager@firemail.cc
Reserve e-mail address to contact us:
helpmanager@mail.ch
Your personal ID:
0204a7d6a8sdaj4mSCzF3yhC0DJadRCZ4LxftIh8CY8isHUYeuYt1

Exemplos


Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.
If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.
Thank you
59:59
1 file will be deleted.
View encrypted files
Please, send $150 worth of Bitcoin here:
15fbyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ
I made a payment, now give me back my files!

O que devo fazer se for infectado ?

- Desconectar de dispositivos externos.
- Desconectar das redes.
- Ter um backup.
- Nunca pague o resgate.

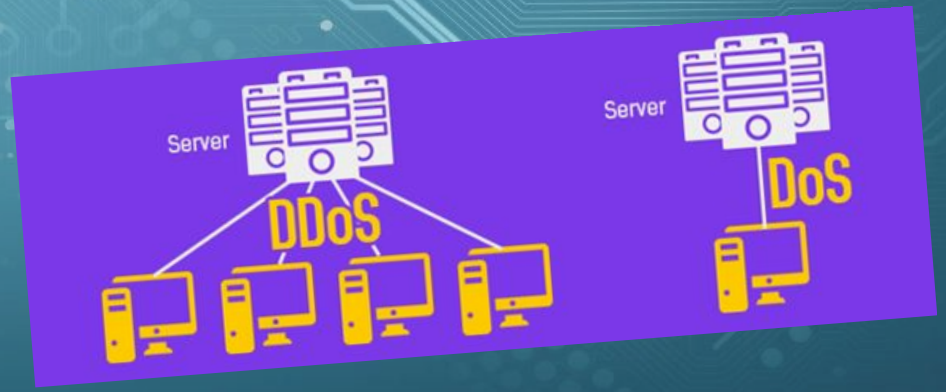
DDoS

Oque é?

- DoS é o acrônimo de Denial of Service, que é um ataque feito por um hacker com o intuito de sobrecarregar um servidor ou um computador esgotando seus recursos como memória ou processamento, fazendo o mesmo ficar indisponível para acesso de qualquer outro usuário que tente.

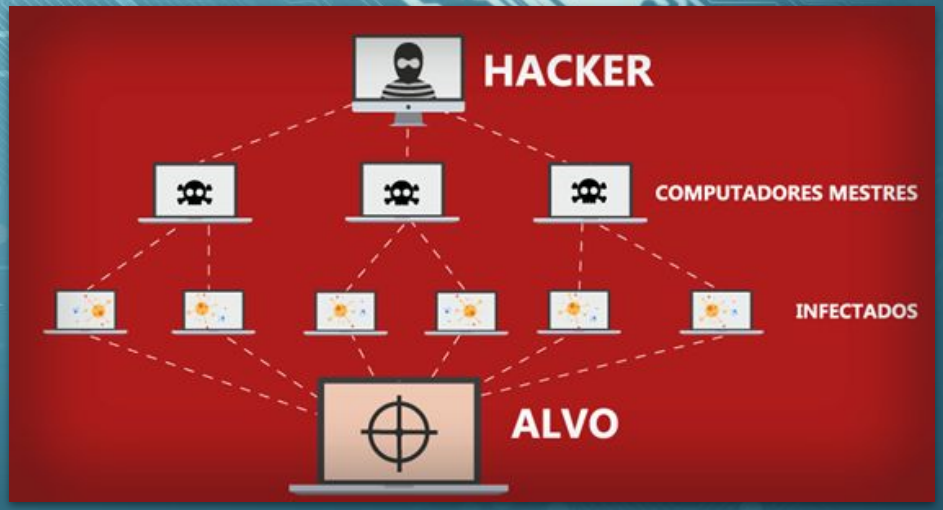
Exemplos

- Flood (mais comum)
- UDP Flood
- NTP Flood
- SYN Flood
- VOiP
- POD (Ping of death)



DoS e DDoS

- A única diferença entre o ataque DoS e DDoS é que o DoS é iniciado de uma única máquina, enquanto o ataque DDoS é realizado por várias máquinas juntamente com as botnets.

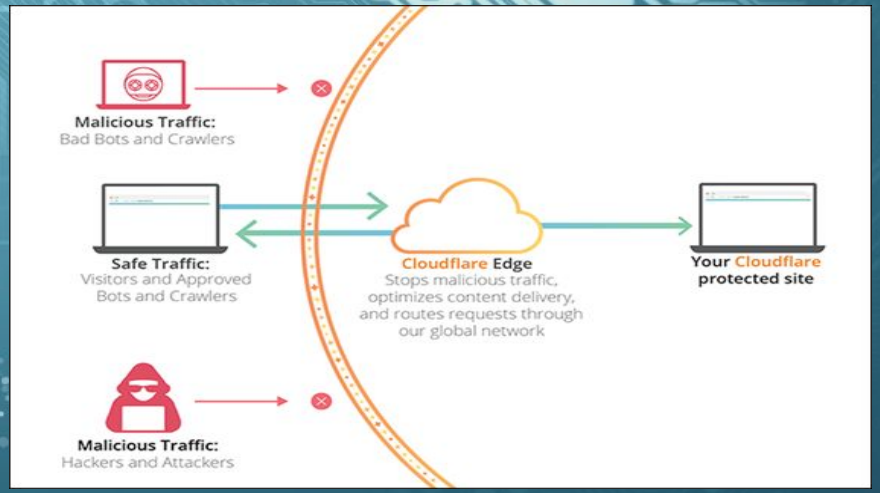


Como funciona o ataque DDoS

- Largura de Banda é a capacidade que o servidor do seu site consegue aguentar com pessoas acessando simultaneamente.
- Botnets são computadores infectados com malware, onde o hacker consegue tomar conta dele para fazer ataque DDoS.
- Ataque via banda ou Flood é quando o hacker, com o uso de botnets realiza inúmeras solicitações para um servidor de diversos pontos da internet para um destino único, até o momento em que a banda do servidor não comporte mais toda a demanda de solicitações e pare de funcionar ou se torne muito lento.

Como evitar um ataque DDoS

- O principal meio para se evitar um ataque DDoS, é expandindo a largura de banda do servidor do site, para que ele consiga, mesmo sob ataque continuar funcionando, até o problema ser resolvido, e também ter uma equipe de TI por perto para conseguir resolver o problema.
- Uso de um firewall como o CloudFlare.



Curiosidade

- Maior ataque já anunciado, aconteceu em Fevereiro de 2018, no site do github tendo um tráfego de dados de 1,35 terabits por segundo, utilizando amplificação e DNS Spoofing, atacando a memória memcache D do site.

Unificação dos Tópicos

- Podemos ver que em segurança trabalham os 3 temas criptografia, hash e certificação digital, tentando inibir qualquer ataque de hackers, seja roubando informações para uso próprio, ou inutilizando serviços de alguns sites, ou derrubando servidores, como citados nos outros temas, fornecendo mais segurança para uso de softwares, hospedagens de servidores mais seguras e maior confiabilidade em uso de serviços on-line para guardar os seus dados, deixando claro que por trás de qualquer serviço ou software, existe um grande projeto de segurança.

Referências

- Certificação Digital
  - https://blog.certisign.com.br/o-que-e-certificado-digital/
  - https://www.senior.com.br/blog/conheca-os-tipos-de-certificados-digitais-e-suas-vantagens
  - https://pt.wikipedia.org/wiki/Certificado_digital
- Malware
  - https://www.avg.com/pt/signal/what-is-malware
  - https://br.malwarebytes.com/malware/
- DDoS
  - https://www.hostinger.com.br/tutoriais/o-que-e-ddos-e-como-se-proteger-de-ataques
  - https://www.bravulink.com.br/o-que-e-cloudflare

Referências

- DDoS
  - https://tudosobrehospedagemdesites.com.br/trafego-transferencia-largura-de-banda/
  - https://www.iplocation.net/denial-of-service
  - https://support.cloudflare.com/hc/en-us/articles/205177068-How-does-Cloudflare-work-
  - https://www.analyticsvidhya.com/blog/2015/07/github-special-data-scientists-to-follow-best-tutorials/
- Criptografia
  - https://www.kaspersky.com.br/resource-center/definitions/encryption
  - https://www.docusign.com.br/blog/criptografia-o-que-e-e-quando-ela-deve-ser-usada

Referências

- Criptografia
  - https://www.kaspersky.com.br/resource-center/definitions/encryption
  - https://www.docusign.com.br/blog/criptografia-o-que-e-e-quando-ela-deve-ser-usada
  - https://pt.wikipedia.org/wiki/Criptografia
  - https://www.gta.ufrj.br/grad/07_1/ass-dig/TiposdeCriptografia.html
- Ransomware
  - https://www.cybereason.com/blog/how-does-ransomware-work
  - https://security.berkeley.edu/faq/ransomware#faq-top
  - https://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html
  - https://www.youtube.com/watch?v=rmoeBbvFObM&ab_channel=TecMundo

Referências

- Ransomware
  - https://www.codigofonte.com.br/noticias/ransomware-jigsaw-se-inspira-no-filme-jogos-mortais
- Phishing
  - https://support.mozilla.org/pt-BR/kb/como-funciona-protecao-contra-phishing-e-malware
  - https://canaltech.com.br/seguranca/O-que-e-Phishing/
  - https://tecnoblog.net/278419/golpe-phishing-itau-itaucard/


Obrigado!!