**Instituto Federal de Educação, Ciência e Tecnologia do Ceará**

**Disciplina: Redes de Computadores Prof. Nídia S. Campos**

**Trabalho 1 - Pesquisa de Tipos de Malwares e Ataques DoS na Internet**

**EQUIPE: Francisco Lucas // Juliana Cardoso**

**OBJETIVO**

* Conhecer tipos de malwares e ataques DDoS/DoS na Internet.

**TAREFAS**

**TAREFA 1**. Pesquisar na Internet por três **vírus** conhecidos e explique como eles funcionam ou atuam em um host.

**Conficker**

Mesmo com mais de dez anos de existência e métodos de remoção efetivos, o Conficker continua infectando computadores. Em seu auge, o vírus infectou mais de 15 milhões de máquinas e causou milhões de prejuízos para negócios e até governos.

O Conficker ataca principalmente pela internet e mídias removíveis, como pen drives. Depois de invadir o sistema, o vírus cria uma espécie de rede com os computadores infectados. Essa rede distribui conteúdo indesejado, realiza ataques de DDoS (ataques de negação de serviço) e rouba dados de usuários.

**Ramnit**

Outro malware que entra na lista dos vírus mais conhecidos é o Ramnit, que também se espalha por dispositivos removíveis. O Ramnit infecta programas executáveis, com extensão \*.exe, com o objetivo de roubar dados como arquivos do HD e cookies dos navegadores.

Esse vírus também utiliza e-mails de spam para se espalhar, por isso, sempre verifique a origem da mensagem. Os antivírus gratuitos atuais já conseguem detectar e remover com sucesso esse worm.

**Sality**

O Sality é uma família de vírus mais conhecida por oferecer grandes riscos. Ao invadir o computador, este vírus infecta programas pré-instalados (como Bloco de Notas) e ainda pode apagar arquivos com determinadas extensões.

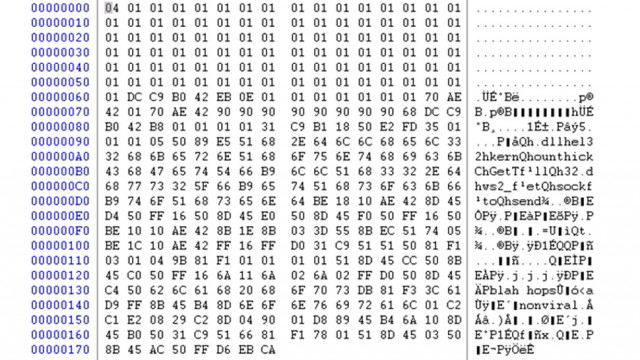
Além de deletar seus arquivos, o programa pode diminuir a segurança do PC, baixar e executar novos arquivos e roubar dados.

Seu combate foi difícil justamente pela inteligência do vírus. Ao detectar que um antivírus iria atacá-lo, o Sality fechava a janela antes que a ação fosse realizada. Manter o computador atualizado com um antivírus é o suficiente para se proteger.

**TAREFA 2.** Pesquisar na Internet por três **worms** conhecidos e explique como eles funcionam ou atuam em um host.

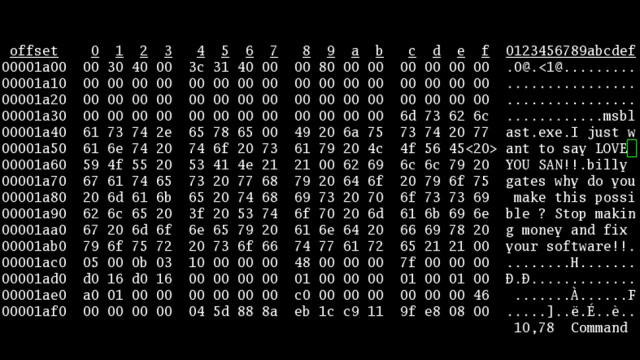
**SQL Slammer (2003)**

Este worm atacou servidores web rodando uma versão vulnerável do Microsoft SQL Server, e gerava endereços IP aleatórios a fim de infectar outros computadores. É incrível como o Slammer era pequeno: ele poderia caber no espaço de cinco tweets. Eis todo o código em hexadecimal:



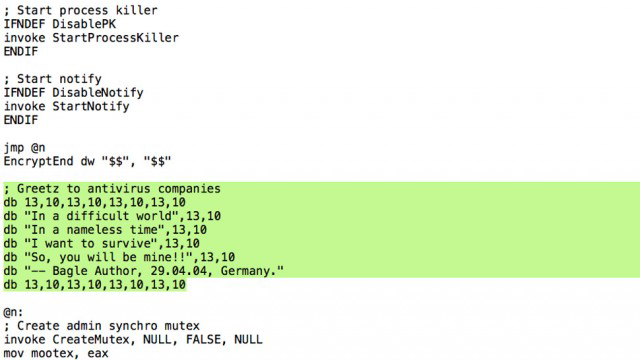
**Blaster, também conhecido como Lovsan e MSBlast (2003)**

Este worm infectou centenas de milhares de computadores através de uma falha de vulnerabilidade no Windows 2000 e Windows XP. Ele abria uma janela de diálogo, dizendo ao usuário que um desligamento do sistema era iminente. O autor escondeu duas mensagens no código: “Eu só quero dizer TE AMO SAN!” e “billy gates, por que você permite isso? Pare de ganhar dinheiro e conserte seu software!!”



**Bagle (2004)**

Este worm se espalhava como um anexo de e-mail, atacando todas as versões do Windows. Ele abria um backdoor onde um usuário remoto podia ganhar controle sobre o computador infectado. Notavelmente, o autor escreveu um pequeno poema no código:

  
Em um mundo difícil / Em um tempo sem nome / Eu quero sobreviver / Para que você seja minha!!

**TAREFA 3**. Pesquisar na Internet por três **cavalos de troia** conhecidos e explique como eles funcionam ou atuam em um host.

**ZBOT (também conhecido como Zeus) - 2006**

Reconhecido como o mais famoso cavalo de Troia, o Zeus é um toolkit que permite que um cibercriminoso crie malware disfarçados. O Zbot é usado para roubo de dados ou informações de contas. Monitora hábitos de navegação do usuário usando títulos da janela do navegador ou URLs da barra de endereços como acionadores de seus ataques. As variantes inserem um código JavaScript em páginas de sites bancários legítimos e coletam informações através de HTTP POST para URLs remotas. Em 2011, um código fonte de Zbot foi vazado em um site de compartilhamento de arquivos e rapidamente se espalhou em fóruns do submundo.

**EMOTET – 2014**

O malware chega como um anexo em mensagens de grayware ou como um arquivo baixado sem saber pelos usuários, quando visitam sites maliciosos. Uma vez no sistema, o malware baixa arquivos de componentes, inclusive um arquivo de configuração que contém informações de outros bancos visados. Em 2014, a atividade do EMOTET cessou, mas reapareceu rapidamente em janeiro de 2015.

**DYRE - 2015**

O DYRE chamou a atenção do setor de segurança devido a sua capacidade de evitar o SSL, uma medida de segurança para sites bancários. Depois que o malware é instalado no sistema, ele pode monitorar e fazer capturas de tela das atividades do navegador, realizar ataques “man-in-the-middle” através de injeções no navegador, roubar certificados de segurança pessoais, roubar credenciais bancárias online e rastrear a localização da vítima através de STUN (Session Traversal Utilities for NAT).

**TAREFA 4**. Pesquisar na Internet por três **ataques DoS/DDoS recentes** conhecidos e explique como eles funcionam ou atuam em um host.

**“Quebrando a internet: estamos sofrendo o maior ataque DDoS da história”**

Um grande ataque de negação de serviço, DDoS, aos servidores do Dyn está causando problemas em diversos sites e plataformas utilizados por milhões de usuários, que estão sentindo instabilidade na navegação e uso. Entre os serviços afetados, estão o Twitter, o Spotify, o Reddit, a PlayStation Network, o Imgur e muitos outros.

A Dyn é uma das maiores companhias que compreende servidores de sites, por isso, o ataque DDoS ainda não foi quantificado, mas deve ter sido gigantesco — recentemente, noticiamos um ataque de negação de serviço que ultrapassou 1 TB por segundo. O DDoS teve início na manhã dessa sexta-feira (21) e, de acordo com a Dyn, todos os serviços já foram restaurados. Ao que parece, estamos passando pelo maior ataque DDoS da história.

Usuário de internet nos Estados Unidos e na Europa foram os mais afetados, porém, também foram sentidos reflexo na América do Sul, com Brasil, Uruguai e Argentina; e na Índia e Austrália. O Twitter, por exemplo, está com a conexão "pipocando" no Brasil. Já a PlayStation Network está fora do ar.

Fonte:<https://www.tecmundo.com.br/ataque-hacker/110842-grande-ataque-ddos-afeta-twitter-psn-spotify-outros-estragos.htm>

**“Maior ataque DDoS da história atinge o site GitHub”**

Um ataque hacker de proporções jamais vistas foi detectado pela equipe do site GitHub, mais famoso repositório de códigos na internet. O ataque DDoS aconteceu no dia 28 de fevereiro e teve picos de tráfego de até 135 Terabits por segundo.

Nesse tipo de ataque, servidores são atingidos com uma carga fora do normal de acessos. Se os servidores não suportarem a carga, o serviço que eles fornecem pode sair do ar. Foi o que aconteceu com o GitHub durante 10 minutos na última quarta.

Para gerar uma onda de acessos tão grande, hackers geralmente utilizam uma botnet - isto é, uma rede de dispositivos com conexão à internet que, por meio de vírus, são controlados remotamente e se transformam em "zumbis".

Fonte: <https://olhardigital.com.br/fique_seguro/noticia/maior-ataque-ddos-da-historia-atinge-o-site-github/74379>

**“Maior ataque DDoS da história atinge servidores da CloudFlare”**

Um ataque DDoS (ou ataque de negação de serviço) de grandes proporções atingiu servidores europeus e norte-americanos da empresa CloudFlare, responsável por uma rede de distribuição de conteúdo. De acordo com o CEO da companhia [Matthew Prince](https://twitter.com/eastdakota/status/433002992694874112), o volume total de tráfego chegou a incríveis 400 gigabits por segundo, tornando este o maior golpe do tipo já visto na web.

O ataque teve como alvo inicial um dos clientes do serviço, não nomeado, e usou reflexão do Network Time Protocol (NTP) para aumentar sua amplitude. O protocolo é usado para sincronizar horários entre diferentes computadores pela rede, e o método do ataque faz pedidos falsos de sincronização aos servidores NTP, sempre usando o “nome” da vítima. Dessa forma, um fluxo enorme de respostas inunda o site-alvo – mais ou menos como demonstrado neste diagrama simples, [do The Hacker News](https://abrilexame.files.wordpress.com/2014/02/7bf42-abusingnetworktimeprotocol28ntp29toperformmassivereflectionddosattack.jpg?quality=70&strip=info).

A adoção da técnica é relativamente recente, mas ela de certa forma lembra os ataques baseados em DNS. O método foi utilizado no último maior ataque DDoS registrado, que atingiu servidores da Spamhaus, e consiste em forjar solicitações de buscas por endereços DNS usando a identidade do alvo e uma botnet. Os pedidos são enviados a servidores abertos, e todo tráfego gerado pelas respostas é redirecionado à página atacada. A sequência é mais ou menos a que está mostrada nesta ilustração divulgada [pelo SecurityAffairs](http://securityaffairs.co/wordpress/wp-content/uploads/2012/03/dns-amplification-attack-big.jpg).

Fonte:<https://exame.abril.com.br/tecnologia/maior-ataque-ddos-da-historia-atinge-servidores-da-cloudflare/>