Instituto Federal de Educação, Ciência e Tecnologia do Ceará

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

**Alunos**: Lucas Cunha, e Francisco Jorge

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

**0**. **Acesse o mapa de ciberameaças em tempo real da Kapersky (**[**https://cybermap.kaspersky.com/**](https://cybermap.kaspersky.com/)**) e registre estatísticas para um país do mundo diferente do Brasil.**

Rússia:

* KAS 2427671
* OAS 1721681
* WAV 973323
* ODS 678285
* IDS 461720
* MAV 57006
* VUL 11544
* RMW 7089
* BAD 170

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

**Malware** é um software malicioso projetado especificamente para roubo de dados, interceptação de informações, sequestro de dados para resgate, bombardeio de anúncios, danos físicos ao sistema, corrupção de dados ou simplesmente irritação.

Os ataques de **ransomware** são feitos através de um processo complexo de engenharia social, disseminado geralmente por meio de mensagens para usuários, simulando um conteúdo real e incentivando o download de um arquivo infectado. Com a abertura do arquivo, o ransomware busca brechas nos computadores/ sistemas que permitam acesso aos à dados privados, os criptografam e o acesso aos dados é completamente bloqueado. E como no nome do ataque (**ransom = resgate**), os proprietários são extorquidos a pagar pelo resgate dos dados sequestrados.

1. CovidLock, ransomware, 2020

Malware onde os cibercriminosos exploram o medo causado pelo COVID-19, infecta as vítimas via arquivo malicioso em um aplicativo que promete oferecer rastreamento da doença e estatísticas sobre a pandemia. E com o aplicativo instalado, o ransomware criptografa dados de dispositivos Android e nega acesso dos dados para as vítimas. Para liberar o acesso, era solicitado o resgate de USD 100,00 por dispositivo.

2. LockerGoga, ransomware, 2019

O LockerGoga é um ransomware que ganhou os noticiários em 2019 por infectar grandes corporações no mundo, como, por exemplo, a Altran Technologies e a Hydro. As infecções do LockerGoga envolvem e-mails maliciosos, golpes de phishing e também o roubo de credenciais, após sua instalação no sistema começa a fazer autocopia e alterações no seu registro para execução automática na inicialização do sistema, assim, começa a procurar por extensões de arquivos conhecidas (.doc, .ppt, .pdf, etc) e os criptografa, impedindo assim o usuário de acessá-los, e passa a deixar mensagens solicitado dinheiro e informações para o resgate. Em alguns casos enviam e-mail com uma nota solicitando o resgate, tenta trocar as senhas dos usuários e desabilitar os adaptadores de rede

3. CryptoLocker, ransomware, 2013

O CryptoLocker é um dos ransomwares mais famosos da história porque, quando foi lançado em 2013, utilizou uma chave de criptografia muito grande, o que dificultou o trabalho dos especialistas. Acredita-se que tenha causado prejuízos de mais de USD 3 milhões, infectando mais de 200 mil computadores com sistema Windows. Esse tipo de ransomware era distribuído principalmente via e-mail, por meio de arquivos maliciosos que se pareciam com arquivos PDF, mas, obviamente, não eram.

**2.** **Pesquisar na Internet por três worms conhecidos e explique como eles funcionam e atuam em um host consumindo recursos computacionais (memória, CPU) ou explorando a vulnerabilidade de uma aplicação.**

Os worms, ao contrário dos vírus, que necessitam que um arquivo infectado se espalhe e, até, da interação direta da vítima, são softwares independentes criando cópias de si mesmo em diferentes locais do sistema e se espalha para outras máquinas por meio de Internet, mensagens, conexões locais, dispositivos USB ou arquivos, se utilizando somente dos recursos do sistema.

1. ILOVEYOU, worm, 2000

O ILOVEYOU é um malware do tipo worm que se disfarçava como uma carta de amor, recebida via e-mail com anexos maliciosos, pedinfo ao usuário para verificá-la gentilmente. Notícias apontam que ele infectou mais de 50 milhões de pessoas nos anos 2000, causando mais de 15 bilhões de dólares em prejuízos. É considerado também um dos primeiros casos de engenharia social usados em ataques de malware. Uma vez executado, o ILOVEYOU, que tratava-se de um script em Visual Basic, o programa sobrescrevia arquivos no computador do usuário, como arquivos do pacote Microsoft Office, arquivos de áudio, imagens, entre outros, mandava uma cópia de si mesmo para todos os contatos do usuário no Outlook.

### 2. Stuxnet, worm, 2010

O Stuxnet foi usado em um ataque político, em 2010, ao o sistema operacional SCADA desenvolvido pela Siemens, utilizado no programa nuclear do Irã, e por explorar inúmeras vulnerabilidades do dia zero do Windows. Esse worm supersofisticado tem a capacidade de infectar dispositivos através de drives USB, não sendo necessária, portanto, conexão com a internet. Uma vez instalado, o malware Stuxnet é responsável por assumir o controle do sistema. Acredita-se que tenha sido desenvolvido a mando de algum governo.

### 3. MyDoom, worm, 2004

Em 2014, o worm MyDoom se tornou conhecido e famoso por atingir grandes empresas de tecnologia, como Google e Microsoft. Para atrair mais pessoas, ele era divulgado usando assuntos de e-mail chamativos, como, por exemplo, "Error", "Test" e "Mail Delivery System”. O MyDoom foi muito usado para ataques de [DDoS](https://gatefy.com/pt-br/postagem/o-que-e-um-ataque-ddos/) e como backdoor para permitir controle remoto. Os prejuízos são estimados, segundo notícias da época, em milhões de dólares

**3**. **Pesquisar na Internet por três cavalos de tróia conhecidos e explique como eles funcionam e atuam em um host com função backdoor, proxy ou keylogger.**

É um malware disfarçado em um software aparentemente normal, onde sua parte maliciosa passa despercebida aos olhos da vítima. Os usuários são, em geral, enganados carregando e executando-os em seus sistemas. Depois de ativado, ele pode causar vários ataques ao host, desde irritar o usuário (com janelas pop-up excessivas ou alterar a área de trabalho) até danificá-lo (excluir arquivos, roubar dados ou ativar e espalhar outros malwares, como vírus).

Cavalos de Tróia também são conhecidos por criarem portas dos fundos (back doors) que permitem o acesso de usuários mal-intencionados ao sistema. Ao contrário de vírus e worms, os cavalos de Tróia não se reproduzem infectando outros arquivos. Geralmente se espalha pela interação do usuário, como abrir um anexo de e-mail ou fazer o download e executar um arquivo da Internet.

1. 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 malwares 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.

2. CARBERP – 2009

O CARBERP registra as teclas digitadas pelo usuário, paródia sites e deliberadamente deixa uma cópia de si mesmo em locais que não exigem privilégios de administrador. Ele é caracterizado como um malware dependente de um plug-in pois depende de módulos baixados/incorporados para completar suas rotinas.

Recentemente retornou com versões aprimoradas, dispendiosas e variantes para aplicativos móveis disponíveis no mundo real. Baixar novos plug-ins para complementar suas rotinas de roubo de informações que ajudam um possível agressor a acessar remotamente um sistema infectado usado para monitorar sistemas de banco por Internet.

3. SHYLOCK – 2010

SHYLOCK é um spyware que tenta substituir os números de contato de determinados bancos por números que são controlados pelos agressores – levando os usuários infectados a divulgar informações bancárias e pessoais aos agressores. Os usuários podem ficar infectados visitando sites maliciosos.

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

Os ataques de negação de serviço (DoS) são a forma de ataque mais divulgada e uma das mais difíceis de eliminar. No entanto, devido à facilidade de implementação e danos potencialmente significativos, os ataques de negação de serviço merecem atenção especial dos administradores de segurança. Os ataques DoS assumem muitas formas. E, por fim, impedem que pessoas autorizadas usem um serviço ao consumir recursos do sistema. Para prevenir ataques (DoS) é importante manter em dia as mais recentes atualizações de segurança para sistemas operacionais e aplicações.

Já os ataques de negação de serviço distribuído (DDoS) aproveita os limites de capacidade específicos que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de uma empresa. O ataque DDoS envia múltiplas solicitações para o recurso Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto.

#### O ataque de fevereiro de 2020 divulgado pela AWS

A AWS divulgou que mitigou um gigantesco ataque de DDoS em fevereiro de 2020. No seu ápice, o ataque disparou um tráfego de entrada a uma taxa de 2,3 terabits por segundo (Tbps). A AWS não divulgou a qual cliente o ataque foi direcionado.

Os invasores responsáveis usaram servidores web sequestrados com Protocolo de Acesso Leve a Diretórios sem Conexão (CLDAP). O CLDAP é um protocolo para diretórios de usuários. Trata-se de uma alternativa ao LDAP, uma versão mais antiga do protocolo. O CLDAP tem sido usado em diversos ataques de DDoS nos últimos anos.

#### 2. O ataque de DDoS ao GitHub em fevereiro de 2018

Um dos maiores ataques verificáveis de DDoS já registrados foi direcionado ao GitHub, um popular serviço de gerenciamento de códigos on-line usado por milhões de desenvolvedores. O ataque chegou a atingir 1,3 terabytes por segundo (Tbps), enviando pacotes a uma taxa de 126,9 milhões por segundo.

O ataque ao GitHub foi um ataque de DDoS do memcached e, portanto, não havia botnets envolvidas. Os invasores tiraram proveito do efeito de amplificação do sistema de armazenamento em cache de um popular banco de dados, conhecido como memcached. Ao inundar os servidores do memcached com solicitações falsificadas, os invasores conseguiram amplificar seu ataque em cerca de 50.000 vezes!

Felizmente, o GitHub estava utilizando um serviço de proteção contra DDoS, que foi alertado automaticamente 10 minutos após o início do ataque. Esse alerta desencadeou o processo de mitigação e o GitHub foi capaz de deter o ataque rapidamente. O gigantesco ataque de DDoS acabou durando apenas cerca de 20 minutos.

#### 3. O ataque à Dyn em 2016

O segundo maior ataque de DDoS foi dirigido à Dyn, um grande provedor de DNS, em outubro de 2016. Foi um ataque devastador e provocou disrupção em muitos sites importantes, incluindo o AirBnB, a Netflix, o PayPal, a Visa, a Amazon, o jornal The New York Times , o Reddit e o GitHub. O ataque foi efetuado usando um malware chamado Mirai. O Mirai cria uma botnet composta de dispositivos comprometidos da Internet das Coisas (IoT), como câmeras, TVs inteligentes, rádios, impressoras e até monitores de bebês. Para criar o tráfego de ataque, todos esses dispositivos comprometidos são programados para enviar solicitações a uma única vítima.