CIBERSEGURANÇA

Universidade de Aveiro

Rúben Gomes, Tiago Garcia

VERSÃO 1

CIBERSEGURANÇA

Dept. de Eletrónica, Telecomunicações e Informática
Universidade de Aveiro

Rúben Gomes, Tiago Garcia
113435 rlcg@ua.pt, 114184 tiago.rgarcia@ua.pt

10 de dezembro de 2022

Resumo

Resumo de 200 - 300 palavras.

Conteúdo

Introdução

Com o passar dos anos, as tecnologias que temos ao nosso dispor tem evoluído de uma forma rápida e sem fim, como, por exemplo, o *hardware* de um computador. Mas, com constantes evoluções, também vem uma necessidade de responsabilidade, pois com quanto mais recursos existirem, maior será o impacto de danos a indivíduos ou entidades.

Com este relatório, iremos falar num tópico bastante sensível na atualidade, a Cibersegurança, bem como as diversas vulnerabilidades associadas de formas de nos protegermos contra as mesmas.

Capítulo 1

Cibersegurança no geral

1.1 Conceito

Quando os sistemas e ambientes digitais foram criados não existia quase nenhuma interação entre dispositivos e a pouca que existia era efetuada por cabo. Porém, quando a internet foi criada, a interação entra dispositivos digitais aumentou e com isso, tal como acontece com interações humanas, vieram diversos perigos e ameaças aos utilizadores. Da mesma forma que existem crimes no mundo físico também existem crimes digitais e da mesma forma que existem soluções e entidades responsáveis pela prevenção e combate a crimes físicos, também os mesmos existem para o mundo digital, proporcionando cibersegurança aos utilizadores da internet e ambientes digitais.

1.2 Tipos de ameaças

1.2.1 Ameaças cibernéticas

Conjunto de malware e software com capacidade de afetar o funcionamento normal de equipamentos digitais. Muitas vezes usadas para ciberterrorismo e causar danos graves com o intuito de lucrar ou impossibilitar o trabalho usual de uma entidade.

Botnets

Botnets são robos digitais que conseguem infetar dispositivos, tal como um vírus e a partir daí permitir que utilizadores remotos tenham acesso à máquina onde se encontram alojados. Estas máquinas são muitas vezes usadas para fazer tarefas ilícitas e ilegais por parte do utilizador remoto sem que este seja exposto por não ser a máquina do mesmo a realizar as ações.

Estes botnets podem contaminar computadores, dispositivos móveis, *routers* e dispositivos Internet of Things (IOT).

Da mesma maneira que um vírus tenta infetar o corpo humano através de falhas no sistema imunitário, também estes bots tentam infetar os dispositivos através de falhas de segurança. É possível detetar que o dispositivo se encontra infetado a partir da deteção de comportamentos anormais por parte da máquina, por exemplo quando esta trabalha de forma mais lenta do que o normal ou quando durante a utilização aparecem mensagens de erro aleatórias.

Tipos de botnets

Dentro dos botnets existem dois tipos: Cliente Servidor e Peer-to-Peer

- Cliente servidor → Este é o modelo dos botnets mais antigos em que os dispositivos infetados (clientes) recebem intruções de um outro dispositivo que os controla (servidor)
- Peer-to-peer → Este modelo corrige algumas falhas que o modelo de cliente servidor tinha. Em vez de ser establecida apenas uma conexão entre dois dispositivos (cliente e servidor), neste modelo todos os dispositivos infetados estão conectados entre si, todos a ser controlados pelo mesmo dispositivo que dá as intruções a todos os outros. Isto permite que no caso de haver uma falha com um dos dispositivos infetados, a rede continue online e funcional.

Distributed denial-of-service (DDOS)

Estas ameaças são das mais comuns e mais utilizadas pela comunidade de atacantes. O objetivo destes ataques é levar o consumo de recursos do servidor/aplicação ao limite. Uma vez sem recursos disponiveis, o servidor acaba por ter falhas de funcionalidade ou pode chegar mesmo a ir abaixo e ficar offline.
A quantidade dste tipo de ataques têm vindo a aumentar substancialmente, segundo a Microsoft[1], a Azure Networking registou, em 2021, um aumento de 25% a mais de casos de DDOS em relação a 2020.

Functionamento de DDOS

Durante estes ataques, um conjunto de Botnets (1.2.1) ataca uma aplicação/servidor com o objetivo de desgastar e levar o consumo de recursos ao limite. Fazem isto procedendo ao uso exagerado de solicitações Hypertext Transfer Protocol (HTTP). Uma vez que os atacantes usam estes bots, conseguem também acesso à base de dados, podendo conseguir roubar informação sensivel e, uma

[1] Fonte: `https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack`

vez que os recursos do servidor já estão no limite, os proprietários e responsáveis pela segurança do servidor têm dificuldade na defesa do seu sistema. Estes ataques podem demorar diversos intervalos de tempo, desde minutos até mesmo dias.

Tipos de ataques DDOS

Existem três tipos de ataques DDOS:

- Ataque volumétrico → estes ataques baseam-se na sobrecarga do servidor com tráfego, sendo o tipo de ataque mais comum.
- Ataque de protocolo estes ataques atacam certas camadas de protocolos de segurança eliminando limites de tráfego o que permite uma mais fácil sobrecarga dos recursos.
- Ataque a camadas de recursos → estes ataques são usados principalmente em redes de servidores pois permitem o bloqueio na troca de informação entre os diversos hospedeiros.

Durante um ataque DDOS podem ser usados apenas um ou mais destes tipos, muitas vezes começa como um dos tipos para debilitar os sistemas de segurança para que depois possam ser usados ataques de exaustão do sistema.

1.2.2 Guerras cibernéticas

Por vezes estas ameaças e armas cibernéticas são usadas para criar guerras. Estas são muito prejudiciais para as vítimas da guerra mas benificial para o atacante pois este consegue muitas vezes vencer a guerra sem qualquer custo para si mas leva a sérios danos à vítimas, explorando falhas de segurança nos seus sistemas.

As vítimas são muitas vezes países ou empresas e não entidades pequenas, sendo atacados não apenas dados das entidades mas também os próprios sistemas, levando ao corrompimento de parte do functionamento da entidade.

Estas guerras são também usadas no roubo de informação desde dados simples até mesmo dados bancários ou na espionagem de dados militares ou diplomáticos. Outro uso dado a estas guerras é a corrupção e a manipulação de dados para benificio de uma certa entidade como acontece em algumas disputas de poder.

Exixtem duas formas de guerras: ARC e ERC .

ARC

Estas guerras são responsáveis pela destruição e degradação de redes e da informação com a qual estas trabalham. Podem ser usados DDOS para provocar sobrecarga no servidor fazendo pedidos de informação de quantidade superior à que o servidor aguenta ou podem-se criar bloqueios nos servidores para impedir o acesso aos mesmos por parte dos utilizadores.

ERC

Estas guerras são as responsáveis pelo espionamento de entidades e por vezes provocar danos colaterais na rede durante o processo.

1.2.3 Internet banking

Tal como o nome sugere estas ameaças procuram tirar proveito de falhas em sistemas bancários quer bancos financeiros quer bancos de dados. Com a exploração de vulnerabilidades nestes bancos, o atacante consegue um grande acesso à informação dos utilizadores, usando essa informação para proveito próprio posteriormente.

Muitos dos sistemas usam uma Application Programming Interface (API) que permite a utilização do sistema por parte de aplicações externas. Por exemplo, o PayPal tem uma API que permite que outras aplicações o usem como método de pagamento. No entanto, estas API são também bastante sujeitas a ataques DDOS (1.2.1), entre outros. Outro problema com a sua encriptação é o baixo nível da complexidade das chaves de autenticação usadas (muitas vezes são pins numéricos com poucos digitos).

1.2.4 Mobile Malware

Este género de malware pode ter a capacidade de roubar a informação do dispositivo, inutilizar aplicações. Estas ameaças podem facilmente se espalhar através do Bluetooth.

Mobile malwares mais usados

- Banking → Captura dados de logins do usuário
- Ransomware → Bloqueia ficheiros locais
- Spyware → Controla a atividade do utilizador
- Adware → Constantes publicidades
- MMS → Usa mensagens para explorar falhas nas bibliotecas do andriod

Com estes malwares, o usuário corre o risco de ter dinheiro, informação pessoal/profissional/empresarial roubadas, podendo ser posteriormente vendidas no mercado negro da internet.

1.3 Programação aplicada à Cibersegurança

Como é óbvio, para a automatização quer seja para os sistemas de ataque ou para os sistemas de defesa é usada bastante programação e como isto não são sistemas dísponivels a todos os utilizadores, cada hacker cria a sua aplicação à sua maneira para atingir os seus objetivos.

1.3.1 Linguagens mais usadas em hacking

1. Python
2. C
3. PHP
4. C++

1.3.2 Sistemas operativos usados em hacking

Todos os hackers optam pelo uso de uma distribuição de linux e embora a maior parte delas funcionem, o Kali Linux é o mais usado, entramos em mais detalhes mais à frente em **??**.

Capítulo 2

Vulnerabilidades

2.1 Análise de vulnerabilidades

2.2 Análise de evidências

Capítulo 3

Soluções de segurança

Capítulo 4

Conclusões

Apresenta conclusões.

Contribuições dos autores

Resumir aqui o que cada autor fez no trabalho. Usar abreviaturas para identificar os autores, por exemplo AS para António Silva.

Indicar a percentagem de contribuição de cada autor.

Rúben Gomes (RG), Tiago Garcia (TG) : xx%, yy%

Acrónimos

API Application Programming Interface

DDOS Distributed denial-of-service

HTTP Hypertext Transfer Protocol

IOT Internet of Things

RG Rúben Gomes

TG Tiago Garcia