Network Security

Miguel Pinto, Pedro Martins e Gabriel Silva

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal

e-mail: {a96106, a97613, a97363}@alunos.uminho.pt

Abstract. Num mundo em que a comunidade global está cada vez mais conectada através da Internet, a importância de nos mantermos seguros nesta rede é ainda maior, uma vez que com um maior volume de usuários, maior serão também as tentativas de ataques. Estes ataques podem tomar diversas formas e ter diferentes objetivos, mas é possível tomar medidas contra estes invasores.

Introdução

A segurança de redes tem vindo a ganhar cada vez mais relevância com a necessidade da modernização das empresas e indústrias e mais recentemente com os ataques informáticos a várias empresas em Portugal, exaltando a necessidade de arranjarmos soluções para mantermos o funcionamento dos diversos serviços que hoje em dia damos como garantidos e consideramos essenciais.

Com este ensaio, temos como objetivo descobrir um pouco mais acerca de tópicos relacionados com Segurança de Redes, e expor a extrema importância que este tema tem no nosso quotidiano.

1 Consequências e motivações para a cibercriminalidade

Ciberataques na forma de roubo de informação, ransomware, DDoS… podem fazer com que certas empresas ou organizações sejam obrigadas a suspender as suas atividades, causando enormes prejuízos e até mesmo falha de serviços urgentes e essenciais como hospitais e serviços bancários.

Estes ataques podem ter várias razões, desde motivos financeiros com o único propósito de conseguir dinheiro, até motivos mais pessoais com a intenção de destruir a reputação de uma empresa/organização.

A manutenção destes serviços é de extrema importância, sendo crucial uma organização investir na sua segurança informática, com a contratação de um departamento de cibersegurança constituído por especialistas formados na área de engenharia de redes e profissionais de segurança capazes de proteger as redes das empresas deste tipo de ataques.

1.1 Tipos de Ataques

- **Vírus e Worms**

  Os vírus de computador são os ataques mais comuns entre os ataques às redes de segurança. Os vírus de computadores são um tipo de malware que, tal como os vírus biológicos, o programa infeta um dispositivo, faz cópias de si mesmo e procura espalhar-se para outros dispositivos. Estes vírus podem ter várias finalidades tais como, roubar informações pessoais do usuário, enviar spam, corromper ficheiros ou até mesmo apagar todos os ficheiros guardados no disco. Como estes ataques se espalham de computador a computador é quase impossível rastrear a sua origem.

  Outro tipo de ameaça são os *Computer Worms* que têm a mesma capacidade de multiplicação dos vírus de computador porém não necessitam de um hospedeiro para se propagarem para diferentes dispositivos. Enquanto que os vírus necessitam de se associar a um ficheiro, e de ativação humana para se propagarem, as worms conseguem fazer isso de forma autónoma.

  Vírus e *Worms* de computadores têm geralmente 2 componentes: um mecanismo de replicação e um *payload*. O *payload* é a porção do malware que executa a ação maligna do programa.

  Um *payload* pode ter várias ações como:

  1- Modificar ou roubar os dados do usuário;

  2- Roubar recursos (CPU) para realizar tarefas malignas;

3- Criar uma *backdoor* que permite ao criador do vírus ultrapassar medidas de autenticação e tomar controlo da máquina mais tarde.

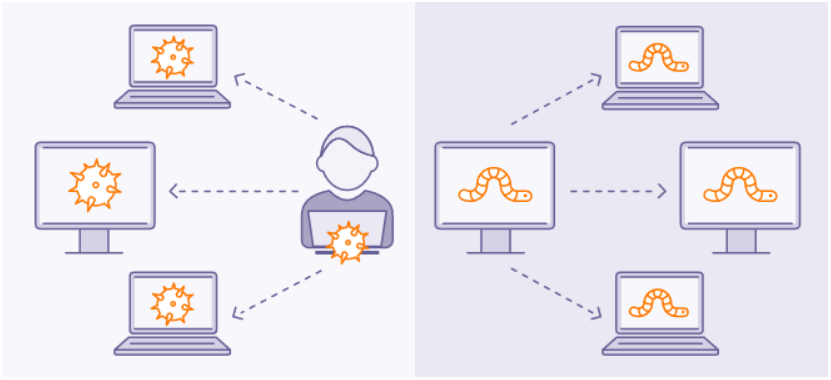

Fig. 1: Diferentemente dos vírus, worms podem se replicar e espalhar sem a necessidade de ativação humana. **[3]**

Em 2010, a *worm* de computador conhecida como Stuxnet, ao que tudo indica criada em colaboração pelos Estados Unidos e Israel, danificou 1⁄5 das centrifugadoras nucleares de uma instalação nuclear no Irão. Acredita-se que este vírus tenha conseguido infetar o sistema através de uma pen que um funcionário utilizou num dos computadores que estavam ligados à rede da instalação. Este malware demonstrou que sistemas controlados por computadores que não estão ligados à Internet, também estão vulneráveis a ciberataques e que capacidade de destruição é que uma ciberarma deste calibre é capaz de alcançar ao conseguir desestabilizar uma instalação nuclear. **[4] [5]**

- **Rogue security software**

  Uma outra forma de cometer fraudes é o uso de softwares de segurança falsos que convencem os usuários que estão a ser atacados ou que não têm as medidas de segurança atualizadas e pedem para que seja instalado um programa para resolver o problema, e assim conseguem instalar malware no computador do usuário.

- **Ransomware**

  Este tipo de ataques tem vindo a ganhar popularidade nos últimos anos e que se trata de um tipo de software malicioso que encripta os dados dos sistemas atacados ou bloqueia o acesso a certos ficheiros até que seja pago um resgate, normalmente exigido em criptomoedas. Quando o resgate é pago, uma chave de desencriptação é fornecida para que os dados da organização sejam desencriptados, recuperando assim o acesso aos ficheiros encriptados.

Fig. 2: Figura ilustrativa do conceito básico de ransomware. **[6]**

Um ataque em que foi utilizado este tipo de malware foi o ciberataque à empresa de gás americana Colonial Pipeline que obrigou à paralisação do fluxo de gás na costa leste dos Estados Unidos da América, forçando o presidente a decretar o estado de emergência no país.
Este ataque foi da autoria do grupo DarkSide conseguindo roubar uma password e aproveitando-se do sistema VPN (Virtual Private Network) desatualizado da empresa, que não pedia autenticação multi-fator como a maioria do software mais recente requer, como medida de segurança adicional. A situação encontrava-se de tal forma preocupante que a empresa viu-se obrigada a pagar o resgate que o grupo de hackers exigiu de 75 bitcoins (aproximadamente 5 milhões de dólares) para recuperar os dados roubados, permitindo à empresa retornar à normalidade e retomar o fluxo de gás e outros combustíveis. **[7]**

- **DoS (Denial of Service) and DDoS Attacks**

  Um ataque de DoS tem o objetivo de fazer com que uma máquina ou serviço de rede se torne indisponível impedindo utilizadores legítimos de aceder a estes serviços. O conceito de DDoS (Distributed Denial of Service) aplica-se quando o tráfego que sobrecarrega o serviço, é originado por várias fontes distintas, tornando impossível parar o ataque ao simplesmente bloquear uma única fonte. Servidores web são os alvos típicos deste género de ataque, com o propósito de tornar estas páginas indisponíveis na rede. Estes ataques são geralmente feitos de duas formas:

  - forçando o sistema a reiniciar ou a consumir todos os recursos (memória, capacidade de processamento, …) de forma a que o sistema não seja mais capaz de fornecer o serviço.
  - obstruir o meio de comunicação entre os utilizadores e o sistema, de forma a não conseguirem se comunicar adequadamente.

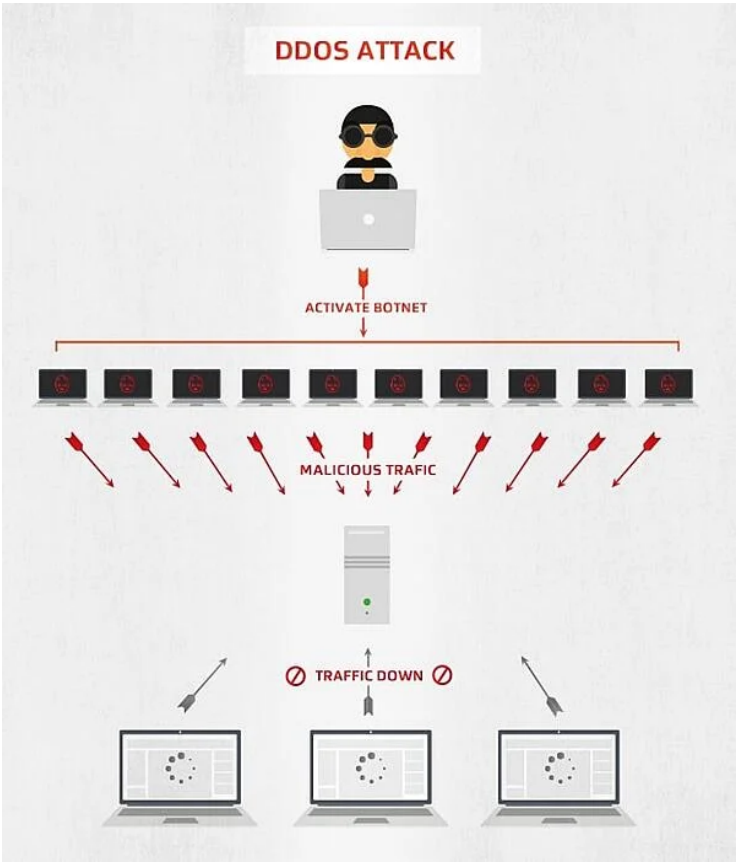

Fig. 3: Figura ilustrativa de como um ataque DDoS é executado. **[8]**

Em fevereiro de 2020, a cloud online da Amazon, que serve de infraestrutura para vários websites, foi alvo de um DDoS com um volume de 2.3 terabites por segundo a serem bombardeados para a plataforma da Amazon, uma taxa fora do normal nunca antes vista. No entanto, há serviços de proteção como AWS Shield, Cloudflare, e Akamai, entre outros, que são uma boa linha de defesa contra este tipo de ataques, limitando a capacidade de perturbação destes atacantes, e que foram capazes de mitigar os efeitos do ataque à Amazon. **[9]**

1.2 Tipos de Defesas

- **Gerenciamento de configurações**

O gerenciamento de configurações é um dos aspetos centrais, senão o principal, no que toca ao impedimento de ataques informáticos. A adoção de comportamentos como a manutenção dos sistemas operativos, assim como a sua contínua atualização e a alteração de passwords predefinidas em produtos aquando da sua instalação, permitem que o utilizador comum consiga lidar com 90% dos tipos de ataques mais comuns. No entanto, tomando escalas mais alargadas, a manutenção de todo o equipamento torna-se demasiado exaustiva e impraticável, sendo, na maior parte dos casos, preferível por grandes organizações a aquisição de softwares externos como antivírus e firewalls ao invés da utilização deste método.

- **Firewalls**

As firewalls são uma das soluções mais utilizadas no que toca a problemas de segurança na Internet. Este dispositivo de monitorização é colocado na fronteira entre a rede local e a Internet filtrando e limitando o tráfego de dados que possam ser maliciosos. As firewalls podem ser organizadas em três categorias, dependendo de onde operam: ao nível do packet de IP 's, da sessão de TCP ou ao nível de aplicação.

Este método, como seria de expectar, possui as suas falácias. Utilizando novamente o contexto nas quais se encontram as grandes organizações, o uso de firewalls parece ser uma solução simples, sendo mais fácil monitorar um número relativamente pequeno de firewalls, ao invés de, cada um dos dispositivos utilizados na empresa. No entanto, é muitas vezes o caso de esta monitorização acabar por não existir por parte das corporações.

- **Encriptação**

A utilização deste método permite que as comunicações realizadas entre diferentes dispositivos eletrónicos, dentro de um ambiente controlado, sejam encriptadas. O uso mais comum deste tipo de defesa contra ataques informáticos recai sobre o uso de VPN (virtual private network). A função principal das vpns é mascarar o IP de um dispositivo dificultando o acesso remoto por parte de eventuais atacantes.

Este tipo de tecnologia é utilizado por grandes corporações com o intuito de tornar segura a comunicação entre os diversos setores, impedindo que a concorrência consiga ter acesso a informações confidenciais.

Apesar de tudo isto, a encriptação também possui as suas desvantagens, na medida em que, ao permitir a passagem de informação encriptada pela firewall não existe garantia de que parte da informação encriptada não seja maliciosa.

- **Antivírus**

Os antivírus são a solução mais comum para prevenção e deteção de ataques.

Não só tem o papel de prevenir ataques, como também de os detetar e eliminar do sistema. Existem dois métodos através dos quais esta deteção pode ser feita.

O primeiro, "misuse detection systems", procura no sistema por comportamentos anormais, tomando o exemplo de uma conta bancária, a extração da quantidade diária máxima permitida de dinheiro de uma conta ao longo de vários dias.

O segundo, "anomaly detection", este tipo de sistemas utiliza inteligência artificial de modo a encontrar padrões de comportamento do atacante, de modo a detetar ataques cujo *modus operandi* ainda não tenha sido catalogado.

Conclusão

Com a realização deste ensaio, pudemos constatar que existem diversas maneiras de sermos atacados, mas também temos imensas opções para nos defendermos, sendo uma corrida constante entre defensores e atacantes nesta guerra cibernética. Estes ataques podem afetar-nos de imensas maneiras diferentes, desde impedir o acesso a um website, a desestabilizar operações de serviços importantes e essenciais, como hospitais ou serviços bancários. Devido à extrema importância da preservação dos serviços que usufruímos, é imperativo darmos importância a este tópico e investir na proteção de redes, para que no futuro não tenhamos que lidar com as consequências de um ataque destruidor.

Referências

1. Security Engineering: A Guide to Building Dependable Distributed Systems, 1st Edition, Ross Anderson, Chapter 18
   https://www.cl.cam.ac.uk/~rja14/Papers/SE-18.pdf
2. Security Engineering: A Guide to Building Dependable Distributed Systems, 2st Edition, Ross Anderson, Chapter 21
   https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c21.pdf
3. Avast: Worms vs Vírus, https://www.avast.com/pt-br/c-worm-vs-virus
4. WikipediaStuxnet,
   https://en.wikipedia.org/wiki/Stuxnet#Target_and_origin
5. Insider: The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought,
   https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11
6. Pplware-SAPO: Ransomware,
   https://pplware.sapo.pt/microsoft/windows/ransomware-sabe-o-que-e/
7. Insider: One Password allowed hackers to disrupt Colonial Pipeline,
   https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
8. AVG, https://www.avg.com/pt/signal/what-is-ddos-attack
9. BBC News Amazon, https://www.bbc.com/news/technology-53093611