

# 

# Securing Microsoft Windows Case Study Report

ST2612

Written by: Lee Yi Terng (1904189)

DISM/FT/2A/04

Submitted To: Ms Teo Seok Ling

Date: 14th June 2020

# Table of Content

[**Securing Microsoft Windows Case Study Report**](#_a7lx1qrnwpld) **1**

[**Table of Content**](#_x48fvqmfdef4) **2**

[**Introduction**](#_7jt1v971y7dy) **3**

[**Denial-of-Service Attacks**](#_wekvuxux3ke) **3**

[Overview](#_2e47vukw0ily) 3

[Difference between DDoS and DoS](#_r0ynzz6fe5u) 3

[Cause and Impact](#_jefoz8gec7yg) 3

[Examples](#_doydzr9oumtg) 4

[**Remote Code Execution Attacks**](#_pbd89rj2okak) **4**

[Overview](#_2xfklqyr9h37) 4

[Cause and Impact](#_e81pwvlnztrm) 4

[Examples](#_shtec1yrujff) 5

[Prevention and Protection Measures](#_90xxacw2ketp) 6

[**Worms**](#_dxqjdp89ww6l) **6**

[Overview](#_8hsmf1zde7yo) 6

[Cause and Impact](#_v54kdb57jmk3) 6

[Examples](#_v54kdb57jmk3) 7

[**Conclusion**](#_71lgb29jml1x) **7**

[**References**](#_8pqdz5d0ov5h) **8**

# Introduction

This document was written for a case study on the causes and impacts of three common windows server attacks as well as a set of preventive and protective measures for one of them. When deploying Windows Servers, it is important to ensure that the server is reliable, secure and protected in order to create a safe environment to work with. This document goes into detail and provides real-world examples on denial-of-service attacks, remote code execution and worms.

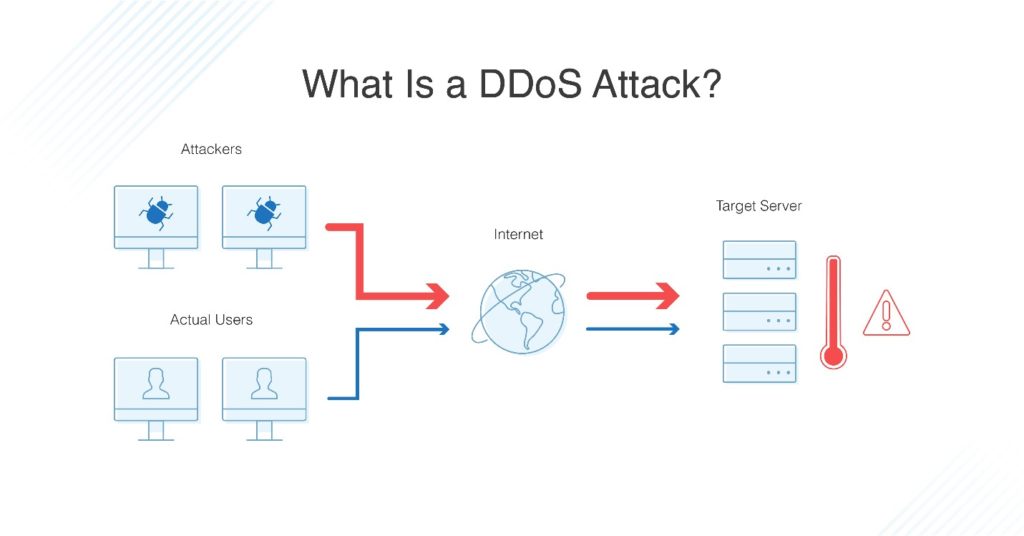
# Denial-of-Service Attacks

## Overview

Denial-of-Service (DOS) attacks are a form of cyberattack that causes a machine or network resource to become unavailable to its intended users by temporarily disrupting services of a host connected to the internet. In a way, DOS attacks are similar to a group of people crowding the entrance to a shop, thus making it hard for actual customers to enter. There are many different types of DOS attacks, such as DDOS, Application Layer Attacks, ICMP Flood, SYN Floods and many more.

## Difference between DDoS and DoS

As technology improves throughout the years, it is inevitable that attacks against it evolve as well. A distributed denial-of-service attack is where there are multiple computers and network connections involved in the attacking process as part of a botnet controlled by the attacker. A normal DoS attack only uses one attacking system, while DDoS uses up to a few hundred or thousands. This makes it hard to defend against as stopping a single source does not stop the rest of the attack.



*Figure 1: What is a DDoS Attack? (DNSStuff)*

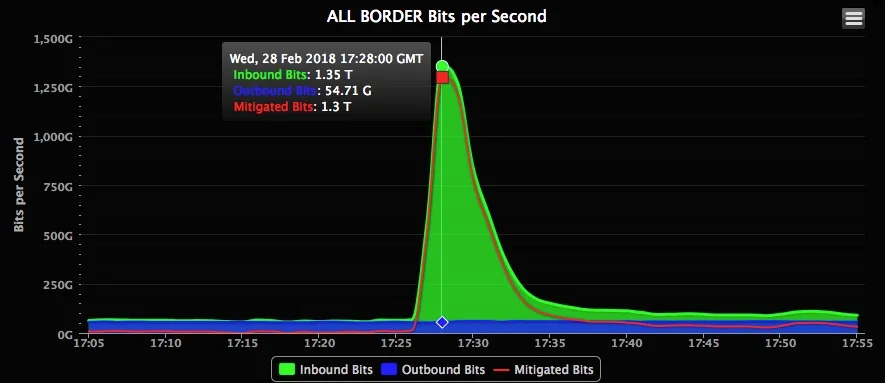
## Cause and Impact

DoS attacks are typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. As mentioned in Section 2.1, the attacker can flood the targeted network in many different ways and attacks.

DoS attacks usually result in abnormally slow network performance and unavailability from the targeted server as well as an inability to access any network resource hosted on the server. A huge flood may overwhelm a machine and cause it to crash entirely as well.

## Examples

One example of a DoS attack occurred on February 28, 2018. GitHub was hit by the biggest DDoS attack ever recorded at that time. Fortunately, the servers managed to survive the attack and only went down for less than 10 minutes despite being flooded with 1.35Tbps worth of attacks. This attack utilized an unconventional method, known as mem-caching instead of traditional DDoS methods.



*Figure 2: GitHub DDoS attack real-time traffic (WIRED)*

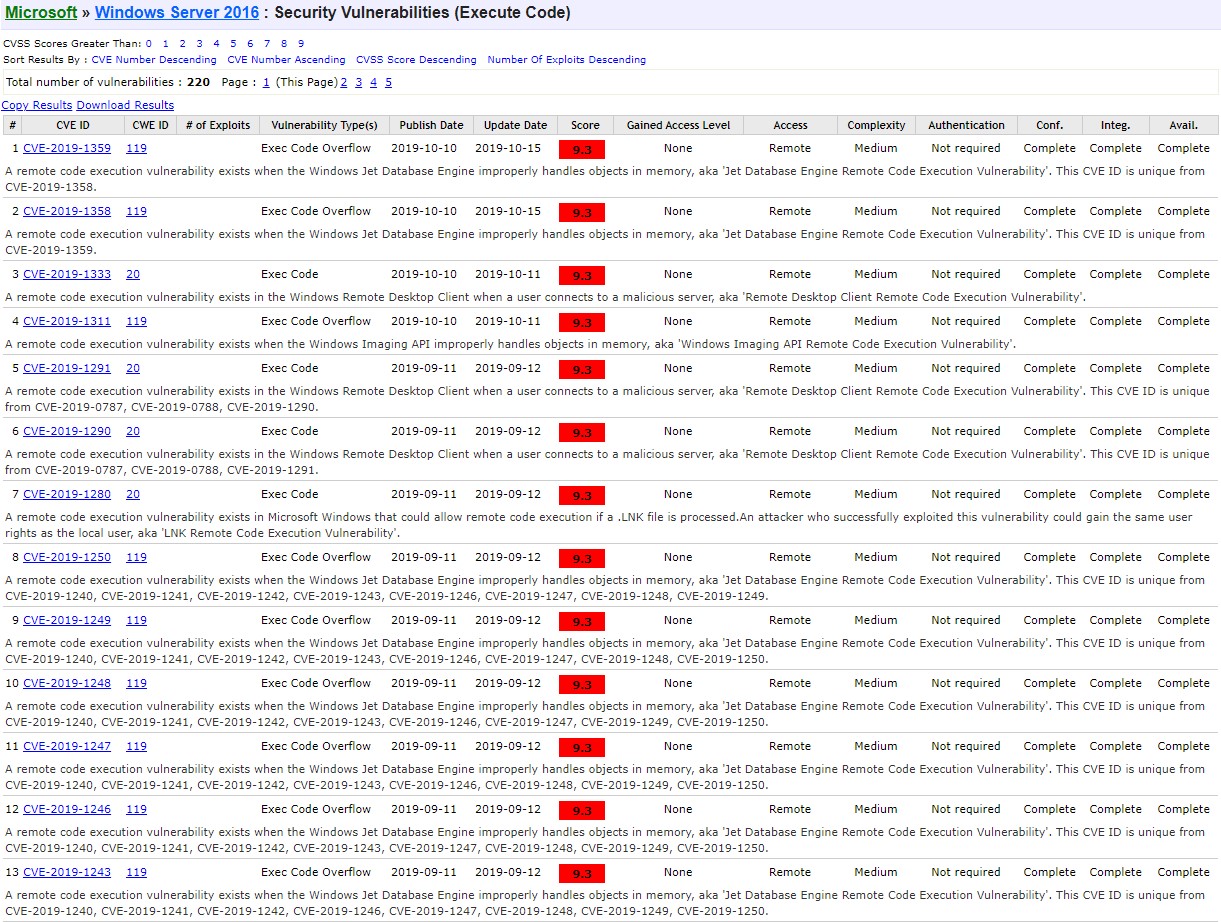
# Remote Code Execution Attacks

## Overview

Remote Code Execution (RCE) is a special type of attack that exploits a zero-day or existing vulnerability found on the target system. The attacker can use services or resources such as Microsoft Internet Information Server or Server Message Block to gain remote access and control of the system, which he can use to run and execute remote code on the targeted system. Fun fact, another form of RCE is Arbitrary Code Execution, where the code is run on the victim machine locally.

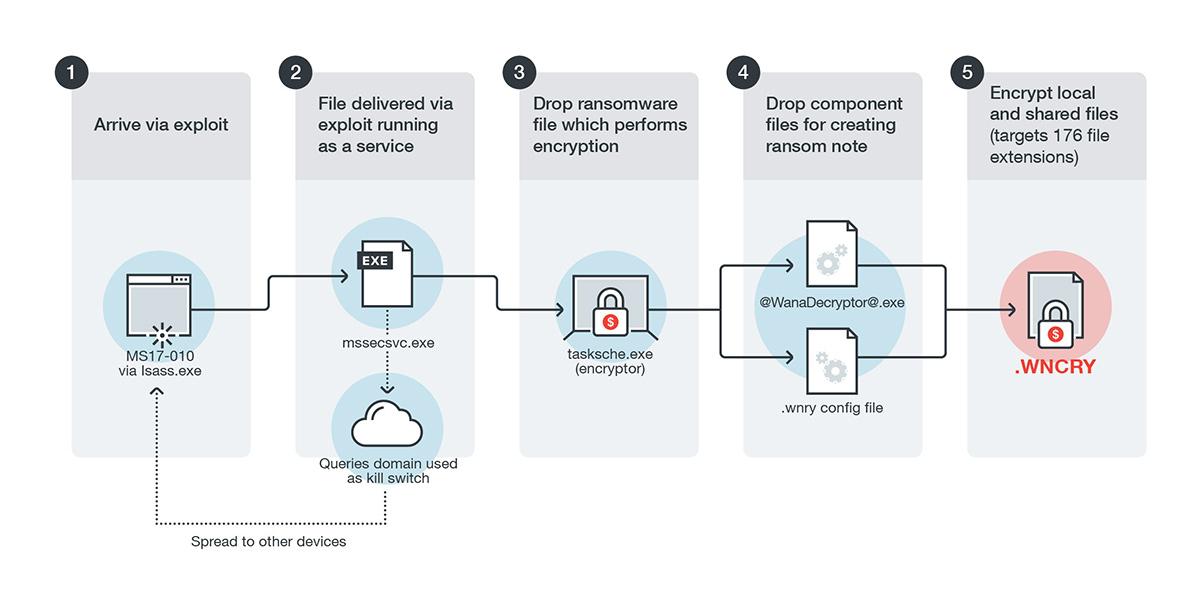
## Cause and Impact

RCE usually occurs when a vulnerability exists within a service which is remotely accessible through the Internet. If this service is vulnerable and not patched, it opens up the system to attacks from the outside and allows attackers to remotely execute code on the system by installing malware and obtaining access to the system. When successful, an RCE attack can potentially be used to spread ransomware or crash systems.



*Figure 3: Remote Code Vulnerabilities for Windows Server 2016 (CVE)*

## Examples

An example of RCE being used to launch a ransomware attack occurred in May of 2017. A vulnerability known as EternalBlue which exploited a vulnerability in Microsoft’s Server Message Block Protocol was used to spread ransomware known as WannaCry. It ended up spreading very quickly and affected around 230,000 computers globally. The attack was so detrimental to Windows Servers that WannaCry even managed to take down Russia’s biggest oil company, Rosneft. 

*Figure 4: WannaCry Attack (TrendMicro)*

## Prevention and Protection Measures

More often than not, preventing RCE attacks can be as simple as ensuring that all computers, servers and systems are always up-to-date with the latest patches. In fact, the reason why WannaCry was so prevalent, was due to the fact that many users did not install the update which patched the vulnerability that it exploited. It is also important to ensure that a firewall is put in place and properly configured to only allow traffic that is authorized and denies all other incoming or outgoing traffic. This helps to block malware from opening a reverse shell to the attacker, which would let him execute remote code on the targetted system.

Updating your systems cost almost next to nothing and it is incredibly useful and crucial to ensuring that your system is as secure as possible. When setting up firewalls, you must consider the cost of each and weigh them against the benefits, such as a more secure firewall resulting in lower availability of network resources for end-users as well as the pricing for the firewall implementation. For example, hardware firewalls are more secure and reliable than software firewalls, but they cost a lot more, up to around $3000 while software firewalls can cost as low as a few hundred. However, convenience should never be the reason to have lax security measures in place. Under most circumstances, it is of utmost importance to ensure that your system is as secure and well-protected as possible to prevent any unexpected attacks or breaches.

# Worms

## Overview

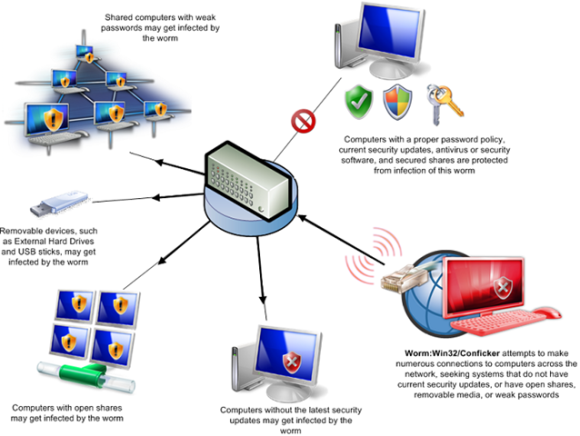
Worms are a type of malware that is programmed to self-replicate and spread itself throughout the entire network the infected system is part of. A worm spreads itself by either sending a copy of itself to various email addresses or exploiting operating system vulnerabilities. In the past, it was even possible to spread worms through Instant Messaging applications such as Skype or MSN Messenger!

Furthermore, worms are a very common form of malware and have the potential to spread and infect new computers and systems in a very short amount of time, making it a very dangerous and contagious attack if not contained properly.

## Cause and Impact

When the worm was first created, it was only meant to just spread throughout a network and not do anything. However, in this day and age, modern worms have been upgraded to contain payloads which are used to launch attacks on the target system. These payloads can do a range of malicious activities such as encrypting files in a ransomware attack, exfiltrate confidential and sensitive information as well as modify computer files.

Worms have various methods of infecting a computer, such as using binary or memory injection code. Modern worms can exploit several modules to execute the worms automatically without any user involvement, making worms very easy to activate.



*Figure 5: Worm Propagation (Ars Technica)*

## Examples

In 2017, Petya, an encrypting malware, was created and used for a global cyberattack that targeted Windows Server operating systems. Like the WannaCry example given in Section 2.3, Perya also utilised the EternalBlue exploit. Petya not only used the EternalBlue exploit to propagate itself, but the Server Message Block Protocol network spreading techniques as well. This allowed it to infect systems that already had the EternalBlue exploit patched, making no system safe from its onslaught.

Petya was so prominent that it cost major companies about $892.5 million dollars in lost revenue. In terms of infections, Ukraine was hit most badly, with 80% of all Petya infections occurring in the country. Moreover, Maersk, a major shipping company, lost between 200 and 300 million dollars that year from Petya infections alone.

# Conclusion

This document is by no means exhaustive. There are still many other attacks that can be used on Windows Servers that could not be fit into this one case study. However, this document details only three of them. It is crucial to always be vigilant and ensure that we do our best to secure all Windows Servers deployed and maintained to protect ourselves from the ever-evolving cyber threats that appear every day.

# 

# 

# References

Securityweek.com. 2020. *Windows Servers Vulnerable To Dos Attacks, Microsoft Warns | Securityweek.Com*.[online]Availableat:<https://www.securityweek.com/windows-servers-vulnerable-dos-attacks-microsoft-warns> [Accessed 9 June 2020].

## Redmondmag. 2020. *Microsoft Issues Windows Server HTTP/2 Attack Advisory -- Redmondmag.Com*. [online] Available at: <https://redmondmag.com/articles/2019/02/21/windows-server-http2-attack-advisory.aspx> [Accessed 9 June 2020].

Zero Day Initiative. 2020. *Zero Day Initiative — CVE-2019-9512 – A Microsoft Windows HTTP/2 Ping Flood Denial Of Service*. [online] Available at: <https://www.thezdi.com/blog/2019/12/4/cve-2019-9512-a-microsoft-windows-http2-ping-flood-denial-of-service> [Accessed 9 June 2020].

En.wikipedia.org. 2020. *Wannacry Ransomware Attack*. [online] Available at: <https://en.wikipedia.org/wiki/WannaCry\_ransomware\_attack> [Accessed 9 June 2020].

En.wikipedia.org. 2020. *Petya (Malware)*. [online] Available at: <https://en.wikipedia.org/wiki/Petya\_(malware)> [Accessed 9 June 2020].

Fruhlinger, J., 2020. *Petya Ransomware And Notpetya Malware: What You Need To Know Now*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html> [Accessed 9 June 2020].

Newman, L., 2020. *A 1.3-Tbs Ddos Hit Github, The Largest Yet Recorded*. [online] Wired. Available at: <https://www.wired.com/story/github-ddos-memcached/> [Accessed 9 June 2020].

Munson, L. (2018). DoS vs DDoS – What Is The Difference?. [online] Security-faqs.com. Available at: http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html [Accessed 9 June 2020].

WIRED. (2018). GitHub Survived the Biggest DDoS Attack Ever Recorded. [online] Available at: https://www.wired.com/story/github-ddos-memcached/ [Accessed 9 June 2020].