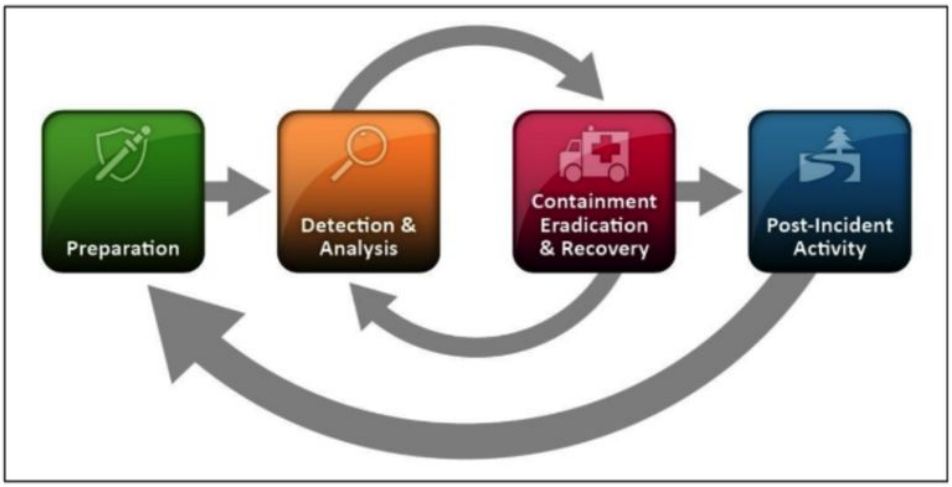
Blue Barracudas Final Project

WannaCry Virus and Ransomware Explained

Ransomware is no joke. By now, just about everyone in the world that's plugged into an online device has heard about it. Even if you live under a rock. And for some, they've lived through it. Ransomware is arguably the largest virus threat that is known of today, using multiple exploits and all have the same goal. To get your money. Some have paid tens of thousands of dollars just to get their data back and even worse, multi-millions of dollars. Hopefully by the time you get through this article, you'll have the understanding of what Ransomware is, how to detect and analyze it, how to remove the virus and further protect against it following the Phases of Incident Response. Let's take a look more into what all this is and go through a few examples using the most infamous WannaCry Ransomware virus.

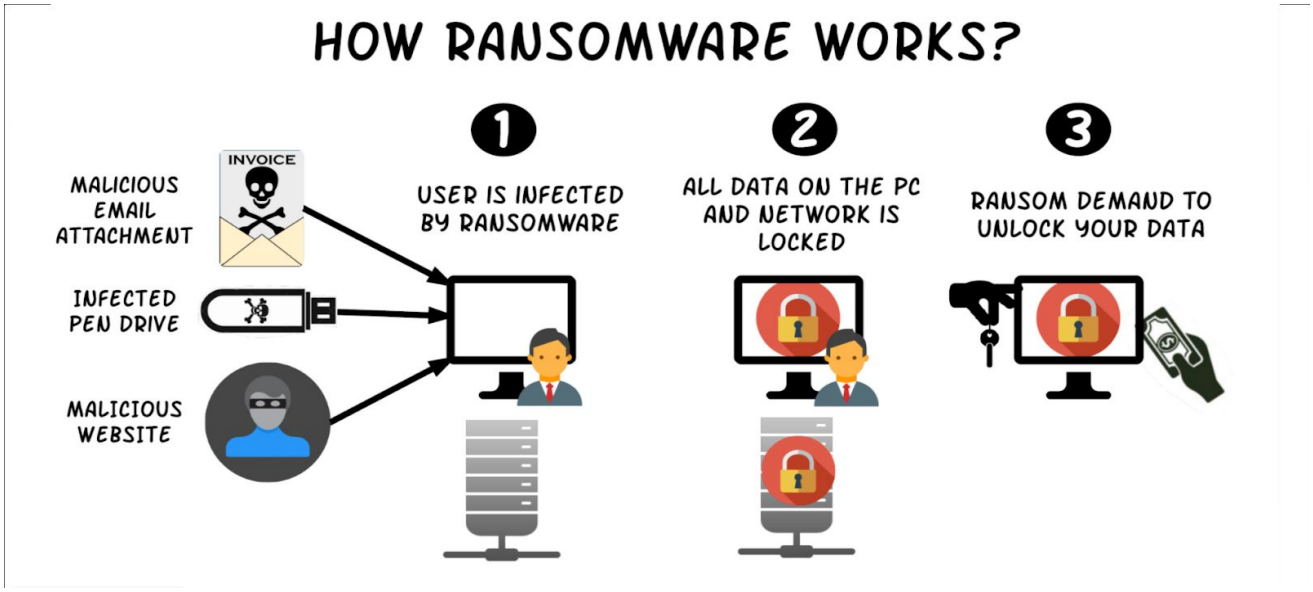


Phases of Incident Response table

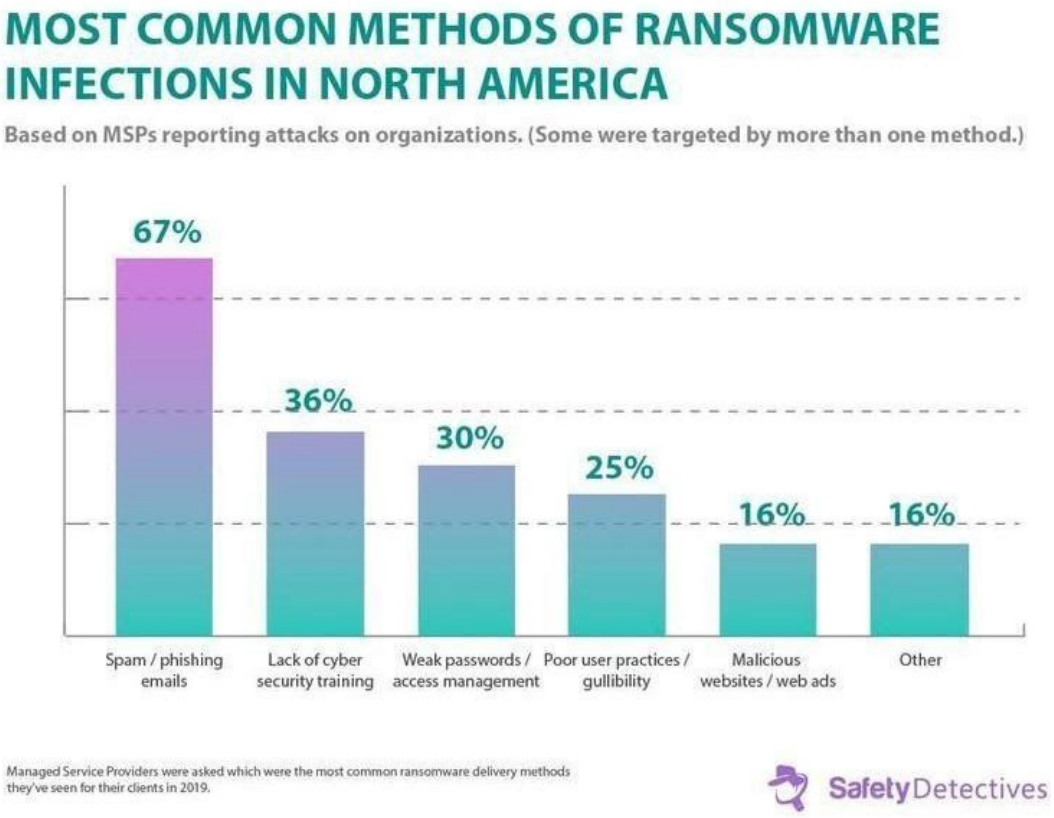
What is Ransomware and How does it work?

Before we get into how all this works and who is doing it, we first need to understand what this thing is before we can protect against it the right way. According to Wikipedia, and so everyone has a general understanding of it, they describe Ransomware as a type of malware from cryptovirology (a field that studies how to use cryptography) that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. So in short, it locks up all your files, pictures and data in a vault and they want you to pay for the key to unlock it. The longer you go without paying, the higher the ransom becomes to unlock it. And they'll typically ask for payment in Bitcoin. Why Bitcoin, you ask? Because Bitcoin is a universal currency that is completely anonymous and untraceable. To put it in perspective, as www.statista.com reports, from the year 2014 to 2019, there were more than 1.2 million attacks of Ransomware reported with a massive spike in 2016 of 638 million alone. That's going from almost nonexistent to the one thing everyone has to worry about in just less than a year with the WannaCry virus being the most famous of them all in May of 2017.

So how does it work? Now that we know what it is and what these guys are after, how does it actually get there? Well, like most people, I like visuals. So here's a quick picture that lays it out there in the simplest of terms.



Just like most viruses and malicious people out there, they will always try to find a way in and the most common of ways is by feeding off the ignorance of people. This sounds very bad, but they know that not everyone out there might be aware of these things and what it looks like. So they play the numbers game. The more people reached, the more times it's likely to happen. This might include (Spear) Phishing emails to you personally or on an enterprise level, physical devices that get left behind or sent to you, or an unsecure website that might be out of date that the hackers exploited before. These are the most common ways this virus, like any, spreads. And the scarier part is, **they still work**. Here is a quick snapshot of the likeliness of how ransomware spreads.



WannaCry Virus with EternalBlue Exploit and Examples

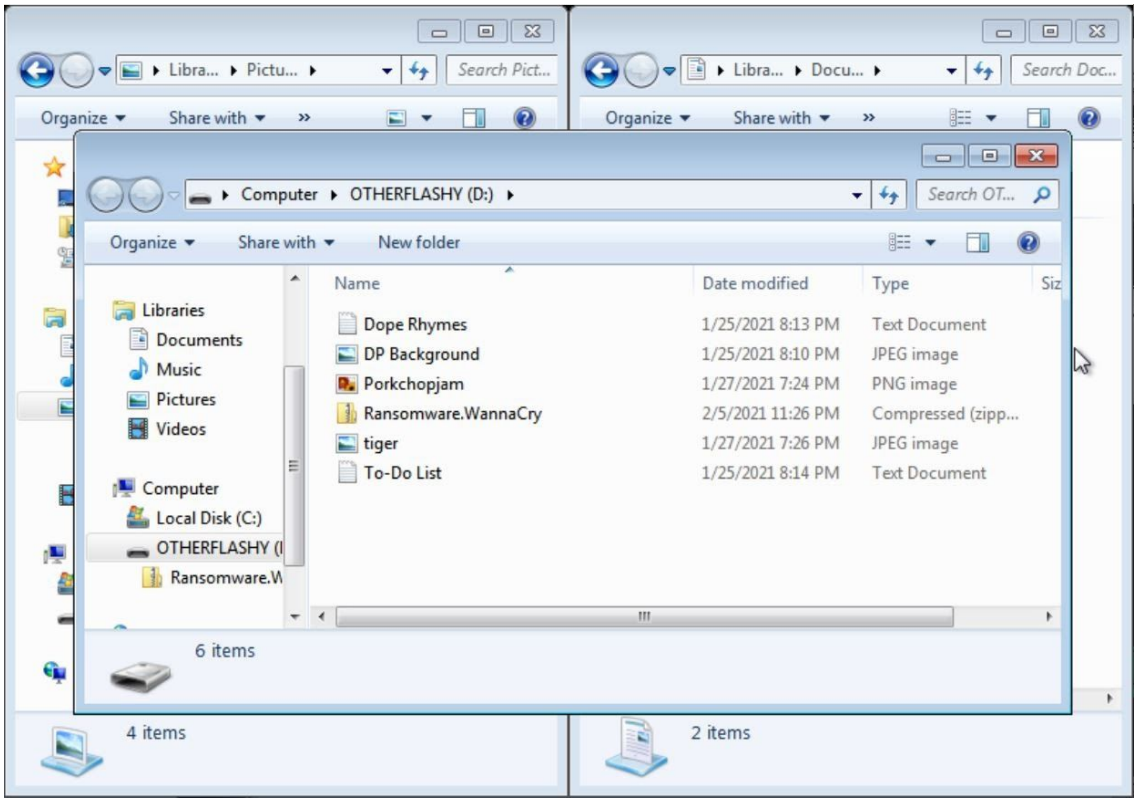
So now that we have a basic understanding of what Ransomware is and how they work, let's get into a little more technical detail of the EternalBlue exploit that WannaCry took advantage of. Like mentioned before, the WannaCry virus took the world by storm in May of 2017. This was because of a vulnerability found in the Windows Operating System at the time. This exploit is known as EternalBlue. EternalBlue allows cyber threat actors to remotely execute arbitrary code and gain access to a network by sending specially crafted packets. It exploits the

Server Message Block version 1 (SMBv1) protocol, a network file sharing protocol that allows access to files on a remote server. This exploit potentially allows cyber threat actors to compromise the entire network and all devices connected to it. Due to EternalBlue's ability to compromise networks, if one device is infected by malware via EternalBlue, every device connected to the network is at risk. This makes the recovery very difficult, as all devices on a network may have to be taken offline for remediation.

Malware that utilizes EternalBlue can self-propagate across networks, increasing the threat to you and your business. That's where the WannaCry virus, a type of "crypto"-ransomware comes in and why it really made the world pay more attention to Ransomware. WannaCry uses the EternalBlue exploit to spread itself across the network infecting all devices connected and dropping the crypto-ransomware payload. This increased the persistence and damage that WannaCry could cause in a short amount of time. This exact attack, more known as a "worm", infected over 300,000 computers in over 150 countries at the time. Though it didn't profit very much for the attackers (only $90k), the sheer amount that it spread was enough to cause over $1 Billion dollars in damages at the time.This increase made EternalBlue quite popular as well with other types of malware, such as Trickbot, a modular banking trojan, Coinminer and WannaMine, cryptominers that use the exploit in order to gain access to computer power to mine cryptocurrencies.

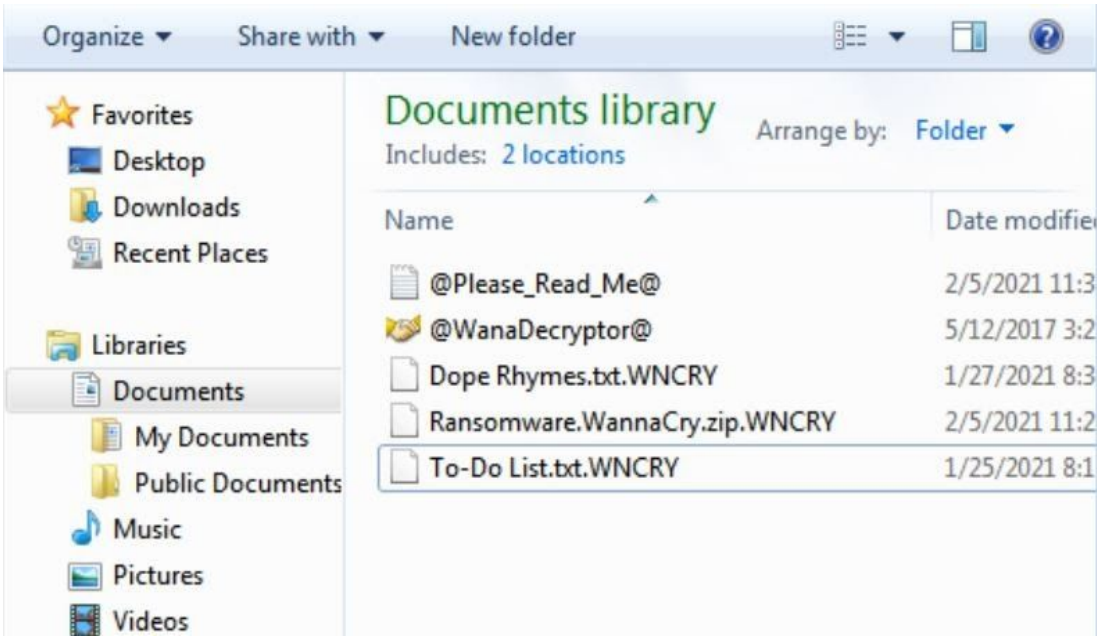
Since the widespread use of WannaCry and the exploit it used, it's not as likely to replicate this even for training purposes, however, let's go through a few steps and demonstrate what something like this looks like and how it can happen to anyone.

1.) Here we have a first look of the payload on a simple 8gb flash drive.



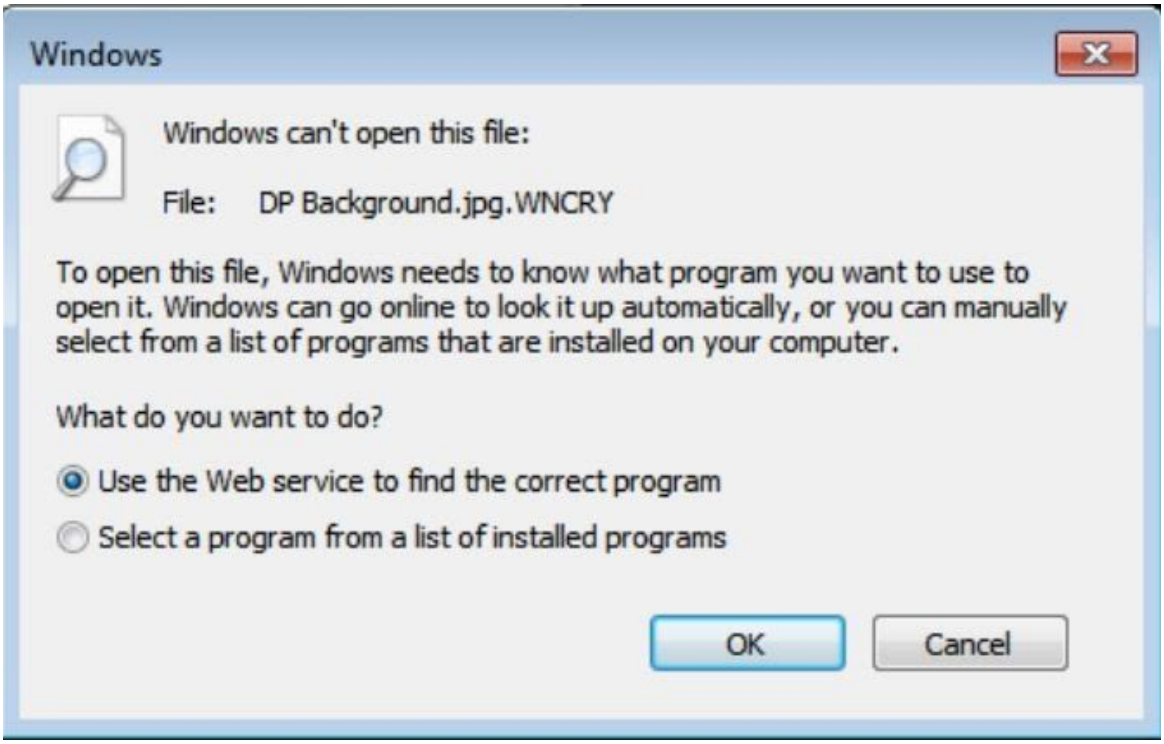
In the zipped file, it isn't doing anything, but it's there waiting to be clicked on.

2.) Next, once opened by simply double-clicking on the file, we'll see how it starts to spread.



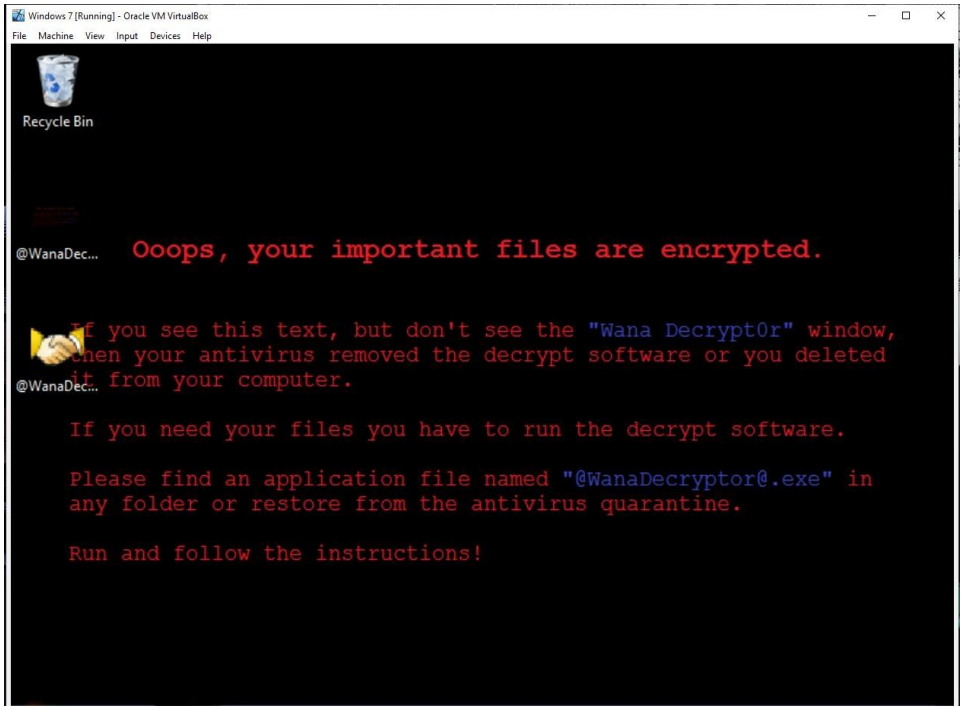
As noticed, after double-clicking the file, it automatically installed files and encrypted ours with the extension of ".WNCRY" and a guide to go through how to pay the ransom.

3.) Next, we have a pop-up after attempting to open one of our files to view. This shows us how our data is now encrypted and cannot be accessed.



By clicking on the file, it just simply will not open and then further directs us to find an application to open the file. The computer will not know it is a part of an infection.

4.) Next, after only a few seconds, the background of our computer is changed completely, notifying the user that the machine has been encrypted and a pop-up then prompts for payment and how to pay.



The ransom payment amount is small at first, but then doubles after only a few hours and goes up drastically from there after days not being paid.

After detecting your machine or network has been infected, there are a few steps and actions you'll want to take right away in order to fully analyze the threat. Keep in mind that Ransomware attacks are difficult to detect quickly enough to prevent any damage, so this example goes through past the upload process. Some questions to ask and make sure you have a policy around are, How far did it spread? Was this the only machine infected? Is the rest of our data secured? What will happen if I shut down the network right now? These of course are subject to change and will be different for everyone and businesses.What you'll want to regardless is to take pictures of the ransom and make sure you take the computer infected offline. Next of course, notify insurance and legal authorities. What you don't want to do is feel scared or fearful of letting others know who needs to be notified or that could help. Don't be quick to pay the ransom, either. You may be able to get a free key and there may be a slim chance that all your files are not encrypted. Lastly, after unplugging the infected device, do not use it again until it is wiped clean by a professional. Now that we've seen how easy this virus can be installed and detected, let's go through how to get rid of it and start a recovery process.

WannaCry Ransom Removal

Unfortunately enough, ransomware for the most part, is mathematically and physically impossible to decrypt, leaving you only two options: pay the ransom, which you want to avoid at all costs, or wipe out your data completely and reinstall your operating system. There might be a few decrypters out there from other web services that offer to try and recover some of your data

if the ransomware isn't sophisticated enough, but the likelihood of you restoring all your data fully is not guaranteed. Unless you pay the ransom or have your data backed up, cutting your losses may be your only option. The best way to go about this will be up to the individual and business with what procedures that may have for themselves. If you are to restore the computer to a previous state or to reinstall the operating system, here is a quick list on what you'll want to do:

- Reboot Windows 10 to **safe mode**
- Install **antimalware software** such as Malwarebytes, Avast or Trend Micro
- **Scan the system** to find the ransomware program
- **Restore the computer** to a previous state

But here's the important thing to keep in mind: while walking through these steps can remove the malware from your computer and restore it to your control, it *won't decrypt your files.* That is why ransomware is as bad as it is.

How to Protect Against Ransomware and Best Practices

That was a lot to take in for sure. But now understanding our foe and what it looks like and how to remove it, what are good ways to protect against and prevent ransomware? Here's a list of a few things you can certainly do to help fight back against Ransomware:

Educate your employees

Provide employees with a list of actions to take if they come across any suspicious emails or links. Go through and show them what different types of phishing emails and what malicious emails look like. Ones such as Corporate-like email accounts, faulty file attachments and unknown, unsecure links to external URLs.

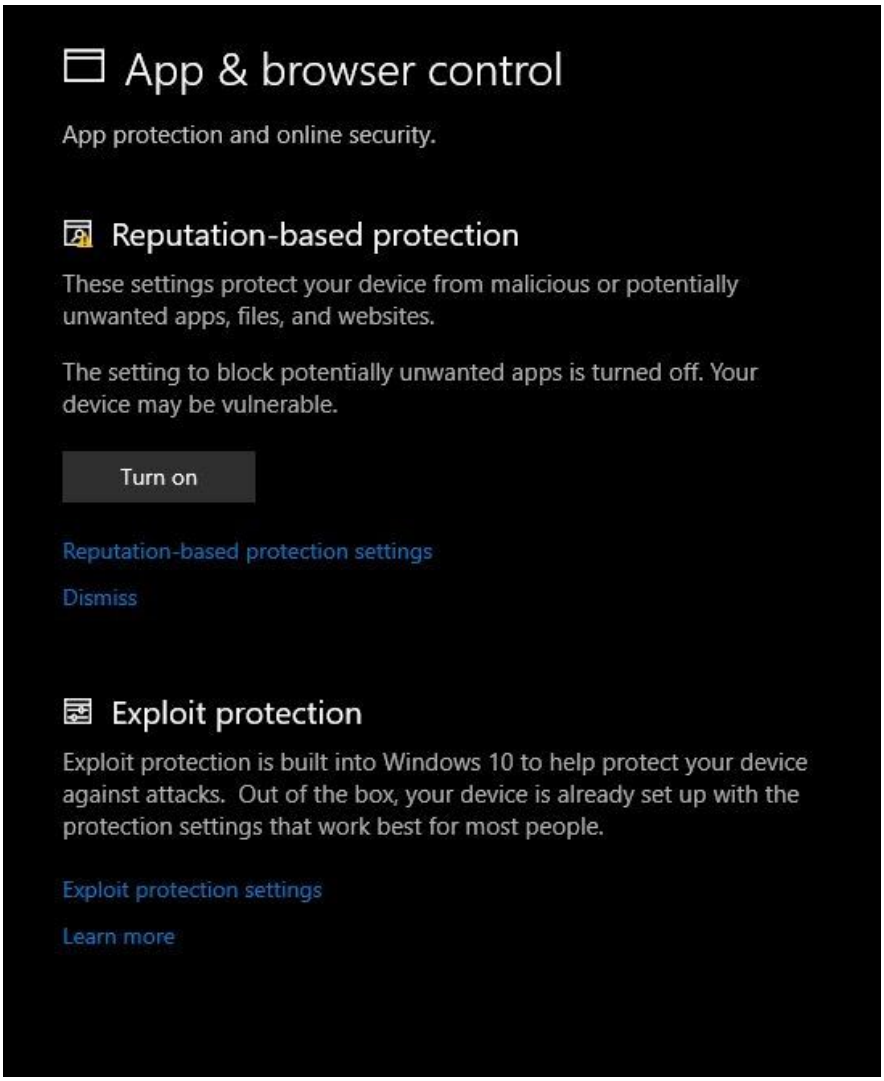
Monitor your systems and networks

- Consistently scan file systems for atypical activity such as, multiple if not hundreds of failed file modifications or failed attempted logins.
- Set up a Firewall and keep logs of all incoming and outgoing traffic.
- Understand in your company or in your network what normal network traffic looks like and what might be something out of the ordinary.
- Without hesitation, investigate any unusual findings.
- Have a paid for and full working Antivirus/Antimalware actively running that will send you alerts of any suspicious activity or potential threats.

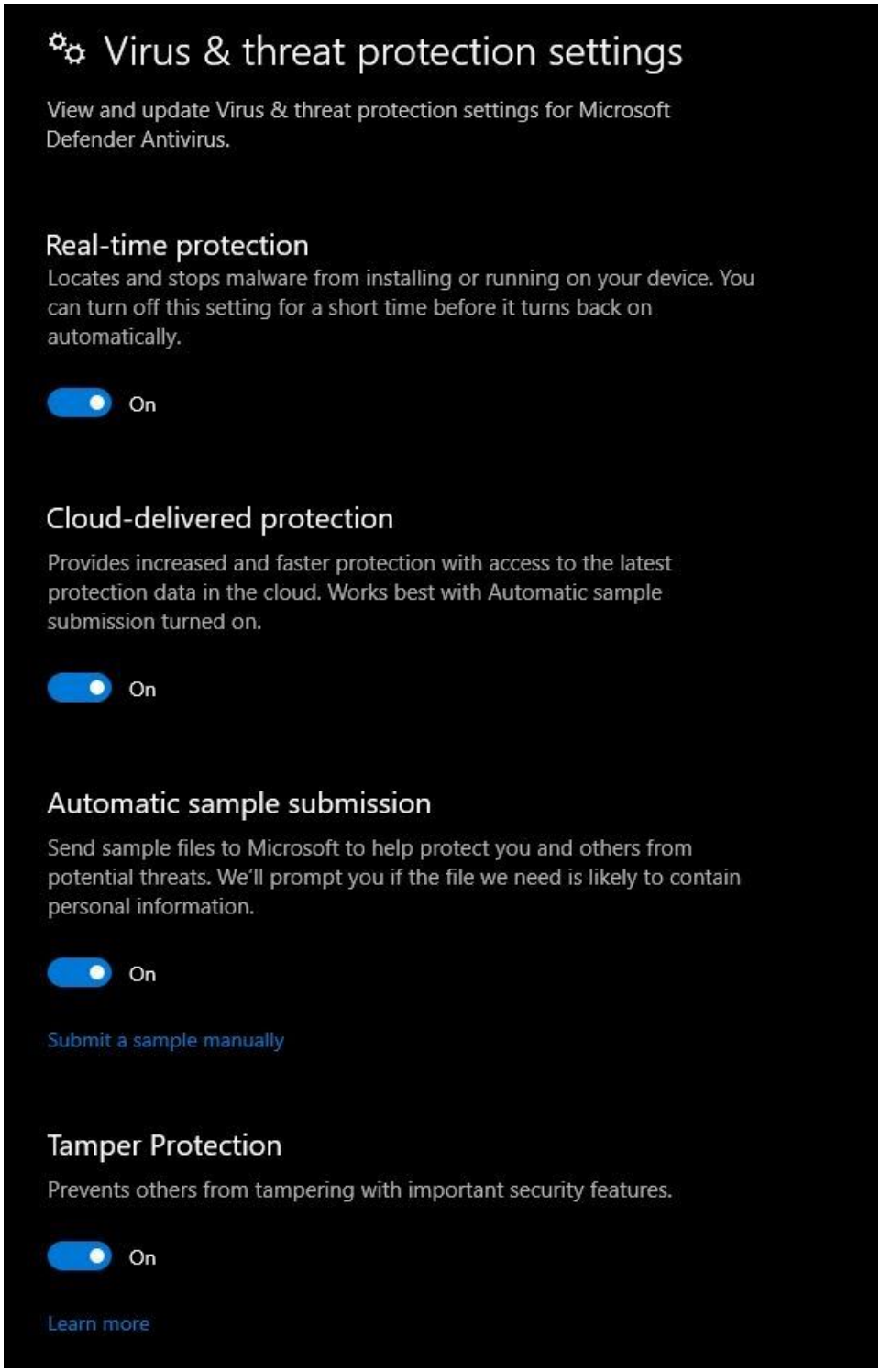
Create Honeypots

Honeypots are decoys. They are fake file repositories that look like the real thing. Hackers will target honeypots, enabling you to spot them. Early detection like this helps with safe malware removal and protects your infrastructure from being compromised, no matter how big or small. Using a File Server Resource Manager (FSRM) is a great example of honeypot usage.

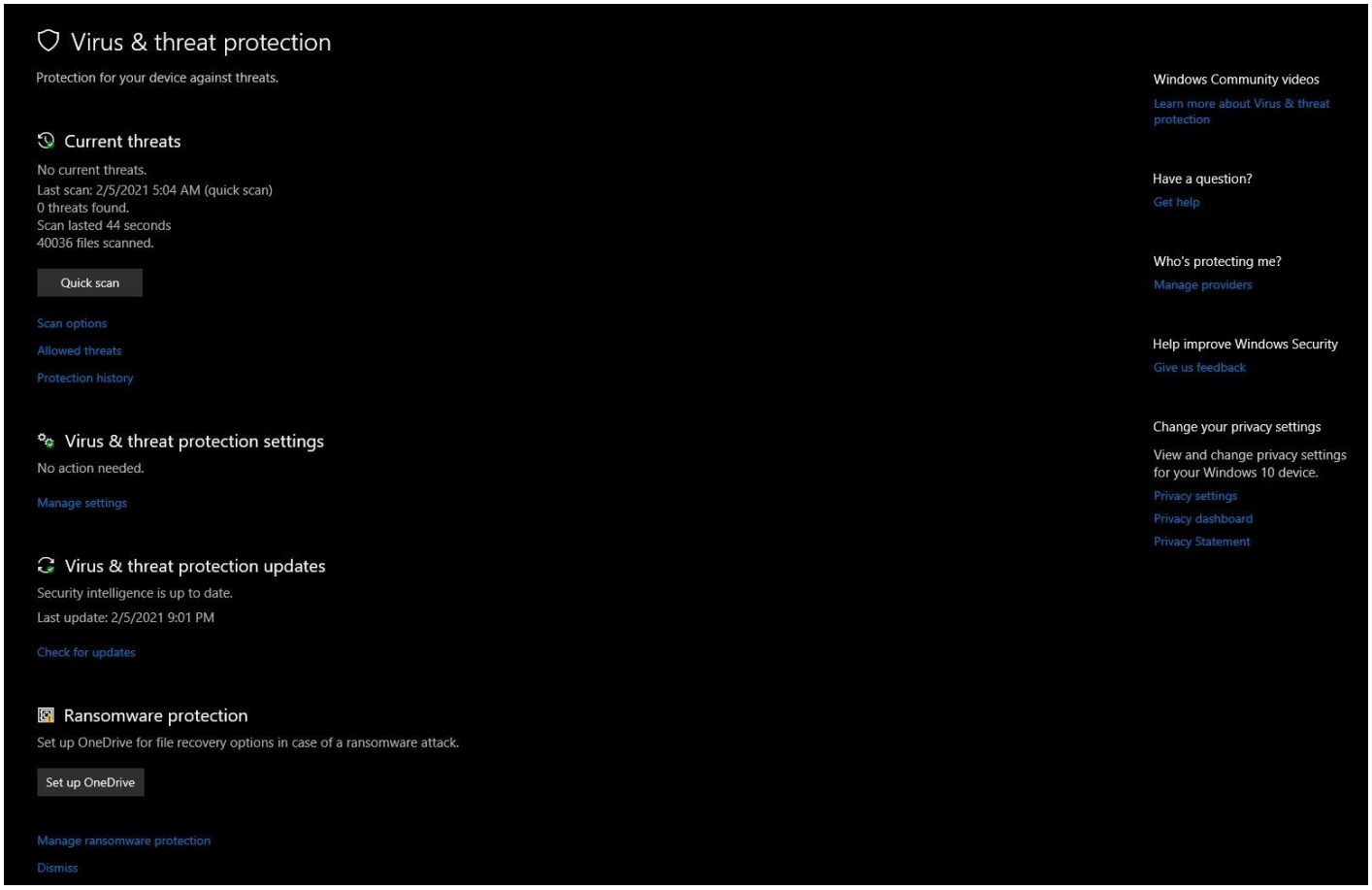
Most people may not have the resources or need to worry about this as much as a corporation would, so a few things you can do are simple and probably set up for most Windows 10 users. If you look in your settings under Update & Security, you'll find a few tabs to make sure your system is safe. Windows Defender and Google Chrome does a great job at keeping its users as safe as possible and has their own alerts built in for you. Here's a few pictures really quick to show you what settings you can look for in your Operating System:



This particular setting is turned off for me because of my own set up and settings, but if you don't have anything extra, it'd be a good idea to have it turned on.



Real-time protection is one of the most important as it is actively working in the background for you while you surf the web and alerts you of any suspicious activity.



Lastly, Windows Defender has its own scanning tool and will run typically once every 24 hours automatically. You can of course always run it manually yourself. Keep in mind this is all preventative maintenance as you will need a full Antivirus/Antimalware program to *fully remove* any threats on the device. Also, because Ransomware is such a threat unfortunately enough to say, they even have their own Ransomware protection, walking you through how to utilize Microsoft's OneDrive cloud based storage.

Conclusion

At the end of day, after all the things that could potentially happen, just remember a few key tips and always be prepared and you should be in the clear. Educate yourself and others on (Spear) Phishing attacks and malicious emails, don't click on suspicious or unsecured links, have some level of threat detection and security set up and lastly, but the most important, backup your data! Ransomware is a notoriously challenging form of malware to detect and protect against. But by taking these necessary precautions, organizations and individuals can effectively safeguard their systems and protect their sensitive data.

Disclaimer

The images and explanations in this presentation were performed in a closed off, sandboxed environment using a Windows 7 Virtual Machine within Oracle's VirtualBox. This was for education and training purposes only. Do not under any circumstances use this knowledge for malicious purposes.

For more information on in depth analysis of the topics discussed here or on how to set up your own sandbox for testing using Oracle's VirtualBox, please go to the ReadMe.txt!

Thank you!