Trent Giever

Project 2-1 and 2-4

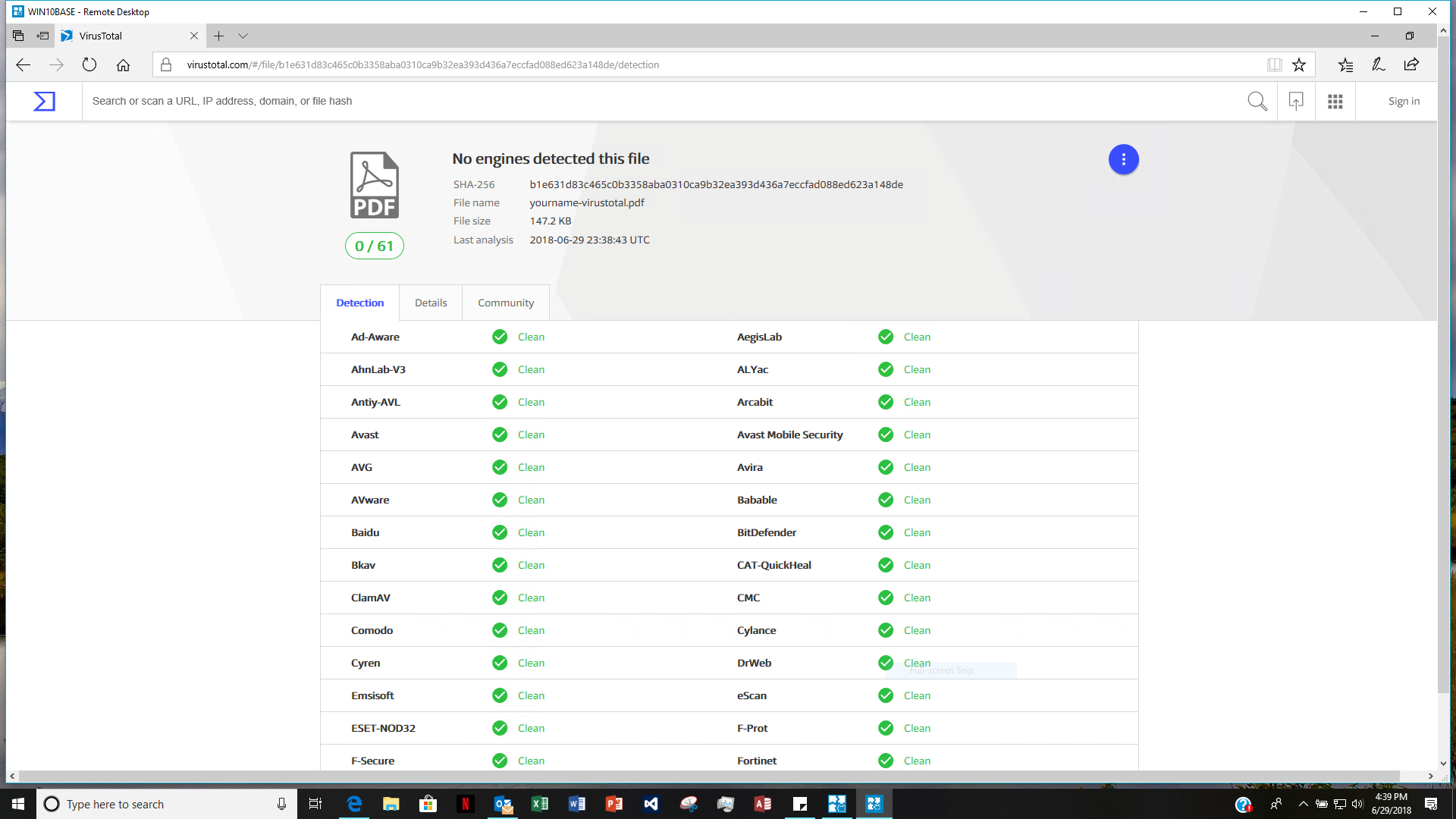
Analyzing Files and URLs for Viruses using VirusTotal

Exploring Ransomware sites

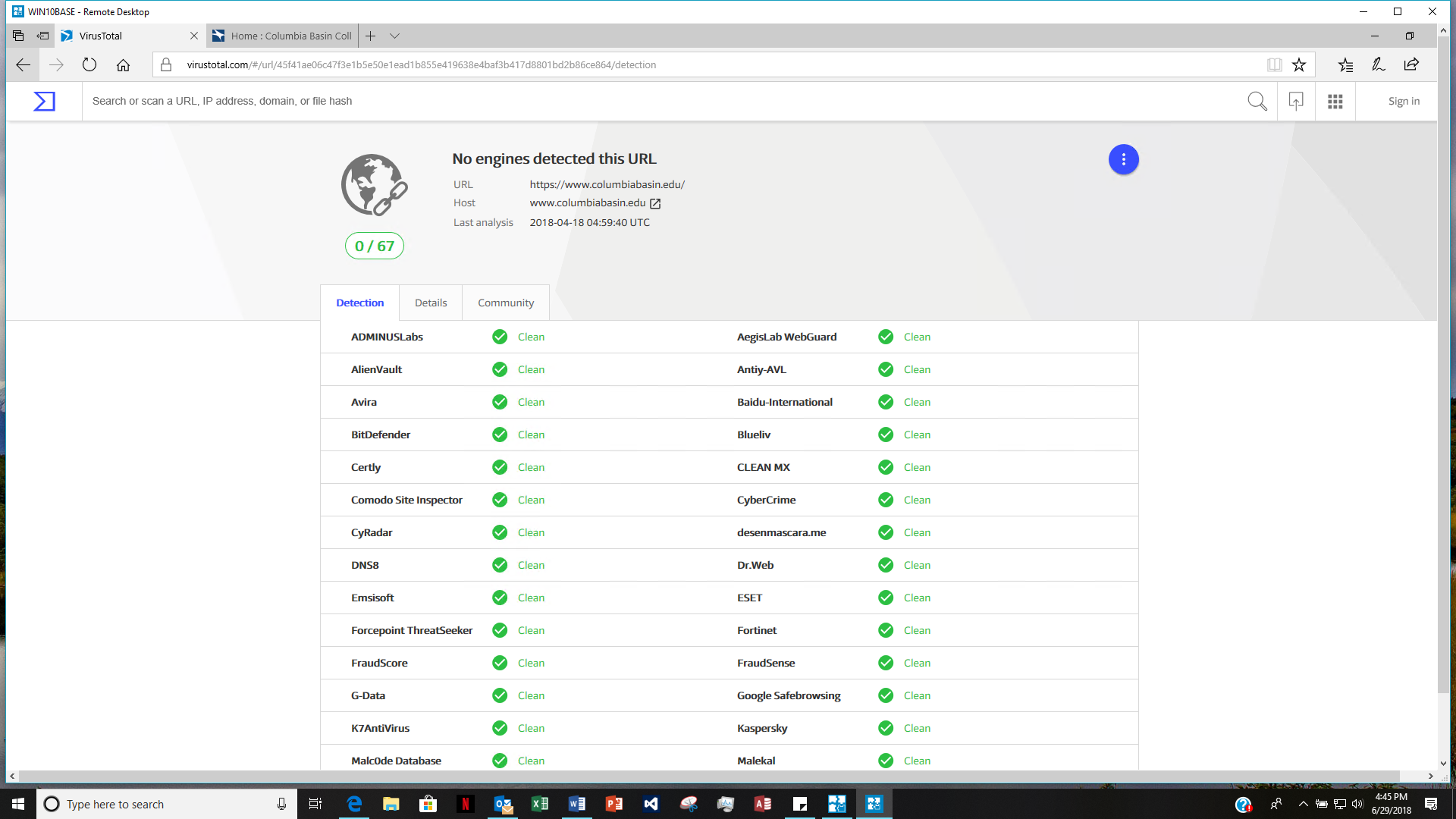
6/29/18

Exploring

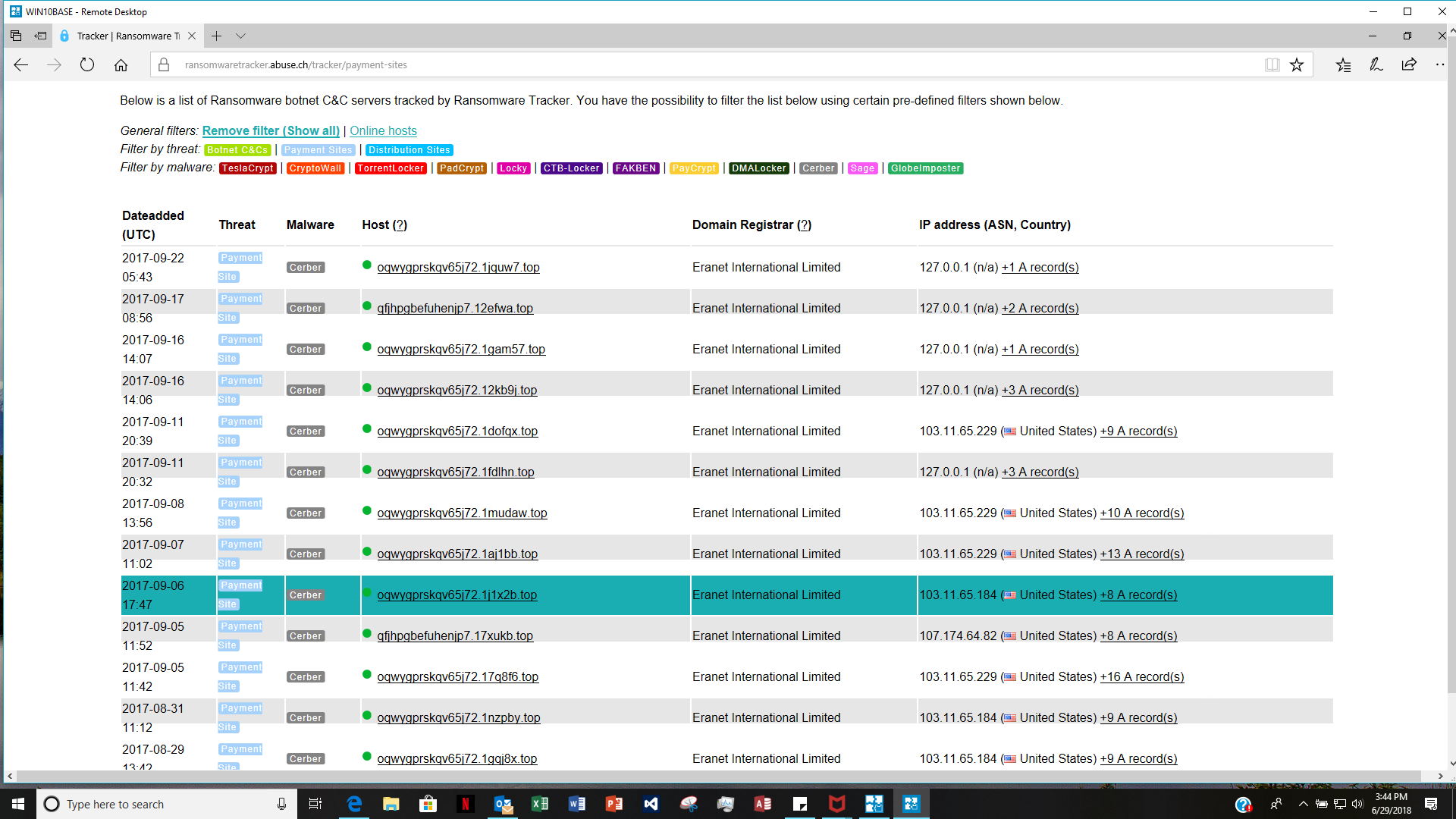
2-1-#15 screenshot



2-1-#22 screenshot



2-4-#5 screenshot



2-1-#15

How would VirusTotal be useful to users? How could it be useful to security researchers? Could it be also used by attackers to test their own malware before distributing it to ensure it does not trigger an AV alert? What should be the protections against this?

This program is like any tool that can help people or harm people. For most users it will scan documents that look suspicious to protect the computer or network. The website might be nice for researchers and the network admins that want to check to see if any files contain the checked malware. There is always the chance that a hacker will check their own work. But most are lazy and know that eventually it will be discovered and blocked, or simply don’t care if it is a sold on the dark web software to hack others. The protections is that the website should also check for unknown malware, but is hard if never scanned before. The best option is to keep a log of scans if it pops up later to have a copy to decrypt faster.

2-4-#7

What Can you tell from it?

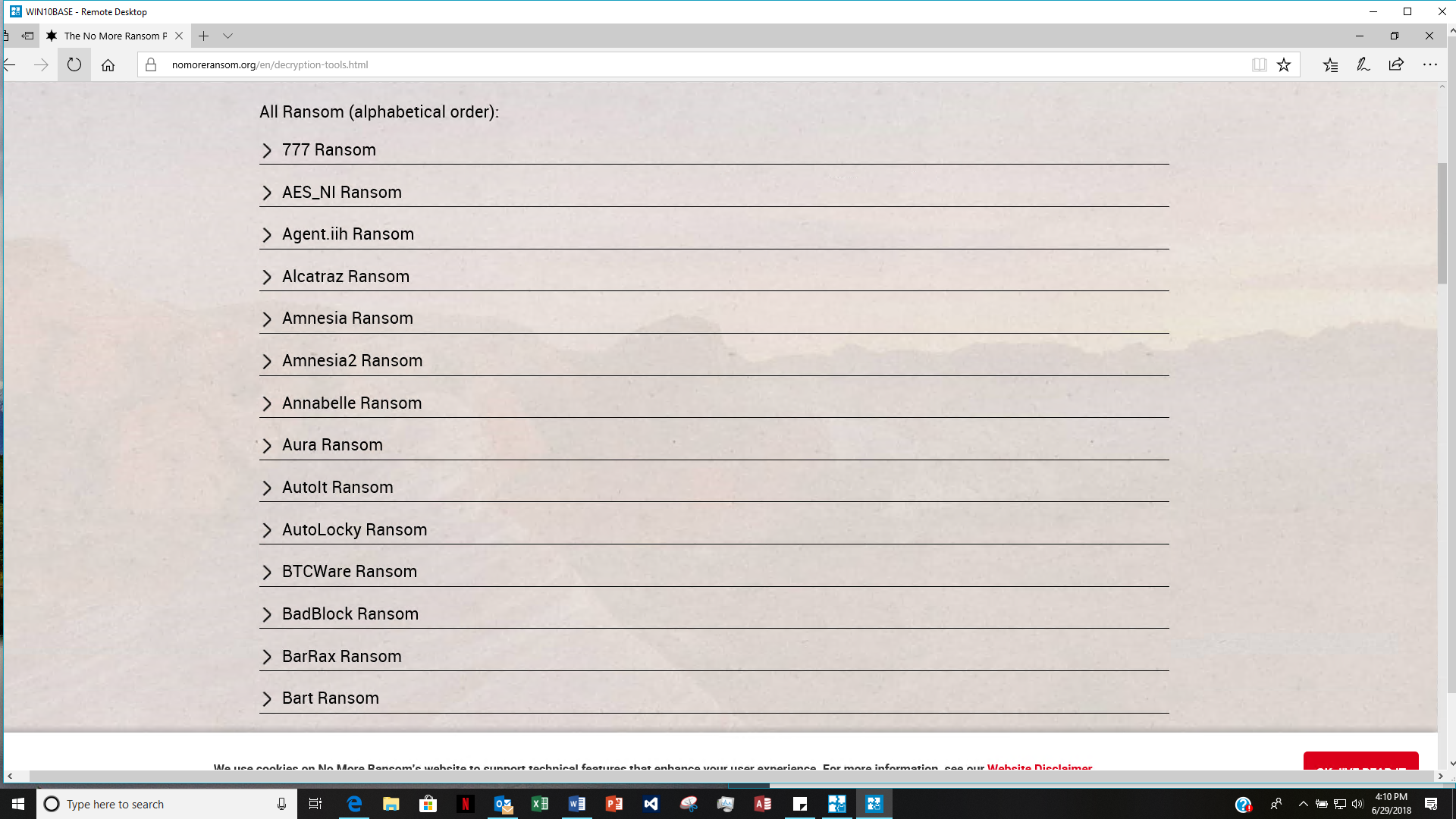
What I can tell from the information in the ransomware tracker website is the URL, IP Address if available, the domain host, and if it is still active along with when created and when abandoned for a different address. The random one I picked had random letters that does not seem to mean anything, and first appeared February 23 of this year, and active for one month. The interesting thing is the website still says it is active botnet even though not active online. I find interesting that bot herders want the IP address online, and that the website says it contains malware.

2-4-#9

How can the be useful to a user who has suffered a ransomware infection?

This can be extremely helpful for everyone. The idea behind it is to upload a copy for either a person or a computer to compare to other ransomware encryptions that have already been solved by the old guess and check method. The other idea is that if a new one has come out then the ransomware needs to be figured out to avoid having to solve it by computers every time it affects a new computer. The upload of two files helps to verify that the file was not already encrypted by the user, and the text box allows the user to relay the information on the screen from the attacker.

2-4-#11 screenshot



2-4-#15

How could these sites be useful?

The first site of ransomware tracker allows people and corporations to download a list of known botnets to prevent that IP address from the system. The other two sites will help people who have had data encrypted to be able to possibly get the data back by uploading samples and by downloading a specific package for that virus. The best solution is to do a scheduled backup to avoid data loss, and to not have to gamble with paying a ransom.