

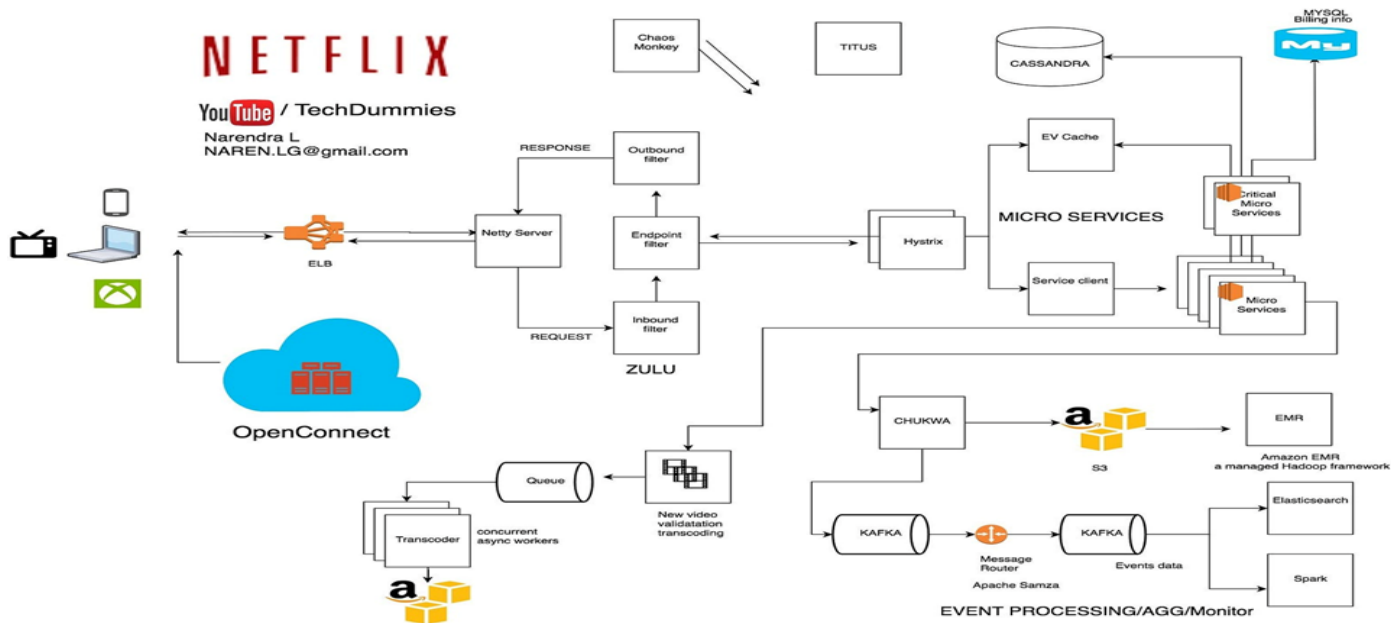
When I come across hacking information using my SAF (Subliminal Acoustic Fingerprinting) technique, I can determine where the access is coming from by investigating, exploring, analyzing, and dissecting the information.

Often clients ask me about different techniques on how they are accessing televisions, gaming systems, computers, phones, appliances and other electronic devices. Truth is, there is more than 1 way to access a persons' network, and not every discovery is the same for all my clients.

I do like to share information on the child/human sex trafficking rings networks when I figure out a huge access point that can affect hundreds of millions of innocent people.

This release of information discusses different applications (apps) that people can use to hack into electronic devices from 1 perspective.

Let's take for instance Netflix streaming service which is **used by over 203.66 million subscribers.** First you must review Netflix network, along with different companies that Netflix uses. This is not the current diagram because ZULU is actually Zuul 2, since 2016 but it is the closest one that I can find for current use.



Using the PAL (Phase Alternating Line) or NTSC (National Television Standards Committee) all depends on your country, location, and frame rates that are authorized to be used by your current place of living. Netflix streaming service is an internet connection that allows a person to download or stream movies, music, gaming services at a faster pace and can connect to multiple different types of electronic devices from computers, gaming, iPads, tablets, television, iOS, Android, with windows operating systems. According to the Netflix diagram, it uses a Netty server for programming and TCP (Transmission Control Protocol), UDP (User Datagram Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) protocols, ZULU (Zuul 2) cloud gateway (Linux/Windows), MySQL database, and Amazon S3 object storing service.

**Now let's pick a port number** which common ports are often numbers 1-4 based on a SOHO (Small Office Home Office) from within a router or modem that a person is using either by a company provider or personal ownership.

Ports are communication endpoints and the number assigned identifies the internet service that the port is being used. Port 3 is a common port number for TCP/UDP services which is what Netflix uses with the Netty Server. There is key information to other operations that coincide with Port 3, like the midnight commander, delta force, and syndrop trojan.

TCP, UDP, FTP, SMTP, use packets to transfer information from one IP address to another IP address. When there is a disruption within the IP and packets get dropped this is called fragmentation. The IP address drops the packets and the Syndrop attacks using a Trojan, which is a virus, connects to the SYN (Synchronization) tag and payload. The synchronization process connects to the operating system, which is either Windows, or now Linux is being used and tested.

A Syndrop Trojan is a type of virus that can be used to infect a computer system and cause internet connection issues, and eventually kill a computer. A Syndrop can be used in the Netflix stream in order to synchronize accounts and electronic devices of the user. To grant access to the Netty server using the main port/3, through the TCP/UDP packets for live streaming capabilities with the use of PAL or NTSC.

PAL and NTSC also uses RGB components with technology systems, which supports (Facial Detection, AI, Biometrics, Law Enforcement: (surveillance, tracking, real-time), Entertainment, ML (Machine Learning), ANN (Artificial Neural Networks), Algorithms, Data Sets, Deep Learning, CNN (Convolutional Neural Network: Image Recognition)) and other BCI (Brain Computer Interface), HCI (Human Controlled Interface), Neural link technology systems.

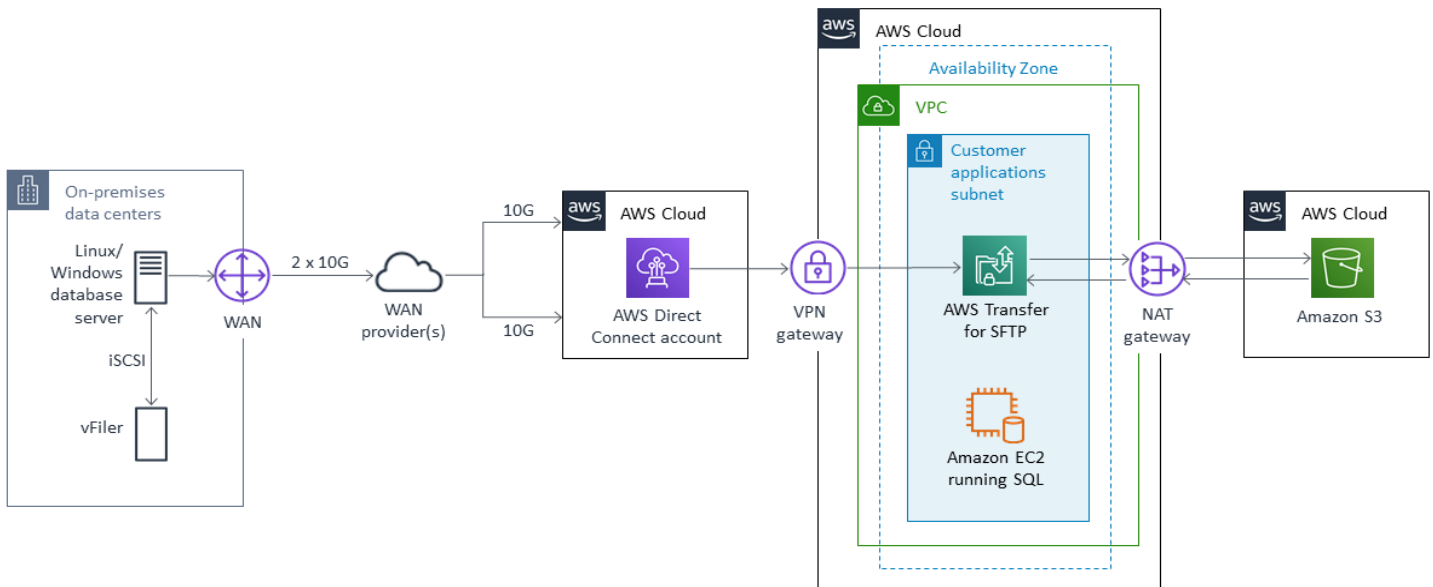
Delta Force, which is a military elite operations group can be granted access to law enforcement surveillance, tracking, GPS locations, and real-time capabilities.

The Midnight Commander also uses port 3 and is a free visual file manager that allows a person to alter, move, delete, copy files within Linux and Windows/SSH. This can help hackers access files, delete or manipulate files of evidence on a person's electronic device, or help with viruses, trojans, malware, through the TCP, UDP, FTP, distribution.

Through fake warrants, illegal warrants, Espionage Act, Patriot Act, 702, etc, would allow access into the users' accounts if they are using Netflix, banking, social media, or access to records and documents.

With Amazon S3 being used as an object storing service, this can give access to a person's individual account if they are an Amazon client or customer. Amazon S3 does have built in data and can run different operations from analytics, AI, machine learning, HPC (High Performance Computing), restores and back up

recovery, and is mobile and web-based cloud services.



Amazon S3 also uses a NAT (Network Address Translation) gateway, this allows private and public use of IP networks that use internet and cloud services. The NAT gateway helps control the packets from IP addresses along with the TCP, UDP, FTP, and SMTP protocols. A NAT gateway sits on the edge of a WAN (Wide Area Network) of a router and is often used with an edge platform. Allowing multiple hosts to share one (1), IP address with port address translation (PAT).

This allows multiple users to hide within a public network so that they cannot be seen within an internal network like the Netflix stream and grants access into a person's account, router, computing and electronic devices. By using the protocols with the TCP, UDP, FTP, HTTP, SMTP, within the Netty Server of the Netflix stream. Linking people into the protocols grants access into the victims account within the Netflix service.

<https://help.netflix.com/en/node/412>

- <https://netty.io/>
- <https://netflixtechblog.com/zuul-2-the-netflix-journey-to-asynchronous-non-blocking-systems-45947377fb5c>
- <https://www.businessinsider.com/guides/streaming/what-is-streaming?op=1>
- <https://www.howtogeek.com/428987/whats-the-difference-between-ntsc-and-pal/>
- <https://www.speedguide.net/port.php?port=3>
- <https://www.adminsub.net/tcp-udp-port-finder/3>
- <https://info.support.huawei.com/info-finder/encyclopedia/en/Local+Attack+Defense.html>
- <https://www.exterminate-it.com/malpedia/remove-syndrop>
- <https://www.military.com/off-duty/2020/02/03/heres-what-we-know-about-delta-force.html>
- <https://midnight-commander.org/>
- <https://aws.amazon.com/s3/>
- <https://www.cisco.com/c/en/us/products/routers/network-address-translation.html>