## Abstract

Following the United States Federal Communication Commission's (FCC) decision to repeal net neutrality, Anonymous has mobilized a digital protest aimed at the FCC, Internet service providers (ISPs) and those that lobby for the repeal of net neutrality. If the repeal of net neutrality is passed by the United States Congress, hacktivists could escalate their protests against those that directly and indirectly support the repeal. Targets could include the FCC, United States Congress, AT&T, Comcast, Spectrum, Charter and other organizations.

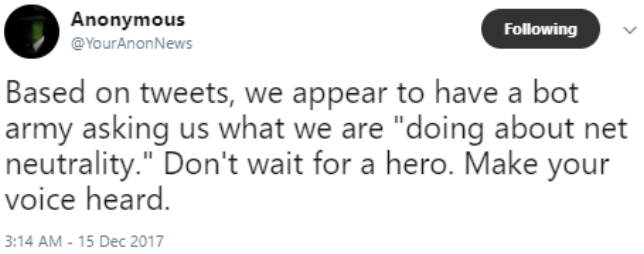


Figure 1: Anonymous preparing for a cyber-attack

## Background

Net neutrality is the principle that Internet service providers must treat all data on the Internet the same and not discriminate or charge differently by user, content, website, platform, application, type of attached equipment or method of communication. On December 14, 2017, the FCC voted to repeal net neutrality.

Following the repeal, different groups within the Anonymous collective began forming digital campaigns to protest the repeal. Currently, there are calls for digital attacks in the form of a denial-of-service attacks, injections and data theft ('doxing'). Some threat actors have pasted[i] "whois" details for fcc.gov under the tag OpFCC while others shared personal information of key figures at the FCC, such as FCC chairman Ajit Pai.

Anonymous says this protest is not a political issue but a human rights issue in regards to net neutrality. The hacktivist group believes the repeal of net neutrality will forever change the way the Internet is accessed in the United States. Anonymous believes that the repeal of net neutrality would result in wide spread censorship while creating a "pay-to-play" system that would drive small companies out of business. Anonymous demands that the FCC and ISPs treat all content equally and not give preference over certain services.

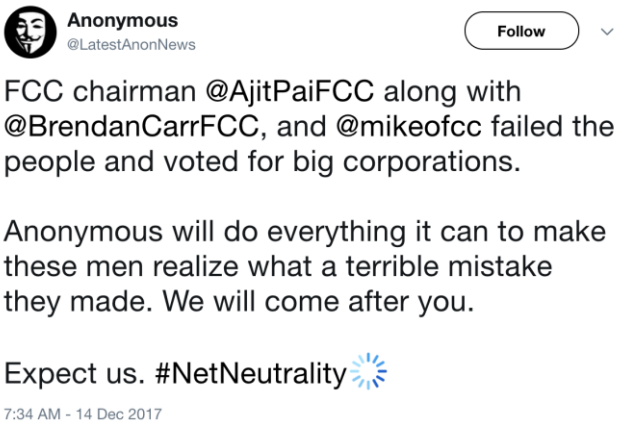


Figure 2: Anonymous threatens FCC officials

## Potential Victims of Cyber-Attacks

Anonymous hacktivists appear to be selecting potential targets from a Sunlight Foundation report that identifies corporations that have lobbied for net neutrality from 2005-2013. Companies listed in the 'Anti' category could expect cyber-attacks if actions are not taken to stop the repeal of net neutrality by Congress.

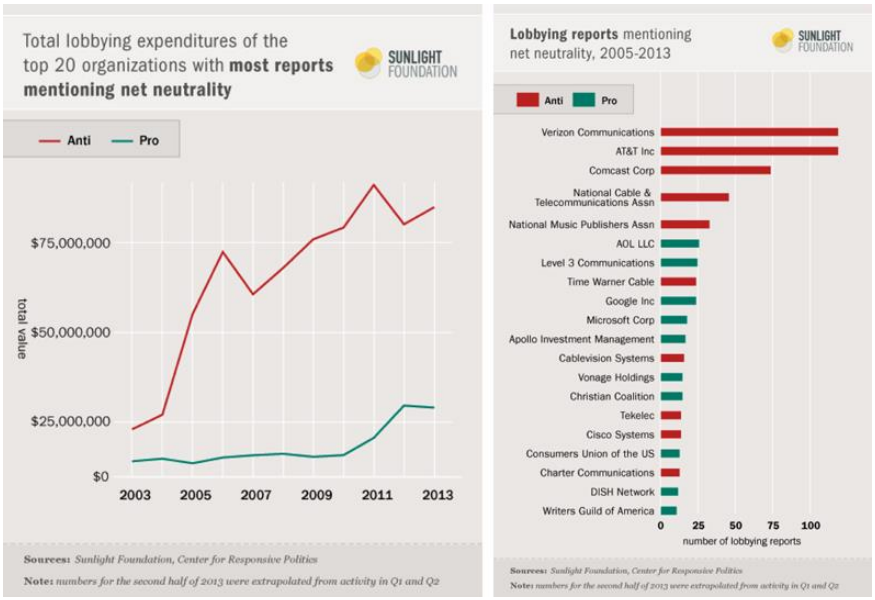

Figure 3: Sunlight Foundation Report on Lobbying for Net Neutrality

## Attack Vectors

### Web Application Attacks

- **Cross-Site Scripting** - In this attack, malicious scripts are injected into websites through a web application flaw where there is no validation of user input used by the application. The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
- **SQL Injection** - This technique takes advantage of poor application coding. When the application inputs are not sanitized it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.
- **Remote File Inclusion (RFI)** - This is a type of vulnerability most often found on PHP running websites. It allows an attacker to include a remotely hosted file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity can lead to arbitrary code execution.
- **Local File Inclusion (LFI)** – This is very much like RFI; the only difference is that in LFI the attacker has to upload the malicious script to the target server to be executed locally.

**Denial-of-Service Attacks**

- **ICMP**: Internet Control Message Protocol (ICMP) is a connectionless protocol used for IP operations, diagnostics, and errors. An ICMP Flood - sending an abnormally large number of ICMP packets of any type (especially network latency testing “ping” packets) - can overwhelm a target server that attempts to process every incoming ICMP request, until a denial-of-service condition for the target server.
- **TCP flood** - One of the oldest, yet still very popular denial-of-service attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall which also has to process and invest in each SYN packet. Unlike other TCP or application-level attacks the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.
- **UDP Flood** – In a UDP flood, the attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is “connectionless” and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. In most cases the attackers spoof the SRC (source) IP.
- **SYN:** A SYN flood overwhelms a target machine by sending thousands of connection requests to it using spoofed IP addresses. This causes the target machine to attempt to open a connection for each malicious request and subsequently wait for an ACK packet that never arrives. A server under a SYN flood attack will continue to wait for a SYN-ACK packet for each connection request, as the delay could be normal and related to network congestion. However, because a SYN-ACK packet never arrives for any of the connection requests; the massive number of half-open connections quickly fills up the server’s TCB table before it can time any connections out. This process continues for as long as the flood attack continues.
- **HTTP/S Flood** - An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server’s resources, and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack’s overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.
- **NTP**: The attacker sends spoofed NTP packets, containing monlist request code, to the vulnerable NTP servers. Monlist is a command requesting a list of the last 600 hosts who connected to the addressed NTP server. The NTP servers then send large replies to the spoofed IP, the victim, thus flooding the victim. This attack generates a great deal of traffic and can easily cause DoS.
- **DNS Amplification Attack:** DNS amplification attack is a sophisticated denial of service attack that takes advantage of DNS servers' behavior in order to amplify the attack. In order to launch a DNS amplification attack, the attacker performs two malicious tasks. First, the attacker spoofs the IP address of the DNS resolver and replaces it with the victim's IP address. This will cause all DNS replies from the DNS servers to be sent to the victim's servers. Second, the attacker finds an Internet domain that is registered with many DNS records. During the attack, the attacker sends DNS queries that request the entire list of DNS records for that domain. This results in large replies from the DNS servers, usually so big that they need to be split over several packets.

**Other Attacks**

- **Phishing -** A digital attempt to obtain sensitive information from a victim by using a malicious email or website. The attacker solicits personal information by posing as a trustworthy organization or the company itself. These attempts are either sent out to everyone in the company or designed to specifically target key associates. Once an associate falls victim to these cyber-attacks, the hacker will then have the sensitive information required to gain access to certain systems.
- **Social Engineering -** A process of psychological manipulation, more commonly known as human hacking. The goal is to have the targeted victim divulge confidential information or give you unauthorized access because you have played off their natural human emotion of wanting to help or provide them with something. Most of the time the attacker's motives are to either gather information for future cyber-attacks, to commit fraud or to gain system access for malicious activity.

## Tools Used by Activists

Democracy.io – This is a project hosted by the Electronic Frontier Foundation (EFF) that allows to email your two senators and representatives through a single website.

Resistbot – This is a project that allows you to text RESIST to 50409 or message the bot via Facebook Messager to find a Congress representative and message them.

Battle for The Net – This is a project that allows you to write to Congress with a pre-scripted letter requesting that they use the Congressional Review Act to pass a resolution of disapproval.

## Social Networks Hashtags

- #opfreenet
- #opfinalstand
- #opdefendthenet
- #OpFCC

## Discord Channel

https://discordapp.com/invite/Vqg3J2r

## YouTube

Operation Free Net - https://youtu.be/0afjs4-7Eio
Message to Ajit Pai and the FCC - https://youtu.be/FFZ-AYasg4A


Figure 4: Anonymous OpDefendTheNet Campaign Banner

## How to Prepare

### Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further DDoS protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

### Effective Web Application Security Essentials

- **Full OWASP Top-10 Application Vulnerabilities Coverage**– against defacements, injections, etc.
- **Low False Positive Rate** – using negative and positive security models for maximum accuracy
- **Auto-Policy Generation** capabilities for the widest coverage with the lowest operational effort
- **Bot Protection and Device Fingerprinting Capabilities** to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, **and** activity tracking mechanisms to trace bots and guard internal resources
- **Flexible Deployment Options** - on-premise, out-of-path, virtual or cloud-based

## Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

## Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

[i] https://hastebin.com/lolaguwipu.scala