1. What are some of the most interesting recent DoS attacks. (Write about 2)

There are a few DoS attacks I have found are interesting. Below are the two recent attacks

1) There were organizations affiliated with Rio Olympics suffered a prolonged DDoS attack since the beginning of September 2015. The attack utilized a DDoS-for-hire service called LizardStresser to launch attack against the targets in size from tens of Gbs into the hundreds of Gbs. The attackers added additional firepower to their UDP reflection/amplification attack vectors, including requests targeting the IP protocol Generic Routing Encapsulation (GRE) and high-volume packet-floods destined for UDP/179 as the Game got closer. The attack ultimately peaked at 540 Gbps.

2) On April 1 2016, Anonymous, the global hacking collective, launched a DDoS attack against Donald Trump. The attackers hoped to take down his presidential campaign website as well as his hotel chain, and the email servers. Around the time of the Election Day, the attackers made an attempt to take down the campaign websites for both Hillary Clinton and Donald Trump.

1. What about attackers that threaten an attack unless a fee is paid?

Many websites can mitigate the attack via some third parity DoS mitigating services rather than paying the fee. Paying a fee will only encourage this type of crime.

1. How can these attacks be prevented?

It is difficult to prevent a DoS attack. Sometimes it requires coordination with the Internet Service Provider (ISP). The ISP can route traffic targeting at the victim to trash. Nonetheless, it trashes all the packets, including those from legitimate users. On the other hand, to reduce the chance an attacker will use your computer to attack other computers, you can follow the following security practices:

* Install and maintain anti-virus software
* Install a firewall, and configure it to restrict traffic coming into and leaving your computer
* Apply email filters to trash unwanted traffic automatically.

It is very difficult to defend against a sophisticated DoS attack launched by a determined adversary. Many organizations struck by a DoS are left to scramble in an effort to stop the attack once it has already begun. Sometimes this requires coordination with the ISP that provides network access. This is especially true when an ISP is forced to "null route" a victim – meaning that to protect other customers, the ISP routes traffic intended for the victim into the trash. This of course effectively prevents all access, including from legitimate users. One of the more well-known countermeasures against a SYN flood is the use of "SYN cookies" either in the server OS or, better yet for network efficiency, in a network security device at the network edge such

the global hacking collective Anonymous launched a DDoS campaign against Donald Trump. Under the banner [#OpTrump](http://www.ibtimes.co.uk/anonymous-hacktivists-launch-ddos-attacks-against-websites-donald-trump-1552750), the group sought to take down the billionaire’s websites for his hotel chain and presidential campaign, as well as his email servers. Anonymous hoped the attack would help end Trump’s bid for the White House and damage his brand.

Later in the year, around the time of the Election Day, attackers once again made the unusual move of targeting political candidates. This time they leveraged a Mirai IoT botnet to [target the campaign websites for both Hillary Clinton and Donald Trump](http://www.techrepublic.com/article/hackers-attempt-ddos-attacks-on-clinton-and-trump-campaign-websites-using-mirai-botnet/). Both DDoS campaigns consisted of HTTP layer 7 attacks that lasted for only 30 seconds.

4. RIO OLYMPICS

Several public-facing web properties and organizations affiliated with the Rio Olympics suffered a [sustained DDoS attack](https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-a-massive-540-gbsec-ddos-attack-failed-to-spoil-the-rio-olympics/) that lasted for several months. Beginning in September 2015, the campaign made use of a DDoS-for-hire service called LizardStresser to launch attack traffic against their targets ranging in size from tens of gigabits/sec up into the hundreds of gigabits/sec.

As the Games drew closer, LizardStresser – along with several other Internet of Things (IoT) botnets – added some additional firepower to their UDP reflection/amplification attack vectors, including requests targeting the IP protocol Generic Routing Encapsulation (GRE) and high-volume packet-floods destined for UDP/179. The attack ultimately peaked at 540 Gbps.

A DDoS campaign of that magnitude and longevity could have easily disrupted the logistics and media coverage of the Olympics. But thanks to the mitigation measures provided by Arbor Networks, Brazilian information security professionals and the International Olympics Committee (IOC) kept their systems up running.

3. CLINTON AND TRUMP CAMPAIGN SITES

On  April 1, the global hacking collective Anonymous launched a DDoS campaign against Donald Trump. Under the banner [#OpTrump](http://www.ibtimes.co.uk/anonymous-hacktivists-launch-ddos-attacks-against-websites-donald-trump-1552750), the group sought to take down the billionaire’s websites for his hotel chain and presidential campaign, as well as his email servers. Anonymous hoped the attack would help end Trump’s bid for the White House and damage his brand.

Later in the year, around the time of the Election Day, attackers once again made the unusual move of targeting political candidates. This time they leveraged a Mirai IoT botnet to [target the campaign websites for both Hillary Clinton and Donald Trump](http://www.techrepublic.com/article/hackers-attempt-ddos-attacks-on-clinton-and-trump-campaign-websites-using-mirai-botnet/). Both DDoS campaigns consisted of HTTP layer 7 attacks that lasted for only 30 seconds.

While it’s unusual for DDoS groups to set their sights on political targets, their decision to do so comes at a time when digital sleuths are [increasingly using their expertise to meddle in states’ internal affairs](https://www.tripwire.com/state-of-security/latest-security-news/russian-hackers-infiltrate-dnc-steal-research-on-donald-trump/).

### How do you avoid being part of the problem?

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

* Install and maintain anti-virus software (see [Understanding Anti-Virus Software](https://www.us-cert.gov/ncas/tips/st04-005) for more information).
* Install a firewall, and configure it to restrict traffic coming into and leaving your computer (see [Understanding Firewalls](https://www.us-cert.gov/ncas/tips/st04-004) for more information).
* Follow good security practices for distributing your email address (see [Reducing Spam](https://www.us-cert.gov/ncas/tips/st04-007) for more information). Applying email filters may help you manage unwanted traffic.

**What about attackers who threaten a DoS attack unless a fee is paid?**

Application Denial of Service attacks have rapidly become a commonplace threat for doing business on the internet. Denial of Service attacks can result in significant loss of service, money and reputation for organizations. DoS attacks are so hard to stop that it's not unheard of for some companies to surrender to extortion attempts, quietly handing their attackers tens or hundreds of thousands of.

**How can these attacks be prevented?**

It is very difficult to defend against a sophisticated DoS attack launched by a determined adversary. Many organizations struck by a DoS are left to scramble in an effort to stop the attack once it has already begun. Sometimes this requires coordination with the ISP that provides network access. This is especially true when an ISP is forced to "null route" a victim – meaning that to protect other customers, the ISP routes traffic intended for the victim into the trash. This of course effectively prevents all access, including from legitimate users. One of the more well-known countermeasures against a SYN flood is the use of "SYN cookies" either in the server OS or, better yet for network efficiency, in a network security device at the network edge such

he FBI adds that, in most cases, victim companies have successfully mitigated the attack using third party DDoS mitigating services rather than paying the ransom. The agency has published the following technical details of what the targeted businesses have experienced:

The first DDoS attack is usually delivered prior to the sending of a ransom demand at 20-40 Gigabytes per second (Gbps) with a duration of approximately one hour.

After the initial DDoS attack, an extortion email is sent to the victim introducing the attacker, highlighting the initial demonstrative DDoS attack, and demanding payment in Bitcoin (ranging from 20-40) to ensure no further DDoS attacks are conducted against the business. If payment does not occur within 24 hours, a second demonstrative DDoS is generally conducted at a higher rate (40-50 Gbps) for an additional hour followed by an additional extortion e-mail.

The types of DDoS attacks primarily consist of Simple Service Discovery Protocol (SSDP) and Network Time Protocol (NTP) reflection/amplification attacks with the occasional SYN-flood and, most recently, WordPress XML-RPC reflection/amplification attacks.

Don't let cyber criminals take your business offline!

We encourage all legitimate businesses to be aware of this extortion scheme and to prepare to fend off any and all targeted DDoS attacks so that your business is unaffected by the attacks. Give us a call to learn about your defense options.

If you do experience an extortion attempt and/or a DDoS attack, the FBI would like to hear from you: