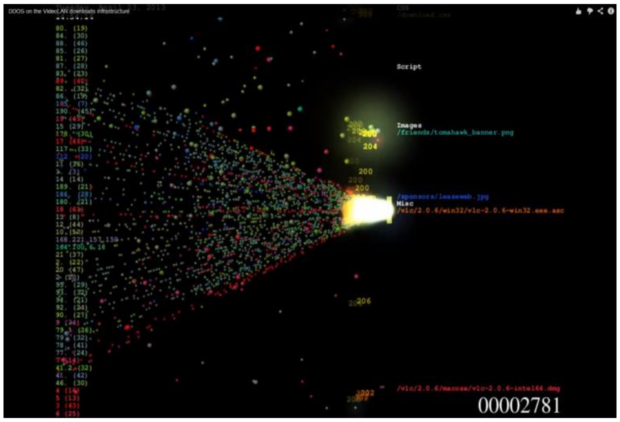
DISTRIBUTED DENIAL OF SERVICE ATTACK DDOS

A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic. Unlike traditional Denial of Service (DoS) attacks, which are carried out by a single source, DDoS attacks involve multiple compromised systems, often referred to as "bots" or "zombies," that are coordinated to flood the target with a massive volume of requests or data packets.


DDOS on the VideoLAN downloads infrastructure
Tuesday, April 23, 2013
CSS
/download.css
Script
Images
/friends/tomahawk_banner.png
/sponsors/leaseweb.jpg
Misc
/vlc/2.0.6/win32/vlc-2.0.6-win32.exe.asc
/vlc/2.0.6/macosx/vlc-2.0.6-intel64.dmg
200
204
206
00002781

Actual cases and examples/How the attack happens

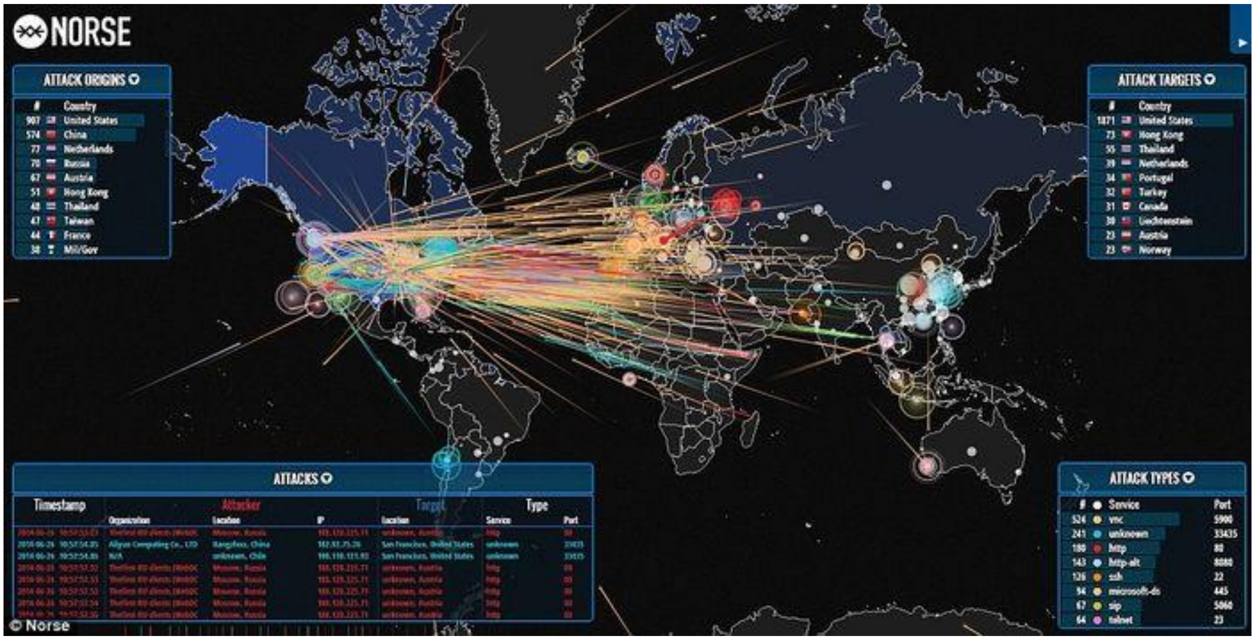
Botnet Formation: The attacker gains control over many internet-connected devices, such as computers, servers, routers, IoT devices, or even smartphones, by infecting them with malware or exploiting vulnerabilities. These compromised devices become part of a botnet, a network of enslaved devices under the attacker's command.

Coordination: The attacker orchestrates the botnet to send traffic to the target server or network. Depending on the attack's nature, this traffic flood can consist of various requests, such as HTTP requests, UDP or TCP packets, or even malformed data packets.

Overwhelm: The targeted server or network becomes overwhelmed by the sheer volume of incoming traffic, causing it to slow down, become unresponsive, or even crash. This results in a denial of service to legitimate users who cannot access the targeted service or website.

DDoS attacks can be categorized based on various characteristics, including the type of traffic they generate (e.g., volumetric, protocol, or application layer attacks) and their duration and intensity. Some attackers may launch DDoS attacks for financial gain, political motives, or competitive advantage or to cause disruption and chaos.

Recent attacks



ATTACK ORIGINS

#	Country
907	United States
574	China
77	Netherlands
70	Russia
67	Austria
51	Hong Kong
48	Thailand
47	Taiwan
44	France
38	Mil/Gov

ATTACK TARGETS

#	Country
1871	United States
73	Hong Kong
55	Thailand
39	Netherlands
34	Portugal
32	Turkey
31	Canada
30	Liechtenstein
23	Austria
23	Norway

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-26 10:57:53.83	[illegible]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:54.85	Aliyun Computing Co., LTD	Hangzhou, China	182.92.75.26	San Francisco, United States	unknown	33435
2014-06-26 10:57:54.85	N/A	unknown, Chile	190.110.121.93	San Francisco, United States	unknown	33435
2014-06-26 10:57:57.50	[illegible]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.51	[illegible]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	[illegible]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.54	[illegible]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.56	[illegible]	Moscow, Russia	188.120.225.71	unknown, Austria	http	80

ATTACK TYPES

#	Service	Port
524	vnc	5900
241	unknown	33435
180	http	80
143	http-alt	8080
126	ssh	22
94	microsoft-ds	445
67	sip	5060
64	telnet	23

© Norse

Multiple botnets exploiting one-year-old **TP-Link flaw** to hack routers: At least six distinct botnet malware operations are hunting for TP-Link Archer AX21 (AX1800) routers vulnerable to a command injection security issue reported and addressed last year.
PurpleFox malware infects thousands of computers in Ukraine: The Computer Emergency Response Team in Ukraine (CERT-UA) warns about a PurpleFox malware campaign that has infected at least 2,000 computers.

No, 3 million electric toothbrushes were not used in a DDoS attack: A widely reported story that 3 million electric toothbrushes were hacked with malware to conduct distributed denial of service (DDoS) attacks is likely a hypothetical scenario instead of an actual attack.

MySQL servers targeted by '**Ddostf**' DDoS-as-a-Service botnet: MySQL servers are being targeted by the 'Ddostf' malware botnet to enslave them for a DDoS-as-a-Service platform whose firepower is rented to other cybercriminals

OpenAI confirms DDoS attacks behind ongoing ChatGPT outages: During the last 24 hours, OpenAI has been addressing what it describes as "periodic outages" linked to DDoS attacks affecting its API and ChatGPT services.

German financial agency site disrupted by DDoS attack since Friday: The German Federal Financial Supervisory Authority **(BaFin)** announced today that an ongoing distributed denial-of-service (DDoS) attack has impacted its website since Friday.

How to prevent your organization from DDOS attacks?

CyberGhost has features to prevent DDoS from happening as the system identifies users and certifies users against the possibility of being subject as enslaved by the orchestrating bad actors. All unrecognized or authorized users will face the Ghost Technology tactics to make the IP blank and divert the attack to the red team or law enforcement.

However, To mitigate the impact of DDoS attacks, organizations can employ various defensive measures, such as:

Network Monitoring: Implementing network traffic monitoring tools to detect abnormal patterns or spikes in traffic that may indicate a DDoS attack.

Traffic Filtering: Using firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to filter out malicious traffic and block known attack sources.

Content Delivery Networks (CDNs): Deploying CDNs to distribute and absorb traffic across multiple servers and data centers, reducing the impact of DDoS attacks on the origin server.

DDoS Mitigation Services: Subscribing to specialized DDoS mitigation services offered by internet service providers (ISPs) or third-party vendors to identify and mitigate DDoS attacks in real time.

Rate Limiting: Implementing rate-limiting measures to restrict the number of requests or connections from individual IP addresses, preventing the system from being overwhelmed.

Scalable Infrastructure: Designing scalable infrastructure that can dynamically adjust resources to handle sudden spikes in traffic during DDoS attacks without impacting performance.