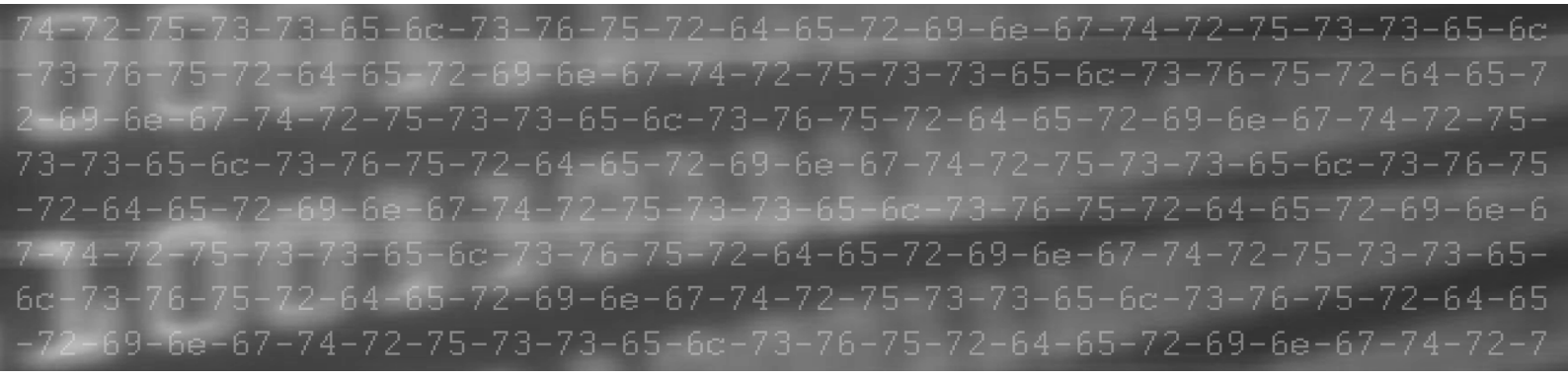
CENTRE FOR
CYBER SECURITY

Threat Assessment

DDoS attacks on the rise in number and scale



Threat Assessment Branch under the Centre for Cyber Security

July 2017

CENTRE FOR
CYBER SECURITY

7 July 2017

Threat assessment: DDoS attacks on the rise in number and scale

Key assessment

- CFCS assesses that the number of DDoS attacks is on the rise. Especially the frequency and size of the largest attacks have increased.

- As DDoS attacks are targeted attacks against specific organizations, some organizations will rarely or never become the targets of such attacks, while others will find themselves frequent targets. Even though an organization may not be the intended target of an attack, it may still risk becoming collateral damage in powerful DDoS attacks against other targets.

- CFCS assesses that Denmark has sufficient capabilities to avert even a coordinated DDoS attack against critical infrastructure in Denmark, ensuring that critical functions are maintained or restored within 24 hours.

- DDoS attacks are commonly used by a variety of cyber threat actors. Though the attacks may target everyone with a visible IP address online, authorities and companies providing online services or online retailers are the industries most likely to suffer from a DDoS attack.

- Cyber criminals pose a serious DDoS threat, primarily launching DDoS attacks against private companies in the pursuit of financial gains.

- CFCS assesses that most DDoS attacks are launched by individuals and that the key motivator behind these attacks is excitement or harassment. Even though most of these attacks are small-scale without the potential to threaten critical functions, this group also includes actors that have the capabilities to launch or buy powerful DDoS attacks.

Analysis

The present threat assessment outlines the threat from Distributed Denial of Service (DDoS) attacks, also known as overload attacks.

All companies, authorities, organizations or private citizens that have a visible IP address on the Internet may become potential targets of a DDoS attack. Launched online, the attacks involve bombarding IP addresses with large amounts of data traffic, causing the underlying homepage, online service or network component to overload, thereby rending it unusable to the users. Traditional IT protection tools such as anti-virus software and continuous patching of software offer no protection against DDoS attacks.

DDoS attack types

Volumetric attacks saturate the available network bandwidth of the target.

Protocol attacks target specific network devices such as firewalls, routers or other network components with the aim of consuming the processing capacity of the target devices.

Application attacks specifically target weaknesses in an application running on a network component like a webserver.

The magnitude of DDoS attacks is hard to determine and there are no accumulated independent statistics on the number of attacks. However, numbers from a leading provider of DDoS protection solutions indicate that in 2016 more than 18 million DDoS attacks were launched globally. Still, the number is subject to great uncertainty as many DDoS attacks are not registered and as the statistics are based exclusively on analysis of part of the data traffic on the Internet. Nevertheless, it suggests that DDoS attacks are common and pose a real cyber threat.

Unlike many other cyber threats, DDoS attacks are targeted attacks against specific organizations, indicating that some organizations will rarely or never become the targets of DDoS attacks, while others will be regular targets. Still, powerful DDoS attacks have the ability to cause widespread collateral damage, putting everyone using the Internet at risk even though they may not have been targeted directly.

A powerful DDoS attacks against, for instance, a website may cause other users sharing IT infrastructure with the target to lose their internet connection. This may be the case if a client with a hosting company is the target of a DDoS attack that is strong enough to overload the hosting company's network, rendering the website of other clients inaccessible online. Internet providers and providers of cloud solutions that involve several clients sharing the same infrastructure face the same challenges, making the DDoS threat particularly serious for these companies.

A very powerful DDoS attack may also cripple or upset central network services or transmission systems on the internet, leaving numerous authorities, companies and private citizens unable to access the Internet.

A very powerful DDoS attack occurred in October 2016 against a US provider of DNS services (DYN). As a result, many users on the US East Coast, among others, who were serviced by the targeted DNS servers lost access to many popular websites and services, including Amazon, Twitter and Spotify. The attack consisted of several separate DDoS attacks that peaked at a bandwidth around 1000 Gbps.

DNS server
An Internet service that translates domain names into IP addresses used by the network components to route online data traffic. Local computers and networks contain DNS servers with IP addresses of websites that have already been visited. If a local DNS server does not contain the address for a website, it will ask a central, so-called authoritative DNS server. If the central DNS server is inaccessible, for instance as a result of a DDoS attack, the computer will be unable to connect to the website.

Denmark is highly digitalized and many of our country's critical functions rely on stable Internet connections, just as many companies rely on their online presence to generate revenue. Some examples are citizen service centres – which today rely extensively on the Internet – Internet service providers, net banks, web shops, social and news media, and online radio and TV streaming. DDoS attacks may render these online services temporarily inaccessible to users and result in loss of revenue and loss of customers and may, ultimately, be harmful to society. The mere threat of a DDoS attack can increase the costs for organizations that feel compelled to invest in additional network capacity or anti-DDoS measures.

A reason for the frequent occurrence of DDoS attacks is the widespread accessibility of DDoS tools online that enables everyone to launch simple DDoS attacks.

Figure 1. DDoS tool for Android downloadable via Google Play

Another reason is the availability of so-called 'booter' or 'stresser' DDoS-for-hire services through online websites.

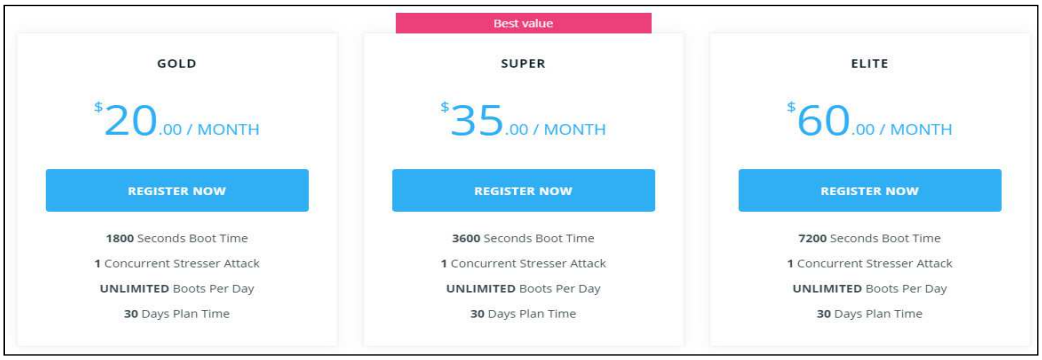


Figure 2. Online price list for Booter service 'Insta Booter'

Apart from giving network owners the opportunity to test the robustness of their own networks to DDoS attacks, the services are available to anyone wanting to launch a DDoS attack against a specific IP address. DDoS attacks can be purchased anonymously, and in addition these websites often offer the possibility of a small 'test' DDoS attack free of charge.

A 2016 doctoral thesis from the George Mason University in the United States proved that three of these booter services had launched more than 600,000 DDoS attacks over a 3-year period.

Even though simple DDoS attacks are easy to launch, a powerful DDoS attack requires substantial resources in the form of infrastructure/attack capacity or funds. As the average cyber actor only has limited resources and does not have access to their own botnet that is capable of generating powerful DDoS attacks against multiple targets simultaneously, the duration of a DDoS attack will always be limited. In recent years, the duration of DDoS attacks has remained fairly constant with around 85 per cent of all registered DDoS attacks lasting less than 30 minutes and less than one per cent lasting more than 24 hours.

Botnet
A network of computers, routers, smartphones and other Internet-connected devices that have been infected by malicious applications or malware, enabling cyber criminals to remotely control a device and stage coordinated DDoS attack.

However, a serious DDoS attack will often comprise a number of separate attacks that vary in type, intensity and duration. A DDoS attack may thus signify that further attacks are imminent. If the first attack proves ineffective, subsequent attacks may increase in intensity. This attack method makes it hard to effectively avert a DDoS attack even if protected by anti-DDoS measures, especially if the DDoS protection must be manually adjusted, activated and deactivated in connection with each attack.

Threat actors and their targets

DDoS attacks have become an increasingly popular tool among cyber threat actors.

Cyber criminals use DDoS attacks for financial gain

Cyber criminals demand payment to stop a DDoS attack or use DDoS attacks as a smokescreen to disguise an even more serious cyberattack. Some cyber criminals offer booter services against payment or use botnets to stage DDoS attack that are powerful enough to even upset companies with significant network capacity. Private online companies are the targets of choice for cyber criminals as these companies are financially vulnerable to DDoS attacks and may thus be more inclined to pay up to stop the attack.

In December 2015, cooperating with a number of countries, Europol unravelled a cybercriminal group called DD4BC (DDoS for Bitcoin) in Bosnia Hercegovina. The group had specialized in DDoS attacks against, in particular, financial institutions and online gaming sites. The target was required to pay a certain amount in Bitcoins for the attack to stop. The registered attacks were launched at a bandwidth designed to upset or cripple access to the targets' websites. Most of the attacks were in the 4 to 30 Gbps range, though the national Swiss CERT claims that the group had sufficient capacity to launch attacks as large as 500 Gbps, if this was required in order to cripple a partially robust target.

Also unravelled in 2015 was the 'Lizard Squad' group, which ran and used the 'Lizard Stresser' DDoS-for-hire service. Lizard Stresser was allegedly hacked in 2015 and leaked data subsequently revealed that nearly 13,000 users had signed up for the service. Our analysis of the leak has shown that several of the infected IP addresses belong to Danish tele and hosting providers.

Most DDoS attacks are launched by thrill-seeking or harassment-driven private individuals

We assess that most DDoS attacks are launched by individuals who have no political or financial motives, whose key motive is excitement or harassment. These individuals base their attacks on knowledge gleaned from a wide range of chat forums where they exchange experiences, buy and sell hacker services or help each other hack into systems or launch DDoS attacks. At present, the Danish hacker forum shellsec.pw has more than 1,700 members and contains several DDoS chat threads. We believe that even though most of the attacks launched by this group are small-scale and not substantial enough to threaten critical functions, the group also includes actors capable of launching or buying powerful DDoS attacks.

The group of private individuals also includes online gamers. In the world of online gaming, DDoS attacks have become a widespread phenomenon, possibly because many gamers are very dedicated to their hobby. As many of these gamers also have in-depth knowledge of the network and computer techniques used in computer games, it is not a far step from aggression to actually launching DDoS attack against a gaming provider, gaming server or adversary with the purpose of harassing or gaining an edge in the game. CFCS assesses that the providers of online computer games are particularly exposed to DDoS attacks.

Cyber activists also use DDoS attacks, albeit on a limited scale

Cyber activists focus on single issues and launch DDoS attacks on authorities and companies which they view as adversaries to their cause. One such example is the 'Anonymous' hacker group which in 2010 launched DDoS attacks against financial companies that refused to handle payments for WikiLeaks. In 2012, Anonymous launched DDoS attacks against Swedish authorities in protest over their raid against a company hosting the Pirate Bay and WikiLeaks file-sharing services. Since early 2016, Icelandic authorities and companies have been repeated targets of DDoS attacks from OpKillingBay, an operation launched by Anonymous in response to the Icelandic whaling trade. Consequently, it would come as no surprise if, in future, the group were to attack Danish targets due to the whaling activities carried out by Greenland and the Faroe Islands. Generally, though, examples of cyber activism in Denmark have been limited, but the threat will increase in case a Danish organization is linked to a case that draws the attention of cyber activists.

Limited extent and effect of DDoS attacks related to terrorism

Hackers with terrorist sympathies also plan and execute DDoS attacks aimed at generating attention to the terrorist organizations and their objectives as part of the intimidation campaigns against civilians. So far, though, the effect of such attacks has been limited, and we have no information on DDoS attacks in Denmark attributable to terrorist groups or their hacker sympathisers, likely because hackers with terrorist sympathies lack the capacity to launch effective DDoS attacks against critical systems and because traditional terrorist groups do not view DDoS attacks as an effective means to their end.

DDoS attacks also employable by states and state-sponsored groups

A number of countries are building offensive cyber capabilities, which may include DDoS attack capabilities. DDoS attacks may be launched as part of a conflict to disconnect or upset critical functions in a country. DDoS attacks may also be launched with a political objective to emphasize a message or sway public opinion in a country, for instance by paralyzing certain media and websites or by upsetting a referendum. The real motives behind such DDoS attacks may be concealed by disguising the attack as cybercrime or cyber activism.
Over a period of three weeks in 2007, Estonia was hit by a wave of coordinated DDoS attacks targeting, in particular, Estonian authorities, media and banks. Estonia and several media saw the attack as a reaction to Estonia's removal of a Russian war memorial.

China is known for its regulation of Internet access that involves blocking the access to certain Internet services, news channels and social media such as Facebook. Internet services that can be used to bypass the 'Great Firewall' have been the targets of repeated DDoS attacks. More public media have speculated that some of these DDoS attacks may have been launched by Chinese authorities. One such example may be the March 2015 powerful attack against the organization Greatfire.org, which addresses the issue of Internet censorship in China. According to technical analyses, the attack originated from China though the analysis did not prove that Chinese authorities were involved in the attack.

Companies may launch DDoS attacks to harm competitors

Companies that sell goods, services or online services may stage DDoS attacks to cause financial and reputational damage to their competitors in a bid to steal their customers. Though we have information that this kind of harassment does occur in Denmark, we hold no information on its extent.

Effect of DDoS attacks

In Denmark, most small and medium-sized companies operate with Internet bandwidths below 50 Mbps, and even large companies often have connections below 1 Gbps. According to reports submitted in 2016 by providers of DDoS protection, the share of registered DDoS attacks exceeding 1 Gbps varies from 20 percent to more than 80 percent of the total number of attacks. Despite major differences in these numbers, CFCS assesses that a significant share of the total number of DDoS attacks may impact even large companies in Denmark.

Internet service provider
Provides Internet connections to customers, typically through fixed or mobile lines.

Website hosting provider
Typically offers the IT infrastructure and IT tools needed to set up a website and connect it to the Internet. The customer manages their own website through the Internet.

Cloud service provider
Offers IT services through the provider's own IT infrastructure to customers that access these services through the Internet. Products range from access to virtual servers or software products such as Microsoft Office to the setting up and operation of advanced IT solutions.

Internet service providers and providers of hosting and cloud services are particularly vulnerable to the DDoS threat as all attacks on their clients are launched through their IT infrastructure. However, such providers often have sufficiently large bandwidth to resist major DDoS attacks. Still, we assess that a DDoS attack of 10 Gbps or more could prove a challenge to several of the Danish providers of internet-based services. There are great variations in the 2016 DDoS reports as to the share of registered attacks exceeding 10 Gbps. CFCS assesses that around 1 percent of the aggregated number of DDoS attacks in 2016 was in the plus 10 Gbps range. However, the trend points towards still more powerful DDoS attacks, increasing the likelihood that in future a greater share of the DDoS attacks will exceed 10 Gbps.

In addition to crippling the website, an effective DDoS attack against a public authority or private company may also disrupt all communication between the organization and the Internet. The Internet outage may occur if a router or firewall, which handles the Internet traffic to and from the organization's internal network, is overloaded or if the so-called 'handshakes' that are required to establish a connection via the Internet cannot be completed due to the DDoS attack. In addition to blocking access to websites, effective DDoS attacks may thus affect other services that rely on Internet connection, including IP telephony, email or access to external cloud solutions.

Today, mobile networks are predominantly used for data traffic to and from the Internet. Simple DDoS attacks can be launched through smartphone apps, and mobile units may form part of botnets, just as DDoS attacks can be launched against the mobile network infrastructure. Both in Denmark and abroad, DDoS attacks have been launched against mobile network infrastructure, temporarily preventing users from accessing mobile services.

The prevention of DDoS attacks may halt legitimate data traffic. If a client with an Internet service provider is the victim of a serious DDoS attack, the provider may choose to protect his network and other clients by blocking all data traffic to the victim or to block all data traffic from the IP addresses or geographical areas from where the attack originates (geo-blocking). From a client perspective, the former method has the unfortunate consequence that it enhances the effect of the attack and geo-blocking may result in blocking of legitimate traffic from the blocked area, impacting negatively on clients whose infrastructure, offices, sub-contractors or own customers are located in the countries or areas that are geo-blocked.

Danish IT infrastructure is generally resilient to DDoS attacks

A powerful and coordinated DDoS attack against the Internet in Denmark may seriously disrupt Internet traffic, in particular during the first hours of the attack. However, CFCS assesses that Danish Internet providers will be able to alleviate and contain such an attack, ensuring that critical functions are maintained or restored within 24 hours.

The aforementioned 2007 DDoS attacks against Estonia may be interpreted as an attempt at paralyzing the country's Internet access, and in November 2016 a DDoS attack against Liberia's Internet affected the majority of the country's citizens' access to the Internet. Estonia successfully alleviated the attack, including by using the above methods, as would Denmark in a similar situation. The reason for the major negative impact of the attack in Liberia was the fact that Internet access in Liberia comes via a single cable. Conversely, Denmark has several external underground and submarine Internet cables.

A DDoS attack on the entire Danish Internet infrastructure may seek to overload the networks of the largest Internet providers to the point where they do not have sufficient capacity to route data traffic to underlying networks. A coordinated DDoS attack may also target critical websites and online services. Finally, an attacker may attempt to overload the authoritative DNS servers that handle the 'address book' for all websites with names ending in '.dk'. However, these networks and servers have significant network capacity and often use different types of DDoS protection. Consequently, they are robust and capable of handling or filtering major DDoS attacks launched against themselves or their clients.

Mitigating a coordinated DDoS against Denmark presents a challenge as it would require huge administrative and practical efforts to coordinate the DDoS detection and mitigation for each individual network that is part of the Danish Internet. The repercussions of such an attack would

thus be most severe during the first 24 hours when the preparedness plans have not yet been fully activated.

The future DDoS threat

The number of DDoS attacks is on the rise as are the frequency and extent of the powerful attacks. Since 2013, there has been a strong increase in the bandwidth of the most powerful registered DDoS attacks. Consequently, attacks may be over several hundred Gbps in size, enabling them to threaten the capacity of central Internet services and the networks of the largest Internet service providers. A global provider of DDoS protection registered the first attack exceeding 100 Gbps in 2013. Since then, the number has climbed to more than 500 in 2016. Even though attacks exceeding 100 Gbps still account for a very small share of the overall number of DDoS attacks, attacks of this magnitude do occur in Denmark. CFCS assesses that the increasing trend will continue.

Internet of Things may promote continued increase in powerful DDoS attack frequency

Contributing to the increase in frequency and size of the most powerful attacks is the fact that more and more products, such as refrigerators and baby monitors are connected to the Internet – the so-called Internet of Things (IoT) trend. When more units are connected to the Internet, some of them will invariably contain vulnerabilities that can be exploited to launch DDoS attacks. The risk is especially present if the manufacturer of the unit does not prioritize or has limited experience in incorporating cyber security into the Internet-connected products. Also, many of the future IoT units will likely never receive the security updates that could otherwise remove potential vulnerabilities.

The October 2016 DDoS attack mentioned above against DYN thus used a botnet comprising compromised IoT units to launch a 1,000 Gbps attack.

According to a November 2016 Ericsson Mobility Report, over 5 billion IoT units are connected to the Internet, a figure which according to Ericsson's estimations will increase to 18 billion in 2021. As a result, the number and size of the most powerful DDoS attacks will likely increase proportionally.

IoT has resulted in the emergence of a host of new network technologies, including Narrowband IoT, which is based on the existing 4G mobile network; LoRa, which is a type of WiFi network; and the new national SigFox network. In Denmark, these networks are already in operation or in the process of being established. All of these networks are connected to the Internet and thus potential components of a DDoS attack. However, the LoRa and, in particular, SigFox network capacity is too small to be used in DDoS attacks. Still, the low data capacity makes the new networks potential targets of DDoS attacks.

Open services in network equipment facilitates continued amplification attacks

Around half of all registered volumetric DDoS attacks are launched as so-called amplification attacks. Amplification attacks are enabled by the fact that the network equipment of many Internet users contains so-called open services that respond to all enquiries from any online computer. As the owner of the network component most often does not experience any problems if the component is part of a DDoS attack, there is little incentive for the owner to check and secure the equipment. DNS servers are often used as part of amplification attacks. According to the openresolverproject.org website, there were more than 10 million open DNS servers online in January 2017. Although the number of open servers has dropped from more than 20 million in 2013, CFCS assesses that the total number of open servers online is large enough for the threat from amplification attacks to remain unchanged in the medium term.

Amplification attack

Volumetric attacks that are amplified by exploiting the fact that some internet services will generate a high volume of data traffic in response to small requests. An attacker may send out thousands of such requests with a spoofed source IP address identical to the victim thereby routing replies back to the victim's network that is overwhelmed with data traffic.

Increased digitization and centralization of data services may enhance the effect of future DDoS attacks

The increased digitization of society deepens the dependence of authorities, companies and citizens on online services. As healthcare systems, the waste collection industry, public street lighting, public utility, indoor climate technology, transportation, etc. are increasingly connected to the Internet, a DDoS attack against these services could potentially be harmful to critical functions.

More and more authorities and companies are using so-called Cloud Computing that enables the moving of data, IT infrastructure or online services to central data centres. The increasing use of cloud solutions may result in proportional centralization of critical IT infrastructure and data. If a cloud solution is connected via the Internet, this enhances the dependence on stable Internet connections. An effective DDoS attack against a cloud solution or a provider of Cloud Computing may target more authorities or companies simultaneously, ultimately resulting in severe repercussions across society.

Recommendations

CFCS recommends that all authorities and companies incorporate the threat from DDoS attacks in their risk assessments. When assessing the risk, it is crucial also to include the DDoS threat against sub-contractors. This is particularly important if critical parts of the business rest with a hosting or cloud provider.

In addition to DNS, a number of other network services can also be exploited in amplification attacks. We recommend that all companies and authorities acquaint themselves with the issue and investigate whether their IT infrastructure contains open services that should be re-configured to only accept enquiries from certain IP addresses.

Falsification of the IP source address is a necessary precursor for amplification attacks. Falsification also makes it harder to mitigate DDoS attacks as the origin of the attack is obscured. We recommend that Internet providers and other companies that administer Internet IP-addresses implement the BCP38 standard. This standard contains recommendations on network configuration to prevent IP packages with false source addresses from leaving the network.

Below is the scale of probability the DDIS applies