THE VOICE OF ADVANCED COMMUNICATIONS

COMMS COUNCIL UK
THE VOICE OF ADVANCED COMMUNICATIONS

Comms Council UK DDoS Briefing: Q4 2021

This document is a summary of the DDoS briefing paper prepared by and circulated to Comms Council UK members. This is an edited version of the final document, and some sections have been reserved for members.

Founded in 2004 (and formerly known as ITSPA) Comms Council UK is a UK, membership-led organisation that represents companies who provide or resell business and residential customers voice services over data networks (VoIP) as well as other "over the top" applications including instant messaging and video. The membership is a mixture of network operators, service providers, resellers, suppliers, and consultants involved in a sector that is diversifying rapidly from just voice services to other innovative IP applications.

Contact

For more information, please contact:

Comms Council UK
team@commscouncil.uk
020 3397 3312

Introduction

In late 2021, several UK & US based Internet Telephony Service Providers (ITSPs) were subjected to Distributed Denial of Service (DDoS) attacks, along with ransom demands claiming to be from a group called REvil ("Ransomware-Evil") demanding payment in bitcoin to halt current and/or future attacks.

These attacks were sophisticated and specific, and resulted in different levels of service disruption - from websites being offline and reduced call quality to complete inbound and outbound voice service outages.

Are you prepared for the 'new normal'?

We have to accept that the cost of providing reliable voice and communication services over the Internet has now increased and that having systems in place for detection & mitigation of DDoS attacks is a cost of doing business in this new age.

Comms Council UK (CCUK) engaged with members to understand the nature of the attacks and then held various meetings with Ofcom, the National Cyber Security Centre (NCSC), Department of Culture, Media and Sport (DCMS) and law enforcement to update them on threats, as well as to secure further engagement on the issue.

As stated at the top of this document, this is a summary of the briefing paper which was written by and distributed to members in December 2021. Some sections have been shortened, and others are redacted altogether, as they are only available for members.

We urge all members to remain vigilant and to develop incident response plans. We also urge all members to report directly to us, via team@commscouncil.uk, if they have received a ransom message or come under attack.

Disclaimer

The information contained in this guidance is for your information only and is not intended to be relied on. It does not constitute legal professional advice, nor is it a substitute for you obtaining your own legal professional advice relevant to your circumstances. Comms Council UK accepts no liability whatsoever for any errors, omissions or statements contained in this guidance or for any loss which may arise from your use of this guidance. Comms Council UK owns absolutely and exclusively all copyright, moral rights, and any other proprietary rights for their full terms throughout the world in respect of the information contained in this guidance. ©2022 Comms Council UK. All rights reserved.

Contents

1. Distributed Denial of Service attacks (DDoS)

A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted IP system. A DDoS attack uses more than one unique IP address or machine, often from thousands of hosts infected with malware.

Multiple machines can generate more attack traffic than a single machine and multiple attack machines are harder to disable than one attack machine. The fact that the behaviour of each attack machine can be stealthier, makes it harder to track and shut down. Since the incoming traffic flooding the victim originates from different sources, it may be impossible to stop the attack simply by using ingress filtering. It also makes it difficult to distinguish legitimate user traffic from attack traffic when spread across multiple points of origin. As an alternative or augmentation of a DDoS, attacks may involve forging of IP sender addresses (IP address spoofing), further complicating, identifying and defeating the attack. These attacker advantages cause challenges for defence mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines.

The largest reported DDoS attack to date was in September 2017 when Google said that they had absorbed an attack that reached a peak of 2.5 terabits per second (Tbps). Other notable DDoS attacks that have been made public include those against Microsoft's Azure cloud service of 2.4Tbps in August 2021, and Amazon Web Services (AWS) in February 2020 of 2.3Tbps.

2. Common types of DDoS attacks

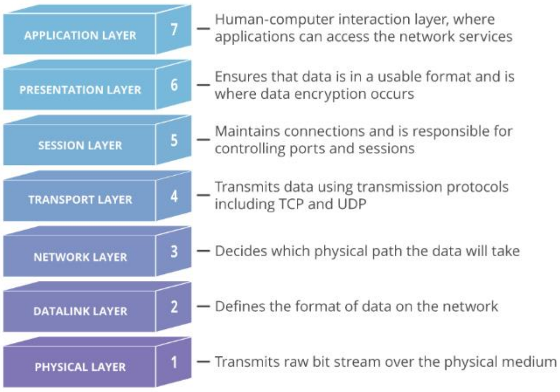
For a good list of the various types of DDoS attacks, refer to the "Denial-of-service attack" page on Wikipedia. Below, we will just cover the three most common types:

1. Application layer attacks
2. Network layer or volumetric attacks
3. Protocol Attacks

Different types of DDoS attacks target varying components of a network connection. In order to understand how different DDoS attacks work, it is necessary to understand how a network connection is made.

A network connection on the Internet is composed of many different components or "layers". Like building a house from the ground up, each layer in the model has a different purpose.

The OSI model, shown below, is a conceptual framework used to describe network connectivity in seven distinct layers.


APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATALINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium

While nearly all DDoS attacks involve overwhelming a target device or network with traffic, attacks can be divided into three categories. An attacker may use one or more different attack vectors, or cycle attack vectors in response to counter measures taken by the target.

3. Identification of a DDoS attack

The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes - such as a legitimate spike in traffic - can create similar performance issues, further investigation is usually required. Traffic analytics tools can help you spot some of these tell-tale signs of a DDoS attack:

- Suspicious amounts of traffic originating from a single IP address or IP range
- A flood of traffic from users who share a single behavioural profile, such as device type, geolocation, or web browser version
- An unexplained surge in requests to a single page or endpoint
- Odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unnatural (e.g. a spike every 10 minutes)
- There are other, more specific signs of DDoS attack that can vary depending on the type of attack

4. Ransom demands

What differentiates these recent attacks is that ransom demands were received directly after the first attack. Typically ransom demands are left on support page forms or in the on-page chat.

The ransom demands were for 10 Bitcoins for 12 months protection. However, the evidence is that this is not the case and if the ransom is paid, attacks will not stop.

We STRONGLY RECOMMEND that you do not pay ransom demands. Comms Council UK members' experience suggests that the attack will not stop if you pay.

An example of an initial message after a "Demo" attack:

A team has been assigned and will now disrupt your services 24/7

You have a limited window to accept our protection before we reactivate the disruption

Once disruption commences, we will not stop until you have paid in full.

x Bitcoin to: [bitcoin wallet number]

REvil
This is OUR Dominion

An example of a follow-up message:
We will be resuming our attacks on your service from tomorrow

The standard protection fee for all voip providers is 10BTC

Your payment remains confidential, and your services will be whitelisted. Once paid, you will be protected for a minimum of 12 months

10 Bitcoin to [Bitcoin wallet number]

We look forward to your cooperation.

REvil
This is OUR Dominion

5. Reporting DDoS attack types

Attacks on CCUK members during September & October 2021 included ransom DDoS attacks on VoIP service providers and their network infrastructure.

Predominate attacks being:

SIP protocol-specific attacks:

Attacks at the application layer are of particular concern because of the higher resource cost of generating application errors versus filtering on network devices.

UDP reflection targeting SIP infrastructure:

These methods, when targeted at SIP or RTP services, can easily overwhelm Session Border Controllers (SBCs) and other telephony infrastructure. The attacker seems to learn enough about the target's infrastructure to target such services with high precision.

UDP floods targeting SIP infrastructure:

Floods of UDP traffic that have no well-known fingerprint, aimed at critical VoIP services. Generic floods like this may look like legitimate traffic to unsophisticated filtering systems.

TCP floods targeting stateful firewalls:

These are being used in "trial-and-error" type attacks. They are not very effective against telephony infrastructure specifically (because it is mostly UDP), but very effective at overwhelming stateful firewalls.

Attack volumes were reported from 450Gb/s to 1.2Tb/s, with durations ranging from a few minutes for probing to multiple days for attacks.

6. Mitigating DDoS attacks

DDoS mitigation is rarely a simple one stop solution. Many traditional approaches aren't appropriate for VoIP. Service providers need to consider a layered approach to defence, according to the make-up of their own specific network.

The key concern in mitigating a DDoS attack is differentiating between attack traffic and normal traffic. For example, if a product release has a company's website swamped with eager customers, cutting off all traffic is a mistake. If that company suddenly has a surge in traffic from known attackers, efforts to alleviate an attack are probably necessary.

The difficulty lies in telling the real customers apart from the attack traffic.

In the modern Internet, DDoS traffic comes in many forms. The traffic can vary in design from un-spoofed single source attacks to complex and adaptive multi-vector attacks.

To mitigate against un-spoofed sources, a simple ACL on the edge of the network may be sufficient. This is fairly simple to do for SIP signalling end points but may be more difficult to implement for media addresses which can frequently change.

A multi-vector DDoS attack uses multiple attack pathways in order to overwhelm a target in different ways, potentially distracting mitigation efforts on any one trajectory.

An attack that targets multiple layers of the protocol stack at the same time, such as a DNS amplification (targeting layers 3/4) coupled with an HTTP flood (targeting layer 7) is an example of multi-vector DDoS.

Mitigating a multi-vector DDoS attack requires a variety of strategies in order to counter different trajectories.

The more complex the attack, the more likely it is that the attack traffic will be difficult to separate from normal traffic. The goal of the attacker is to blend in as much as possible, making mitigation efforts as inefficient as possible.

Mitigation attempts that involve dropping or limiting traffic indiscriminately may throw good traffic out with the bad, and the attack may also modify and adapt to circumvent countermeasures. In order to overcome a complex attempt at disruption, a layered solution will give the greatest benefit.

7. DDoS mitigation services

This section has been redacted and is only available for Comms Council UK members.

8. Public cloud vs data centre hosting

This section has been redacted and is only available for Comms Council UK members.

9. Peering, transit & direct connections

This section has been redacted and is only available for Comms Council UK members.

10. CCUK DDoS recommendations

Prepare for DDoS attacks

While it is not possible to fully mitigate the risk of a denial-of-service attack affecting your service, these are five practical steps that will help you be prepared to respond.

Understand your service

Understand the points in your service where resources can be overloaded or exhausted. Determine whether you, or a supplier, are responsible for each. Stateful resources are the highest risk (e.g. stateful firewalls, Linux Conntrack or SBCs that do not send authentication challenges statelessly).

Upstream defences

Ensure your service providers are ready to deal with resource exhaustion in places where they are uniquely placed to help. This includes keeping an up-to-date list of contacts of your upstream providers to hand.

Scaling

Ensure your service can scale to deal with surges in concurrent sessions.

Response plan

You should design your service, and plan your response to an attack, so that the service can continue to operate, albeit in a degraded fashion.

Having network status pages hosted by a third party will ensure that customers will have access to status updates and reduce calls into your care & support teams.

Testing and monitoring

Gain confidence in your defences by testing them, and gain confidence you'll notice when attacks start by having the right tooling in place and keeping access logs for at least one week. NCSC recommends keeping logs using IPFIX protocol for 13 months.

Penetration testing, including DDoS simulations, should be performed regularly. Tests should be designed to ensure that they can indicate potential problems without affecting live services.

Have a DDoS response plan

IF AN ATTACK BEGINS:

1. Confirm that you are under attack
2. Understand the nature of the attack
3. Deploy the mitigations you can quickly put in place
4. Monitor the attack and recover

You should design your service, and plan your response to an attack, so that the service can continue to operate, albeit in a degraded fashion.

11. Reporting

This section has been redacted and is only available for Comms Council UK members.

12. Action plan

This section has been redacted and is only available for Comms Council UK members.

13. Resources

This section has been redacted and is only available for Comms Council UK members.