Cyber Security for ISP

Diep Ko

Table of Contents

CYBER Security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

CYBER Security RISK

- Network Security
- Application Security
- Information or Data Security
- Cloud Security
- Mobile Security
- Critical Infrastructure Security
- Internet of Things (IoT) Security

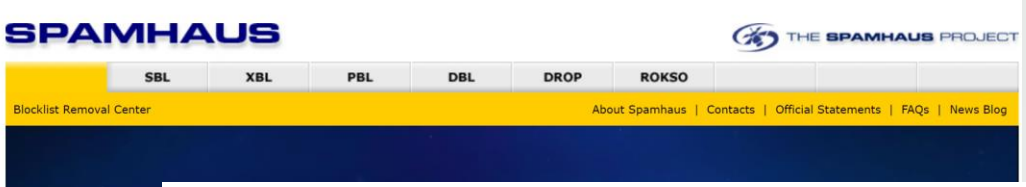
ISP Challenge

- Ransomware
- IP Blacklist/IP Reputation
- DDoS
- Botnet

RAMSOMWARE

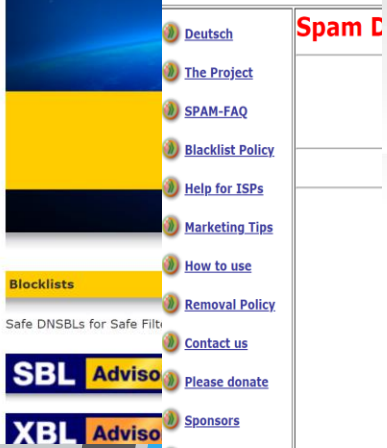
- Ransomware is malicious software (malware) that leverages data encryption to extort organizations for substantial ransoms. Once paid, ransomware attackers theoretically restore access to or unencrypt affected data using a decryption key.
- Ransomware attacks often begin with a social engineering tactic, such as phishing emails or watering hole attacks, which trick users into downloading the malware. The attackers may then demand payment in cryptocurrency, credit card payments, or wire transfers.

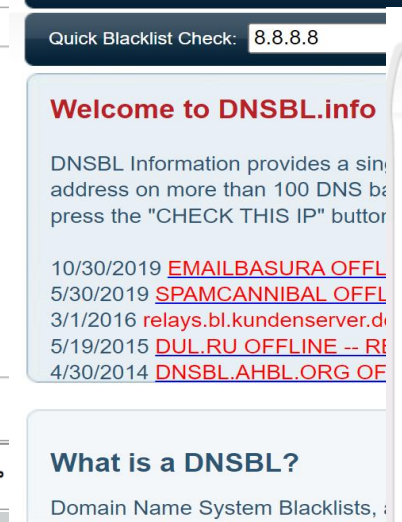
IP Blacklist/IP Reputation

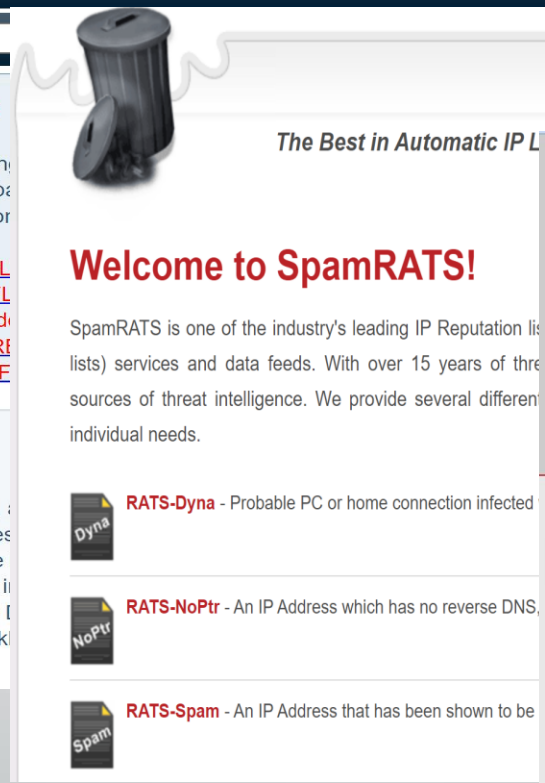

SPAMHAUS
THE SPAMHAUS PROJECT
SBL
XBL
PBL
DBL
DROP
ROKSO
Blocklist Removal Center
About Spamhaus | Contacts | Official Statements | FAQs | News Blog

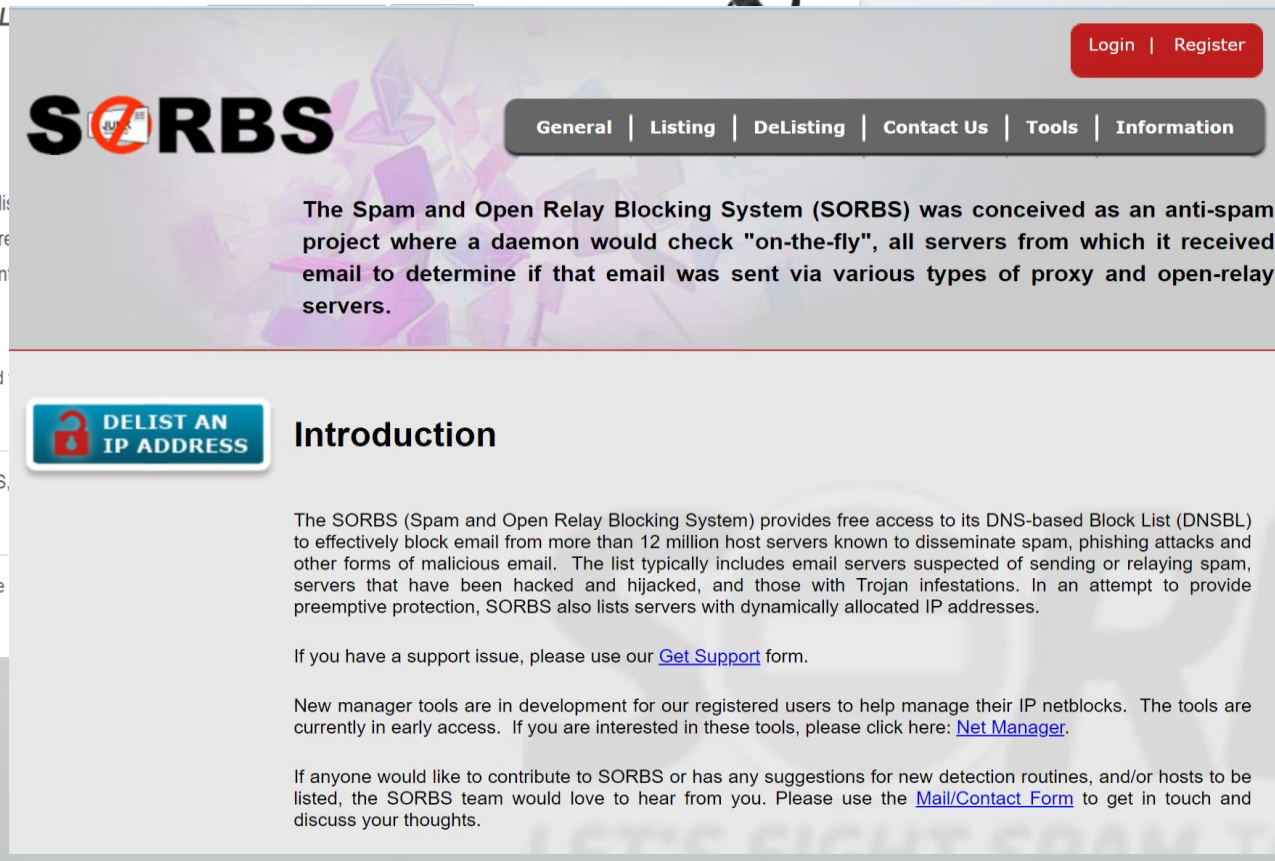

UCEPROTECT-NETWORK
Spammer listings within the last 7 days:
Level 1: 83495 IP's, Level 2: 18204 Allocations, Level 3: 1183 ASN's. Last Updated: 20.09.2023 08:04 CEST


DNSBL .info
SPAM DATABASE LOOKUP
HOME
BLACKLISTS
REMOVAL
REPORT SPAM
SUPPORT
Quick Blacklist Check:
8.8.8.8


Deutsch
The Project
SPAM-FAQ
Blacklist Policy
Help for ISPs
Marketing Tips
How to use
Removal Policy
Contact us
Please donate
Sponsors
News
License
Query Database
Pillory
Netstatus
Blocklists
SBL Adviso
XBL Adviso


Welcome to DNSBL.info
What is a DNSBL?


Home
About
Usage
Removal
Stats
Subscription
The Best in Automatic IP
Welcome to SpamRATS!
RATS-Dyna
RATS-NoPtr
RATS-Spam


Login | Register
SORBS
General | Listing | DeListing | Contact Us | Tools | Information
The Spam and Open Relay Blocking System (SORBS) was conceived as an anti-spam project where a daemon would check "on-the-fly", all servers from which it received email to determine if that email was sent via various types of proxy and open-relay servers.
DELIST AN IP ADDRESS
Introduction
The SORBS (Spam and Open Relay Blocking System) provides free access to its DNS-based Block List (DNSBL) to effectively block email from more than 12 million host servers known to disseminate spam, phishing attacks and other forms of malicious email. The list typically includes email servers suspected of sending or relaying spam, servers that have been hacked and hijacked, and those with Trojan infestations. In an attempt to provide preemptive protection, SORBS also lists servers with dynamically allocated IP addresses.
If you have a support issue, please use our Get Support form.
New manager tools are in development for our registered users to help manage their IP netblocks. The tools are currently in early access. If you are interested in these tools, please click here: Net Manager.
If anyone would like to contribute to SORBS or has any suggestions for new detection routines, and/or hosts to be listed, the SORBS team would love to hear from you. Please use the Mail/Contact Form to get in touch and discuss your thoughts.

MX TOOLBOX®

Pricing Tools Delivery Center Mon

SuperTool | MX Lookup | Blacklists | DMARC | Diagnostics | Email Health | DNS Lookup | Analyze Headers

SuperTool Beta7

104.100.2.100 [Blacklist Check]

blacklist:104.100.2.100 [Monitor This] [Solve Email Delivery Problems] blacklist

BLACKLISTING isn't the ONLY email delivery issue LEARN MORE

We notice you are on a blacklist. [Click here for some suggestions]

Checking **104.100.2.100** against **84** known blacklists...
Listed **1** times with **3** timeouts

	Blacklist	Reason	TTL
LISTED	UCEPROTECTL3	104.100.2.100 was listed [Detail]	2100
OK	0SPAM		
OK	0SPAM RBL		
OK	Abuse.ro		
OK	Abusix Mail Intelligence Blacklist		

BlacklistMaster

Blacklist monitoring | Mail server monitoring | Reverse DNS test | Blacklist check | Prices | Log in | Sign up

Blacklist Check

The Blacklist Check Tool tests your IP address and domain against RBL database.

IPv4, IPv6 or domain name: 104.100.2.100

RBL check: (•) IP blacklist check ( ) Domain blacklist check

[Test]

Want blacklist alerts instantly delivered to your mail box? Try blacklist monitoring free!

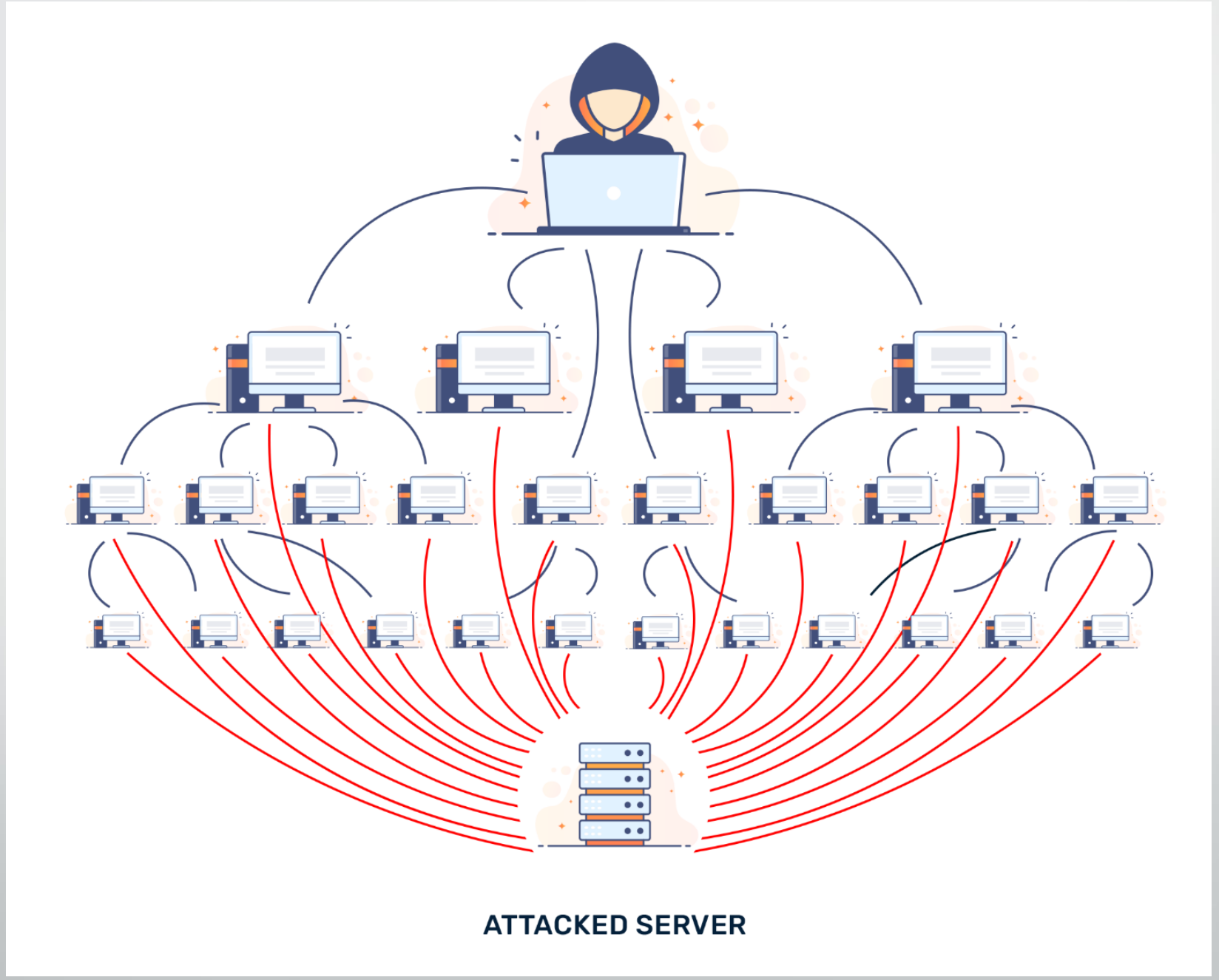
104.100.2.100 blacklist lookup result

Blacklist	Description	Status
bl.0spam.org	0spam Project	Not Listed
UrlhausIP	Abuse.ch Urlhaus IPs	Not Listed
rbl.abuse.ro	Abuse.ro RBL	Not Listed
cbl.abuseat.org	Composite Blocking List	Not Listed

DDoS

DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

Motivations for carrying out a DDoS vary widely, as do the types of individuals and organizations eager to perpetrate this form of cyberattack. Some attacks are carried out by disgruntled individuals and hacktivists wanting to take down a company's servers simply to make a statement, have fun by exploiting cyber weakness, or express disapproval.


ATTACKED SERVER

INDUSTRY NEWS • 1 min read •

DDoS attack on Cambodia"s top ISPs reached 150Gbps

Luana PASCU
November 09, 2018

APNIC

Get IP | Manage IP | Training | Events | Insights | Community

DDoS tsunami: A Cambodian case study

By Robbie Mitchell on 25 Jun 2019

Category: Tech matters

Tags: Cambodia, DDoS, security

Like 4 Share

Tweet

Blog home

A natural early warning sign of a
unexpected recession of water le

Although Cambodia's capital, Ph
tsunamis — being some 150km f
data-tsunami of sorts last Noven
Distributed Denial of Service (DD

THE CYBER EXPRESS By CYBLE

MAGAZINE DOWNLOAD | FIREWALL DAILY | ESSENTIALS | FEATURES | BUSINESS | EVENTS

Home › Firewall Daily › Dark Web News

Cambodia Angkor Air Cyber Attack: 'Host Kill Crew Hackers' Claims Responsibility

A lesser-known hacker group, which calls itself Host Kill Crew, has taken responsibility for the Cambodia Angkor Air cyber attack

by Vishwa Pandagle — May 10, 2023 - Updated on June 26, 2023

in Dark Web News, DDoS Attacks News, Firewall Daily, Hacking News

0

eyerys

Home | About | Services | Articles | Contact

4 Cambodia ISPs Hit By Some Of The Biggest DDoS Attacks In Its History

06/11/2018

Digi, Telcotech, SINET and EZECOM, which are 4 of the largest internet service providers (ISPs) in Cambodia, have been attacked by large-scale DDoS attacks.

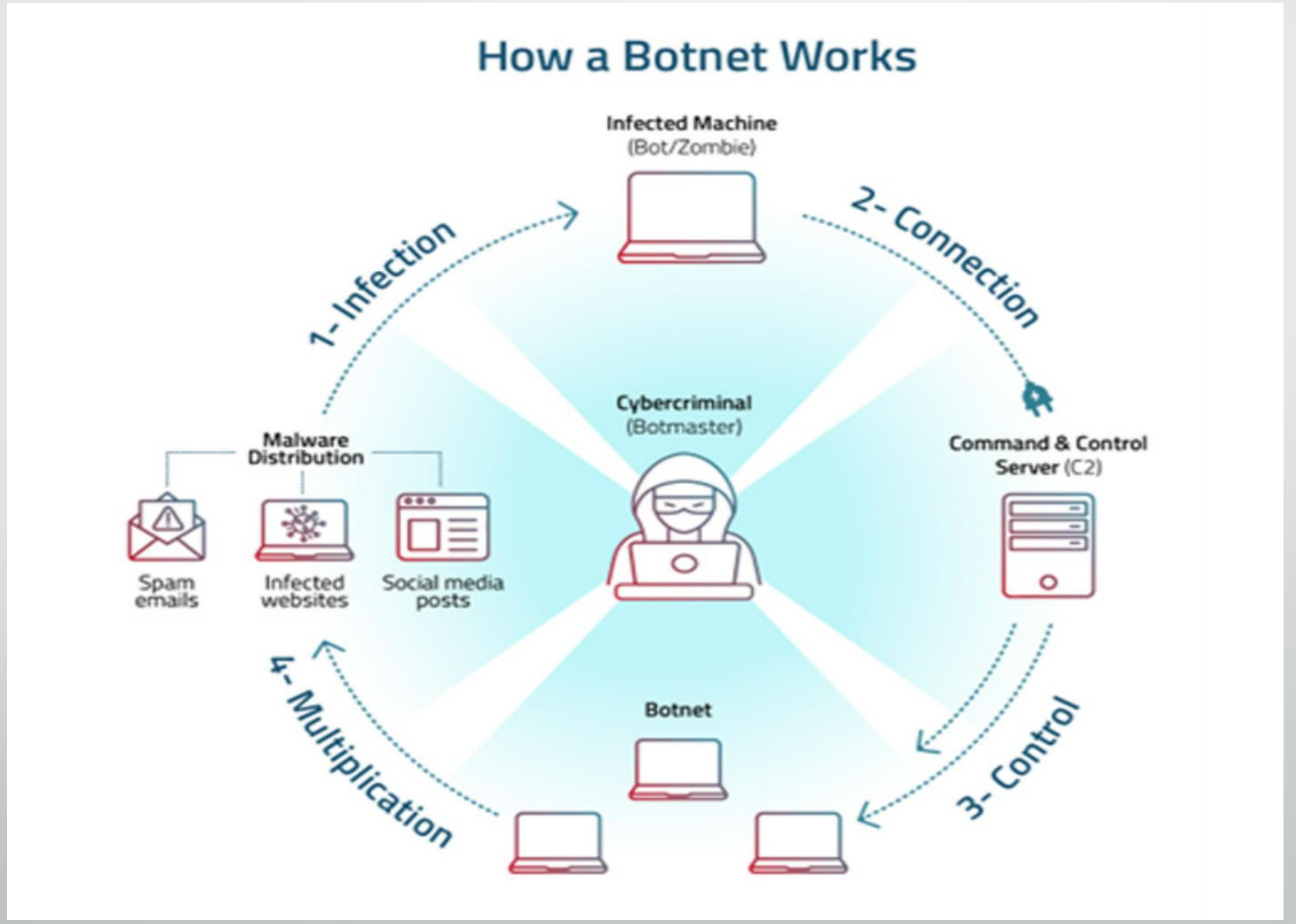
Local news in Cambodia called the DDoS attack as the biggest attack to have occurred in the history of the country. Sources familiar with the incident revealed that the DDoS attacks have struck the ISPs with a peak of 150Gbps on November 5 and 6.

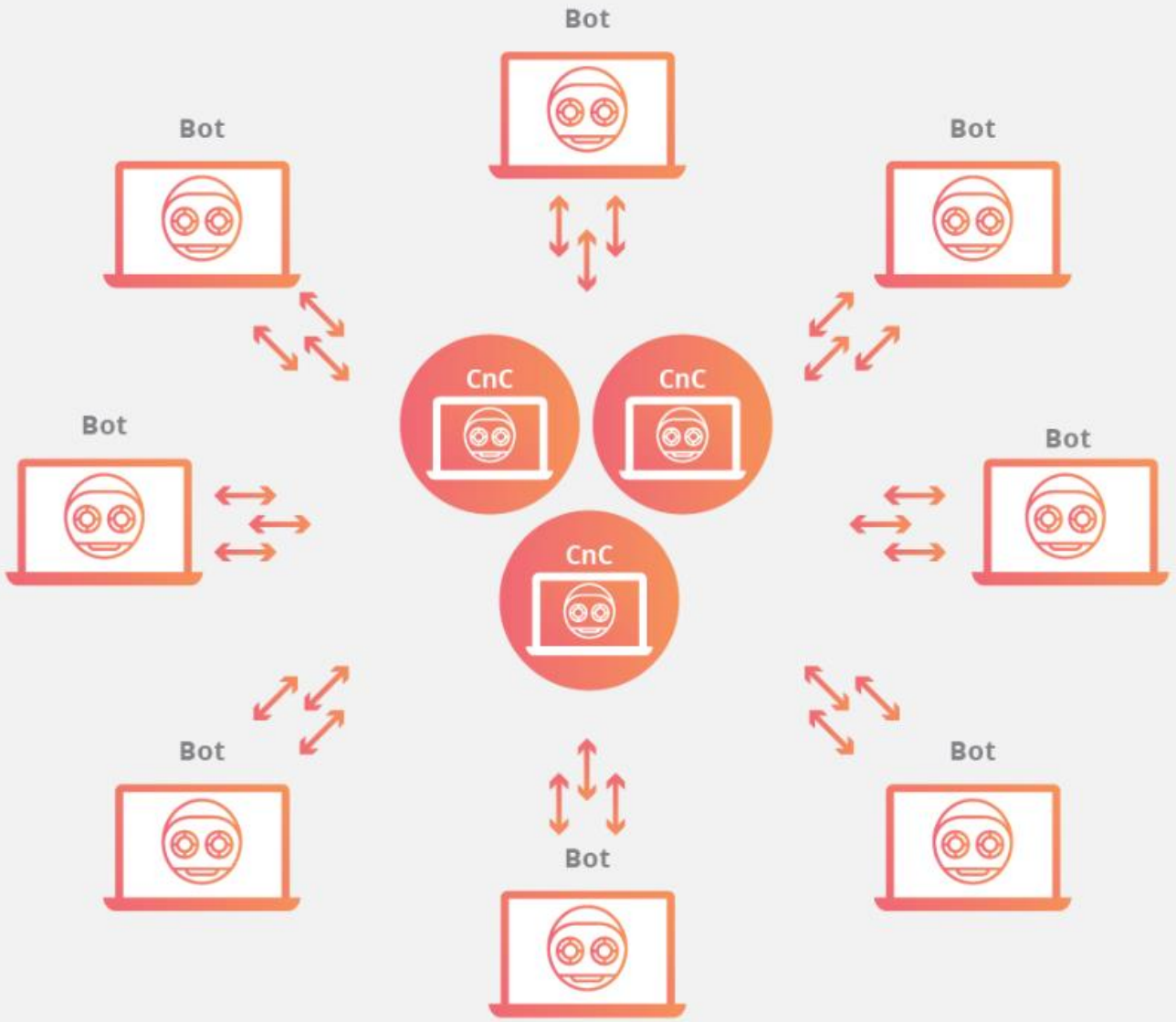
What was the largest DDoS attack of all time?

- The biggest DDoS attack to date took place in September of 2017. The attack targeted Google services and reached a size of **2.54 Tbps**.
- AWS reported mitigating a massive DDoS attack in February of 2020. At its peak, this attack saw incoming traffic at a rate of **2.3 Tbps**.
- One of the largest verifiable DDoS attacks on record targeted GitHub, the attack reached **1.3 Tbps**, sending packets at a rate of 126.9 million per second.
- On October 21, 2016, Dyn, a major domain name service (DNS) provider, the DDoS attack may have actually achieved a rate of **1.5 Tbps**.
- On Feb. 28, 2018, GitHub, a platform for software developers, was hit with a DDoS attack that clocked in at 1.35 Tbps and lasted for roughly 20 minutes.
- In February 2021, Akami announced that they had dealt with “three of the six biggest volumetric DDoS attacks” the company has ever recorded. In this case the threat attack weighed in at **800Gbps**.

Botnet

Botnets are networks of hijacked computers and internet-connected devices that are infected by malware (i.e., malicious software). The malware runs bots on the compromised devices without the knowledge of device users. Botnets—a combination of the words “robot” and “network”—are usually controlled by a botmaster or bot herder. The bot herder essentially turns these hijacked computer devices into remote-controlled “zombie” computers. By linking compromised devices in large numbers, it becomes possible to create botnets that can be leveraged against various targets to carry out distributed denial of service (DDoS) attacks, account takeover, data theft and several other types of attacks.


How a Botnet Works
Infected Machine
(Bot/Zombie)
1- Infection
2- Connection
Cybercriminal
(Botmaster)
Malware
Distribution
Command & Control
Server (C2)
Spam
emails
Infected
websites
Social media
posts
Botnet
4- Multiplication
3- Control


Bot
Bot
Bot
CnC
CnC
Bot
Bot
CnC
Bot
Bot
Bot

Thank you