SOCRadar®

2021

Threat Landscape Report

UNITED KINGDOM

TABLE OF CONTENTS

EXECUTIVE SUMMARY

SOCRadar Threat Landscape Report provides UK organizations with an understanding of evolving cyber threats relevant to their geographical operating locations to enable security leaders to make better decisions. The intelligence provided in this report can help plan enterprise-wide security programs, make investment decisions, and define cybersecurity requirements.

SOCRadar characterizes the threat landscape based on recently observed threat actor activities, malware campaigns, recent critical vulnerabilities, exploits, data gathered from open threat sharing platforms, and leveraging the comprehensive data monitoring, collection, classification, and analysis capabilities of SOCRadar Platform.

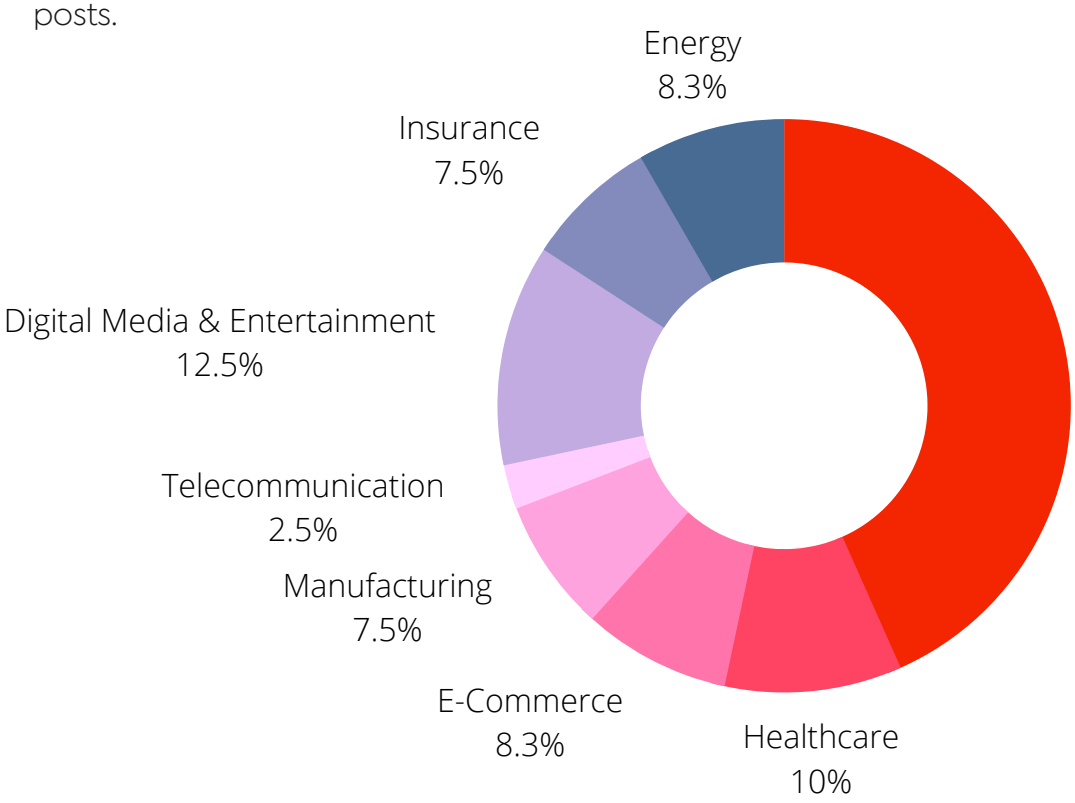
This report shows that the UK remained a prime target for APT actors and financially motivated ransomware gangs in 2021. Unsurprisingly, the Finance/Banking vertical is far and away from the most targeted in the UK as “The City” is the largest financial hub for Europe and the world.

KEY FINDINDS

- **Based on 500+ deepweb posts, financial institutions are the TOP targeted industry in the UK.**
- **Top ransomware gangs targeting the UK are "LockBit, Conti, and Pysa".**
- **Iranian and Chinese APT groups have recently targeted leading organizations in the military, government, high-tech, and finance verticals.**
- **SOCRadar has detected 37,358 phishing attacks targeting the UK since the beginning of 2021.**
- **In 2021, ProxyShell vulnerability on MS Exchange Servers is the most exploited vulnerability in the UK.**
- **In 2021 alone, SOCRadar discovered 23.4 million stolen credentials related to the UK.**
- **DDoS attacks in 2021 impacted critical emergency services.**

Dark Web Threats On The Rise

The dark web underground ecosystem is the #1 communication channel and a global marketplace with various hacking tools and stolen databases available for purchase. When it came to the target countries, the UK was tied for #2 globally, just behind the US. Most important to highlight is that over the last 12 months, the SOCRadar CTIA Team detected more than 521 posts.



The most targeted verticals in the UK based on DarkMirror Intelligence data

62 different threat actors are targeting the UK entities. 18% of these posts were customer database sales, and 12% were unauthorized network access sales. These campaigns have exposed an extensive dataset of organizations from various verticals, including local government, finance, digital media, and healthcare.

521
Threat posts over the last 1 year

62
Dark web threat actors / aliases

Government
The most targeted vertical

Leaked database
The most common threat category

RECEIVE A FREE
DEEP WEB REPORT

Major Dark Web Incidents of 2021

Unauthorized Citrix Access Sale Detected for a British-American Banking Giant

On June 26, on a dark web forum tracked by SOCRadar, a vendor attempted to sell unauthorized Citrix access allegedly for a British-American bank. While the dark web vendor did not give the name of the victim bank, it is claimed that its revenue is more than $30 billion.

The buyer would have Citrix access for the firm and can manage access and permissions based on both the endpoint device and the user. The dark web vendor auctioned the Citrix access setting a starting price of $5000.

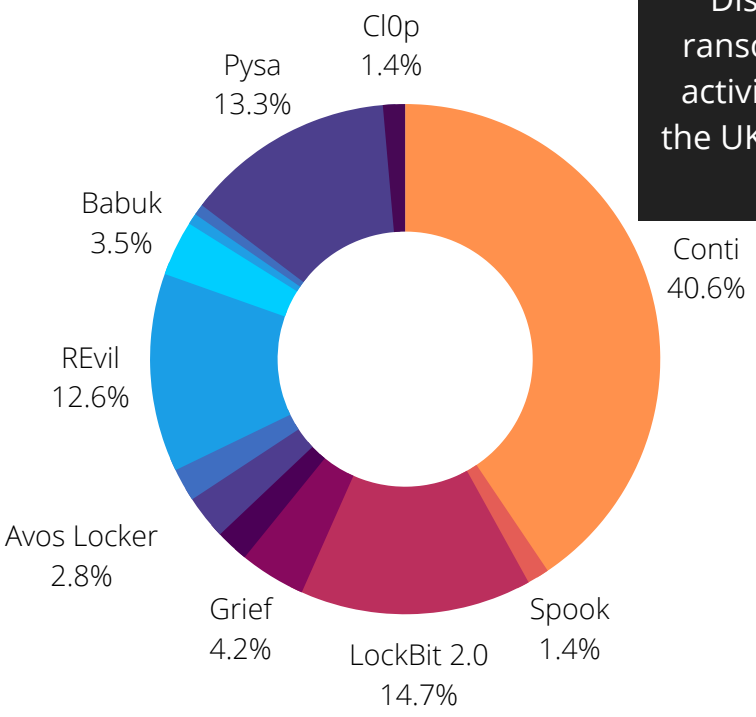
On November 11, a dark web vendor offered to sell unauthorized network access for an international telecommunication firm from the UK on a dark web forum monitored by SOCRadar.

According to the dark web post, the buyer would have VPN access to the firm's web corporate systems and servers. The vendor also stated that the victim firm has a revenue of $1 billion.

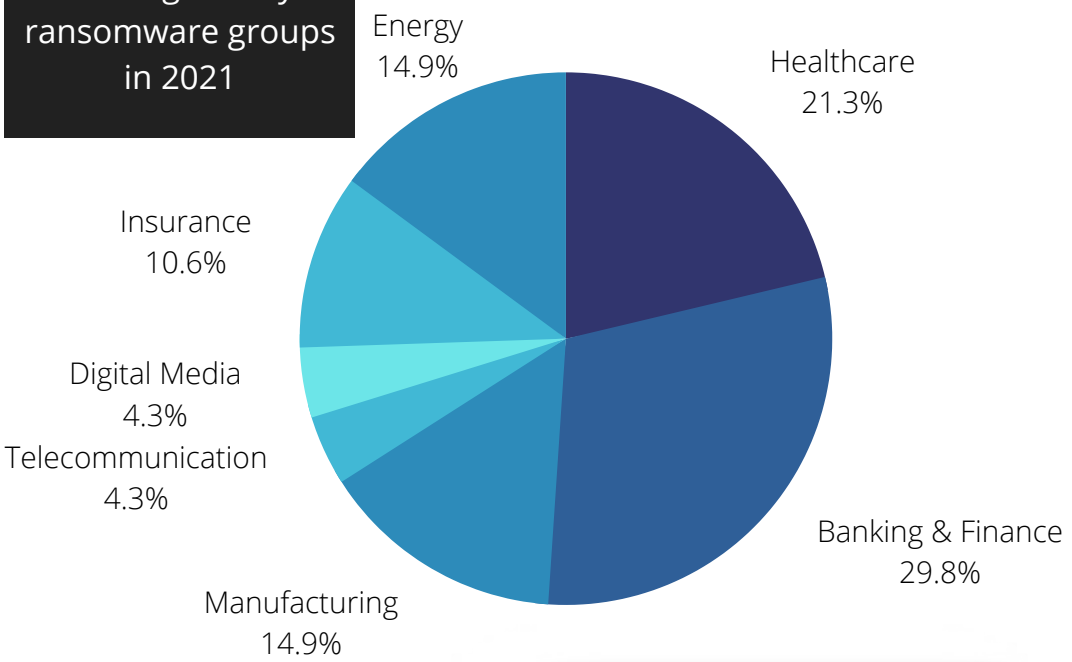
Ransomware Threats

Ransomware attacks dominated the headlines in 2021. The top 10 ransomware gangs believed to be behind criminal activity had moved about $5.2bn worth of bitcoin over the past three years. This year, Ireland's Health Service Executive also faced a significant attack, leading to months of disrupted appointments.

Distribution of ransomware gang activities targeting the UK organizations in 2021



The verticals in the UK targeted by ransomware groups in 2021



In the last three months of 2021, the increase in ransomware attacks skyrocketed. Alarmingly, the activities of ransomware groups targeting the UK more than doubled from July to November 2021. Financial Services and Healthcare are the most targeted verticals based on the insights gleaned from SOCRadar DarkMirror.

Top Ransomware Gangs Targeting the United Kingdom

LockBit

- Ransomware-as-a-service (RaaS) operator.
- It's one of the best-designed lockers regarding encryption speed and overall functionality.
- Lately, the long list of victims has included Merseyrail UK, Accenture, and Bangkok Airways.

Conti

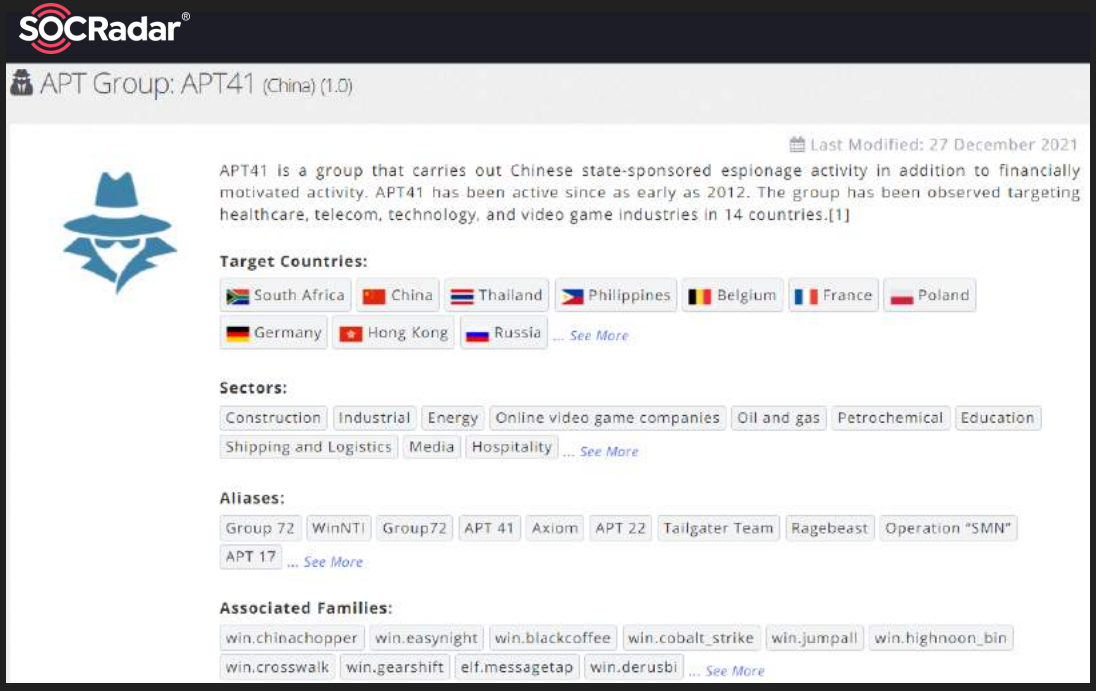
- Ransomware-as-a-service (RaaS) operator, operating out of Russia.
- The group has pulled off several high-profile attacks on the UK companies such as Graff Diamonds Limited.
- A playbook related to Conti was allegedly released by an affiliate upset with Conti in September 2021.

Pysa

- First observed in December 2019.
- Specifically targeting higher education, K-12 schools, and seminaries in the US and UK
- Routinely dump stolen data even after the victim company has paid the ransom.

State-Sponsored APT Activities

Organizations in the UK continue to be targets of advanced threats with diverse motivations. Specific APT groups from Iran and China have recently targeted leading organizations in the military, government, high-tech, and finance verticals. To reach the state goals through the collection of strategic intelligence is believed to be the primary motivation of the state-sponsored actors.



Financial gain through the direct theft of funds is another common motivation. Over the last few months, the SOCRadar CTIA team has observed multiple activities reflecting these motivations by continuously collecting data across the surface, deep and dark web sources while tracking 12 APT groups that have targeted the UK government, military, and private sectors in the past.

Significant APT Groups

APT41

Last activity:
November 14, 2021

APT1

Last activity:
November 13, 2021

APT28

Last activity:
November 13, 2021

APT35

Last activity:
September 9, 2021

SOCRadar collects Advanced Persistent Threat (APT) IOC Feeds from several public and private sources and sensors. These feeds are free and refreshed daily.

DOWNLOAD

Major APT Activities

The UK's NCSC Blames China for the Hafnium Microsoft Incident

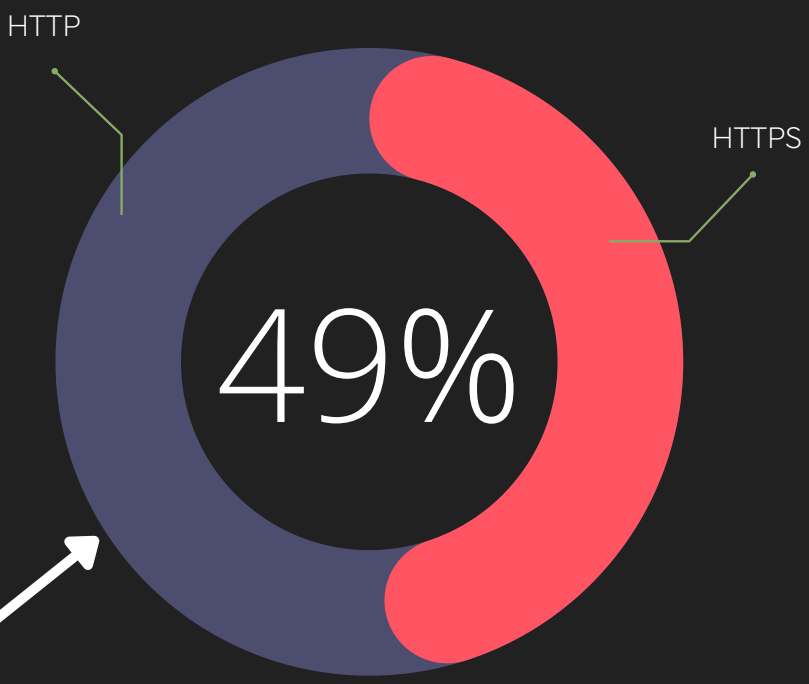
In March 2021, various organizations worldwide found their internal discussions cracked open by Chinese hackers - initially attributed to the Hafnium threat group. Four undiscovered vulnerabilities in Microsoft Exchange software, which affected software released from 2012, enabled the hackers to take continual control of the corporate servers, calendars, emails, and anything else they solicited. After a detailed investigation, the UK's National Cyber Security Centre (NCSC) has announced. Hafnium may relate to the Chinese state. The attack on Microsoft Exchange software was considered highly likely to allow large-scale espionage, including obtaining intellectual property and personally identifiable information. The UK also associates the Chinese Ministry of State Security as behind the APT40 and APT31, targeting maritime industries, naval defense contractors in the US and Europe, and government entities, including the Finnish parliament in 2020.

Iran-linked Charming Kitten (APT 35) Impersonate the UK Scholars

In a sophisticated campaign, Charming Kitten APT Group (aka TA453, APT35, and Phosphorus) has been found to approach individuals pretending to be British academics with the University of London's School of Oriental and African Studies (SOAS) to obtain sensitive information. The phishing campaign starts with detailed and lengthy chats with professors, journalists, and think tanks on Middle Eastern studies. Charming Kitten released a registration link to a website looking reliable and belonging to the University of London. The compromised site was designed to capture credentials as their phishing infrastructure. In the subsequent campaign steps, Charming Kitten also targeted the personal emails, and in following phishing emails, the APT group changed their tactics and started to release the registration link earlier in their commitment with the target without needing a comprehensive conversation. Previously in early 2021, APT35 had compromised a website affiliated with a UK university to host a phishing kit, indicating a focus shift from the US to the UK.

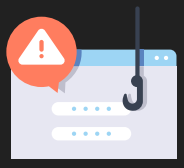
Phishing Threats

Email phishing remains the top ransomware attack vector. The typical tactic is to deliver malicious macro-enabled Office documents attached to the email. Combined with business email compromise (BEC) scams and social engineering methods, the effects can increase dramatically.



Attackers are increasingly using https to lure their victims into clicking malicious links

SOCRadar has detected 37,358 phishing attacks targeting the UK since the beginning of 2021. SOCRadar CTIA team is seeing a phishing-enabled fraud trend targeting particularly fast-growing digital industries, including e-commerce, FinTech, and cloud/SaaS.



37,358

Total phishing attacks detected over the last 1 year

Microsoft

Top SaaS phishing scheme for credential harvesting

Most us Ds

Top targeted brands in the UK

Search On Phishing Radar

Enter your domain

The Digital Industries Commonly Targeted by Phishing Attacks

Comman Platforms

Social Media /IM

Cloud / Webmail

E-commerce

FinTech

Attackers Objective

To distribute malware and steal the social media login credentials of individuals.

To steal the corporate email credentials to gain an initial foothold to the victim's communication channels.

To steal the credentials of individuals/companies and other personal info (PII) for using in fraudulent e-shopping activities.

With London as the "superhub" of FinTech, attackers' objective is to steal the login accounts of individuals/businesses for financial gain or use them in illegal transactions.

Critical Asset Exposures & Vulnerabilities

When SOC analysts, vulnerability management teams, and security leaders have limited time and budget, prioritizing vulnerabilities to reduce the public attack surface becomes paramount. Following is a high-level statistical view of the critical ports and vulnerabilities on the internet-facing infrastructure and technologies.

Ransomware gangs heavily exploit these as they are exposed, but we can still observe them unpatched or exposed to any remote actors. It is highly recommended to check the technologies listed so far for unpatched, critical, exploited vulnerabilities.

Vulnerable Hosts | CVE ID | CVSSv3

The most commonly exploited vulnerabilities in the UK.

5,398	Microsoft Exchange Server Unauthenticated Remote Code Execution Vulnerability	CVE-2021-31206 #ProxyShell	CVSS: 9.2
107	VMware vCenter PreAuth Remote Code Execution Vulnerability	CVE-2021-21985 #vSphere	CVSS: 9.8
27	SolarWinds Serv-U* Remote Code Execution Vulnerability	CVE-2019-1579 #GlobalProtect	CVSS: 10.0
186	Palo Alto Networks VPN Unauthenticated Remote Code Execution Vulnerability	CVE-2021-3064 #GlobalProtect	CVSS: 9.8

Other Critical Findings

14,112
Exim Server v4.92

120,217
Open RDP 3389

3418
CVE-2014-0160
#Heartbleed

94
CVE-2019-0708
#BlueKeep

* NCC Group Research | TA505 exploits SolarWinds Serv-U vulnerability (CVE-2021-35211) for initial access

Identity & Credentials Intelligence

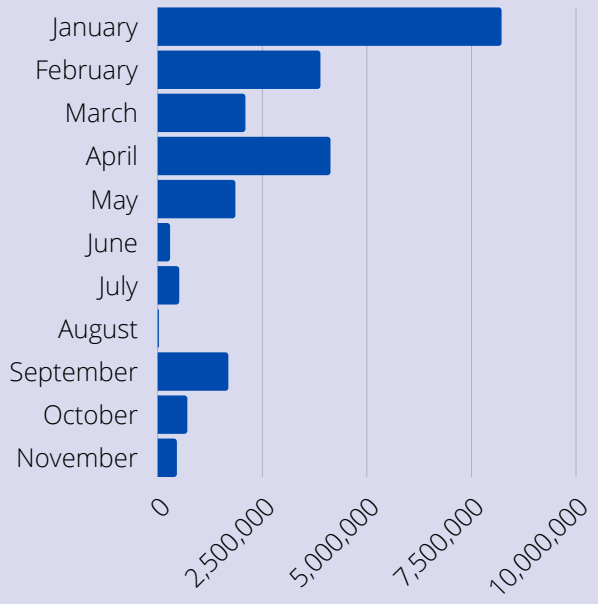
Using stolen credentials is one of the most common initial access techniques leveraged by your adversaries. C-level credentials are significantly more helpful for BEC attackers. Last year, SOCRadar detected more than 1 billion exposed credentials by analyzing the breach datasets shared on the deep and dark web forums, most of which are tied to plain-text passwords.

Password reuse remains a concern for security professionals. A bigger problem arises when password reuse is combined with the lack of MFA mechanisms. This makes it easier for ransomware and APT actors to continually access sensitive information, intellectual property, and confidential business data through stolen identities. Following are the statistics about the current risk situation of the UK.

CHECK FOR ACCOUNT BREACH

Enter your domain/email

Figure 5. Month-over-month number of detected credentials related to the United Kingdom in 2021



9114

Bots for sale | UK

442K

Total bots for sale

The Genesis Marketplace is a dark web underground avenue for threat actors to buy digital identities. Currently, the UK ranks #10 among the countries of listed available bots.

68,6 Million

total leaked credentials

Country code TLDs: co.uk | gov.uk | police.uk | nhs.uk | org.uk

676,000

leaked credentials from government agencies

In 2021 alone, SOCRadar discovered 23.4 million stolen credentials related to the UK, which added up to 45.2 million credentials found before 2021.

DDoS | Risk-to-others

The global internet ecosystem is currently vulnerable and carrying high malicious traffic. Sophisticated threat actors take advantage of these weak points for amplifying disruptive DDoS attacks against businesses, resulting in financial losses and critical service disruptions.

UK VoIP operators (e.g., Voiphone) to the likes of police, critical emergency services, and the NHS were also among the victims of DDoS attacks in 2021. Based on the global risk condition dataset provided by Cyber Green Initiative, the United Kingdom can generate ~96TBit/sec DDoS traffic, ranking #10 globally.

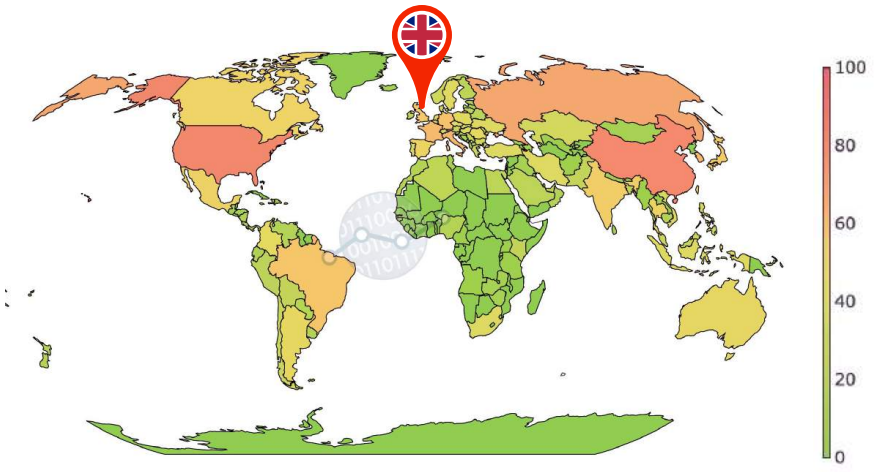


Figure 5. Global heatmap view of total potential DDoS bandwidth by country

Data source: CyberGreen

Protocol	Bandwidth Amplification Factor
DNS	28 to 54
SNMPv2	6,3
SSDP	30,8
CHARGEN	358,8
NTP	556,9

ABOUT SOCRadar®

SOCRadar platform is an all-in-one solution that provides Extended Threat Intelligence, Digital Risk Protection, and External Attack Surface Management. Its false-positive free platform helps companies proactively defend themselves against cyber incidents. SOCRadar is empowered with robust AI algorithms and a highly talented analyst team; together, they eliminate false positives.

FOLLOW US!

DISCOVER SOCRADAR® FREE EDITION

With SOCRadar® Free Edition, you'll be able to:

- **Discover your unknown hacker-exposed assets**
- **Check if your IP addresses tagged as malicious**
- **Monitor your domain name on hacked websites and phishing databases**
- **Get notified when a critical zero-day vulnerability is disclosed**

TRY FOR FREE

CONTACT US info@socradar.io +1 (571) 249-4598 651 N Broad St, Suite 205, Middletown, DE 19709