CLOUDFLARE

# Internet Threat Radar

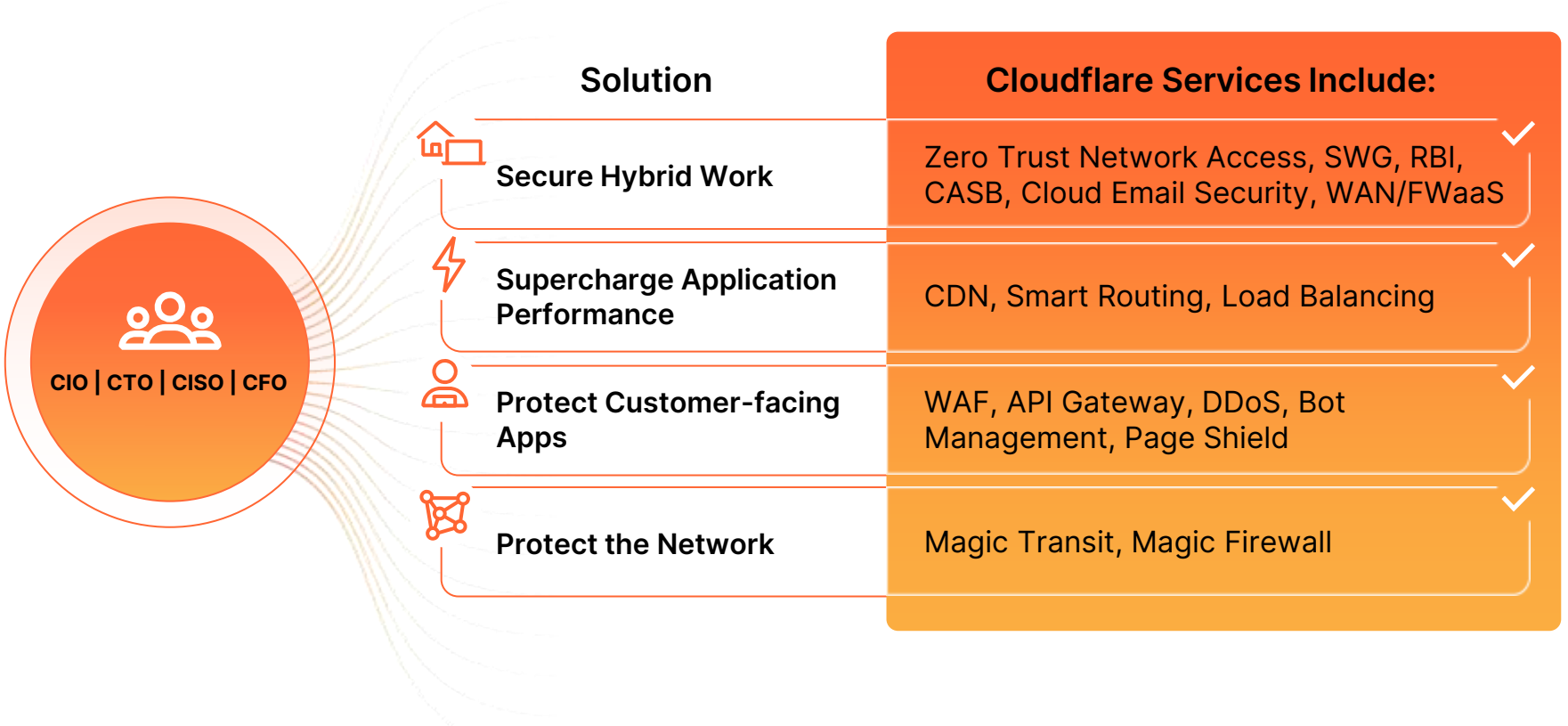
## *Current Cyber Threats in Cloud Networking*

March. 2024

Parul Sharma
Solutions Engineer, Cloudflare

# Cloudflare is the Network for Digital Transformation

## *The Connectivity Cloud*



CLOUDFLARE

# Cloudflare is the only composable, Internet-native platform

That delivers local capabilities with global scale


**310**

cities in 120+ countries, including mainland China

**13,000**

networks directly connect to Cloudflare, including every major ISP, cloud provider, and enterprise

**248 Tbps**

global network edge capacity, consisting of transit connections, peering and private network interconnects

**~50 ms**

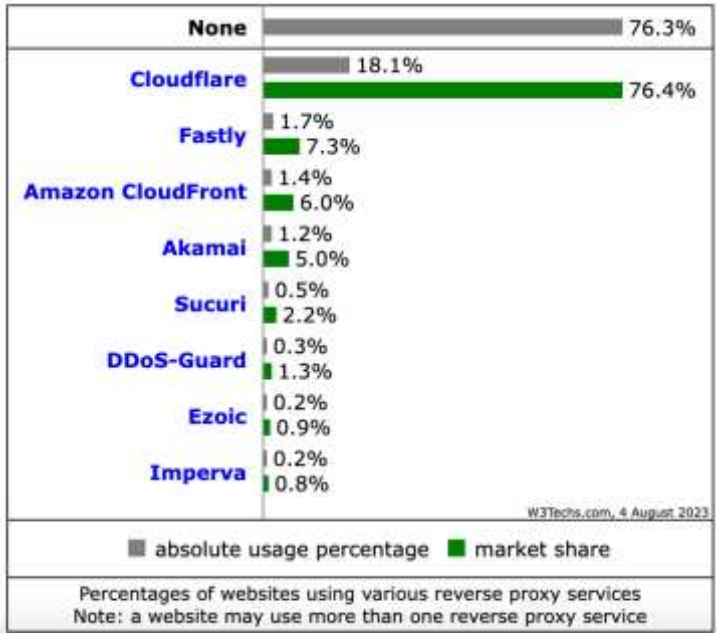
from 95% of the world's Internet-connected population

## W3techs: Usage statistics of reverse proxy services for websites

>4x Market Share of:

- Fastly
- AWS
- Akamai

**Combined**




Source: https://w3techs.com/technologies/overview/proxy


1.1.1.1

# Threat Intelligence: A View of the Internet Threats

# Cyber Industry Trends

CLOUDFLARE

1. Phishing continues to be primary entrypoint for compromise
2. Machine learning needed to mitigate <0 Day attacks
3. APIs are a growing target for attacks, often poorly defended
4. Compliance complexity increasing with cyber regulatory frameworks

CLOUDFLARE

Deloitte. Services Industries Careers

91% of all cyber attacks begin with a phishing email to an unexpected victim

8 simple practices towards cyber-resilience

KUALA LUMPUR, 9 January 2020 - Cybersecurity practitioners have, for many years, been promoting the adage 'it's not if, but when' organisations will be impacted by a cyber attack. With attackers adopting and deploying increasingly advanced and sophisticated tools, and organisations struggling to address cybersecurity challenges - not least talent and skill shortages - 'if, not when' is probably true for most organisations today.

The cybersecurity community generally believes that many of the security breaches in recent history were avoidable. For instance, research[1] suggests that 95% of security breaches in 2018 could have been prevented, and that many of the techniques attackers used to successfully breach systems in 2018 remain the same as those used historically. In a more specific example, investigative reports[2] describe the 2017 data breach suffered by the US credit bureau Equifax, which disclosed personal detail of more than 140 consumers, as 'entirely preventable'.

Press contact:

Samantha Yong
Marketing and Communications
+603 7624 3502
zeyong@deloitte.com

- **Get the basics right**
- **Training alone will not solve this issue**

Source: https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

CLOUDFLARE

# ML Detections find attacks *before* day zero

Many new CVEs are similar yet different enough to bypass signatures. However, ML classification techniques with high quality training data yield surprisingly good results.

Sitecore and Ivanti are recents example of correct classification on newly created CVEs:

| CVE | Date | Score | Signature match | Classification match (score less than 10) |
|---|---|---|---|---|
| CVE-2023-35813 | 06/17/2023 | 9.8 CRITICAL | Not at time of announcement | Yes |
| CVE-2023-33653 | 06/06/2023 | 8.8 HIGH | Not at time of announcement | Yes |
| CVE-2023-33652 | 06/06/2023 | 8.8 HIGH | Not at time of announcement | Yes |
| CVE-2023-33651 | 06/06/2023 | 7.5 HIGH | Not at time of announcement | Yes |

CLOUDFLARE

# Signatures are here to stay

Without signatures we would not be able to build this. And they are a core competency to keep improving...


Our internal analyst team now focus a percentage of their time reviewing bad traffic that does not match signatures.

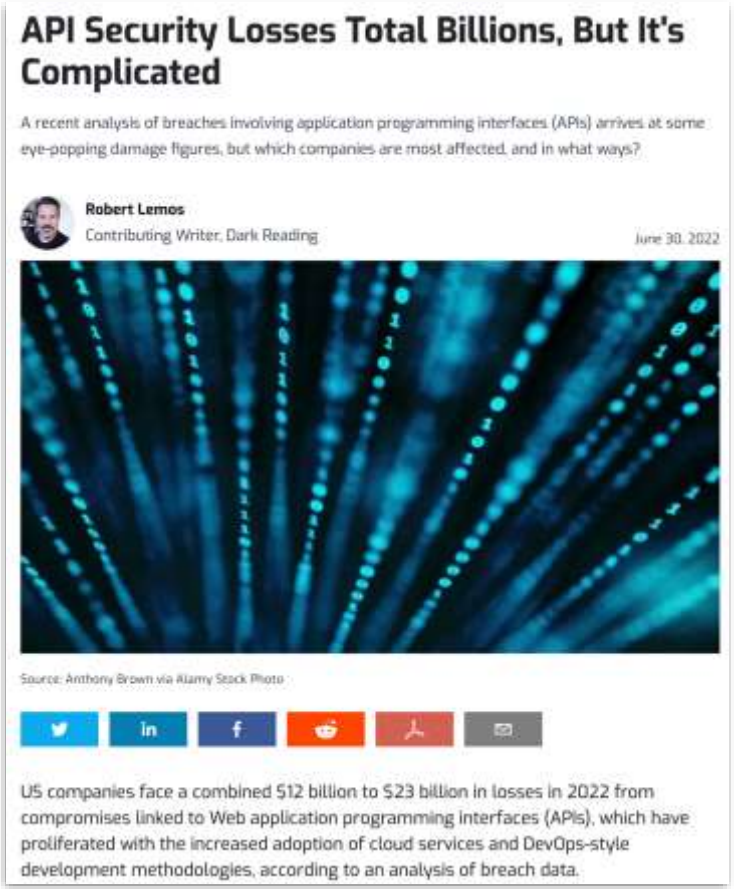
This in turn, leads to **improvements to the signatures** system while keeping a very low rate of false positives.

Which leads to a better training set.

## API Statistics

CLOUDFLARE

- Very high cost incidents
- 58% of Cloudflare traffic, and growing
- Inventory is first step
  - 30%: Average of APIs unknown
- Schema validation as 2nd step
- Then advanced protections



# API Security Losses Total Billions, But It's Complicated

A recent analysis of breaches involving application programming interfaces (APIs) arrives at some eye-popping damage figures, but which companies are most affected, and in what ways?

**Robert Lemos**
Contributing Writer, Dark Reading

June 30, 2022

Source: Anthony Brown via Alamy Stock Photo

US companies face a combined $12 billion to $23 billion in losses in 2022 from compromises linked to Web application programming interfaces (APIs), which have proliferated with the increased adoption of cloud services and DevOps-style development methodologies, according to an analysis of breach data.

Source: https://www.darkreading.com/application-security/api-security-losses-billions-complicated

CLOUDFLARE

# New SEC Incident Disclosure Rules

***Effective December 18, 2023***

Requires companies to

*“disclose…any cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the registrant”*

**…within 4 business days of the incident**

# Current Attack Tactics

CLOUDFLARE

1. Hacktivism
2. DNS Laundering
3. VPS Botnets
4. Growth in Layer 7 Attacks
5. Shift to Residential Proxies

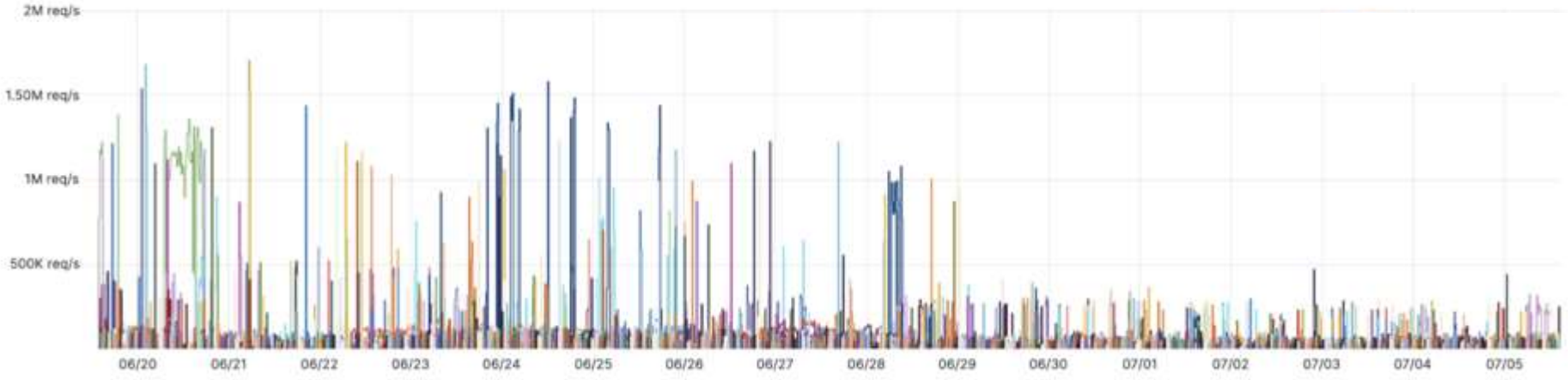
CLOUDFLARE

# Pro-Russian hacktivist groups: Killnet, REvil and Anonymous Sudan take aim

Publicly, aimed at Western banks and SWIFT network.

In reality, also attacked many other industries.

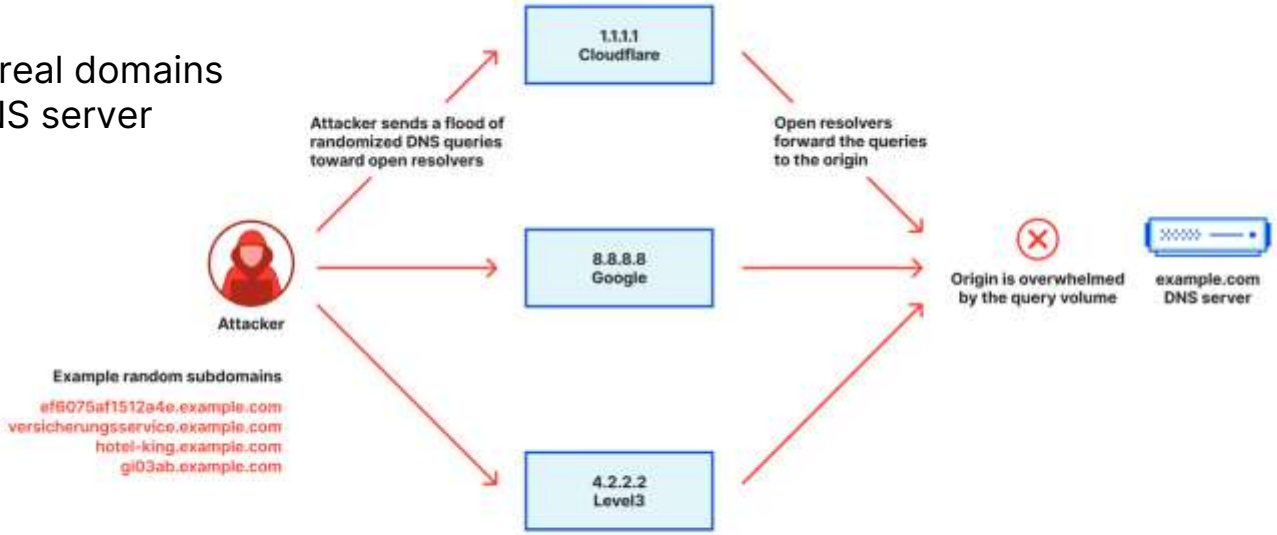
10,000 DDoS attacks from Darknet Parliament on Cloudflare-protected websites



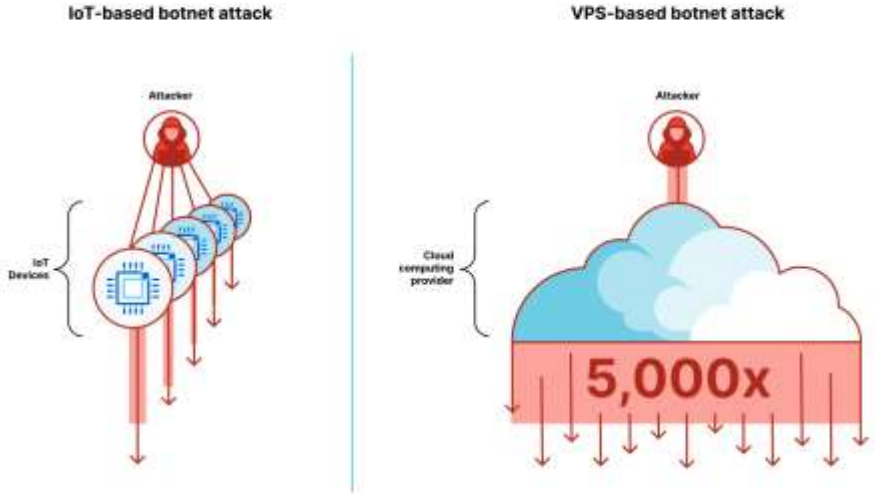
CLOUDFLARE

# Attack chain of a DNS laundering DDoS attack

- “Laundering” queries off of legit DNS resolvers such as Google’s 8.8.8.8 and Cloudflare’s 1.1.1.1
- Random-prefix queries of real domains managed by the target DNS server



# Powerful VPS-Based Botnets with 5000x Capacity

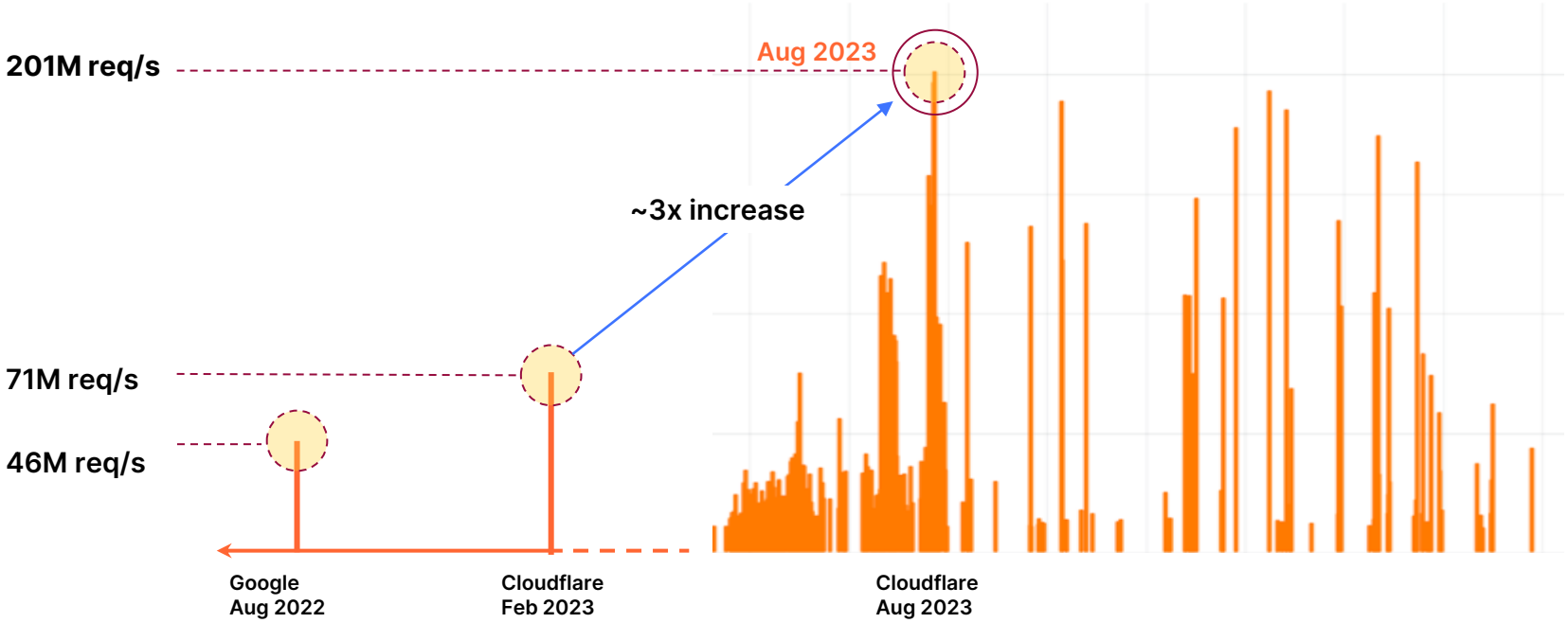



- HTTP/2 improves website and Botnet performance
- Virtual Machines (VMs) / Virtual Private Servers (VPS)

  not Internet of Things (IoT) devices
- 5000x capacity
- Cloudflare collaboration with cloud computing providers to neutralise the threats

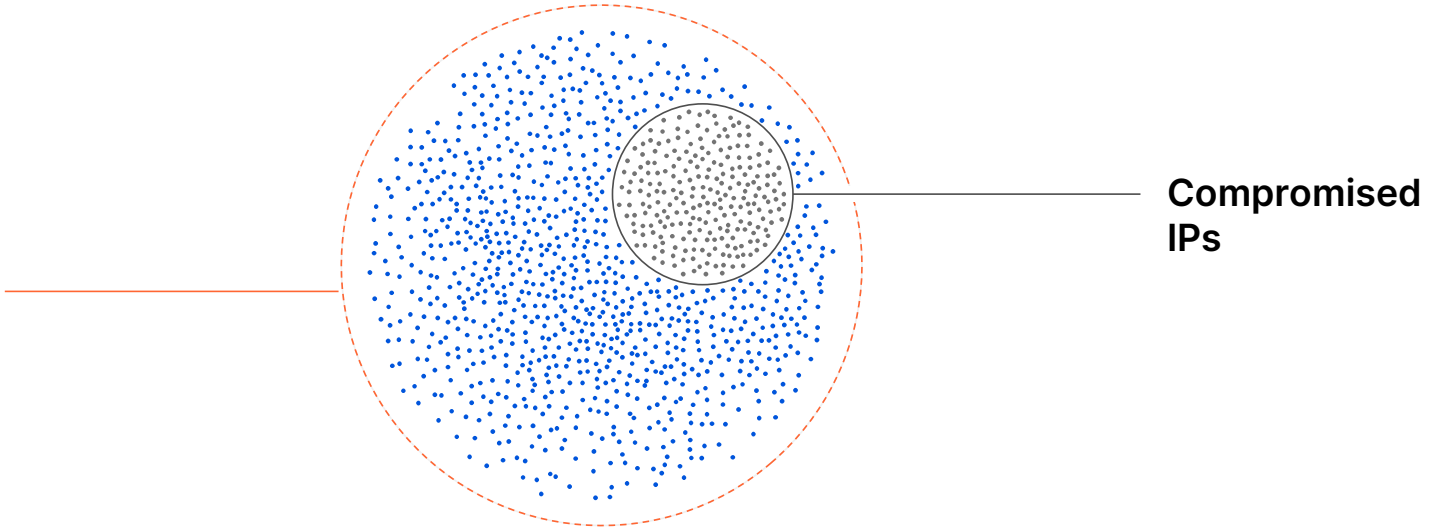
# Massive growth in application layer attacks

*Few organizations have effective Layer 7 DDoS protection*



# Fraud shifting to residential proxies

*Botnets with 50M+ IP addresses*



# Recap Lessons Learned

Trends

- Phishing protection (past)
- ML powered WAF (present)
- API Security (future)
- Boards lean in due to regulations

Tactics

- Broad spectrum, automated mitigations
- Internet-scale DNS infrastructure protections
- High volume layer 7 protections
- Threat from residential proxies

# Thank you

1 888 99 FLARE

enterprise@cloudflare.com

www.cloudflare.com