INDUSFACE™

THE STATE OF APPLICATION SECURITY - Q1, 2023

INDEX

About Indusface 05

Executive Summary 06

Global Trends 06

- Vulnerability Exploits 06
- DDoS & Bot Attacks' Trends 11

India Data Insights 15

Necessary Definitions 17

APPTRANA

Fully Managed WAF with Integrated Application Scanner (DAST), API Protection, DDoS/Bot Protection, and CDN

START YOUR FREE TRIAL NOW

ABOUT INDUSFACE

Indusface is a leading application security SaaS company that secures critical Web, Mobile, and API applications of 5000+ global customers using its award-winning fully managed platform that integrates web application scanner, web application firewall, DDoS & Bot Mitigation, CDN, and threat intelligence engine.

Indusface, funded by Tata Capital Growth Fund II, is the only vendor to receive 100% customer recommendation rating three years in a row and is a global customer choice in the Gartner Peer Insights™ Web Application and API Protection (WAAP) Report 2023. Indusface is also a "Great Place to Work" 2022 Winner in the Mid-Size category in India and is PCI, ISO27001, SOC 2, GDPR certified and has been the recipient of many prestigious start-up awards.

INDUSFACE IS THE ONLY CLOUD WAAP (WAF) VENDOR WITH 100% CUSTOMER RECOMMENDATION FOR 3 CONSECUTIVE YEARS

A CUSTOMERS' CHOICE FOR 2022 AND 2023 GARTNER® PEER INSIGHTS™

Gartner Peer Insights Customers' Choice 2023™

OUR CUSTOMERS

TCS TATA CONSULTANCY SERVICES | IndusInd Bank | L&T Infotech | ADITYA BIRLA CAPITAL

HDFC ERGO Take it easy! | marico | TITAN | ACT FIBERNET

Khatabook Business hua Easy | CRISIL An S&P Global Company | AEGON Life | MYn

R. | TATA PLAY | NASSCOM® | YES SECURITIES

EXECUTIVE SUMMARY

The State of Application Security - Q1, 2023 report is based on a sample size of 1400+ applications.

Here are the findings from the study –

- 1 billion attacks were blocked during this time. Over 500 million of them were from India.
- Bot attacks are on the rise. We saw a 59% increase in Bot attacks. 5.9M vs 3.7M - (Q1, 2023 vs Q4, 2022)
- The Banking and Healthcare Industries were the most hit with Bot attacks.
- The Insurance industry was the most attacked as it received 12X more attacks than all industries.
- 24K critical, medium, and high vulnerabilities were found.
- 31% of vulnerabilities have been open for more than 180 days. This includes 1727 critical and high vulnerabilities.
- Customers are increasingly taking the virtual patching route at the WAF level
- 68% of the attacks were blocked by using AppTrana's core rules set.
- 32% of the attacks were blocked using custom rules. This signifies the importance of managed services and custom rules for security teams across the world.
- DDoS attack was the major attack type.
- The top attack countries were India, UK, and Senegal.
- Other than India, the major countries from where Bot attacks were observed – the United States and the UK.

GLOBAL TRENDS - Q1, 2023

VULNERABILITY EXPLOITS -

Total no. of vulnerabilities found: 24K

Top 10 vulnerability categories found:

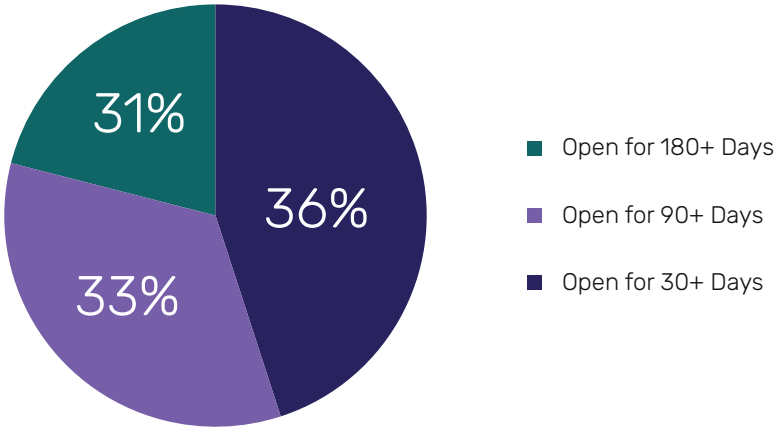
VULNERABILITY TYPE	TOTAL ALERTS FOUND
Cross-Site Scripting (XSS)	911
Server Side Request Forgery Detected	846
HTML Injection	629
TLS/SSL Server Certificate Will Expire Soon	603
Directory Listing - log	186
Script Source Code Disclosure	94
SQL Injection	77
SSL Certificate Common Name Mismatch	47
TLS/SSL Server Certificate Expired	43
Core Dump File - log	32

AGING TREND OF THESE VULNERABILITIES:

Across 1400+ sites were analyzed. We have found 24K critical, high, and medium vulnerabilities and around 31% of the critical and high vulnerabilities have been open for more than 180 days. This includes 1727 critical vulnerabilities that have been open for 180+ days.

With AppTrana, customers can ensure that vulnerabilities are virtually patched immediately reducing the time to fix ensuring the security team becomes an enabler of business instead of blockers. Many of our customers leverage the risk-based protection of AppTrana to get vulnerabilities patched in WAF immediately enabling rapid deployment.

AppTrana also ensures the detection and protection of zero-day vulnerabilities with more than 95% of zero-day vulnerabilities protected by default using AppTrana default rules.



No. of critical and high vulnerabilities open for 30 days – **36%**

No. of critical and high vulnerabilities open for 90 days – **33%**

No. of critical and high vulnerabilities open for 180 days – **31%**

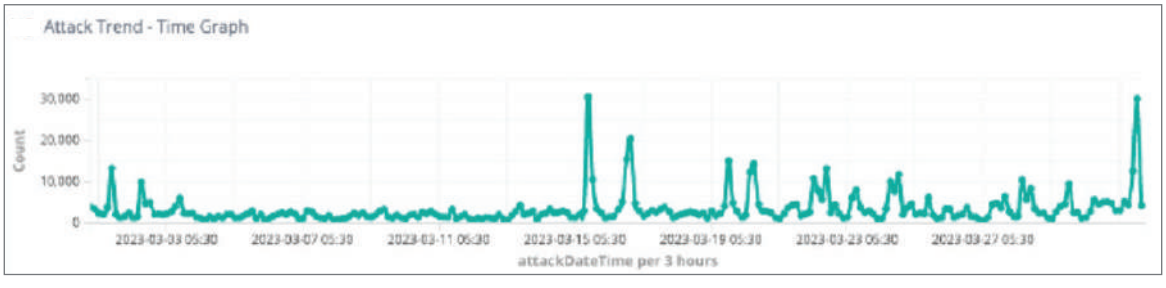
PROTECTION TRENDS:

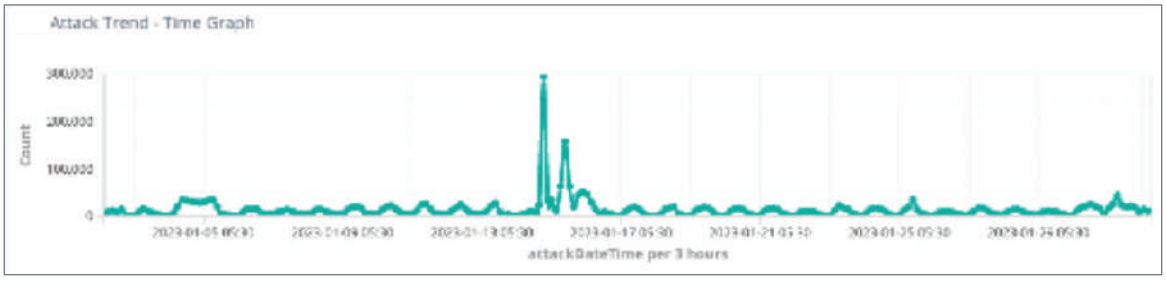
Total Attacks Count

1071793063

We saw over 1 billion requests that got blocked across all sites protected by AppTrana. It's a 29% increase in attacks when compared to 829M attacks in Q4, 2022.

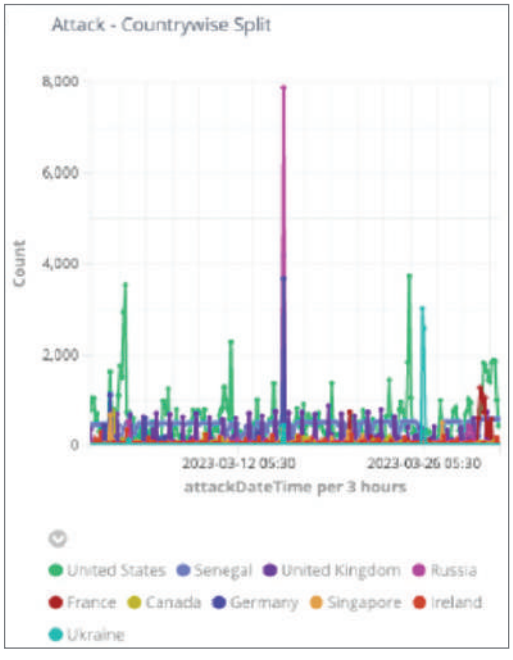
Past 180 days attacks' (Q1, 2023 monthly split) trend across all sites:





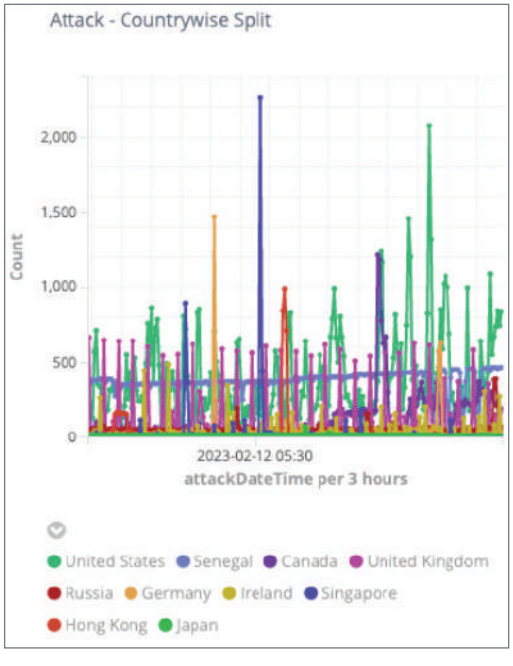
Attacks - Country-wise Split

Given majority of customers business is targeting Indian markets, large number of these attacks originate from India. The next major countries we see attacks from is United States and Senegal.



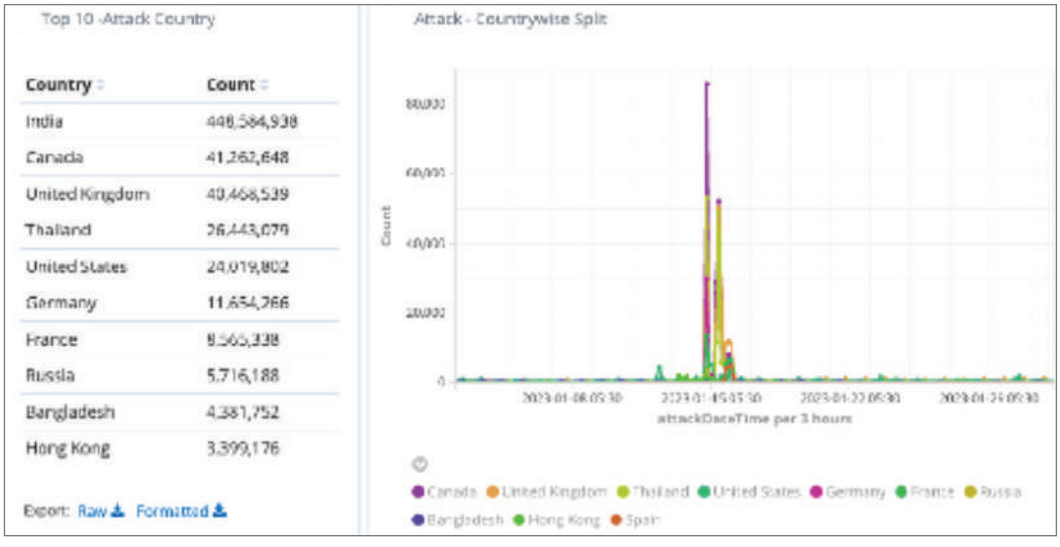
Top 10 -Attack Country

Country	Count
India	79,426,429
United States	25,064,380
Senegal	19,593,085
United Kingdom	5,484,420
Russia	4,611,059
France	2,030,062
Canada	2,006,786
Germany	1,990,242
Singapore	1,528,484
Ireland	1,491,859



Country	Count
India	213,784,105
United States	15,511,218
Senegal	15,384,998
Canada	4,159,883
United Kingdom	3,886,779
Russia	2,518,725
Germany	1,684,230
Ireland	1,374,789
Singapore	1,244,184
Hong Kong	844,396

Export: Raw Formatted



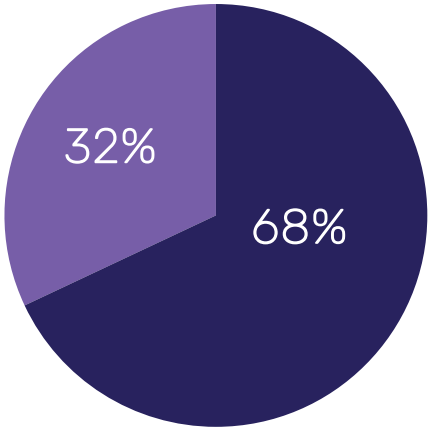
In the past 180 days across sites:

No. of blocks by Core Rules Set across sites:

338832135

No. of blocks by Custom Rules across sites:

162393973



68% of requests were blocked by AppTrana's default rule set and 32% of requests were blocked by custom rules created based on the specific need of applications highlighting the value of managed service that AppTrana provides as well.

DDOS & BOT ATTACKS

As new attack trends of DDoS and Bot attacks emerge against web applications and APIs, business continuity becomes very important.

- AppTrana WAAP guarantees zero false positives and ensures 99.99% uptime against layer 3-7 DDoS attacks with behavioral DDoS mitigation, AI-based rate-limiting based on URI, IP, host, and geo.
  Click here to know more.

- Against Bot attacks such as account takeover, credential stuffing, and scrapping, AppTrana WAAP provides protection from day zero with behavioural & real-time visibility and analysis of bot traffic, correlated risk scoring & anomaly detection, and custom controls. Click here to know more.

Unmetered DDoS Mitigation

Zero false positives guaranteed with behavioural & AI-based rate-limits on URI, IP, host and geo.

We see the following DDoS & Bot trends:

The total number of sites where DDoS & Bot Attack trends were observed in the last 180 days are:

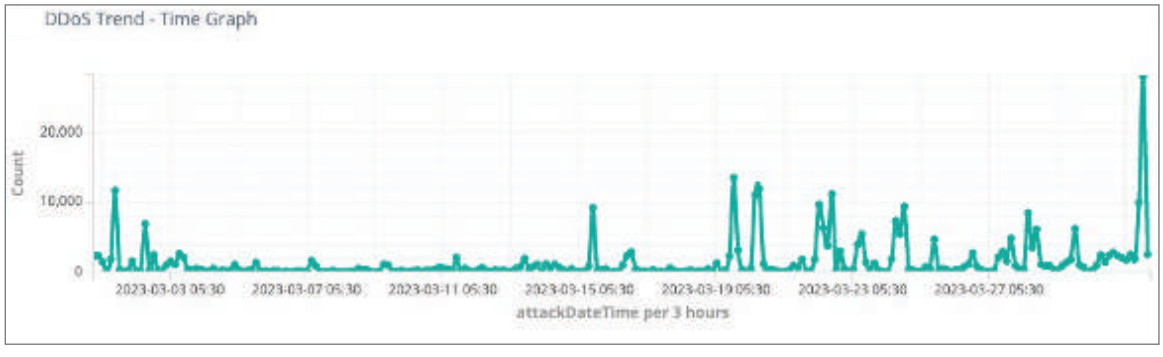
Total DDoS Attacks Blocked - Sites **446**	Total DDoS Attacks **498971127**
Total Bot Attacks Blocked - Sites **1226**	Total Bot Attacks **59484431**

Q1, 2023 vs Q4, 2022 -

- In Q4, 2022, 743 sites were attacked by bots. This shows a 65% increase in the no. of sites attacked by bots in Q1, 2023.
- There is a 48% increase in DDoS attacks. 498M vs 336M (Q1, 2023 vs Q4, 2022)
- There is a 59% increase in Bot attacks. 5.9M vs 3.7M (Q1, 2023 vs Q4, 2022)

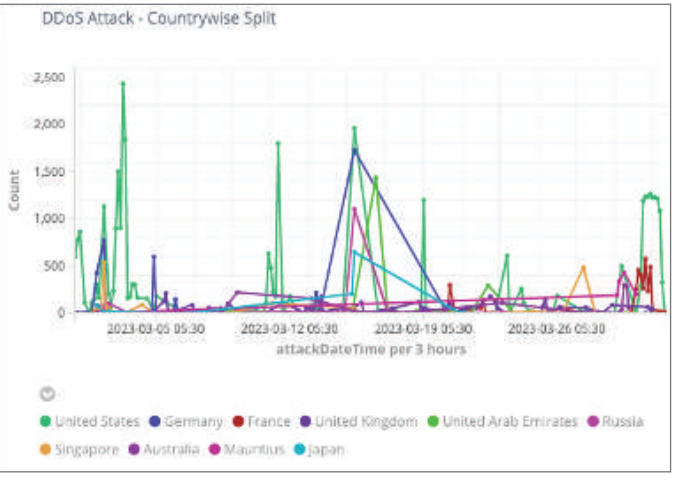
DDoS & Bot Attacks Trends (Monthly & Country-wise Split)

DDoS attacks trends



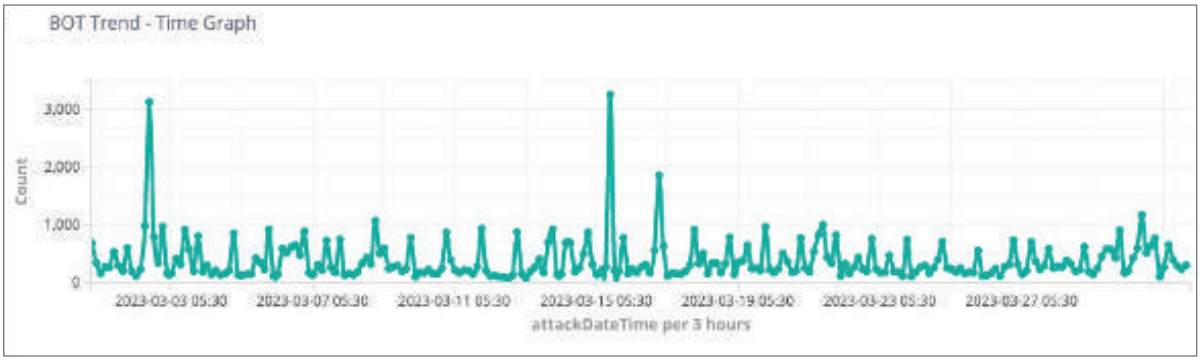
Top 10-DDoS Attack Country

Country	Count
India	51,928,679
United States	5,974,169
Germany	765,442
France	637,272
United Kingdom	603,733
United Arab Emirates	327,348
Russia	263,606
Singapore	261,825
Australia	224,454
Mauritius	212,221



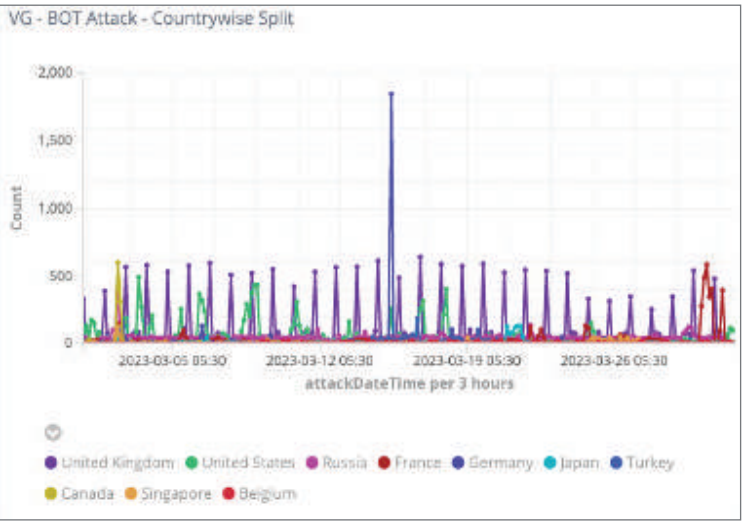
Major countries from where DDoS attacks were observed other than India are the United States and the UK. These trends are in accordance with the changes in the geo-political trends.

Bot Attacks Trends



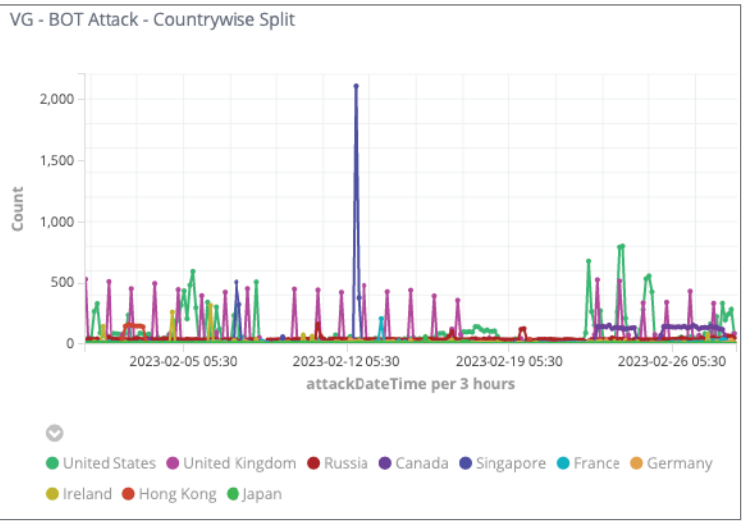
Top 10-BOT Attack Country

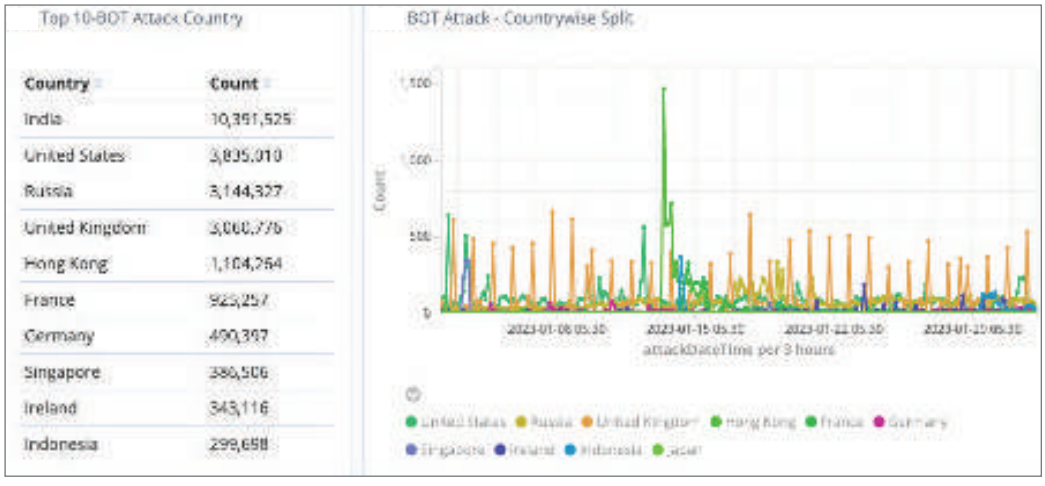
Country	Count
India	5,004,958
United Kingdom	3,333,305
United States	2,734,594
Russia	2,050,970
France	1,024,723
Germany	640,468
Japan	324,629
Turkey	253,533
Canada	249,773
Singapore	239,058



Top 10-BOT Attack Country

Country	Count
India	5,004,165
United States	3,756,354
United Kingdom	2,046,624
Russia	1,649,835
Canada	966,181
Singapore	703,951
France	406,221
Germany	319,760
Ireland	314,117
Hong Kong	259,556





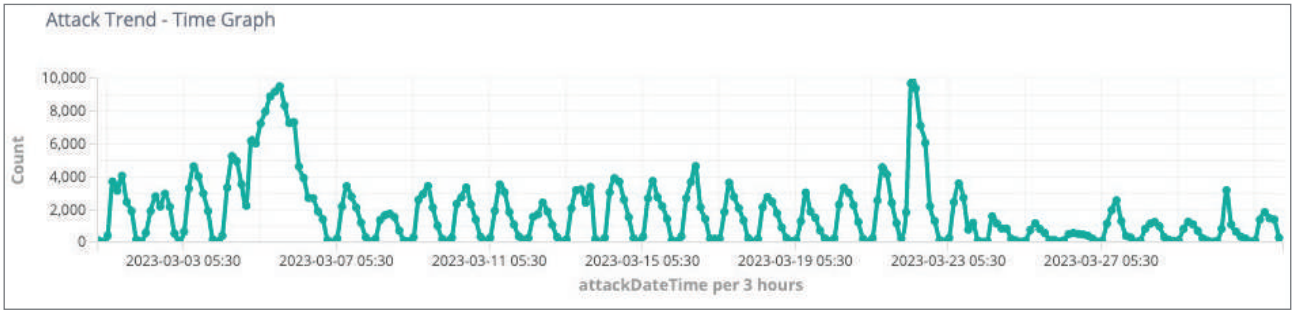
Major countries from where Bot attacks were observed other than India are the United States and the UK. These trends are in accordance with the changes in the geo-political trends.

INDIA DATA INSIGHTS

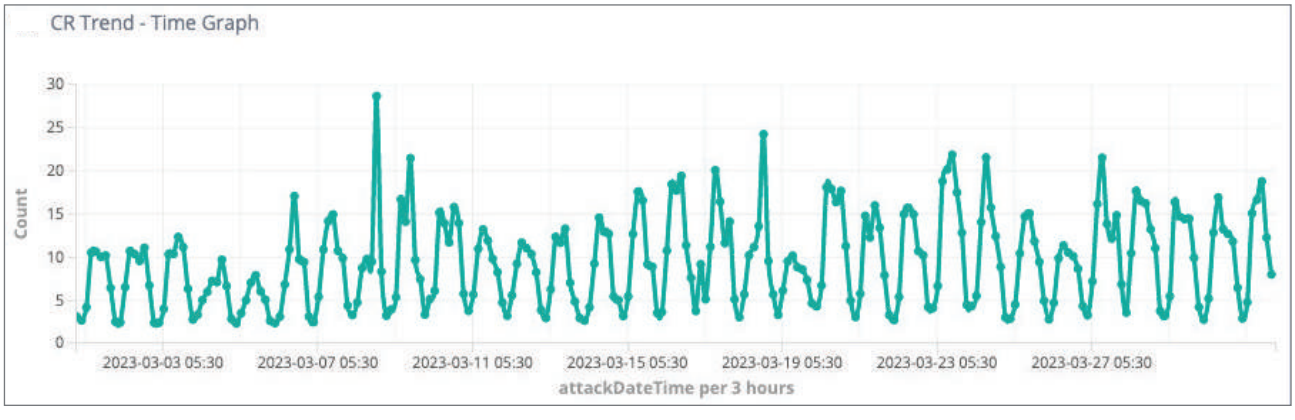
- Over 500 million attacks were blocked during this time.
- The Banking and Healthcare industries were the most hit with Bot attacks.
- The Banking industry relies on custom rules. More than 50% of the attacks were blocked using custom rules.
- The Insurance industry was the most attacked as it received 12X more attacks than all industries.

No. of attacks per site for Insurance Industry	No. of attacks per site for All Industries
995455	**83264**

Attack Trend in the Insurance Industry



Custom Rules Trend for the Banking Industry



NECESSARY DEFINITIONS:

- **Cross-Site Scripting –**
    - XSS or CSS is a web application attack used to gain access to private information by delivering malicious code to end-users via trusted Web sites. Typically, this type of attack is successful due to a web application's lack of user input validation, allowing users to supply application code in HTML forms instead of normal text strings.

- **HTML Injection -**
    - A type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page. This vulnerability leads to many consequences, like disclosure of a user's session cookies that could be used to impersonate the victim, or it can allow the attacker to modify the page content seen by the victims.

- **DDoS Attack –**
    - A distributed denial of service (DDoS) is a type of cyber-attack where target web applications/ websites are slowed down or made unavailable to legitimate users by overwhelming the application/ network/ server with fake traffic.

- **Bot Attack –**
    - A botnet is the collection of malware-infected computers and networked devices (IoT, smart devices, etc.) that work together under the control of a single malicious actor or an attack group. Such a network is also known as a zombie army and each infected device is called a bot/ zombie.

CUSTOMER TESTIMONIALS

Biswa Prasad Chakravorty

CIO, IndusInd Bank

With Indusface, we have worked together on a model that looks at different types of risks in the bank and this model scales on demand and at the same time effectively mitigate risks.

Mayuresh Purandare

Head – IT Infrastructure and Cyber Security, Marico

We do not have a special SOC for Application Security. As our AppTrana product license includes managed services, the Indusface team is the AppSec SOC for us.

Dilip Panjwani

Global Head - Cybersecurity Practice & CoE, LTIMindtree

We were looking for a WAF that focuses on attacker behaviour rather than variance signatures to mitigate the risk from application vulnerabilities. We decided to take the leap and partner with Indusface to protect our enterprise application footprint.

INDUSFACE IS THE ONLY CLOUD WAAP (WAF) VENDOR WITH 100% CUSTOMER RECOMMENDATION FOR 3 CONSECUTIVE YEARS

A CUSTOMERS' CHOICE FOR 2022 AND 2023 GARTNER® PEER INSIGHTS™

Gartner Peer Insights Customers' Choice 2023™

BENGALURU | VADODARA | MUMBAI | NEW DELHI | SAN FRANCISCO

Contact Us - +91 265 6133021 | +1 866 537 8234

Email - sales@indusface.com | Website - www.indusface.com