Financial Services Threat Brief

APRIL 2017

India

Akamai
FASTER FORWARD

Is your organization prepared?

Thank you for taking part in our security survey. We hope that with this survey you can gauge your organization's readiness against the growing number of advanced security risks that can negatively impact your business continuity, brand reputation and IT efficiency. In today's security landscape, it is critical that organisations identify their security posture, and the gaps in terms of handling attacks such as web defacements, data breaches, ransomware, and Distributed-Denial-of-Service (DDoS).

The following report is an exclusive Financial Services Threat Brief designed to help you gain a deep understanding of the security landscape specific to your region. The information provided is aimed at helping businesses and IT leaders prioritise their organisation's investments in web and application security.

The threat environment on the Internet is a constantly evolving arms race, and the activities of adversaries vary greatly by geography, industry, and even individual websites. As a result, security managers often seek the latest attack information that is relevant to their specific country and industry to predict what they should look for in the present and how attacks will evolve in the future. In response, Akamai creates this monthly industry threat report to inform approaches for customers to improve their defensive posture.

What is in this report?

This report is a monthly snapshot of attack traffic and trends against financial services organizations in India, as a companion to our quarterly global State of the Internet/Security report. It is intended to highlight threats relevant to decision makers and to support actionable responses.

The information in this report can help organizations better defend themselves against threats, model risks, and improve visibility into the thread landscape.

Where does Akamai get its data on web application attack activity?

As the world's largest cloud security provider and Content Delivery Network (CDN) that protects and delivers 15–30% of the World Wide Web at any given time, Akamai is in a unique position to report on attacks and dangers that our customers face on both a global and local scope. This insight gives Akamai unique visibility into attack activities across most of the Internet from the point of view of web servers, DNS servers, and the infrastructure that supports them.

Akamai's customers use its managed service offerings, including its Kona Site Defender attack mitigation services and Web Application Firewall, to protect web services and systems against attack. Every day, Akamai protects thousands of customers against a wide variety of attacks such as defacements, data breaches, and Distributed Denial of Service (DDoS).

The hundreds of thousands of servers that Akamai has deployed around the world report events from Web Application Firewall, Operating System Firewall, and Content Delivery Network logs to our big-data systems. These logs are analyzed to detect attacks, highlight repeat offenders, and generate an IP reputation database. Some of these observations are reported on a global scale in our quarterly State of the Internet/Security Report at https://www.akamai.com/SOTI.

Akamai's threat observations can be filtered in four main ways:

1. **By source IP address.** Almost all routable IPv4 IP addresses worldwide access services through Akamai.
2. **By the targeted organization type.** Akamai's customers are most of the world's most heavily targeted organizations and websites: government, finance, news, online retail, and most other major online sectors.
3. **By the type of malicious actor.** Akamai's Client Reputation focuses on scoring malicious activities associated with the four following actor types; the score of each is associated with the volume, persistence, severity, and breadth of the associated events observed:
    a. DoS Attacker: an IP address engaged in large-scale volumetric or resource drain types of activities against one or more targets
    b. Web Attacker: an IP that attempts to break into, execute code on, deface, steal information from, or otherwise compromise an online service or site

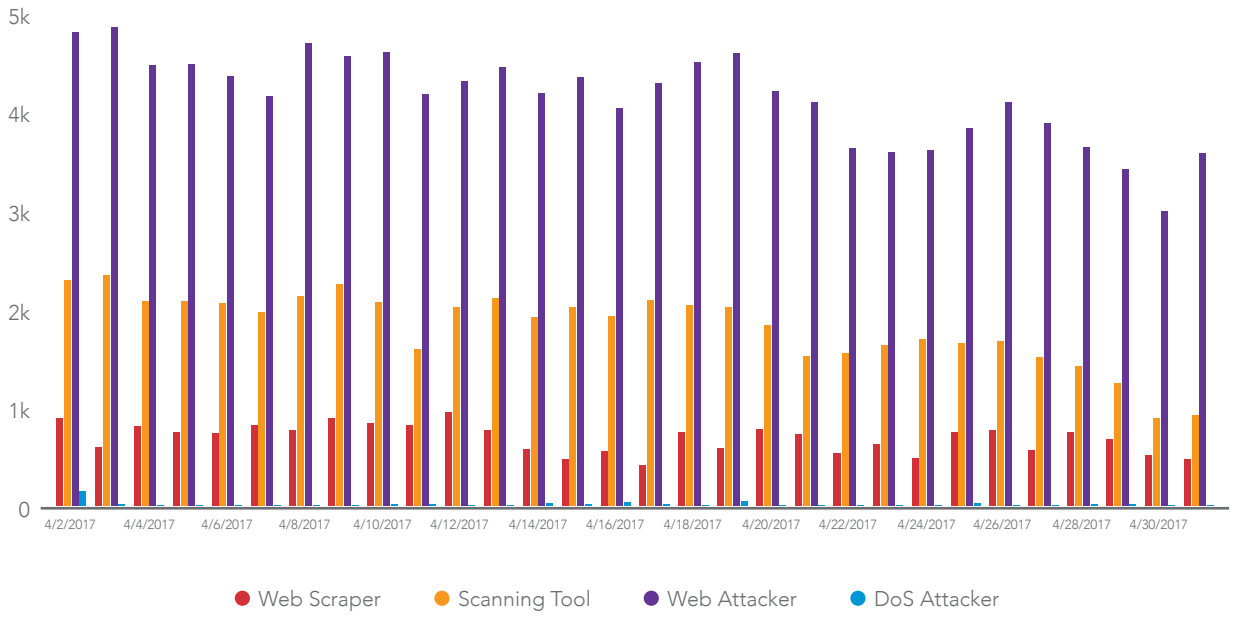
c. **Web Vulnerability Scanner:** an IP that explores avenues for attacking a targeted site by issuing requests that are primarily indications of a vulnerability test, or a tool to do the same

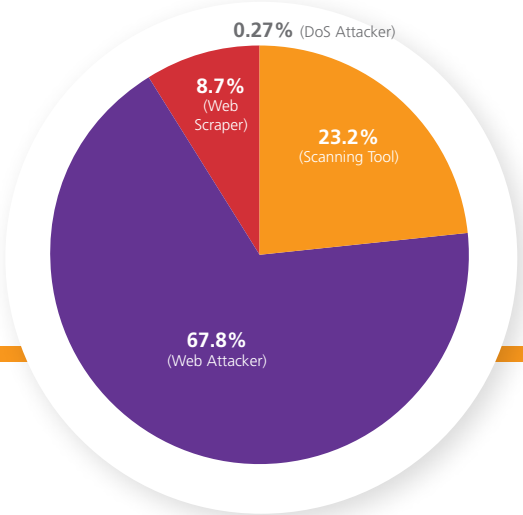
d. **Web Scraper:** an IP harvesting information from websites, usually for commercial exploitation

4. **By the type and volume of events observed.** Various types of events contribute to the determination of a malicious actor.

Macroscopic Trends of Actors Targeting Organizations in India

Attacking IPs over Time





Categories by Unique IP

DoS Attacker	471
Scanning Tool	40,528
Web Attacker	118,328
Web Scraper	15,204

The graphs above demonstrate the overall breakdown of the quantity of IP addresses that are specifically engaged in targeting any online organization located in India and served by Akamai. Note that the prevalence of web attackers is a general reflection of the number of addresses engaged in such activity, but not necessarily the volume of activity or its overall severity.

Industry Breakdown - Attacking IPs

Business Services	2.4%
Consumer Goods	1.4%
Consumer Services	1.3%
Financial Services	6.1%
High Technology	15.6%
Hotel & Travel	4.4%
Manufacturing	0.2%
Media & Entertainment	42.4%
Miscellaneous	11.9%
Pharma/Health Care	0.3%
Public Sector	2.3%
Retail	10.1%
Software as a Service	1.6%
Other	-----

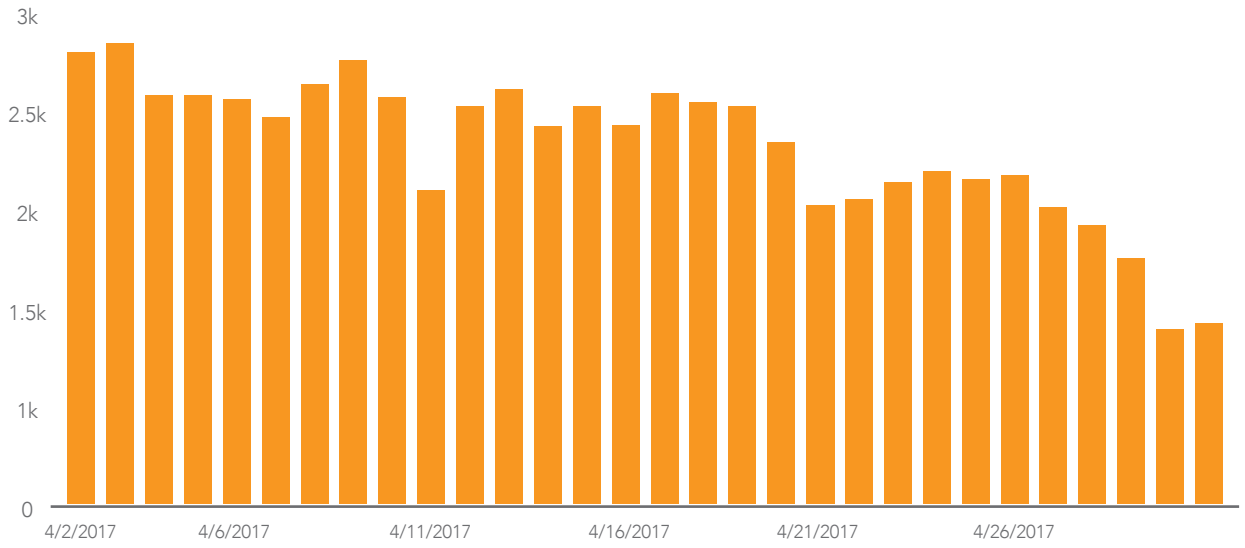
The above graph reflects the relative number of IP addresses observed targeting individual online industries in India, based on the industry of associated Akamai customers who were targeted. The chart includes a highlighted segment focusing on the top sector — Media & Entertainment — by overall percentage of IPs that targeted it.

Activity Levels Targeting India

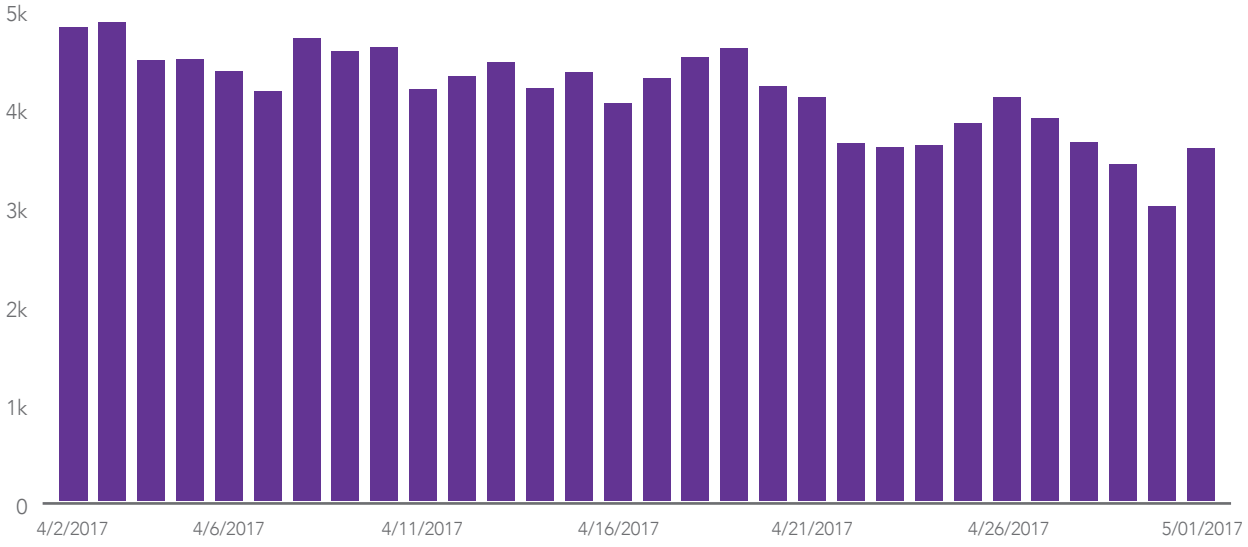
For specific details regarding the patterns of activities observed as targeting India organizations and specifically Financial Services, we present several drill-down views into the activities by attack type.

The graphs presented below showcase overall daily trends in numbers of attacking IPs targeting all India-based organizations. We focus on scanning tools and web attackers because these attack types are most closely related with data breach, defacements, and watering-hole attacks. "Scanning tools" refers to indications that attempts were made to scan for vulnerabilities on a website or service, either by a tool or by other automated vulnerability scanning methods. "Web attackers" refers to attempts to break into a website to steal information, inject code, or otherwise hack into a site or service, such as when SQL Injection (SQLi), Cross-Site Scripting (XSS), or Remote File Include (RFI) attempts are observed.

Attacking IPs - Scanning Tools

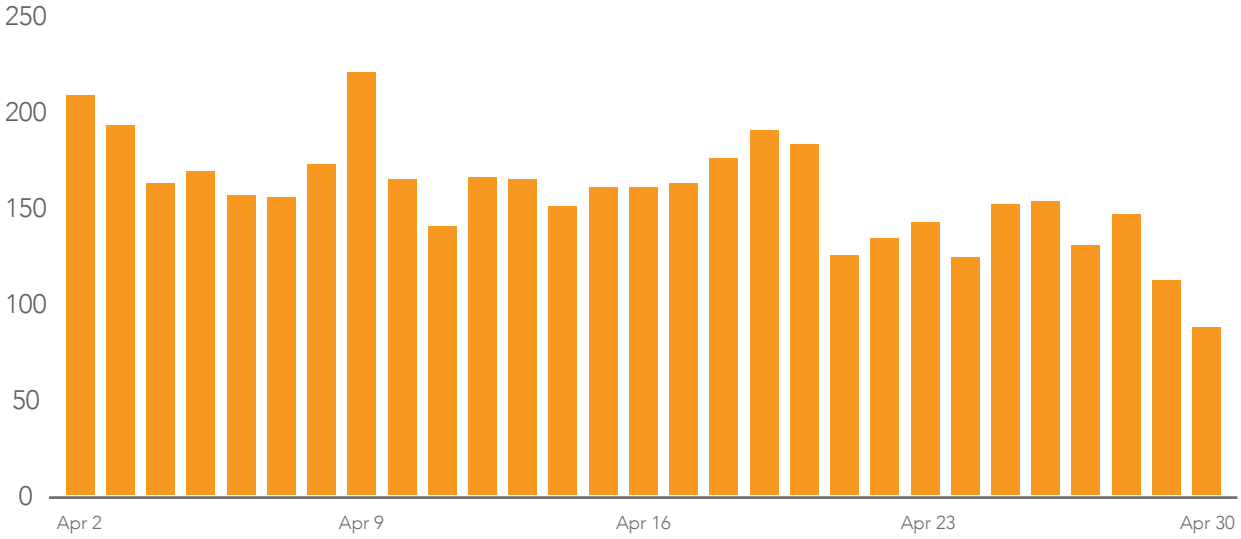


Attacking IPs - Web Attackers

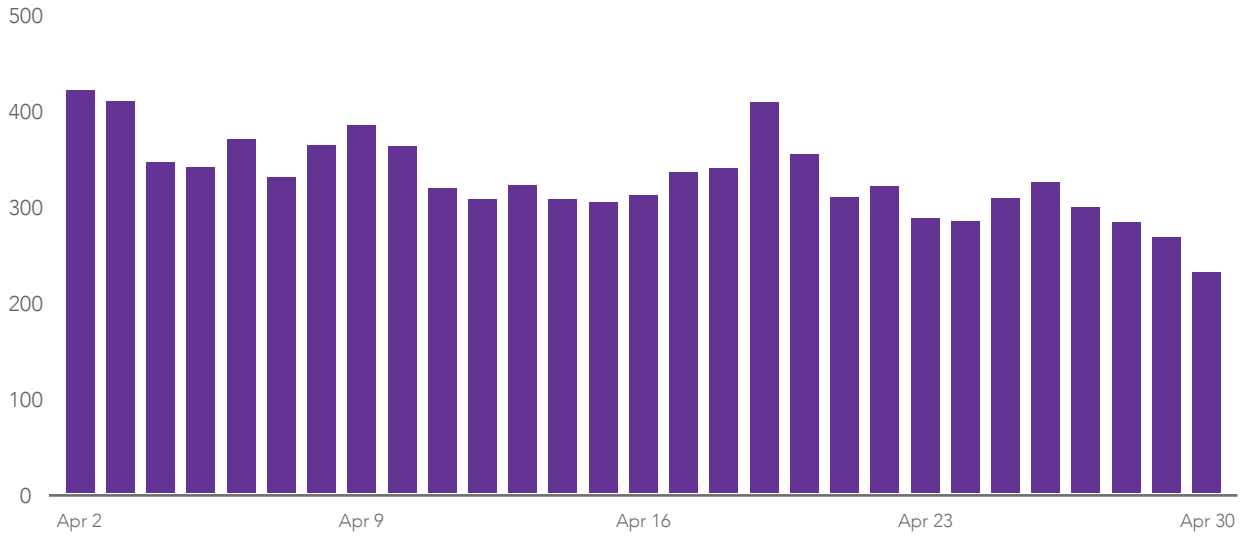


The charts included below outline total IPs actively targeting India-based Financial Services organizations. Note that the overall trend is consistent with India-wide activity, but the volume of addresses seen targeting Financial Services targets in India is approximately 6% of those seen targeting all industries combined.

Financial Services - Scanning Tools



Financial Services - Web Attackers

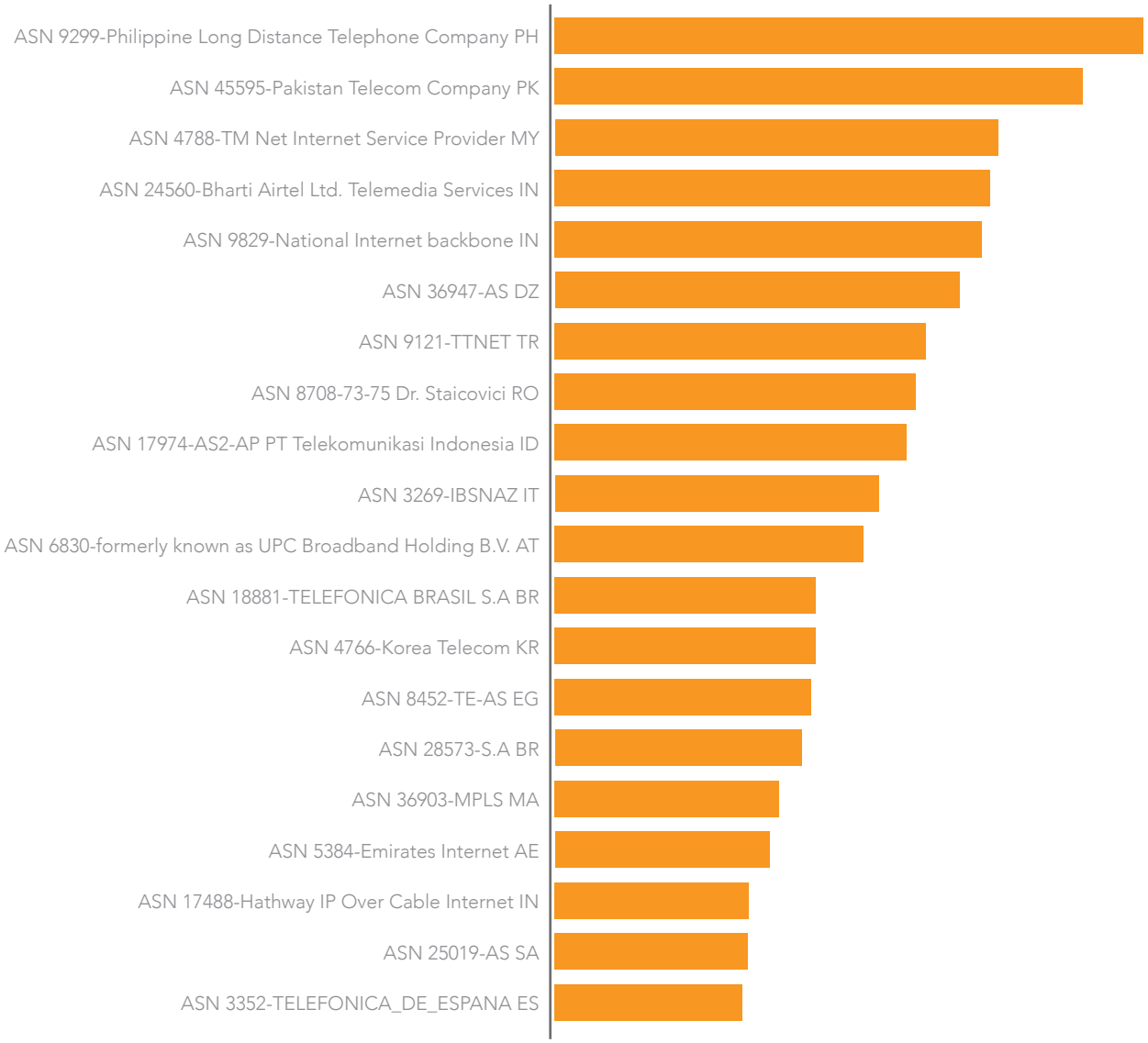


Most Malicious Networks Targeting India

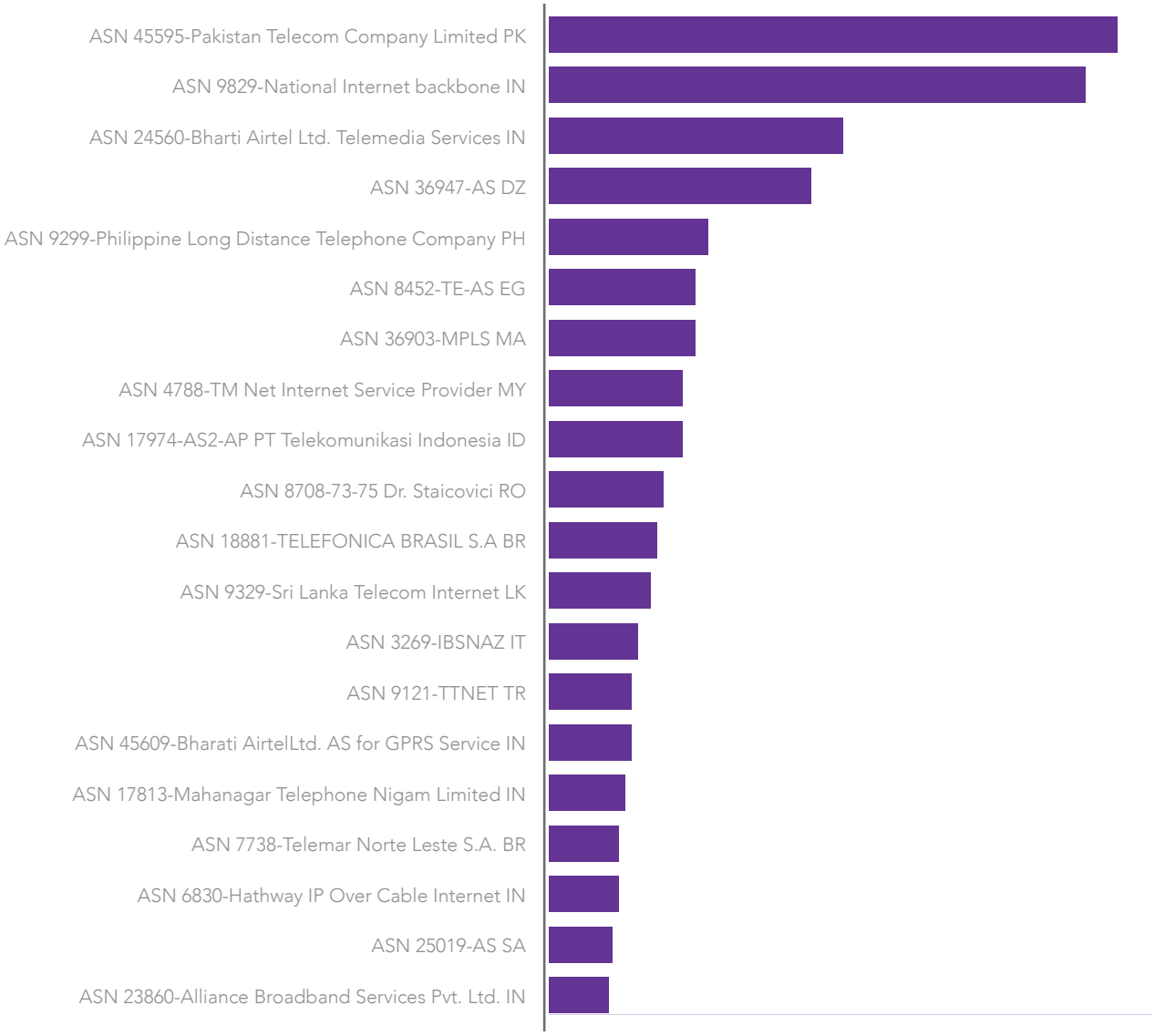
Filtering the observations by the volume of unique IPs seen by network (Autonomous System Number, or ASN) provides a way of viewing which networks may source the most malicious activity against an organization from India. It may be wise to treat requests from these networks as high risk, particularly if one's customers do not typically reside in these locations.

Note further that the networks seen conducting the most web attacks do not align directly with those engaged in vulnerability scanning, and that the vulnerability scanning activity does not necessarily reflect the use of common vulnerability testing tools, based on the sources observed.

Top 20 Network Sources - Scanning Tools



Top 20 Network Sources - Web Attackers



Types of Attacks Targeting India

To better understand the attacks targeting India's organizations, we present a summary of the types of malicious events that occurred with the highest overall volume during this period. This information can inform efforts to prioritize refinement of existing defensive measures, to ensure that the most frequently used and commonly exploited adversarial methods are prioritized.

We present information with web scraping events filtered out, as they tend to have extremely high volumes of requests by definition. The prevalence of observations targeting WordPress login exploits should provide a strong indication that this method appears to be preferred, or most heavily exploited, during the time period. Many other common attack vectors are observed, including SQLi, PHPi, XSS, Joomla-related exploits, and path traversal. In lieu of more detailed information, it may be preferable for an organization to prioritize ensuring that its web services are protected against these types of attacks due to their prevalence in this time period.

Note that this table represents the total number of events observed from IP addresses that had targeted at least one India organization maliciously. In other words, it includes events observed from those addresses that were observed against foreign targets, but from an IP address that had targeted India organizations in some manner. The total hostnames targeted is similarly from the full list of all targeted hostnames from the IPs in question, not just hostnames tied to India organizations.

Top Event Types (Excluding Scrapers)

Event	Request Count	Hostname Count
WordPressLoginExploit	13,262,623	10,831,931
highRequestRateOnPath	3,370,025	0
SQLi	446,926	31,514
webAttackAttempts	313,440	52,917
scanning	255,365	4,499
JoomlaAdminPagesExploit	98,952	37,927
pathTraversal	81,510	1,864
PHPi	48,611	7,428
PHPiOrRFI	32,458	2,204
bruteForceLogin	26,309	295
XSS	21,471	410
byteInjection	3,572	349
CMDi	267	24
JoomlaExploit	258	56
restrictedFileAccess	15	3
highErrorRate	0	0
phpAccessOnNonPhpApps	0	1,143,102
vulnerableFilesAccess	0	124,323

Observations and Summary

In general, the following observations apply to most countries:

1. Web attackers come from a wide dispersion of source IP addresses, but the amount of requests sent by each one is relatively low.
2. Vulnerability scanners are less distributed by source IP address than web attackers, but each source IP address sends more requests.
3. Web scrapers come from a small set of source IP addresses, primarily at Infrastructure-as-a-Service cloud service providers, and send a large volume of requests per each attacking IP address. Sometimes, this is as high as several millions of requests per day from a single source IP address.
4. Application-layer DDoS is relatively low in frequency. The vast majority of DDoS attacks are at layers 3 and 4 and are mitigated before they are evaluated by our Web Application Firewall.
5. Most scrapers are targeted against Hotel & Travel and online retail sites.

Akamai believes the information can inform approaches for customers to better defend themselves against threats, model risks, and improve visibility into the threat landscape. If your organization is interested in protecting its web applications and infrastructure, please contact your Akamai representative for further information.

Identify and address the gaps in your organization

Now that you are up to date on the threat landscape in which your business operates in, you need to start building up your organization's readiness against the ever-present threats. Besides ensuring business continuity, your business needs to protect its brand reputation and improve IT efficiency. By understanding the threats to your business, you will be able to identify the gaps in your security posture, and address them in the near future.

Recommendations

Ensure Business Continuity

1. Plan a DDoS response process / strategy.

   Most companies do not have a proper response strategy in place. By responding quickly to attacks, organizations can mitigate the large potential losses these attacks cause. According to an IDC study, DDoS attacks can cost up to US$1M before mitigation starts.

2. Ensure an appropriate level of confidence, staffing and resources

   Threats are always evolving, which is why businesses need to maintain vigilance and threat mitigation capabilities. This is particularly important because downtime costs financial service firms more than just revenue—it also affects long-term business due to loss in trust and loyalty.

3. Improve your organization's security profile

   According to PricewaterhouseCoopers, FSI companies that manage data privacy and security often gain a competitive advantage in the market place.

Data Protection

4. Assume a potential cost of an attack based on the number of users in your organization

   Data theft can occur to companies of any size. Understanding the impact that a potential attack will cost you, can help your organization justify and manage spending on securing your business from tangible and intangible negative effects.

5. Discover the critical areas that need protection against security threats

   In reported web attacks, 60% of initial compromises occur within minutes. Attackers are quick to find and exploit vulnerabilities. This means your organization needs to take the first step in securing the areas deemed critical.

Brand Reputation

6. Prepare a runbook to manage your organization's reputation

   Media coverage of high-profile attacks is growing. Companies affected may find their brand damaged, and customer trust eroded. A carefully prepared runbook—with cyber security as an integral part of it—can help keep your organization out of the headlines and prepare for the imminent attack.

IT focus on core competency

1. Assume a potential cost of an attack based on the number of users in your organization

   This ensures that your applications and servers are kept safe, while notifying you instantly if your organization is under attack. Having a reputable WAF provider also grants you metrics on false positives and negatives, allowing your security team to be more efficient.

2. Ensure your platform's architecture can scale to address increasing size of attacks

   Recent DDoS attacks have reached a massive 300 Gbps. Experts estimate that yet-to-be discovered attacks may swell to 1 Tbps in the near future. Current architectures are already struggling to deal with a 300 Mbps. To keep your organization safe, you need to invest in platform that allows for the capability to scale.

Compliance

3. Evaluate your security readiness against key regulations compliance

   Having a strong security posture for your organization is critical to your organization's business continuity. However, ensuring that your readiness complies with FSI regulations in your country may require additional vigilance by your service provider. Finding the right security partner to manage the compliance process will ensure that your organization fulfills the regulation requirements, without tying up your already limited IT resources.

We hope the recommendations we have provided will be able to help steer your business towards a compliant and robust security posture. If you prefer a fully managed security solution to protect your business, please contact your Akamai representative for further information.