Dear Customer,

Radware is happy to share our *Monthly Global Security Report*, which is based on attack activity witnessed throughout our cloud security infrastructure during June 2020.

In this report, we provide an overview of the current threat landscape globally, by industry, and by region.

ERT Alerts Issued This Month

- **NXNSAttack**—On May 19, 2020, academics from the Tel Aviv University and The Interdisciplinary Center in Israel discovered a vulnerability in the implementation of DNS recursive resolvers that can be exploited to launch disruptive DDoS attacks against any victim. The researchers dubbed the vulnerability *NXNSAttack*, which they described in their research paper.
  Read the full alert here.

- **Australian Cyberattacks**—On June 19, 2020, Australia's Prime Minister Scott Morrison warned Australian businesses and governments about a sustained cyberattack. Morrison said that Australian organizations were currently being targeted by a sophisticated foreign "state-based" attacker and emphasized the attacks "hadn't just started" but were ongoing and constant threats to Australia. The accumulation of attacks required a firm warning to the government and private sectors to take the appropriate actions to protect their valuable business and personal data.
  Read the full alert here.

Global DDoS Attack Insight

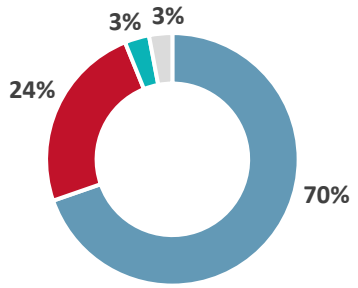
Total DDoS Attacks Blocked:	Total DDoS Attacks Volume Blocked:	Volumetric DDoS Attacks Blocked (> 10Gbps):
167,533	3,258,726 GB	101

In June 2020, Radware observed a massive attack against one of our Hybrid Cloud DDoS customers, a well-known European SaaS provider. This was a very long and continuous attack, utilizing ACK floods, which persisted over an entire month. In all, the total attack volume was 3,131 TB, including nine attacks, which peaked at more than 40 Gbps.

As the volume of this attack obscured all other data, the data is not represented in the following graphs.

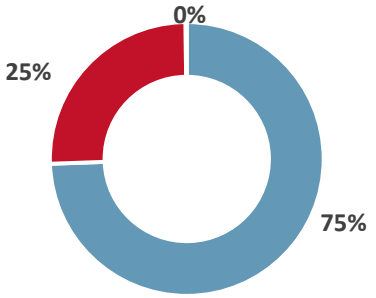
TOP ATTACKED VERTICALS

- ONLINE COMMERCE & GAMING
- BANKING & FINANCE
- HIGH TECH PRODUCTS & SERVICES
- SERVICE PROVIDERS



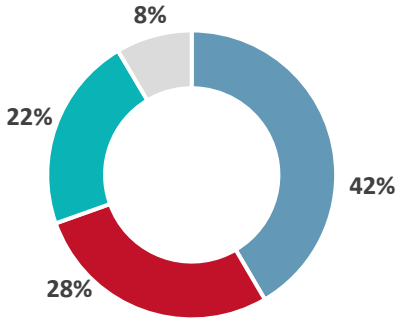
TOP ATTACKED REGIONS

- EMEA
- North America
- APAC



TOP ATTACK VECTORS

- UDP flood
- SYN flood
- TCP out-of-state
- RST flood



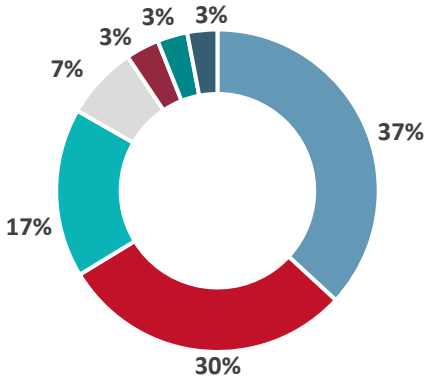
Global Web Application Attack Insight

Total Web Application Attack Transactions Blocked:

139,194,733

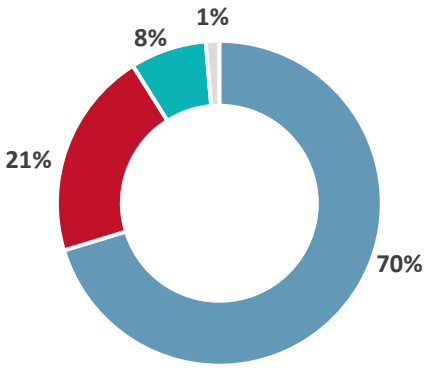
TOP ATTACKED VERTICALS

- HIGH TECH PRODUCTS & SERVICES
- BANKING & FINANCE
- RETAIL & WHOLESALE TRADE
- GOVERNMENT
- TRANSPORTATION
- HEALTH CARE
- MEDIA



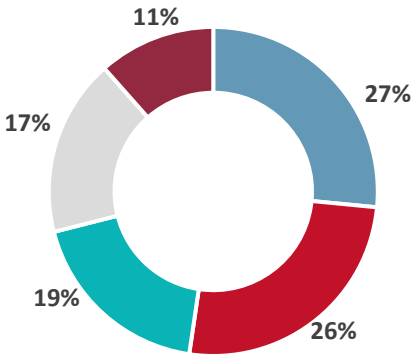
TOP ATTACKED REGIONS

- North America
- EMEA
- APAC
- CALA



TOP ATTACK VECTORS

- Blocked data-leakage attacks
- Blocked access-violation attacks
- Blocked by signatures
- Other
- Blocked SQL-injection attacks

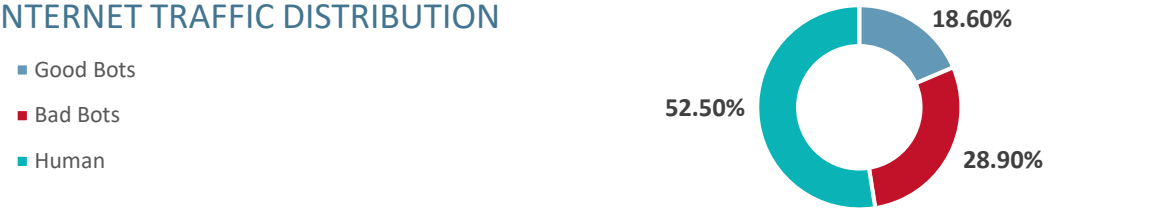


Global Bot Manager Insights

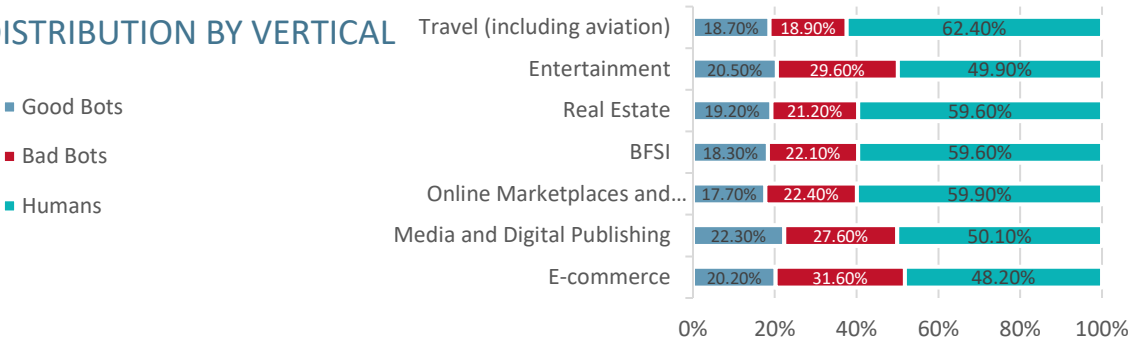
Bad Bots' Volume in Internet Traffic Inspected:

28.9%

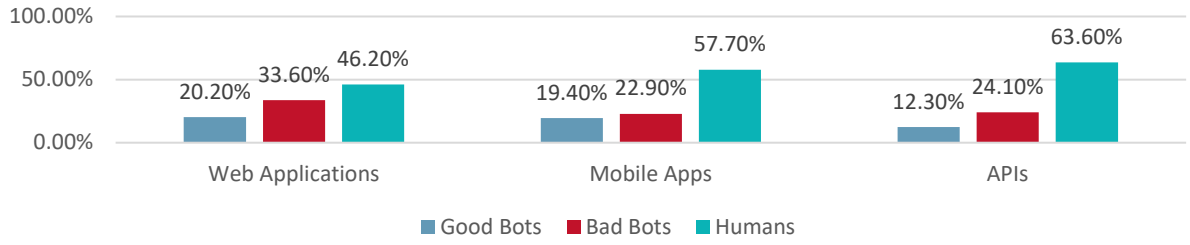
INTERNET TRAFFIC DISTRIBUTION



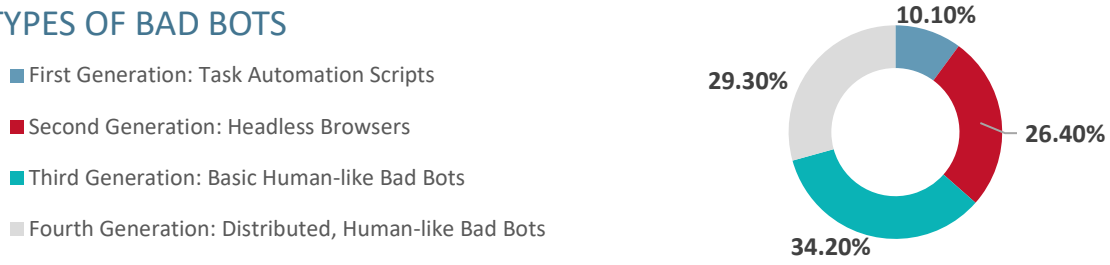
DISTRIBUTION BY VERTICAL



DISTRIBUTION BY ATTACK SURFACE



TYPES OF BAD BOTS



Global Cloud Workload Protection Insights

The following charts are based on security-related data of workloads run on public cloud environments, such as AWS and Azure, protected by the service.

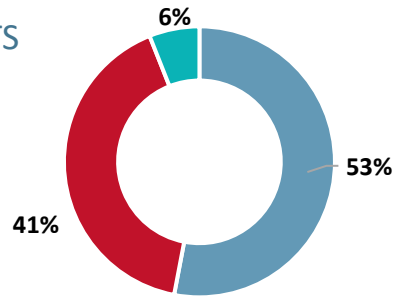
Cloud Assets* with Excessive Permissions:

30%

* Users, Roles, Groups

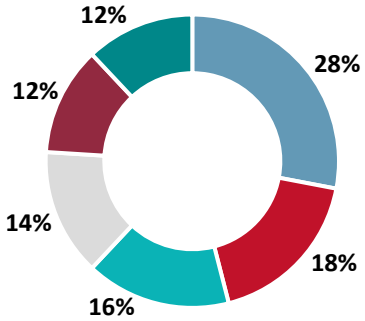
DISTRIBUTION OF PUBLICLY EXPOSED ASSETS

- Machines
- S3 Buckets
- Databases



MISCONFIGURATIONS BY CATEGORY*

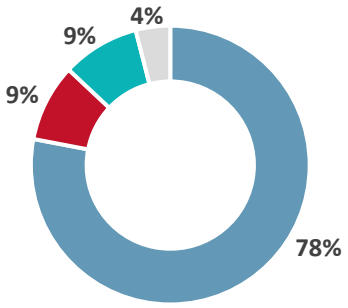
- Monitoring
- Logging
- Encryption
- User Authentication
- Password Policy
- Networking



* Misconfiguration categories according to CIS Foundation Benchmark

DISTRIBUTION OF EXCESSIVE PERMISSIONS

- Roles
- Users
- Inactive Users
- Groups



Additional Resources

Stay connected using these resources:

- **ERT Alerts**—New cybersecurity attacks and DDoS threats are lurking in the shadows every day. Read the latest information and stay head of vulnerabilities with updated DDoS reports and cybersecurity threat reports from Radware's Emergency Response Team (ERT).
- **DDoS Warriors**—An in-depth resource that provides comprehensive analysis of denial-of-service (DoS) and distributed denial-of-service (DDoS) attack tools, trends and threats.
- **Radware Blog**—Blogs with Radware industry experts who understand, advise on, and address application delivery and security for enterprises and carriers alike. Also, collaborate with your peers to learn how others deploy and manage Radware solutions.
- **Radware Community**—A place to connect with experts and join the conversation about Radware technologies.
- **Radware Mobile app**—Stay up to date with Radware on the go. Check out our latest research and insights, blog articles, press releases, and new Live Threat Map. The app also features quick access to technical support, our sales teams, and the customer and partner portals.

About Radware Cloud Services

- **Cloud WAF Service**—The industry's best application protection against OWASP Top-10 vulnerabilities and more, using a positive security model with policies that adapt to changing user behavior patterns, so customers are always protected against evolving threats.
- **Cloud DDoS Protection Service**—Radware's Cloud DDoS Protection Service protects against today's largest and most sophisticated DDoS attacks, with advanced protection against emerging attack vectors such as burst DDoS attacks, SSL DDoS floods, and more. Radware's service is based on a globally distributed network with dedicated, multi-terabit DDoS mitigation capacity.
- **Cloud Bot Manager Service**—Protects websites, APIs, and mobile applications against malicious bot traffic, using behavioral modeling for granular intent analysis, collective bot intelligence, and device fingerprinting. Radware Bot Manager protects against all forms of account takeover, denial of inventory, DDoS, card fraud, web scraping, and other OWASP Top 21 automated threats.
- **Cloud Workload Protection Service**—Protects workloads hosted on public cloud environments such as AWS and Azure against accidental exposure, permission misuse, and data theft. Radware provides extensive visibility into cloud-hosted assets, with granular compliance and intelligent hardening mechanisms, to help customers fortify their cloud security posture.