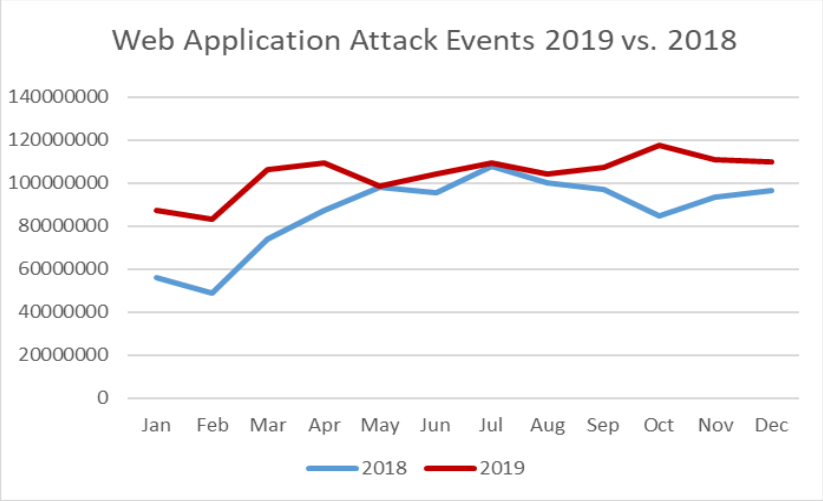
BaishanCloud Global Internet Security Report 2019

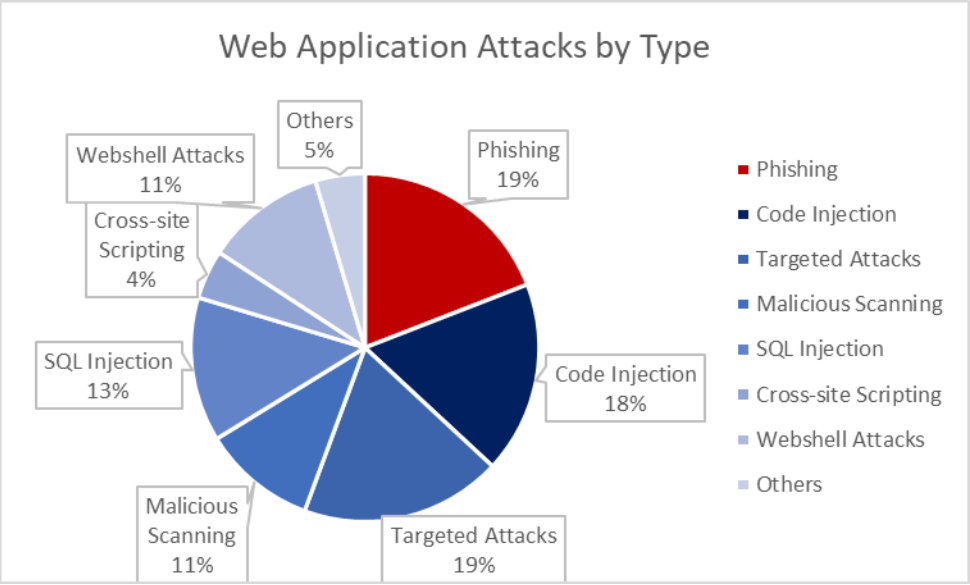
The world is contending with an increasing amount of cyber threats today: Tb-level DDoS attacks have become a new normal; web application threats are on the rise; crawler attacks are steadily increasing. The ever-more sophisticated cyberattacks have placed the data and assets of corporations, governments and individuals at constant risk. This research report, produced by BaishanCloud in partnership with Beijing Digital World Consulting*, aims to shed some light on the global internet security landscape by investigating three key types of cyberattacks (web application, DDoS, business-scenario-based attacks), and inform coping strategies for internet security professionals.

Trends of Web Application Attacks

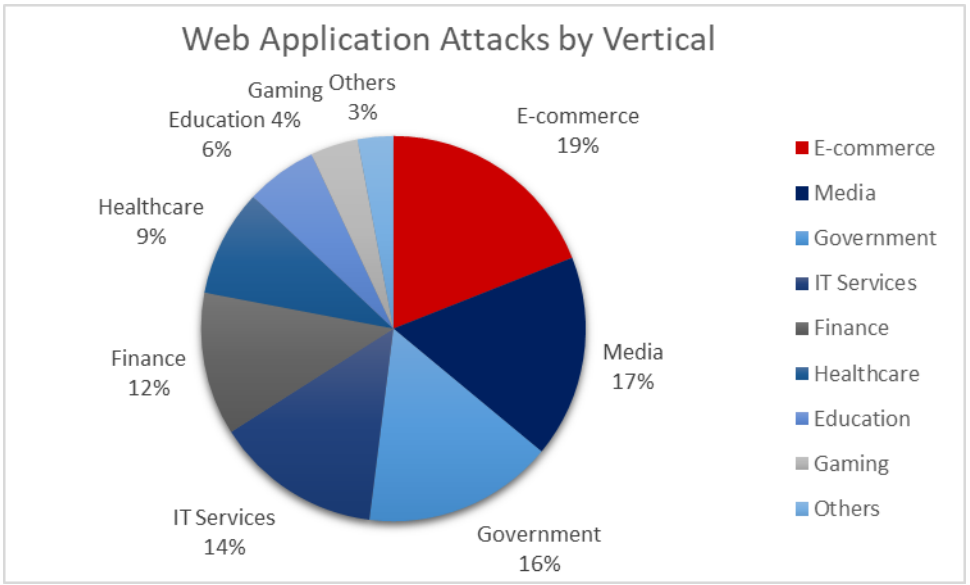
In 2019, Baishan Cloud Shield recorded a trend of the continued growth of web application attacks. A total of 1.26 billion web application attack events was detected, peaking at 1.18 billion events in October in the wake of the PhPStudy backdoor incident, a 20% increase from that of the same period in the previous year.



20% of all web application attacks are phishing, indicating that attackers tend to target the confidential documents unintentionally made publicly accessible during the development process. The attackers capture these files through scanning, and then obtain access to the database and configuration files of websites or applications. After it was revealed that the development architectures for web apps like ThinkPHP and WebLogic have critical vulnerabilities, the number of attacks targeting specific web apps has increased dramatically, accounting for 19% of all web application attacks in 2019.

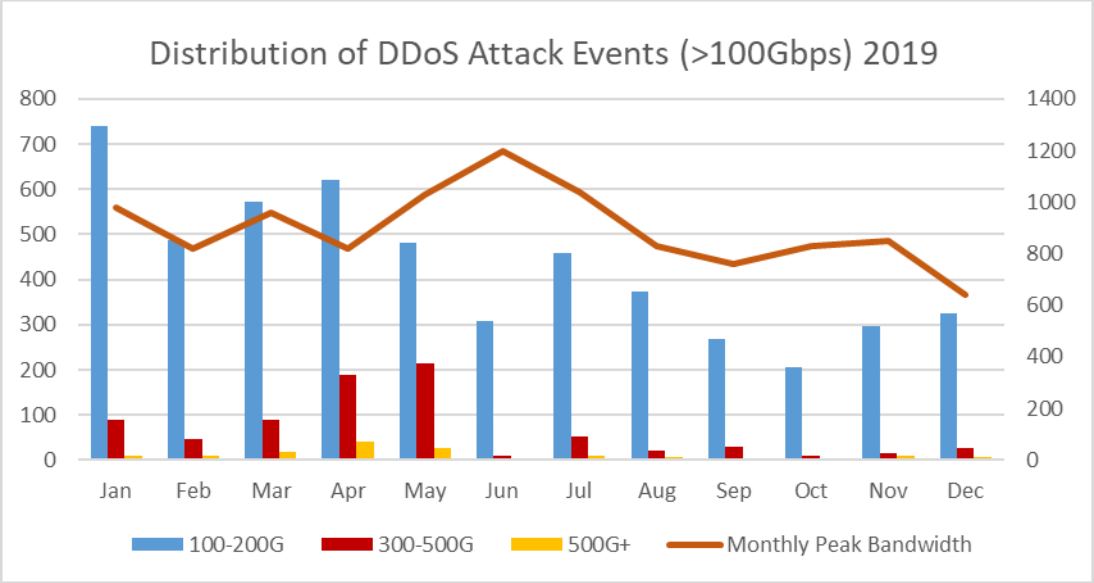


Comparing among different industry verticals, e-commerce is the most attacked industry (19% of total) on the web application layer due to the amount of personal information and transaction data involved. Similarly, the media industry is a major target for attackers seeking to "steal" visiting traffic because it has a huge internet user base and hosts a large amount of sensitive information. Media received 17% of all web application attacks in 2019.

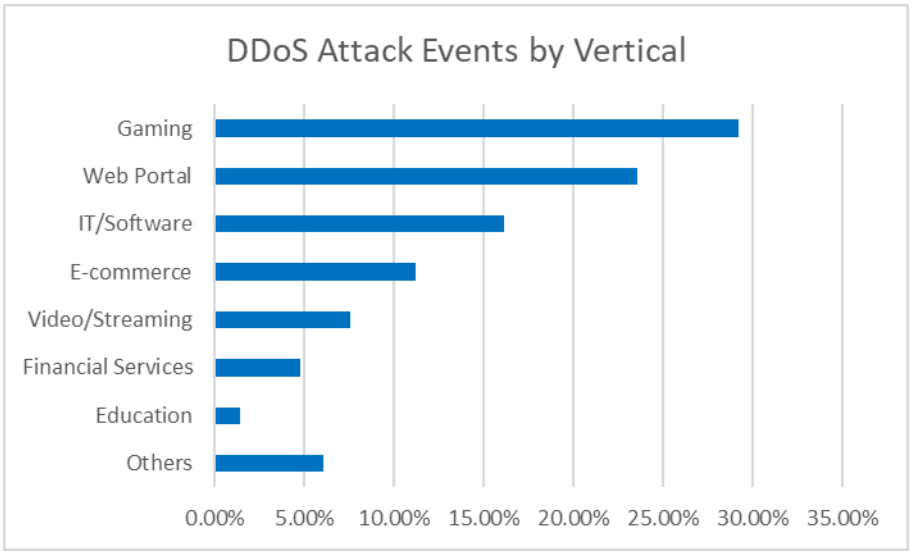


Trends of DDoS Attacks

With the development of IoT and its security vulnerabilities, an increasing number of devices have been taken advantages of by hacker attacks (so-called Zombie devices). More than300 Gbps DDoS attacks, account for 15% of all DDoS attacks throughout 2019; the average monthly DDoS peak bandwidth gets close to 1Tbps, signifying the arrival of the "Tb-attack era."

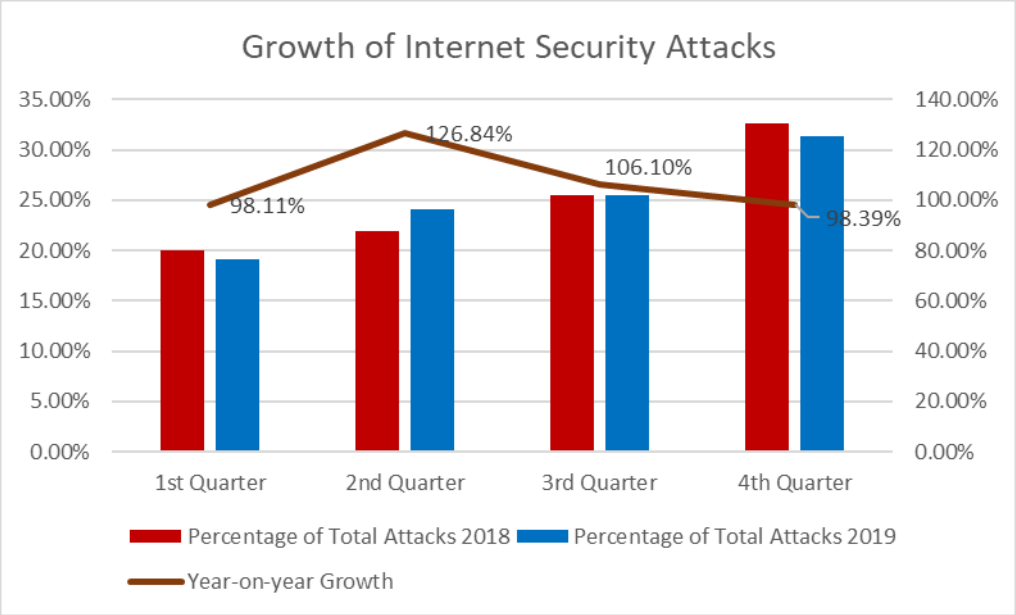


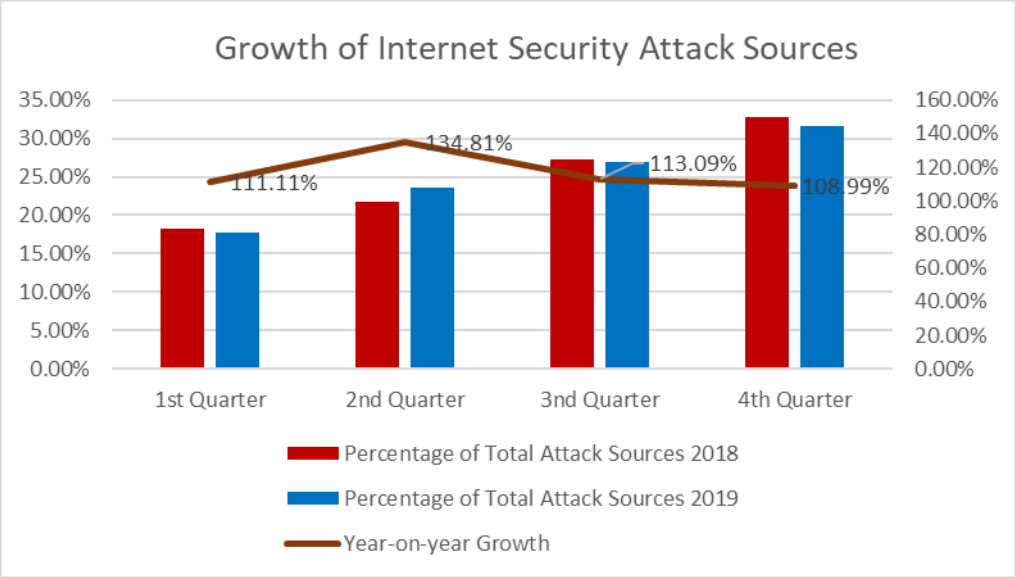
Comparing among different industryverticals, gaming is the most DDoS-attacked industry, receiving 29% of all DDoS attacks in 2019. Web portals and IT/Software receive 23% and 16% respectively of all DDoS attacks. As an increasing amount of internet traffic is moving from desktop to mobile, mobile applications are becoming more vunelrable to DDoS attacks compared to webs and APIs.



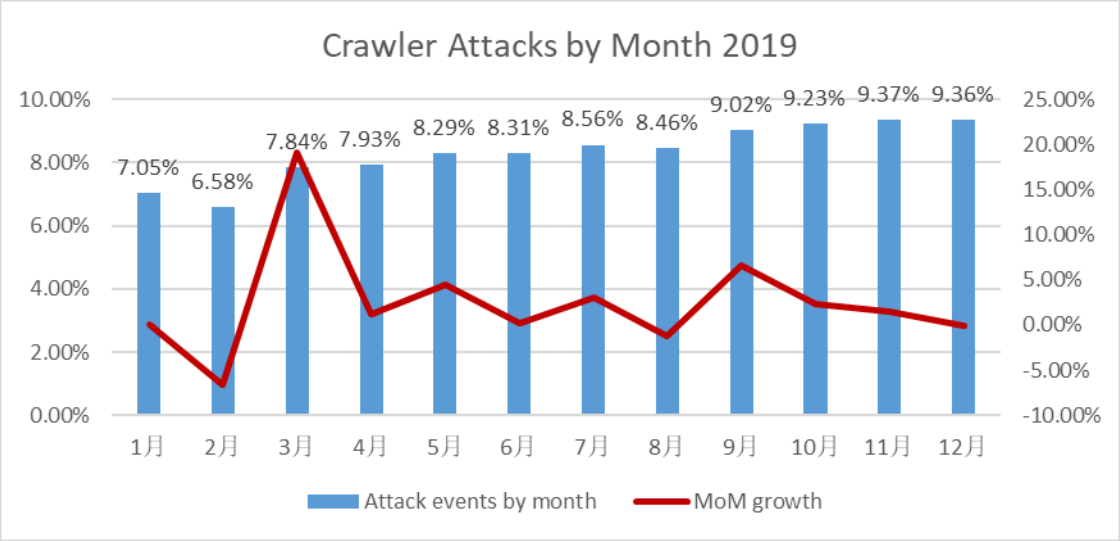
Trends of Business-scenario-based Attacks

In 2019, Cloud Shield detected a total of 956.65 billion Internet security attacks, a 116.11% increase on a year-on-year basis. There were 2.45 billion attacking sources, an increase of 106.53% on a year-on-year basis. The overall number of attacks and attack sources have maintained rapid growth throughout the year.

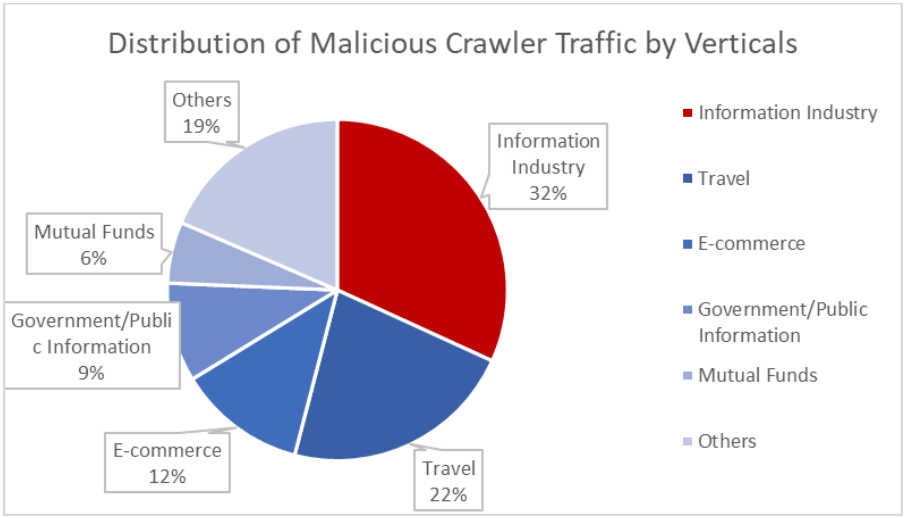




Crawler attacks, a main cause of data and digital assets leakage, are steadily increasing.



Comparing crawler attacks by verticals, Information industry, travel, e-commerce, government/public institutions and mutual funds are the most attacked industries. Because the information industry hosts an enormous amount of content that directly impacts the retention and conversion of internet users and the industry highly values the data's availability online, it becomes a major target for crawlers, accounting for 32% of all crawler attacks in 2019.



Even though companies and organizations have taken a variety of security protection measures to safeguard their digital assets, Cloud Shield's research has revealed some persistent challenges:

- Crawler is a main cause of digital asset leakage but have been overlooked by traditional security technologies.
- Single-layersecurity solution does not meet the security needs under an ever-evolving threat landscape; there is a need to build multi-layered defense approaches based on deep insights of the traffic and data of digital assets.
- Security management tends to be rules-driven.

- Maintenance cost of security system is high.
- Security approach is designed to only mitigate known-threats.
- Security solutions are not tailored to meet the unique needs of companies and organizations.

Baishan Cloud Shield tackles these challenges by providing a new generation of security products and services. Building on the concepts of "Accelerated Defense-in-Depth" and "Zero-Trust Security", Cloud Shield integrates global intelligent edge security platforms and provides a one-stop solution to mitigate web application, DDoS and direct-to-origin attacks to meet compliance requirements and improve user experience. For more about Baishan Cloud Shield, visit www.baishancloud.com/cloud-security.To receive more content about cloud security, please subscribe to BaishanCloud newsletter at www.baishancloud.com.

*__Data Sources:__ Baishan Cloud Shield global security platform and researches conducted by BaishanCloud in partnership with Beijing Digital World Consulting