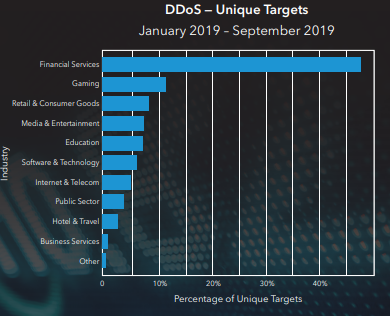
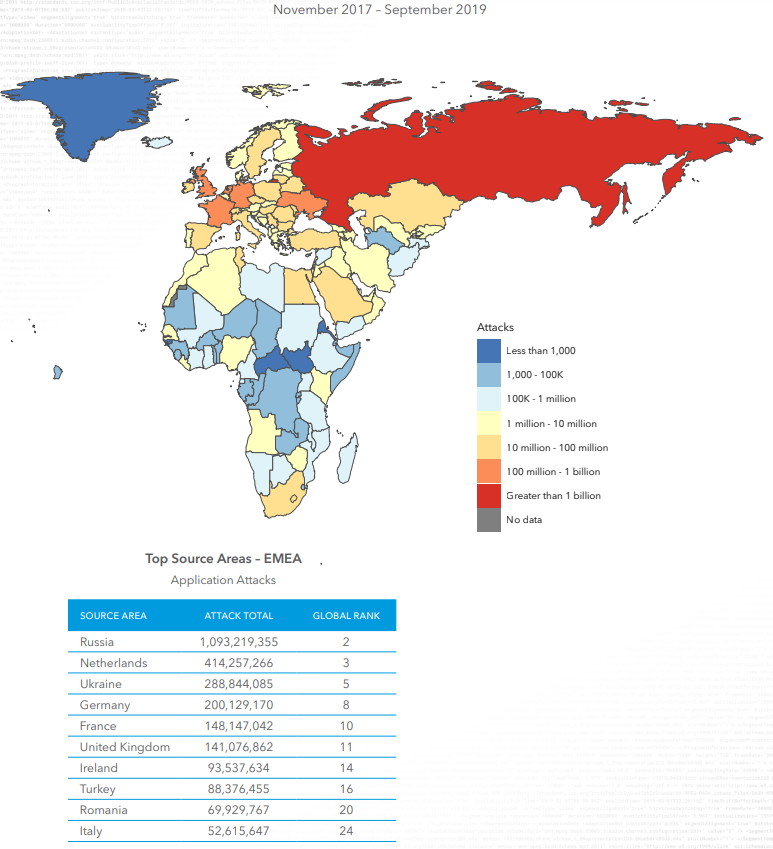
# Cybersecurity Threat Landscape (Part 2 - Akamai)

In this part, you should primarily use the *Akamai\_Security\_Year\_in\_Review\_2019* and *Akamai State of the Internet/ Security* plus independent research to answer the below questions.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. DDOS attack events from January 2019 to September 2019 largely targeted which industry?   
     
   Akamai observed 55 billion credential stuffing attacks over 17 months, and 12 billion of them were aimed directly at the gaming industry
2. Almost 50% of unique targets for DDoS attacks from January 2019- September 2019 largely targeted which industry?  
     
   Half of all unique organizations impersonated by phishing domains were in the financial services sector, according to Akamai data.  
     
    
3. Which companies are the top phishing targets, according to Akamai?   
     
   Microsoft, PayPal, DHL, Dropbox, DocuSign, and LinkedIn are all top phishing targets, according to Akamai’s monitoring
4. What is credential stuffing?   
     
   [Credential stuffing](https://en.wikipedia.org/wiki/Credential_stuffing)

Credential stuffing is a type of cyberattack where stolen account credentials typically consisting of lists of usernames and/or email addresses and the corresponding passwords are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.

1. Which country is the number one source of credential abuse attacks? Which country is number 2?  
    **Overall, the United States is still the top source for credential stuffing, followed by Russia. But when looking at gaming data alone, Russia is the number one source.**
2. Which country is the number one source of web application attacks? Which country is number 2?  
     
   
3. In Akamai’s State of the Internet report, it refers to a possible DDoS team that the company thought was affecting a customer in Asia (starts on page 11).

* Describe what was happening.  
    
  DENIAL OF SERVICE VIA DISTRIBUTED BUGGY CODE:   
  By the time SIRT had finished their work, and the SOCC had things under control, everyone involved realized the incident wasn’t an attack at all. Earlier analysis, backed by additional SIRT research, concluded the high volume of traffic hammering this customer’s URL was the result of a warranty tool gone haywire. Once the SOCC started filtering traffic, the warranty tool kept visiting the URL. However, the subsequent visits didn’t alter anything in the headers (such as the UserAgent) that could’ve assisted in bypassing mitigations, proving that this incident wasn’t a malicious attack.
* What did the team believe the source of the attack was?   
    
  When another department flagged this traffic as something to investigate, the initial report and associated data showed all the hallmarks of a major DDoS attack.
* What did the team actually discover?   
    
  This conclusion was later confirmed by the customer, as well as the vendor responsible for the tool. A fix was pushed within hours to all of the affected systems.

1. What is an example of a performance issue with bot traffic?   
     
   MORE BOTS, MORE PROBLEMS Distributed computing has made life a little easier for businesses and consumers, but these advances have also opened up new attack vectors. One of the most common threats against networks and applications is bots. Akamai’s research reveals that not only are these malicious bots constantly evolving, the people developing them are actively looking for evasion techniques, going so far as to hire developers with unique brand- and vendor-specific expertise.  
     
   This ripple effect spreads across multiple risks associated with bot traffic, including performance issues (e.g., slow websites and frustrated customers) and increases in IT expenses. Additionally, there are brand-related risks such as bots that scrape your website for inventory assets, pricing data, or content. If that’s not enough, you’ve also got to deal with the bots responsible for DDoS attacks, ad fraud, SEO spam, and credential stuffing, to name a few.
2. Known-good bots are bots that perform useful or helpful tasks, and not do anything malicious to sites or servers. What are the main categories of known-good bots.   
     
   We refer to the following main categories when considering known-good bots:  
     
   • SEARCH ENGINE CRAWLERS – web search engines operate for a wide variety of purposes, going from global search engines (e.g., Google, Bing) to more targeted ones such as job search engines, media and entertainment, commerce-focused search engines, or academic and research (publications, citation search, semantic analysis).   
   • WEB ARCHIVES – scanning the web periodically and recording its content to searchable indexed databases.   
   • SEARCH ENGINE OPTIMIZATION, AUDIENCE ANALYTICS, AND MARKETING SERVICE – scraping websites and social media for content that might provide customers with market insights such as positioning, mentions, and other references.   
   • SITE MONITORING SERVICES – automated tools that monitor a site’s health, availability, and performance under load.   
   • CONTENT AGGREGATORS – bots operated in this category would scan multiple sources on the web such as news, trends, product updates, price changes, stock quotes, etc.
3. What are two evasion techniques that malicious bots use?   
     
   To avoid detection, the bots visiting your website will employ various tricks and tactics. The most basic evasion technique is altering the User Agent, or other HTTP header values, allowing the bot to impersonate widely used browsers, mobile applications, or even known-good bots. Bots will also change the IP addresses used in order to mask their origin, or use multiple IP addresses. The IP address change-out is also used to bypass rate limitations, as the bot will use a “low and slow” method where multiple IP addresses send a low number of requests each hour.  
     
     
     
     
     
   Other rate limitation evasion methods include using mobile and API endpoints, as well as morphing IP addresses via proxies, VPNs, and Tor. Some bots will tamper with browser properties, spoofing known fingerprint characteristics that are often whitelisted. Bots may also do cookie tampering in the hopes of evading detection, such as dropping cookies, or harvesting good cookies and playing them back.