Executive Summary:

[state of the internet] / security

Volume 6, Issue 2

Gaming — You Can’t Solo Security
If you’re a gamer, then this issue of the State of the Internet / Security report is for you! Even if you’re not a gamer, then you should look at this edition as something to share with your friends, family, acquaintances, and coworkers as we tackle the hows and whys of gaming security.

We get deep into the gaming world, not only because it’s an increasingly popular target for nefarious actors, but because many of us on the editorial team are gamers, too.

In the spring of 2020, Akamai and DreamHack worked together to send a survey to gamers to gather their insights on security, as it relates to their gaming experience. The survey results, coupled with data from the Akamai platform, shaped this report.

More than 80% of the DreamHack/Akamai survey respondents said they play games every day or several times a day. So, keeping this in mind, this report focuses not only on the threats gaming companies face, but also how those threats impact and influence gamers.

Between July 2018 and June 2020, Akamai observed more than 10 billion web application attacks across all customers, including 152 million attacks in the gaming industry. Moreover, between July 2019 and June 2020, Akamai observed 3,072 distinct DDoS attacks in the gaming industry, making it the largest DDoS target across our customer base.
Gaming was a $159 billion industry in 2019, and it will reach $200 billion by 2023, according to Newzoo. The market analytics house also noted the COVID-19 pandemic, and subsequent lockdowns, led to increases in engagement and revenue across the gaming industry.

During the COVID-19 lockdowns, everyone (especially gamers) looked for alternative ways to socialize, since PC cafes, gaming houses, bars/pubs, and other social gathering points were all closed during the early months of 2020. The availability of cross-platform gameplay, as well as gaming-friendly social platforms (e.g., Discord), enabled a common element of interaction.

In April, Steam reported a record-setting day, shortly after the previous record was set in March. On April 4, 2020, 24 million players were online, with 8 million of them in-game at the time.
Looking at the attack landscape, SQL Injection (SQLi) is still the number one attack vector, with 76% of attacks across all customers taking this format (58% in gaming). SQLi is followed by Local File Inclusion (LFI) attacks, with 16% of attacks across all customers and 31% in the gaming industry alone.

Mobile games and web-based games are big SQLi and LFI targets, because criminals who successfully pull off attacks against these platforms will gain access to usernames and passwords, account information, and anything game-related that is stored on the server.

Criminals target gamers directly via two different paths: phishing and credential stuffing.

One-fifth of the frequent players in the DreamHack/Akamai survey said they’re worried or very worried about having their gaming accounts compromised (hacked or hijacked). Yet 55% of the same players said they’ve had one of their accounts compromised in the past.
From July 2018 until June 2020, Akamai observed 100,195,620,436 credential stuffing attacks across all industries. Within the gaming sector alone, there were 9,831,295,227 attacks recorded.

As the COVID-19 lockdowns started in Q1 2020, there was a noticeable spike in credential stuffing activity. This was due to a number of factors, including a push by criminals to test the credentials exposed during older data breaches to see if there were new accounts to compromise.

More than half of survey participants who have been hacked in the past say the issue of security is the shared responsibility of the gamer and the game developer/game company.

The fact remains: Gamers are highly targeted because they have several qualities that criminals look for. They’re engaged and active in social communities. For the most part, they have disposable income, and they tend to spend it on their gaming accounts and gaming experiences.
Web attacks are constant. Credential stuffing attacks can turn data breaches from the days of old (meaning last week) into new incidents that impact thousands (sometimes millions) of people and organizations of all sizes. DDoS attacks disrupt the world of instant communication and connection.

These are problems that gamers, consumers, and business leaders face on a daily basis. This year, these issues have only gotten worse, and the stress caused by them was compounded by an invisible deadly threat known as COVID-19.

If you’re interested in helping, especially if you’re a gamer, share this report with those outside of the security and technology space, and help them protect themselves. A little awareness and preparedness go a long way toward thwarting an attack.