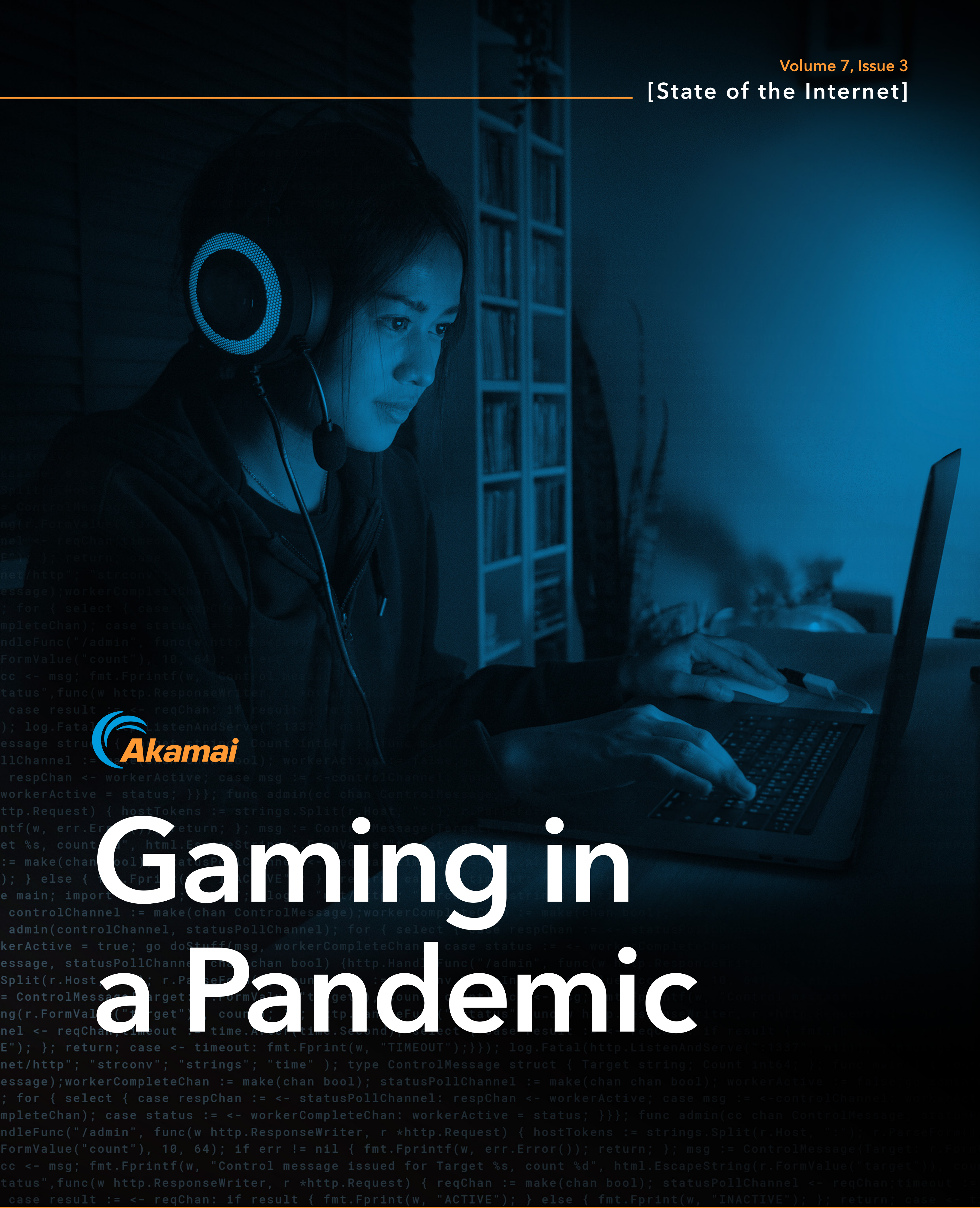
Volume 7, Issue 3
[State of the Internet]



Akamai

Gaming in a Pandemic

SOTI: RESEARCH

Introduction

Welcome to the second edition of SOTI Research. In this edition, we look at the attacks and trends in the gaming industry during 2020. It was a volatile year, and we're not just speaking about the pandemic. Web attacks targeting the gaming industry were up 340% year over year between 2019 and 2020, and credential stuffing attacks were up 224%. Strangely enough, DDoS attacks against the gaming industry fell by nearly 20% during the same period.

Gamers are a focused, highly engaged, and motivated demographic. Criminals, on the other hand, are cold and ruthless — and gamers, as well as gaming companies, are some of their favorite targets.

Note

SOTI Research is a condensed, shorter version of our traditional State of the Internet / Security reports, offering focused data points and contextual awareness across a number of threat landscapes.

Web Application Attacks

Gaming companies are constantly working to secure their infrastructure against all types of attacks. Online gaming companies, just like other enterprises, pay close attention to web-based attacks and trends. In 2020, Akamai tracked 246,064,297 web application attacks in the gaming industry, representing about 4% of the 6.3 billion attacks we tracked globally.

This figure is significant, because this represents a 340% increase in attacks against gaming companies since 2019. When we track web application attacks in the gaming industry from 2018 until 2020, we see a 415% increase. In fact, the year-over-year change globally for web application attacks was only 2%, meaning that gaming saw more growth in attack traffic than any other industry in 2020.

Some of this statistical growth is due to additional visibility on Akamai's part, as new customers were added to the global network. However, the main driver behind the increase in attacks isn't new customers; it's persistent criminals. Criminals, on a daily (sometimes hourly) basis, test defenses and probe externally faced servers looking for even the slightest vulnerability to gain a foothold on the server or expose information.

2020 was wild — let's not ignore that. While we were all at home, adjusting to the "new normal," trying to balance work, school, and day-to-day existence during a pandemic, many people turned to gaming as an outlet and means of personal connection.

Criminals did this too. Make no mistake: While their intentions are malicious, they are still people. They talked to each other, they played games, and in some cases this social bond meant they coordinated their efforts, to varying degrees.

We know from our own research that there were group chats on Discord (a popular social platform) dedicated to SQL Injection (SQLi), Local File Inclusion (LFI), and Cross-Site Scripting (XSS) techniques, tools, and "best" practices. The popular discussions and tutorials centered on all-in-one tools and using services like Shodan and Censys to locate databases, unprotected assets, and more. The key to many of these discussions was leveraging known tools and services as a means of obfuscation during their searching and scanning efforts.

> ***Gaming saw more growth in attack traffic than any other industry in 2020.***

Looking at the data (Figure 1), SQLi is still the number one attack vector in the gaming industry at 59%, followed by LFI attacks at 24%. XSS attacks and Remote File Inclusion (RFI) attacks are a distant third, at 8% and 7%, respectively. Over the past three years, this really hasn't changed at all.

The criminals pushing SQLi and LFI attacks are mostly automating their efforts. They are looking for opportunistic situations, where a new app, API, or account function wasn't properly hardened and exposed. Mobile games and web-based games are prime targets for LFI and SQLi attacks, often because it is presumed that such platforms are not as robustly defended as their desktop and console counterparts.

LFI attacks are looking to expose sensitive details within applications or services running ASP, JSP, or PHP languages. Typically, LFI attacks lead to information disclosure, such as configuration files (that can be used to further compromise the server or accounts). In the case of the gaming industry, these attacks can expose player or account details that could be used for cheating or exploitation. SQLi attacks could yield login credentials, personal information, or anything else that is stored in an exposed database.

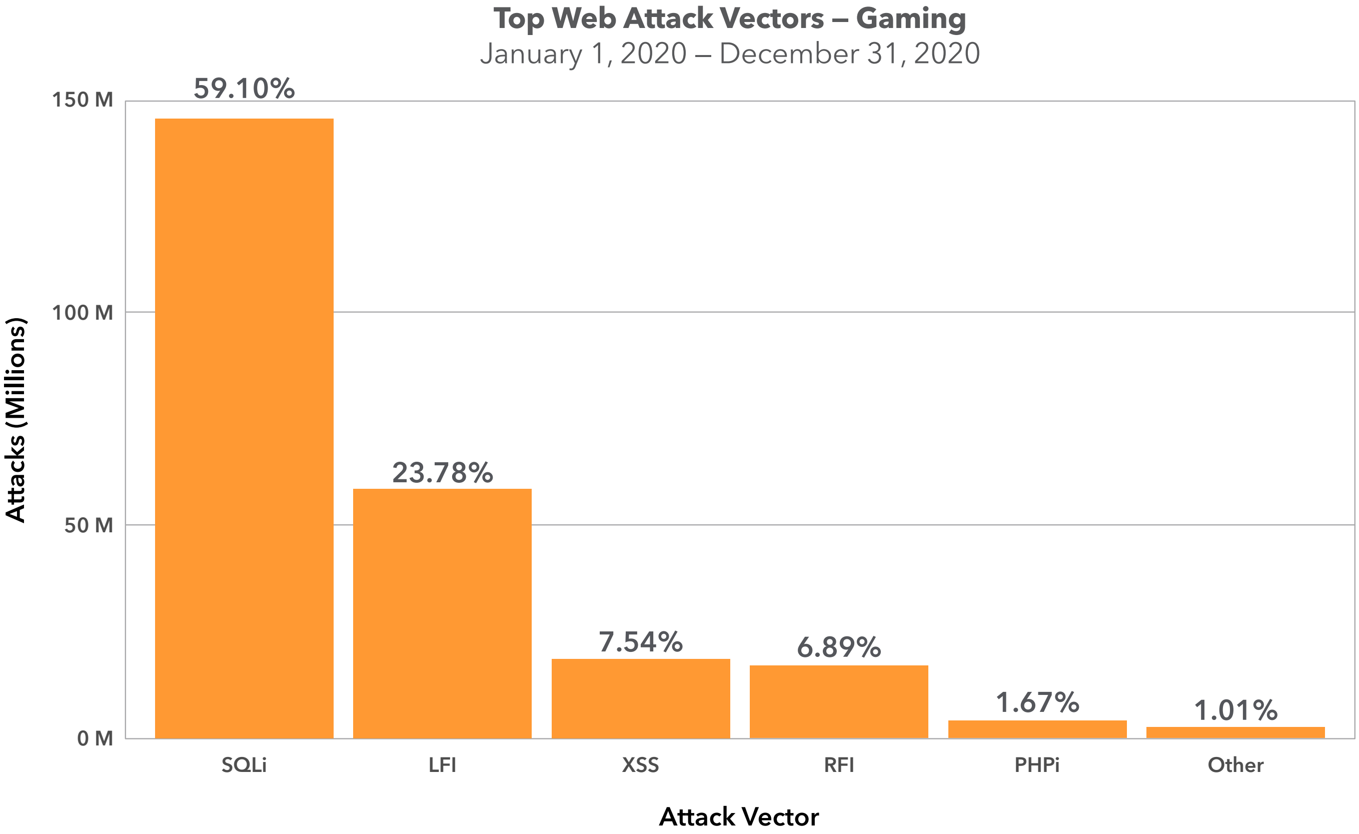


Fig. 1: SQLi and LFI remain the top two types of attack in the gaming industry, mostly due to automated tools and opportunistic attacks

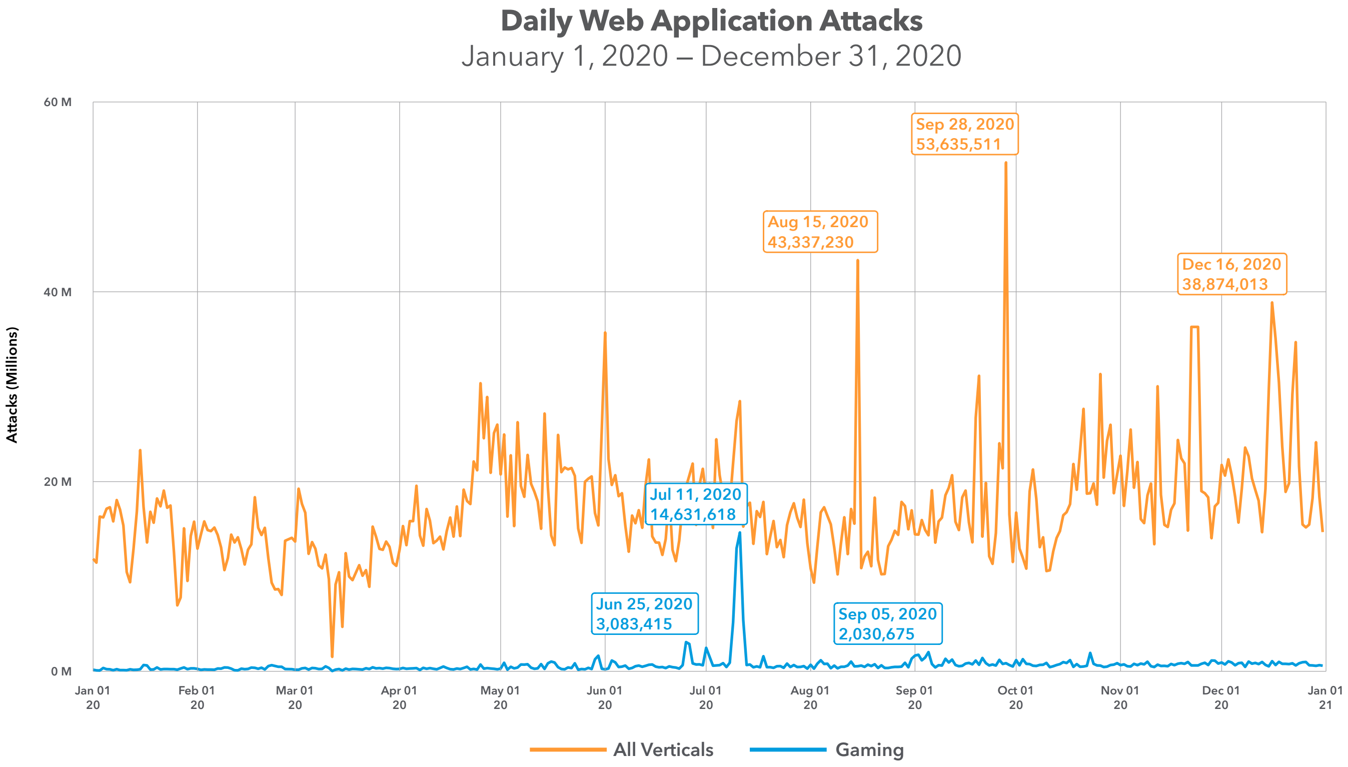
When criminals targeted the gaming industry in 2020, they focused most of their efforts on games or gaming companies located in the United States (242 million attacks), but also directed attacks toward targets in Asia (2.2 million attacks) – both massively popular areas when it comes to desktop, console, and mobile gaming.

Looking at the attack graphs for 2020, there are a few notable instances worth pointing out (Figure 2). On July 11, 2020, Akamai recorded 14.6 million attacks, which surpassed the previous month's peak of 3 million attacks in a single day. Two months later, in September, another peak of more than 2 million attacks was observed.

The fact that attacks were consistent all year long is the standout observation, however, proving that criminals were relentless as they focused on gamers and the gaming companies they support.

Looking back at the spikes in June, July, and September of 2020, there is no real direct connection to what was taking place in the criminal world and their sudden explosive focus on the gaming industry.

However, earlier in the summer, Akamai researchers observed several tutorials passed around on various criminal forums, which included a focus on automated SQLi and LFI attacks, including "dorks," which help criminals new to this type of attack understand what to look for. Many of these tutorials were pirated copies of established training, such as books and courses offered by SANS and Offensive Security, and classes taught at Udemy.



Daily Web Application Attacks

January 1, 2020 – December 31, 2020

Sep 28, 2020
53,635,511

Aug 15, 2020
43,337,230

Dec 16, 2020
38,874,013

Jul 11, 2020
14,631,618

Jun 25, 2020
3,083,415

Sep 05, 2020
2,030,675

Fig. 2: Attacks in the gaming industry were consistent all year long in 2020, with a massive spike taking place in July

Credential Stuffing

Credential stuffing was also a major problem for the gaming industry in 2020, representing about 6% of the 193 billion attacks Akamai has tracked globally.

In all, there were 10,851,228,730 credential stuffing attacks in the gaming industry in 2020, amounting to a 224% increase year over year compared to 2019. Over three years, between 2018 and 2020, credential stuffing attacks in the gaming sector grew by 24%.

Once again, some of this growth is due to additional visibility on Akamai's part, as new customers were added to our global network over the past year. But as the chart in Figure 3 shows, the attacks can be blamed on persistent criminals. Millions of attacks each day, spiking on April 11 to 76 million, followed by massive spikes in October (101 million) and December (157 million).

Second only to phishing, credential stuffing is the most common type of account takeover attack, mostly due to the multiple ways a compromised account can be leveraged by criminals. During the summer of 2020, bulk lists of usernames and passwords were going for as little as $5 per million records.

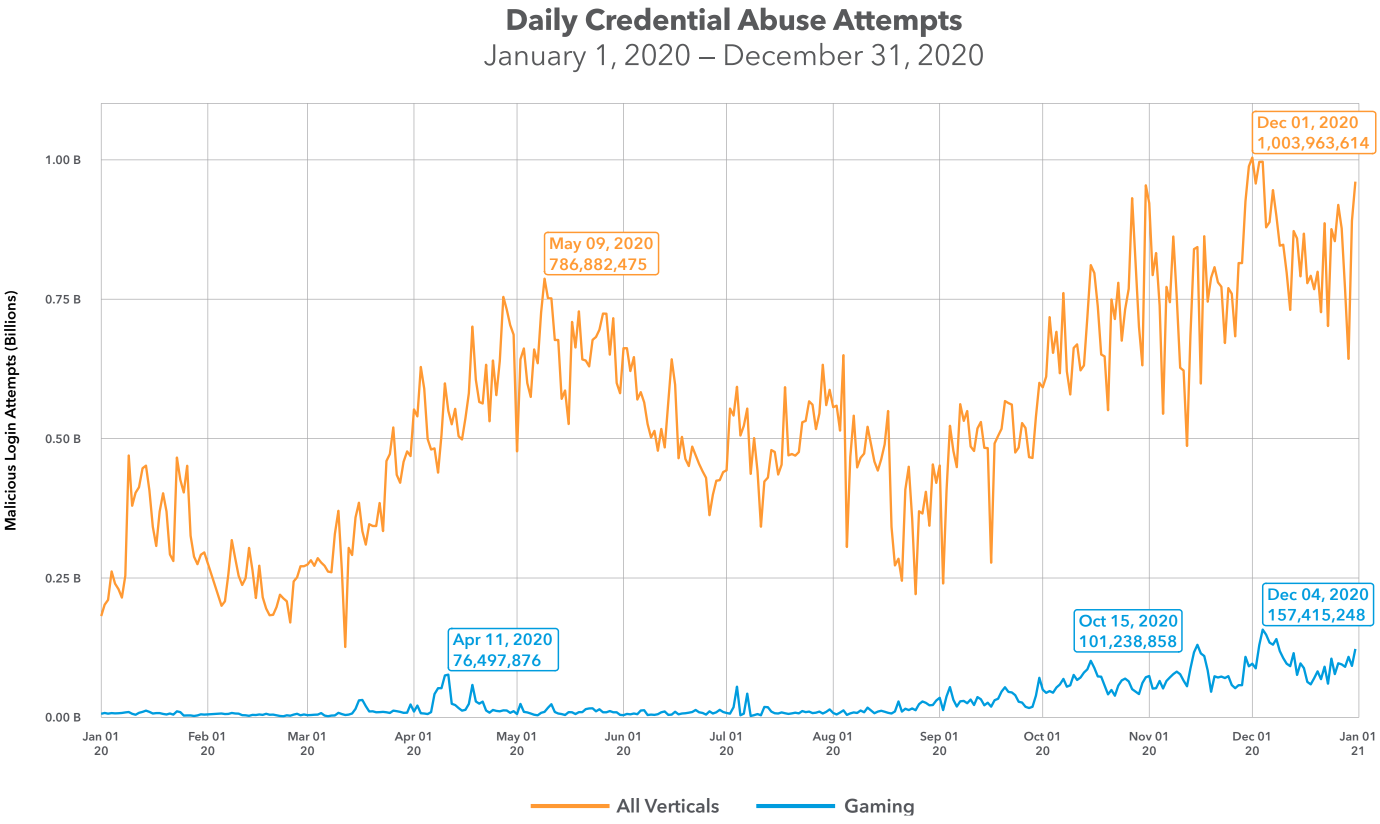


Fig. 3: Criminals launched credential stuffing attacks, millions of them each day, throughout 2020, with notable spikes in October and December

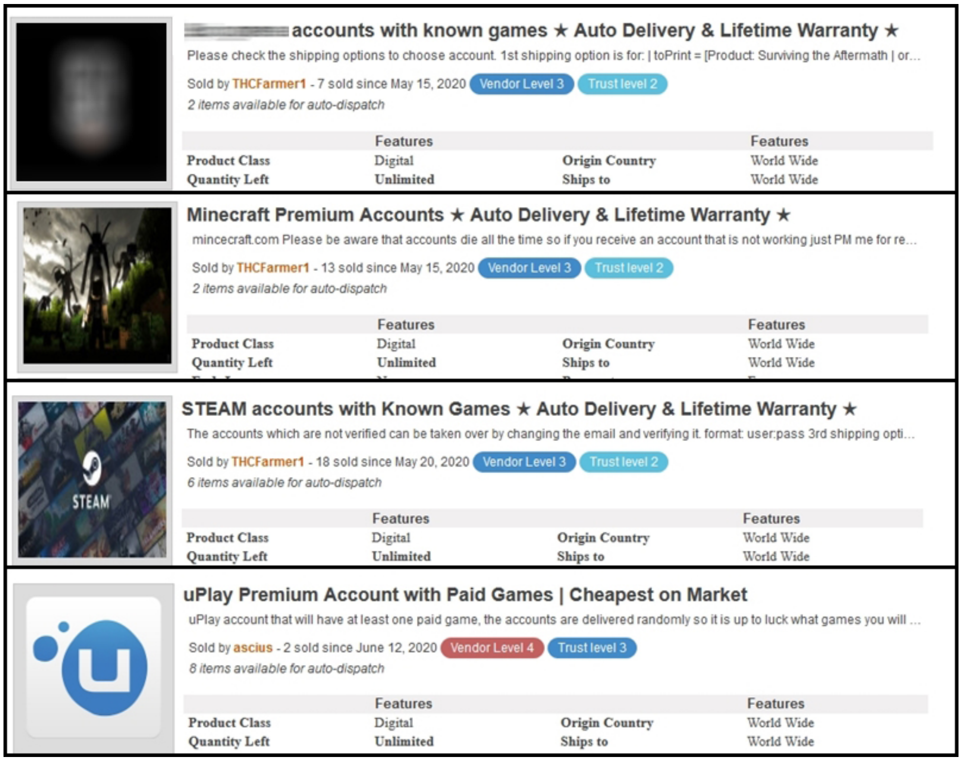
Like they do for other industries, criminals will package and sell targeted credential lists (Figure 4), including lists of known gamers, lists focusing on certain games, and lists for gaming platforms or companies.

As we mentioned in our 2020 gaming report, criminals used their downtime during the COVID-19 lockdowns to recycle old credential lists and test them against new targets. This activity started in early 2020 and continued throughout the year.

Part of the reason that credential stuffing is such a constant problem is the use of recycled or easily guessed credentials. When gamers, or the public in general, reuse credentials across platforms and services, a successful attack against one will directly lead to a successful attack against all the other places where that password exists.

Criminals check their lists often. So when a new account is compromised, they will test those same credentials across a number of other platforms and services, including streaming media, finance, and corporate assets. For example, if the gaming password is the same password used on a banking website, when a criminal compromises one account, they will compromise all of them, because that recycled password will be tested against multiple platforms and services.

This is why password managers are essential: They help prevent the recycling element.



[redacted] accounts with known games ★ Auto Delivery & Lifetime Warranty ★

Please check the shipping options to choose account. 1st shipping option is for: | toPrint = [Product: Surviving the Aftermath | or...

Sold by THCFarmer1 - 7 sold since May 15, 2020 Vendor Level 3 Trust level 2

2 items available for auto-dispatch

	Features		Features
Product Class	Digital	**Origin Country**	World Wide
Quantity Left	**Unlimited**	**Ships to**	World Wide

Minecraft Premium Accounts ★ Auto Delivery & Lifetime Warranty ★

mincecraft.com Please be aware that accounts die all the time so if you receive an account that is not working just PM me for re...

Sold by THCFarmer1 - 13 sold since May 15, 2020 Vendor Level 3 Trust level 2

2 items available for auto-dispatch

	Features		Features
Product Class	Digital	**Origin Country**	World Wide
Quantity Left	**Unlimited**	**Ships to**	World Wide

STEAM accounts with Known Games ★ Auto Delivery & Lifetime Warranty ★

The accounts which are not verified can be taken over by changing the email and verifying it. format: user:pass 3rd shipping opti...

Sold by THCFarmer1 - 18 sold since May 20, 2020 Vendor Level 3 Trust level 2

6 items available for auto-dispatch

	Features		Features
Product Class	Digital	**Origin Country**	World Wide
Quantity Left	**Unlimited**	**Ships to**	World Wide

uPlay Premium Account with Paid Games | Cheapest on Market

uPlay account that will have at least one paid game, the accounts are delivered randomly so it is up to luck what games you will ...

Sold by ascius - 2 sold since June 12, 2020 Vendor Level 4 Trust level 3

8 items available for auto-dispatch

	Features		Features
Product Class	Digital	**Origin Country**	World Wide
Quantity Left	**Unlimited**	**Ships to**	World Wide

Fig. 4: Criminals sell targeted credential lists that are used for credential stuffing against the gaming industry

Password managers, multi-factor authentication (MFA) apps like Google Authenticator, and universal 2nd factor (U2F) authentication devices like YubiKey are solid defensive elements that can be deployed to fight against credential stuffing. They don't stop all attacks, but solutions like this make them harder to pull off and, in some cases, render the attacks impotent. This is why criminals are focusing their efforts on targeting basic two-factor authentication methods like SMS-based one-time passwords, via interactive phishing pages.

In order to be successful, organizations need to implement and actively require the use of MFA and/or U2F and, at the same time, educate their users and customers on why such a step is important. This task, however, is easier said than done.

DDoS Attacks

DDoS attacks are a disruptive and serious resource drain for the organizations facing them. In the gaming industry, DDoS attacks have a ripple effect. They have the ability to knock infrastructure offline, impacting business operations and game performance. For gamers, DDoS attacks are frustrating instances that ruin gameplay.

As mentioned, DDoS attacks fell by nearly 20% in 2020, but DDoS attacks against the gaming industry accounted for 46% of the DDoS traffic observed by Akamai last year. Just because DDoS attacks have fallen over the years (down 31% year over year between 2018 and 2020) doesn't mean they can be ignored or dismissed. They're still happening, and their impact is enormous.

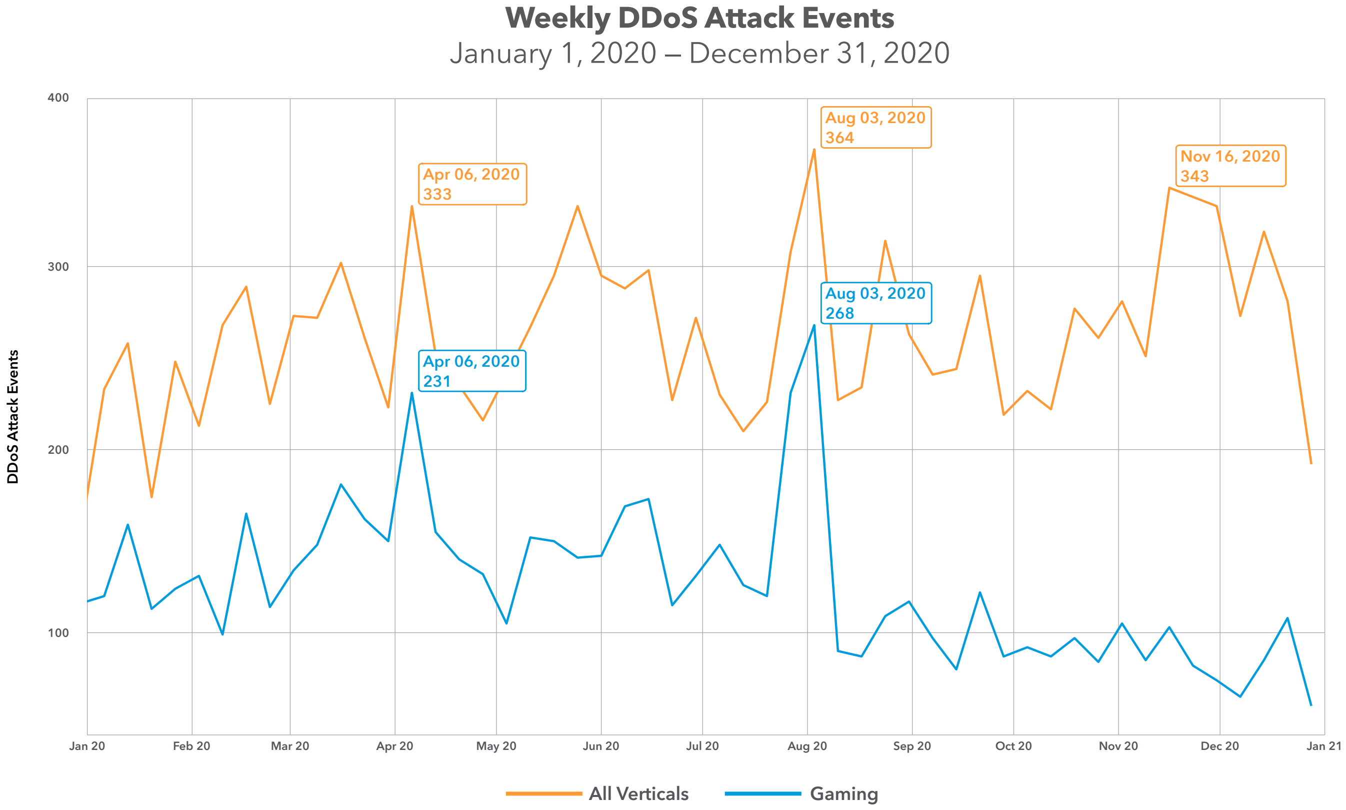


Fig. 5: DDoS attacks have fallen, but that doesn't mean they went away entirely

The DDoS attacks observed by Akamai in 2020 (Figure 5) were significant, reaching hundreds of gigabits per second. In fact, in March of 2020, one mobile gaming company experienced one of the largest DDoS attacks observed last year, peaking at about 412 Gbps, followed by another attack a few days later that hit 392 Gbps.

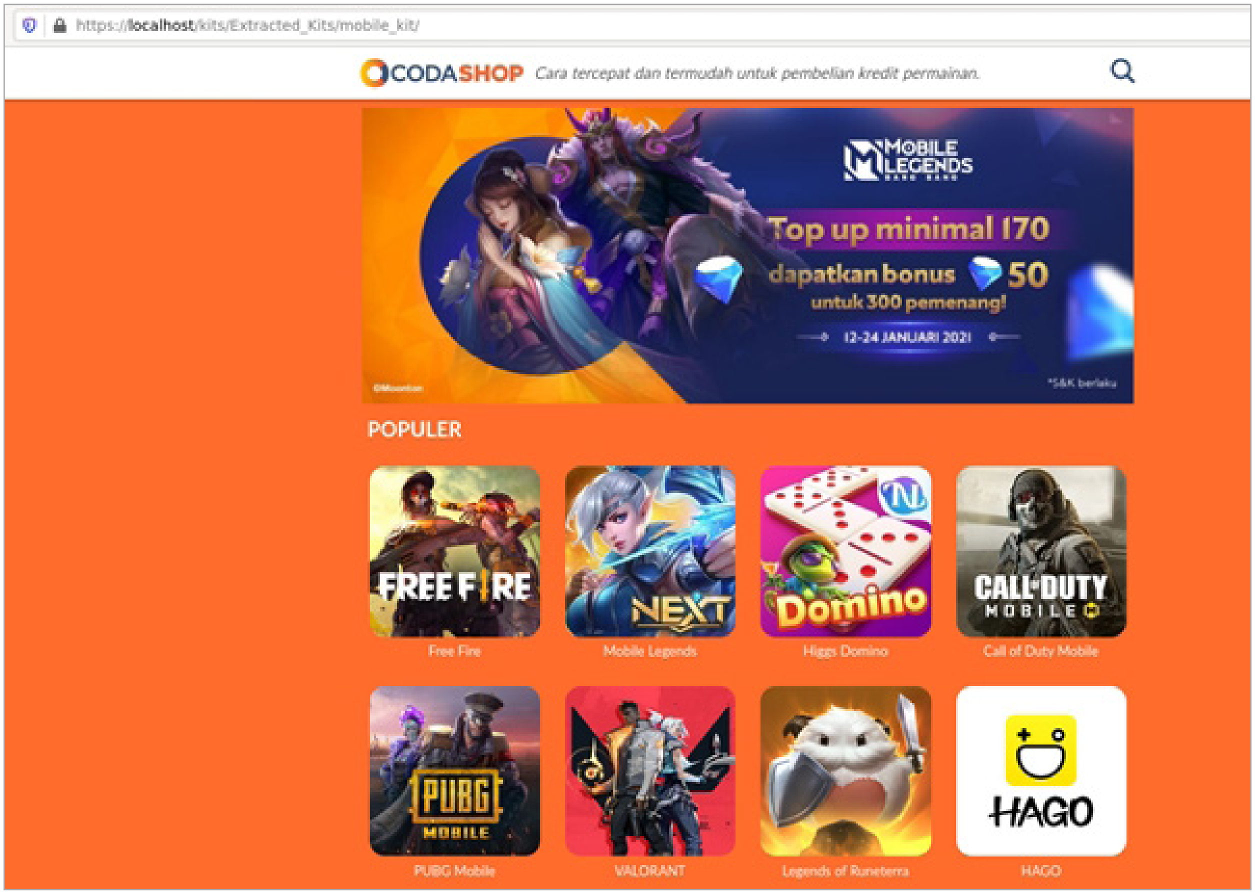
Mobile Gaming Attacks

The global gaming market will hit $175 billion in 2021, according to analytics firm Newzoo, with mobile game revenues accounting for 52% of that market share. We've highlighted phishing attacks against gamers in the past, but for this report, we're going to look at a phishing attack focusing directly on mobile gamers.

Gamers tend to spend money on something they like. While there is always going to be a segment of players who are completely against the in-app purchase model, or the free-to-play business model, the fact remains that plenty of others are completely fine with this shift in the gaming sector and happily trade their real money for virtual currency.

Criminals are well aware of in-app purchase models and seek to exploit them whenever, wherever possible. As shown in Figure 6, criminals are focusing some of their efforts on scamming mobile players who are looking to spend real money on in-game items such as skins and custom character enhancements.

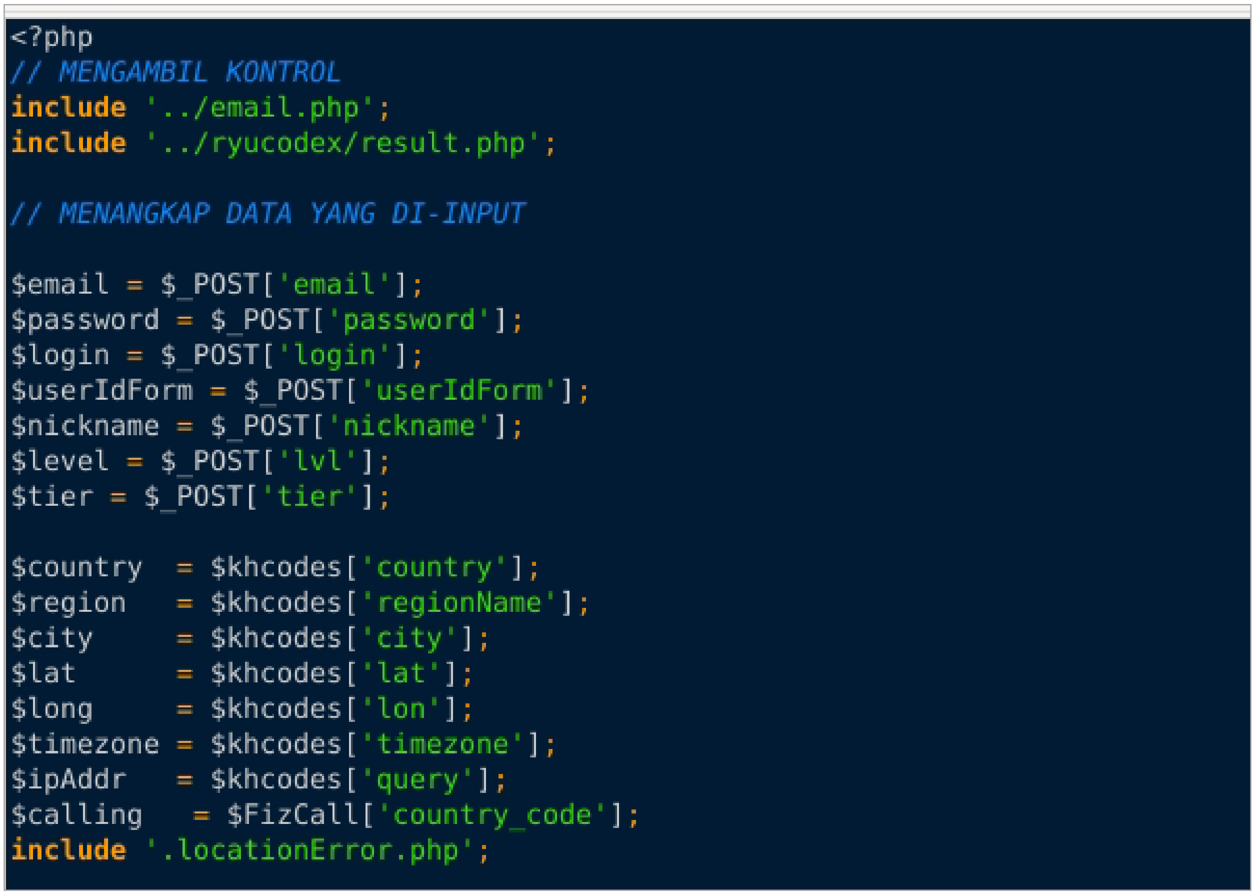
In this example, the criminals are targeting a company called Codashop. Codashop is one of the largest "top-up" portals for gamers with presences in Indonesia, Canada, Argentina, Mexico, Brazil, UAE, Turkey, Japan, South Korea, Russia, and Hong Kong SAR.



https://localhost/kits/Extracted_Kits/mobile_kit/

Cara tercepat dan termudah untuk pembelian kredit permainan.

Fig. 6: Criminals have spoofed Codashop and used it as a lure to compromise personal information and game credentials



```php
<?php
// MENGAMBIL KONTROL
include '../email.php';
include '../ryucodex/result.php';

// MENANGKAP DATA YANG DI-INPUT

$email = $_POST['email'];
$password = $_POST['password'];
$login = $_POST['login'];
$userIdForm = $_POST['userIdForm'];
$nickname = $_POST['nickname'];
$level = $_POST['lvl'];
$tier = $_POST['tier'];

$country  = $khcodes['country'];
$region   = $khcodes['regionName'];
$city     = $khcodes['city'];
$lat      = $khcodes['lat'];
$long     = $khcodes['lon'];
$timezone = $khcodes['timezone'];
$ipAddr   = $khcodes['query'];
$calling   = $FizCall['country_code'];
include '.locationError.php';
```

Fig. 7: The Codashop phishing kit targets a number of data points, which can then be collected and sold

The phishing kit used (Figure 7) will collect a victim's email address, password, game login details, username in game, geolocation data, and other passive data points such as player level and tier. All of this information can be collected and then sold on criminal markets.

Given that Codashop doesn't require log-in details, phishing attacks like this only have a moderate success rate against experienced players. However, the criminals usually deploy these websites as part of a larger campaign and direct people to them via chat messages, forum posts, email, and black hat SEO techniques.

Conclusion

While the total volume of DDoS attacks is down, the attacks themselves are still massive, disrupting communications and gameplay. These attacks are frustrating for players and impact the relationship gaming companies have with them. Credential stuffing attacks, as shown in this report, are still a major and consistent type of attack. The same can be said for web application attacks.

Criminals are relentless, and the data proves it.

The good news is that gaming companies are working hard to protect their players, as well as the sensitive information associated with their accounts. Many of the players who were part of the Akamai/DreamHack survey acknowledged their willingness to use layered defenses, including MFA and password management.

Globally, there were 193 billion credential stuffing attacks last year, and 6.2 billion web application attacks. The endgame is to get these numbers down and keep them low. The only way to do that is to beef up existing protections, secure API access, and shift away from older protections such as SMS-based one-time passwords.

If you need help with securing your gaming account, our last report had resources to help achieve this goal.

Stay safe!

> ***Gaming companies are working hard to protect their players, as well as the sensitive information associated with their accounts.***

Credits

SOTI: Research Contributors

Editorial Staff

Martin McKeay
Editorial Director

Steve Ragan
Senior Technical Writer, Editor

Amanda Goedde
Senior Technical Writer, Managing Editor

Chelsea Tuttle
Senior Data Scientist

Marketing Staff

Georgina Morales Hampe
Project Management, Creative

Shivangi Sahu
Program Management, Marketing

More State of the Internet / Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet / Security reports. akamai.com/soti

More Akamai Threat Research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/threatresearch

Access Data from This Report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained. akamai.com/sotidata

Akamai

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 06/21.