ATTACKER ECONOMICS

WHAT FINANCIAL SERVICES INSTITUTIONS NEED TO KNOW
ABOUT CYBERATTACK COSTS VS. VALUE

INTRODUCTION

As the financial services sector continues its digital transformation, organizations like yours become an increasingly attractive target for cyberattacks. Organized crime rings are targeting the applications of financial institutions with increased sophistication to gain access to valuable information, like credential pairs, to maximize their post-breach monetization opportunities.

The struggle is real. Financial services institutions are hit by cyberattacks 300 times more than companies in other industries.[1] That makes cybersecurity a top priority that requires continuous investment. According to Accenture, banks, capital market firms, and insurers spend a per-firm average of $18.5 million annually to address cybercrime, over 40% more than the average of $13 million per firm across all industries.[2]

Cyberattacks are not only on the rise, but they are becoming more relentless. Every time your organization puts a new defense in place, cybercriminals come up with a next-generation method of attack. And since the cost of entry for each new type of attack goes down over time, threats keep expanding.

Given these formidable challenges, how can your organization stay one step ahead of attackers? It starts with understanding the economics of today's most prevalent cyber threats and how you can use those economics to demotivate attackers. Armed with this insight, you can wage a more effective defense to limit attackers' return on investment and better protect valuable customer and corporate data.

With the massive digital transformation underway in financial services, CISOs must balance addressing current vulnerabilities with implementing security to protect new technologies.[3]

CALCULATING THE CYBERATTACK RATE OF RETURN

Cybercrime is a lucrative business—especially in an industry centered on managing money. But just how big is the potential payoff? As the formula below illustrates, calculating the rate of return for attacks is similar to calculating the rate of return for playing a carnival game.

$$\frac{\text{VALUE} \times \text{CHANCE OF SUCCESS}}{\text{COST}} - 100\% = \text{RATE OF RETURN}$$

The value will be different depending on the type of attack and the target, but if a cybercriminal attacks enough times, they will break even, and eventually the payoff will offset the cost. In the carnival game example, it may cost $1.00 to play, with a 10% chance of winning a stuffed animal valued at $10.00.

$$\frac{\$10 \times 10\%}{\$1} - 100\% = 0\%$$

If the value or the chance of success improves, the rate of return will be higher and, over time, the carnival goer—or the attacker—will come out ahead.

VALUE + $10

$$\frac{\$20 \times 10\%}{\$1} - 100\% = 100\%$$

Conversely, if the value or the chance of success decreases, the rate of return will be lower.

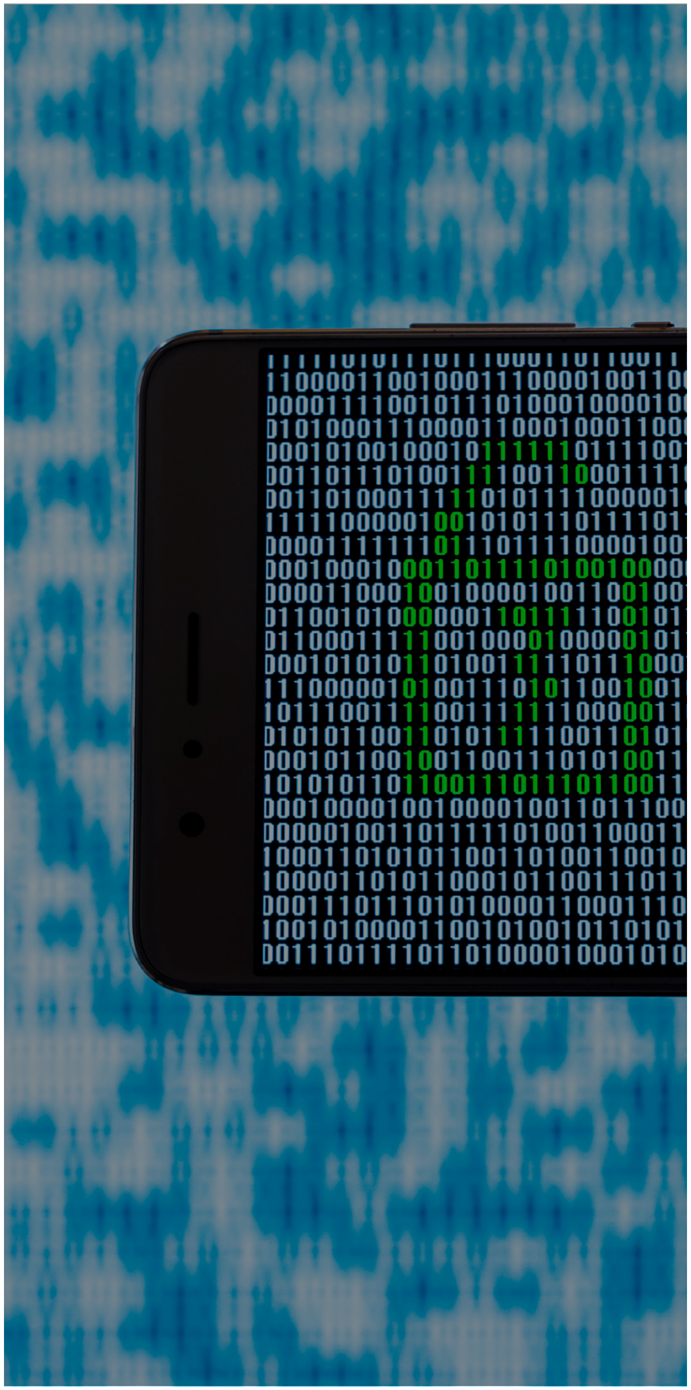
CHANCE – 5%

$$\frac{\$10 \times 5\%}{\$1} - 100\% = -50\%$$

Therefore, if the cost increases, attackers must make sure their expenses are still less than the value, or they'll start to realize a negative rate of return and eventually go broke.

CHANCE – 5%

$$\frac{\$10 \times 5\%}{\$2} - 100\% = -75\%$$

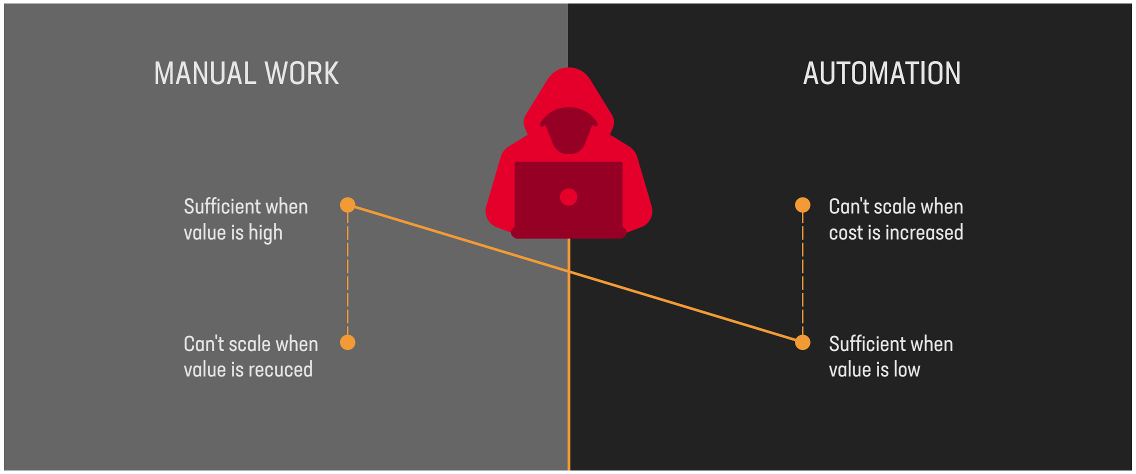


The best way to expand your defenses is by implementing security strategies and solutions that drive down the attack rate of return to zero or below.

COST VS. VALUE: A CONSTANT REEVALUATION IN FINANCIAL SERVICES

Because security budgets are high and the appetite for risk in financial services is low, attackers incur much greater costs to bypass existing defenses. At the same time, however, the value organized crime rings can extract from attacks on financial firms justifies the cost. They have incentives to invest more to realize bigger payoffs.

Attackers are constantly figuring out how to adjust cost vs. value to maximize their rate of return. This involves determining how to invest in manual work (higher cost, most effective) versus automated tools (lower cost, less effective) to extract the greatest value. It's a perpetual balancing act for attackers looking to cash in on their efforts.


MANUAL WORK
AUTOMATION
Sufficient when value is high
Can't scale when value is recuced
Can't scale when cost is increased
Sufficient when value is low

As long as there's money to be made, organized crime rings will continue to target the financial sector with new and sophisticated approaches. As a result, financial services institutions are constantly struggling to keep up with a moving target.[4] Given this reality, the best way to expand your defenses to demotivate the root cause—the fraudsters themselves—is by implementing security strategies and solutions that drive down the attack rate of return to zero or below.

TOP SECURITY THREATS FACING FINANCIAL SERVICES

Because it can provide a high rate of return, credential stuffing is one of the most common types of attacks in the financial services industry. According to the F5 Security Incident Response Team (F5 SIRT), the most prevalent security incidents at financial services institutions between 2017 and 2019 were credential stuffing and brute force attacks at 41%, with distributed denial-of-service (DDoS) attacks next at 32%. And both continue to grow.[5]

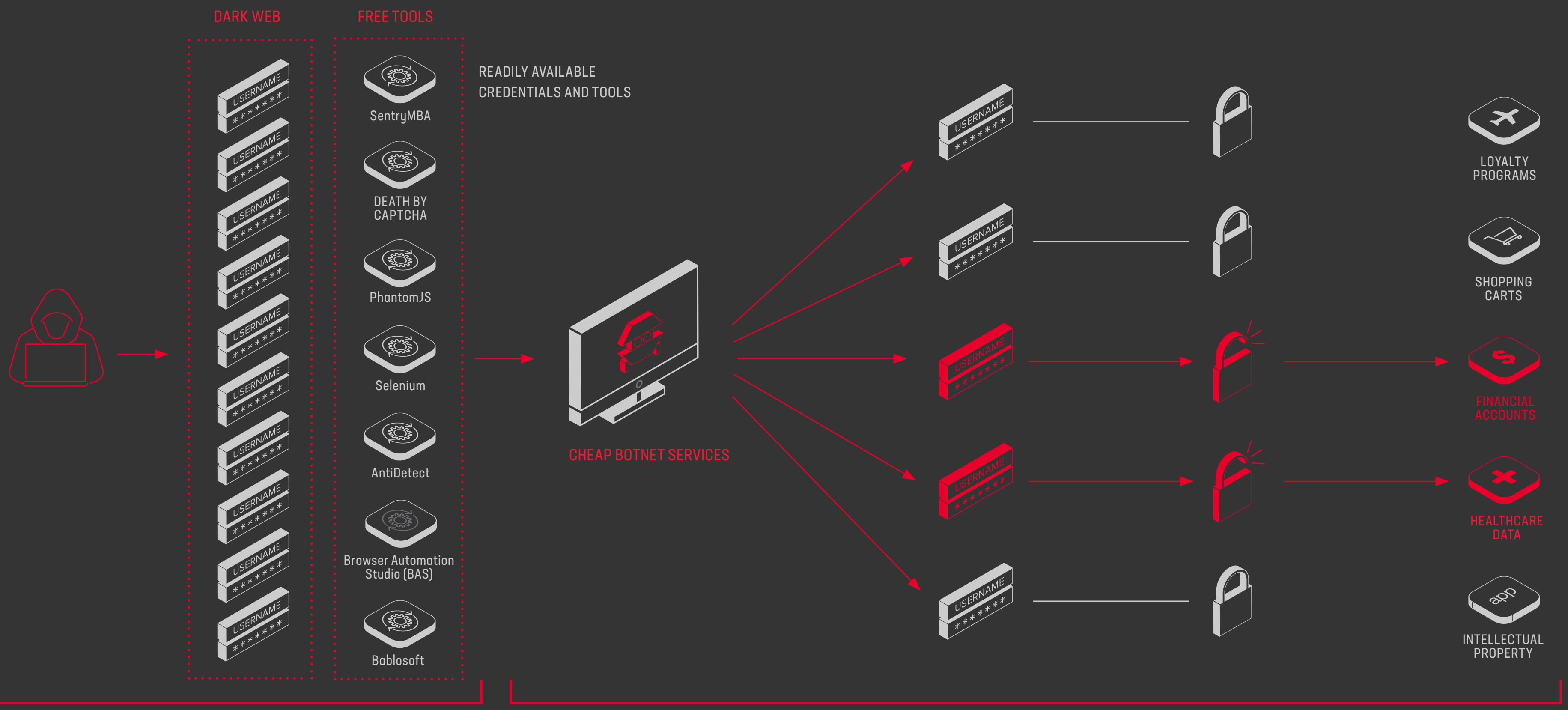
Fraudsters prefer methods like credential stuffing to other approaches when attacking financial firms with well-funded security programs. The stronger defenses you have in place may prove too much for many malicious actors, forcing them to revert to simpler, albeit less efficient, techniques such as authentication attacks.[6] Cybercriminals are also launching DDoS attacks as a distraction while they conduct credential stuffing attacks or exploit a web-based vulnerability.[7]

While many threat actors use bots and other forms of automation for credential stuffing at scale, others wage human-powered attacks when they cannot achieve the same results through less expensive automated methods.

> Credential stuffing and brute force attacks represented 41% of reported security incidents in financial services from 2017-2019.

With ready, inexpensive access to breached credentials, proxy services, and toolkits to counteract defenses, attackers are able to generate hundreds of thousands of account takeover (ATO).

CREDENTIAL STUFFING IN 3 EASY STEPS



1: Get Credentials

Massive numbers of user credentials are spilled or stolen every day. Attackers acquire credentials in myriad ways, from discovering misconfigured databases, to infecting users' devices with malware, to obtaining breached combo pairs for next to nothing from sources such as RAIDFORUMS.com. A 2019 report revealed that more than 21 million stolen user credentials belonging to Fortune 500 companies are available on the dark web.[8]

2: Automate Attacks

Attackers use bots to automatically check the list of breached credentials. They often purchase toolkits, including CAPTCHA solvers or anti-fingerprinting scripts, to defeat existing defenses.

3: Distribute Globally

Attackers route their login requests through proxy servers to avoid IP denylists and other forms of detection. Cybercriminals can purchase access to proxy services from bot herders on dark web forums for as little as $2–$8 per hour. Plus, cloud services like Microsoft Azure, Amazon Web Services, and Google Cloud Platform make it cheap and easy to spread code across hundreds or thousands of IP addresses across the globe.

Clearly, the costs involved in credential stuffing are low, but is the value high enough to deliver a significant rate of return? The simple answer is yes. Shape Security, part of F5, estimates an average of 232.2 million malicious login attempts per day with a 0.05 percent success rate, which translates to 116,106 successful account takeover attacks every day with an average of $400 stolen from an individual account.[9]

The U.S. consumer bankving industry loses up to $1.7 billion annually as a result of credential stuffing.[10]

$0: 2.3 billion credentials

$50: for tool configuration

$139: for 100,000 CAPTCHAs

$10: for 1,000 global IPs

Less than $200 for 100,000 ATO attempts

DEMYSTIFYING THE ATTACK SOFTWARE DEVELOPMENT LIFECYCLE

With all the methods of attack out there, you need a defense strategy that goes beyond blocking IP addresses, scripts, or bots in a never-ending game of whack-a-mole. One way to demotivate attackers—and more effectively combat cyber fraud—is to disrupt the attack software development lifecycle.

Because the first four phases of the attack software development cycle are all cost-incurring, the goal is to implement security countermeasures to keep attackers there as long as possible—delaying or preventing value realization in the release phase.

For example, advanced bot detection capabilities can mitigate fraudulent application requests in real time and allow requests from legitimate humans without additional friction. You could implement defenses to simply block the malicious bot requests. Even better, you could redirect them, thereby forcing fraudsters back into early development phases to retool or deploy a different attack vector. Defense strategies like these demotivate attackers by limiting their ability to achieve value, thereby diminishing their rate of return.

ATTACK DEVELOPMENT SOFTWARE LIFECYCLE

Planning

- Identify URLs to attack and data sources needed
- Determine which tools work and which don't
- Commit to a framework

Development

- Invest in and configure a framework of choice
- Perform custom developent against a site
- Build in proxy/botnet hooks

Testing

- Wage prolonged test attack to determine:

  — Does it bypass protection?

  — Does it handle edge-case responses?

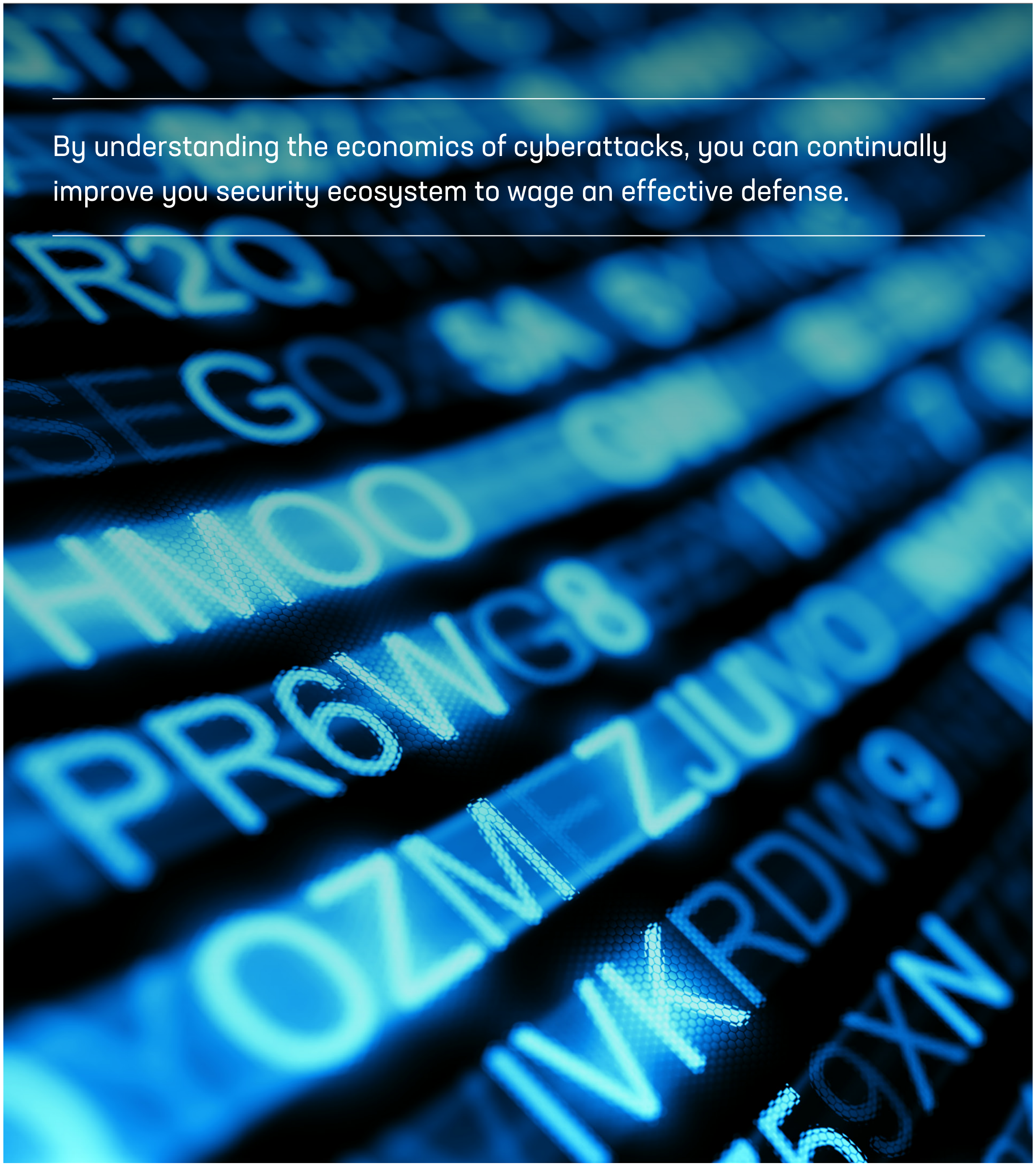
  — Does it consume input data properly?

Integration

- Check integration with services/botnets
- Ensure health checks work
- Deploy to cloud services

Release

- Initiate attack
- Realize Value



By understanding the economics of cyberattacks, you can continually improve you security ecosystem to wage an effective defense.

IN FINANCIAL SERVICES, CYBER VIGILANCE IS YOUR BEST DEFENSE

With so much at stake, your organization must continue to invest in top-notch talent and advanced technology to support a rigorous cyber risk management program that protects your expanding digital properties with minimal customer friction. As the cyber threat landscape evolves, it's imperative that you stay vigilant and implement continuous protection that hinders rapid iteration of attacks.

As long as there is money to be made, organized crime rings are going seek out and exploit vulnerabilities in your applications. By understanding the economics of cyberattacks you can continually improve your security ecosystem—including web application firewalls, bot mitigation, DDoS protection, and threat intelligence—to wage an effective defense and keep the bad guys at bay.

Learn more at f5.com.

SOURCES

[1] Naomi Eide, “Cyberattacks Hit Financial Services 300 Times More than Other Sectors,” *CIODIVE* (June 21, 2019) https://www.ciodive.com/news/cyberattacks-hit-financial-services-300-times-more-than-other-sectors/557372/

[2] Chris Thompson, “What Will Cybercrime Cost Your Financial Firm?,” Accenture (July 15, 2019) https://www.accenture.com/us-en/insights/financial-services/cost-cybercrime-study-financial-services#:~:text=2019%20Financial%20Services%20Cost%20of%20Cyber%20Crime%20Study&text=Globally%2C%20across%20all%20industries%2C%20our,and%20capital%20markets%20%2447%20billion

[3] Sam Friedman, “Taking Cyber Risk Management to the Next Level,” Deloitte (June 23, 2016) https://www2.deloitte.com/us/en/insights/topics/cyber-risk/cyber-risk-management-financial-services-industry.html

[4] Ibid.

[5] Raymond Pompon, Malcolm Heath, and Sander Vinberg, *Top Attacks Against Financial Services Organizations 2017-2019*, F5 Labs (April 27, 2020) https://www.f5.com/labs/articles/threat-intelligence/top-attacks-against-financial-services-organizations-2017-2019

[6] Ibid.

[7] Alison DeNisco Raymone, “Capital One is Not Alone: 3.5 B Malicious Login Attacks Target Banks and Customers,” *TechRepublic* (July 31, 2019) https://www.techrepublic.com/article/capital-one-is-not-alone-3-5b-malicious-login-attacks-target-banks-and-customers/

[8] Ed Targett, “16 Million Fortune 500 Passwords Added to Dark Web in 12 Months,” *Computer Business Review* (October 30, 2019) https://www.cbronline.com/news/stolen-user-credentials

[9] Shape Security, Inc. “2.3 Billion Account Credentials Compromised from 51 Organizations in 2017, New Research Shows Breadth of Breach Impacts” (July 18, 2018) https://www.globenewswire.com/news-release/2018/07/18/1538956/0/en/2-3-Billion-Account-Credentials-Compromised-from-51-Organizations-in-2017-New-Research-Shows-Breadth-of-Breach-Impacts.html

[10] Ibid.

ABOUT F5

F5 powers applications from development through their entire lifecycle, so you can deliver differentiated, high-performing, and secure digital experiences.

Find more banking and financial service resources at f5.com/solutions

US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com