WHITE PAPER

Defending Financial Applications from Attacks, Unwanted Automation and Online Fraud

Bot and Anti-Fraud Solutions for Financial Institutions

THE ATTACKERS SIMPLY WALK IN THE FRONT DOOR OF AN APPLICATION, PRETENDING TO BE REAL CUSTOMERS OR PROSPECTS.

The rise and risk of fake application traffic. As the defenders of some of the most heavily used financial applications in the world, F5 is in a unique position to observe how criminals are evolving their attacks against financial institutions' web and mobile applications.

Many of the most damaging attacks—those which cost the most money, harm the greatest numbers of customers, and occur most often—leverage novel and emerging attack techniques. These attacks are powered by fake traffic: synthetic identities and the emulation of real customers. The attackers simply walk in the front door of an application, pretending to be real customers or prospects. These attack techniques bypass mainstream security controls because they don't require any coding flaws or vulnerabilities in an application. They even work against correctly-coded applications that are part of a well-run, secure software development lifecycle. As a result, telling real from fake online is one the biggest challenges financial institutions face in today's security environment.

Fake traffic to financial institution applications drives many forms of attacks, unwanted automation, fraud, and abuse.

Figure 1: Fake traffic and respective impact to business

Fake Traffic Threat or Challenge	Business Impact
Credential stuffing	Credential stuffing attacks on web and mobile apps, APIs, and OFX lead to account takeover and new account creation fraud, driving material fraud losses. Large-scale credential stuffing attacks also contribute to site performance issues and can even lead to site outages.
Unmanaged third-party fintech apps	By default, user-enabled, third-party fintech tools log into financial institution apps as if they are actual users. Without proper visibility, management, and controls, these tools can create unnecessary application load and are also being used by cybercriminals as an attack vector to disguise credential stuffing attacks against financial institution apps.
Client-side malware attacks	Man-in-the-browser (MiTB) client-side malware can abuse Zelle and Interac systems to make fraudulent money transfers by hijacking legitimate user browser sessions.
Manual fraud	Fraudsters emulate real users in order to take over accounts or create fake new accounts.

Credential Stuffing: The Leading Application Threat for Financial Institutions

Credential stuffing attacks against financial institutions occur when cybercriminals use credentials stolen from any of the seemingly daily data breaches to either fraudulently log in to financial institution applications or create fake new accounts.

In research recently published by F5 Labs, financial institutions report that credential stuffing is their top application threat, and trends show the problem is only getting worse. This is not surprising, given the relatively low cost to mount credential stuffing attacks and the ever-increasing digital channels customers use to manage their financial accounts.

	2016	2017	2018	2019	2020
Number of Spills	52	49	101	77	117
Total Credentials Spilled	3,301,824,415	2,328,576,631	1,978,746,345	2,255,253,881	1,860,648,946
Average Spill Size	63,478,585	47,521,972	19,591,548	29,289,011	16,762,603
Median Spill Size	2,750,000	996,000	411,755	598,683	2,000,000
Maximum Spill Size	1,000,000,000	2,000,000,000	336,000,000	763,117,241	538,000,000
Minimum Spill Size	100	3,120	858	277	2,200

Figure 2: Summary of credential spills from 2016 through 2020.

For many applications, credential stuffing and other automation attack traffic can represent 50% or more of total traffic to login, new account creation, password reset, and other critical application flows.

USER-ENABLED FINTECH TOOLS: MANAGEMENT HEADACHES AND SECURITY RISK

Third-party, user-enabled fintech tools can pose a number of challenges for financial institutions. These tools can represent up to 20% or more of a typical bank's application traffic, and log in 2.5 times as often as real users. Lack of visibility and management controls for fintech tools can create challenges for financial institutions as they work to optimize and secure their apps and APIs.

In addition, attackers have found new and creative ways to launch credential stuffing and other automation attacks through fintech tools, which can be less well-protected than financial institution apps themselves. And these attacks via fintech can be especially hard to detect and manage without turning off access to all third-party APIs.

MITB MALWARE HAS ATTACKED ZELLE AND OTHER FINANCIAL INSTITUTION SYSTEMS BASICALLY FROM THE FIRST DAY AND HAS BEEN RESPONSIBLE FOR MANY MILLIONS OF DOLLARS IN FRAUD LOSSES.

CLIENT-SIDE MALWARE: POST-LOGIN FAKE ACTIVITY

Another form of fake traffic comes from client-side malware. For example, man-in-the-browser (MiTB) malware infects users' browsers on their personal devices, and lies in wait for a user to log into a financial institution application. Then, in the background and unbeknownst to the user, this malware triggers steps to steal funds, including adding and deleting payees, transferring funds, and even displaying false balance information so the users aren't aware of the theft. MiTB malware has attacked Zelle and other financial institution systems basically from the first day, and has been responsible for many millions of dollars of fraud losses.

MANUAL FRAUD: FAKE TRAFFIC WITHOUT THE BOTS

Bots and other forms of fraudulent, automated traffic deservedly garner a lot of security focus today. However, manual fraud against financial institution applications continues to represent a material source of risk and losses, despite having numerous fraud tools deployed. Cybercriminals focus these human-powered attacks on high-value targets, including account takeovers and new account creation when they cannot achieve the same results through less expensive automation attacks.

F5 Defends Financial Institution Applications from Fake Traffic

F5's converged platform leverages a variety of advanced technologies to help financial institutions defend their web and mobile applications and APIs against a broad array of security threats and fraud risks.

- F5® Distributed Cloud Bot Defense defeats automation attacks, including credential stuffing and the rest of the OWASP automated threats to web applications.
- F5® Distributed Cloud Account Protection gives fraud teams new and powerful tools to defeat fraudsters and slash online fraud in real time.
- F5® Distributed Cloud Aggregator Management provides visibility and control to help manage fintech tools, and defend against attacks through these tools.
- F5® Distributed Cloud Client-Side Defense can detect and prevent non-human money transfers caused by infected client browsers.

SECURITY OUTCOMES, NOT JUST ANOTHER TOOL

F5 delivers security and fraud prevention outcomes as a fully managed service, requiring zero effort to operate. And since attackers are always evolving, F5 solutions leverage advanced AI and machine learning and F5's 24x7 Security Operations Center to ensure a real-time response to emerging threats.

GET THE SECURITY SOLUTIONS THAT DEFEND THE TOP GLOBAL FINANCIAL INSTITUTIONS

The U.S. consumer banking industry loses up to $1.7 billion annually as a result of credential stuffing. With the cost and reputation damage these incidents can cause, you need solutions you can depend on.

F5 successfully detects and defends billions of application attacks a day. Everything F5 has learned in defending the world's leading financial institution apps can now be leveraged by every financial institution to defend its applications from fraud and abuse.

To learn more, contact your F5 representative, or visit f5.com.