Protecting Against Online Banking Fraud with F5

Fraud is a relentless threat to financial services organizations that offer online banking. The F5 Web Fraud Protection solution defends against malware, phishing attacks, and automated transactions to prevent asset loss and brand damage.

White Paper

by F5

Introduction

Financial institutions have the most high-profile, high-value assets on the Internet: millions of bank accounts. The global nature of the Internet means that these assets attract ambitious attackers all around the world.

Banks used to be frequent targets of robbery even in the days of brick and mortar, before the Internet. Back then, the maximum amount of loot taken was limited to the physical currency holdings of that branch. The bank robbers had to physically invade the branch office. If they were caught, they faced the legal framework of the jurisdiction around it.

Those two restrictions (the limited asset exposure and the legal jurisdiction) no longer apply in the Internet age. It is as if every bank robber in the world can perform a heist anywhere and their total addressable loot has increased to the assets of the bank's worldwide clientele. If the virtual bank robber is based in a different country from the clientele, the chances of facing legal proceedings are slim to none, and slim just logged out.

This thievery, broadly known as fraud, is a constant and persistent reality for online banking today. To effectively combat the perils of fraud, organizations that offer financial services over the Internet must defend their businesses with a combination of security technologies. The F5 Web Fraud Protection solution provides both the breadth and depth of coverage financial services organizations need to gain a full defense against asset loss due to fraud.

The Perils of Fraud

Instead of using masks and guns, today's bank robbers typically use spear phishing. This involves sending emails forged to look like they are from the target bank to trick users into installing malware (malicious software) that will compromise their account once they log in. The malware may simply record the username and password and then send it along to a drop zone for later pickup, or it may steal currency via hidden financial transactions.

Asset loss

While they are not compelled to do so, nearly all retail financial institutions cover these losses incurred by users when those users are robbed by an attackers' malware. For many organizations, these asset losses amount to millions of dollars of per year, making them a high priority. Some banks tried to push these costs onto customers, but the resulting PR backlash was so severe that they retracted those efforts. The banks suffered the financial losses and the bad PR as well.

Organizations have had to evolve their own banking applications to provide better account protection (for example, by using SMS messages as two-factor authentication). This has helped, but given the potential rewards, attackers work to defeat new countermeasures. Organizations must continue to deploy multiple solutions to stay current, and those solutions must work together if online banking is to continue to scale.

Damage to the brand

The story isn't over even for banks that accept these financial losses. Forty-six U.S. states require financial institutions that have been compromised to publically disclose the breaches. This forced disclosure can help customers by notifying them of a higher-risk situation (perhaps causing them to more closely monitor their other bank accounts) but it also causes damage to the financial institution's brand.

These breaches are common enough that a single event may not cause much brand damage, but a large one might and repeated breaches certainly will.

Ultimately, repeated breaches to multiple brands in the retail banking sector will unsettle customers to the point where they may lose confidence in online banking, and by extension, perhaps even e-commerce.

Overwhelmed anti-fraud teams

Today, nearly all global retail financial institutions have an anti-fraud team and these teams are busy. First, they have to deploy a range of anti-fraud solutions to combat the various threats they face. Getting all of these solutions to work together can be complex and time-consuming.

Anti-fraud teams also have to deal with the constantly evolving threat landscape. For example, there is a new and interesting twist on the financial mechanics of the fraud industry: extortion. When attackers steal account usernames and passwords, they may demand a ransom from the targeted bank. This can be an attractive approach because it means a single negotiation and lump-sum payment for the attacker. Often the victim will pay a reduced and negotiated ransom to “make the problem go away.” But this leaves the anti-fraud team with a dilemma: in addition to reporting the breach itself, should the team contact each end user individually, and if so, how? By phone? That would be costly and intrusive and could further damage the brand.

The potential for asset loss and brand damage makes it critical for retail financial institutions to deploy the highest levels of security for their online banking transactions. At the same time, busy anti-fraud teams are looking for solutions that can be deployed broadly and quickly, and that play well with other anti-fraud solutions.

Introducing the F5 Web Fraud Protection Solution

The F5 Web Fraud Protection solution has been developed specifically to address the challenges of online banking. It combines the best security with a frictionless experience and a proactive security posture. The solution protects against a full range of threats— including man-in-the-browser attacks and man-in-the-middle attacks as well as evolving threats—to help financial organizations reduce loss and exposure. And because attacks are always evolving, the solution includes both technological and services components to ensure real-time response to emerging threats.

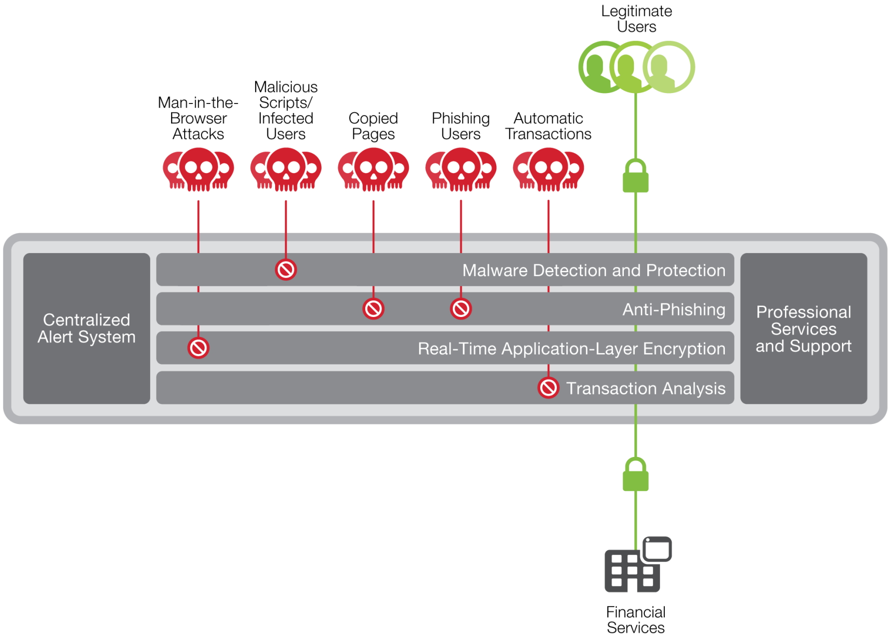
Legitimate Users
Man-in-the-Browser Attacks
Malicious Scripts/ Infected Users
Copied Pages
Phishing Users
Automatic Transactions
Centralized Alert System
Malware Detection and Protection
Anti-Phishing
Real-Time Application-Layer Encryption
Transaction Analysis
Professional Services and Support
Financial Services

Figure 1: The F5 Web Fraud Protection Solution

Detect and mitigate to reduce asset loss

The technological component of the F5 Web Fraud Protection solution detects targeted and generic malware, man-in-the-browser attacks, man-in-the-middle attacks, zero-day attacks, phishing attacks, and other threats that occur in the online channel. It applies a variety of identification techniques to recognize malware patterns such as changes in HTML code, injection of malicious script, or attempted automated transfers. The solution:

- Detects malware targeted at financial applications
- Prevents malware from stealing user credentials
- Mitigates automated transactions with behavioral analysis of the end user
- Protects against phishing with real-time feedback

Focusing on malware and phishing together reduces the number of compromised accounts. Fewer compromised accounts and protection from automated transactions equates directly to fewer asset losses on the bottom line.

Limit breaches to protect the brand

It's not just about asset loss. Even a breach that grabs no loot can cause damage to the brand by requiring breach notification. The F5 Web Fraud Protection solution reduces the number breaches, the number of users affected, and the number of requisite breach notifications.

This is possible because the F5 Web Fraud Protection solution has a clientless security model. Client-based solutions require the end user to download special software to monitor the security of the endpoint device and to launch a secure browser. Only a fraction of users actually do this; in fact, today's users are trained not to download software in case it is a Trojan.

Instead of relying on user-installed software, the F5 solution resides at the Application Delivery Controller. From this strategic point of control in the network, the Web Fraud Protection solution is injected into the application as it being delivered to the end user. Organizations appreciate the fact that no client software is required. This approach provides much broader security coverage for the user base than anti-fraud technologies that rely on user behavior to protect the endpoint device.

An additional benefit of the clientless security model is that the user experience is unchanged. Because the solution is injected from the Application Delivery Controller and there are no changes to the application, organizations do not need to retrain their users; indeed, those users are not even aware that they are being protected.

Scale the anti-fraud teams

In order for busy anti-fraud teams to be effective, they need tools that:

- Play nicely with other anti-fraud tools
- Provide proper alerting when attacks are detected
- Leverage community malware expertise

Today's retail financial institutions know that tools that meet these criteria must be designed specifically for the most rigorous security environments in the world. Environments like these will have multiple anti-fraud solutions deployed, such as two-factor authentication, geolocation, and adaptive authentication. The F5 Web Fraud Protection solution cooperates with all of these complementary solutions and supports most organizations' SIEM solutions.

To ensure rapid and efficient response to the latest malware, zero-day, and phishing attacks as they evolve, the F5 Web Fraud Protection solution includes a critical services component through the F5 malware analysis team. This group of experienced threat and attack researchers operates the Security Operations Center, which provides detection, real-time alerting, analysis, and mitigation to organizations' anti-fraud teams through a central dashboard as well as via email and SMS. The Security Operations Center monitors current malware and phishing sites and works with law enforcement and ISPs to get malicious sites taken down when possible, benefiting the community as a whole.

Conclusion

The perils of fraud are not going away. Moving forward, banking functions will continue to migrate online and fraudsters will continue to evolve their attacks. Financial services organizations must meet these challenges in order to protect the bottom line, defend the brand, and enable their staff.

The F5 Web Fraud Protection solution is designed specifically to provide the high-profile online banking environment with deep security coverage to protect end users from malware, phishing attacks, and automated transactions. Fewer compromised accounts translates directly into fewer asset losses.

The most agile organizations will be able to deploy a suite of security services to maximize their security posture. The Web Fraud Protection solution delivers security from a strategic point of control in the network, which is key to helping organizations easily deploy it with other solutions in their current architecture. Additionally, the F5 Security Operations Center ensures that organizations receive the best, most current threat intelligence available. Working together, these services give organizations a full defense to keep their business, their brand, and their users secure from the threat of fraud.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com