BANKING’S NEW CYBER ENEMY:
ANATOMY OF BANKING FRAUD

INDUSTRY GUIDE: BUGFRAUD FOR FINANCIAL SERVICES
Users are not properly protected. Online banking fraudsters know that bank customers demand more digital services and usually lack any security measure or making them the weakest link in the online fraud chain. It’s much easier to gain access through a user’s online banking activity than it is to break through bank security systems.

<table>
<thead>
<tr>
<th>INVESTMENT AMOUNT</th>
<th>RISK</th>
<th>ROI</th>
<th>PERIOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Banking Fraud</td>
<td>Very low</td>
<td>Very low</td>
<td>300%</td>
</tr>
<tr>
<td>Stock Market</td>
<td>Medium</td>
<td>High</td>
<td>10%</td>
</tr>
<tr>
<td>Real Estate</td>
<td>High</td>
<td>Moderate</td>
<td>5%</td>
</tr>
</tbody>
</table>

Banking customers around the world conduct more of their business online than ever. According to the CapGemini World Payments Report 2017, non-cash transactions reached 433.1 billion by 2017. As banking customers move online, so do cyber criminals that are targeting their accounts.

Easily and safely. It’s easy and very profitable for fraudsters. Tools and services can be purchased on the black market for the creation and execution of fraud campaigns in online banking. There is no longer need for extensive technological knowledge or large amounts of money. Compared to traditional forms of investing, banking fraud delivers returns quickly and with low risk.

New Cybercriminal techniques, tactics and procedures (TTP). Attacks can bypass bank security measures at any time during the user’s online banking session. For example, phishing, Man-in-the-Browser (MitB), Remote Access Trojans (RATs), session hijacking, account takeover, and bot attacks easily bypass banks’ current two-factor and three-factor authentication methods.

Users are not properly protected. Online banking fraudsters know that bank customers demand more digital services and usually lack any security measure or making them the weakest link in the online fraud chain. It’s much easier to gain access through a user’s online banking activity than it is to break through bank security systems.

IN THIS CONTEXT, THE MAIN CHALLENGES FOR BANKS ARE:

- the ability to quickly acquire deep knowledge of new cyber-criminal patterns,
- agility and accuracy to identify fraudsters,
- early detection of fraudulent activity to prevent them from interacting with their customers.

As digital fraud attacks become more sophisticated and identity theft becomes more complex, it’s time to rethink traditional anti-fraud solutions.
Preventing Online Fraud

Preventing online banking fraud requires banks to fulfill two critical principles:

1. Ensure that the online banking customer is really who they say they are

Sometimes users are impersonated by fraudsters who have previously compromised login credentials through phishing, or malware attacks.

2. Ensure that the online banking customer is performing actions without being manipulated or deceived

The online banking customer might be legitimate, but his navigation of the online banking application is being manipulated by fraudsters. The attacker can change forms, scripts, URLs, and even displayed data to persuade the victim to compromise personal information or funds.

Fraudsters use multiple techniques to violate these two principles of fraud prevention. These techniques are classified into three primary categories.

**Imitation Threats**
- Phishing
- Pharming
- Vishing
- SMishing
- Cross-Pharming
- Fake Apps

**Infection and Static Code Injection Threats**
- Old Trojan Bankers (zeus, spyeye, keyloggers)

**Infection and Dynamic Code Injection Threats**
- Modern Trojan Bankers (Gozí, Dridex, Dyre...)
- MitB/MitM
- Remote Session Hijacking

**Automatic Remote Control Threats**
- RATs
- RItB
- Screen Overlay

**Manual Access Threats**
- Anti-bot detectors
- 24x7 Human Operators
- Targeted Accounts
- Local Session Hijacking
Imitation threats, most commonly known as phishing and their variances (Vishing, SMishing, etc.), are the oldest and by using sophisticated social engineering techniques to redirect users to sites that are copies of legitimate bank sites. These fake sites run on different infrastructures from legitimate ones and eventually try to get sensitive user information. Some phishing and ransomware attacks also affect legitimate banking mobile apps (fake apps).

2016 1Q

Threats Based on Imitation

44.16% OF ALL PHISHING ATTACKS TARGETED BANKS, PAYMENT SYSTEMS, AND ONLINE SHOPS.

54.17% OF THESE, SPECIFICALLY TARGETED

99.83% ANDROID DEVICES ARE THE MOST-TARGETED MOBILE PLATFORM WITH 99.83% OF ALL DISCOVERED ATTACKS FOCUSED ON THIS OS.¹

¹Financial Cyber Threats Q1, 2016, Telefonica, September 5, 2016
The most dangerous and recent threats are dynamic infections and injections, which actually change legitimate websites to deceive the user. Once the user’s machine is infected by malware, fraudsters update the malware remotely and dynamically add new features or bank sites for which the malware can inject code. This way, fraudsters through the use of dynamically generated Command & Control Servers, can easily update their botnets increasing the list of potential banks to attack and code injections by using latest toolkits delivered in the Black Market, therefore maximizing their chance to commit fraud with low exposure.
Remote Control Threats

Automated Remote Control threats take control of an online banking session after the user has been authenticated with an authorized device.

Fraudsters often use commercial software for remote control or malware specifically designed for this purpose. These attacks are especially dangerous because they combine multiple techniques, such as blocking sessions with a web injection and manipulating account balances in the background with a RAT.

Fraudsters can purchase services from botnet operators that monitor account balances and create automatic mechanisms to take manual control over user accounts.

Besides all these techniques, there are always situations where fraudsters or mafias directly bribe or even blackmail internal bank employees as to get banking sensitive client information.
The Challenges in Preventing Online Banking

Financial services organizations have deployed billions of dollars to protect their networks, applications, and data. Now they must expand their security focus to protect their customers from attack, which creates significant challenges.

**LACK OF VISIBILITY TO IMPROVE PROTECTION**

Without visibility into users’ devices, banks can’t gather threat data that would help them strengthen protection.

**ENSURING PROTECTION WITH A HIGH-QUALITY USER EXPERIENCE**

Banks must be able to implement adaptive protection measures that protect a wide range of user profiles and associated risks without impacting the customer’s experience.

**CURRENT MARKET SOLUTIONS RARELY DETECT EMERGING THREATS**

Online banking fraudsters continually adapt their techniques, and current market solutions lack effectiveness against emerging threats. Traditional malware protection uses a blacklist approach that can detect threats once they are known but often miss emerging threats. Other solutions, such as latest biometric solutions can be easily bypassed by new Malware attackers that collect the data used to feed their biometric statistical models and apply the same algorithms to impersonate the victim.
Now customers can often access their accounts through two or more devices. In addition, the banks’ network connections can be global and include hundreds of partners and entities that need to share information. This further expands the attack surface and exposes the bank to a wider range of threats.

FALSE POSITIVES ARE AN EXTENDED PROBLEM

According to Anthony Fenwick, global head of treasury and trade solutions and AML compliance at Citi Group, “Our biggest problem in this industry is false positives”. A study conducted by the Ponemon Institute found that 37 percent of respondents faced more than 10,000 daily alerts, with 52 percent of them being false positives. False positive alerts waste thousands of hours, which are costly, but the cost of missing a real threat is higher yet. Banks need a way to accurately detect legitimate fraudsters to avoid wasted resources and minimize the risk of a legitimate attack.

3) Computerworld UK, May 2, 2017
**bugFraud**

**bugFraud** is a next-generation fraud prevention solution for mobile and web applications that helps banks protect online users.

**WHEN A USER ACCESSES HIS ONLINE ACCOUNT, BUGUROO BUGFRAUD PROFILES FOUR LAYERS OF DATA WHILE MAINTAINING DATA PRIVACY COMPLIANCE:**

**BIOMETRY**
Identifies the user’s bio-behavior and cognitive analytics to uniquely profile each human behind a device

**WEB CONTENTS**
Checks the information a user displays to detect if it’s being manipulated by third-party attackers, without false positives or negatives

**ENVIRONMENT**
Profiles the user’s context information such as devices, network, and geo-location and crosses it with threat intelligence data to identify anomalies in the user’s environment

**OMNI-CHANNEL**
Correlates data from multiple inputs, such as web browsers, mobile devices, and application servers to make sure solution is not bypassed by attackers

**BUGFRAUD THEN PROCESS AND ANALYSES ALL THESE INDICATORS IN ORDER TO MAKE SURE IT DETECTS NEW EMERGING THREATS EVENTUALLY COVERING ALL 3 TYPES OF THREATS PREVIOUSLY MENTIONED (EVEN THOSE FRAUDS BASED ON BLACKMAILING OR BRIBING INTERNAL BANKING EMPLOYEES) AND PROVIDE THIS INFORMATION TO THE BANK IN REAL TIME.**
buguroo bugFraud uses very advanced technologies such as Deep Learning to deliver precise protection coverage to ensure that online banking users are really who they claim to be and that they are accessing their accounts without being manipulated. Regardless of the threats targeting them, bugFraud provides unmatched protection and adaptability.

**PREDICT AND ADAPT TO PREVENT ANY KIND OF THREAT**

bugFraud uses biometric profiling during the user’s entire session. It gathers data about mouse movement, keyboard use, user location, and devices and analyzes it using Deep Learning technology and advanced neural networks.

bugFraud processes millions of pieces of data and can detect any anomaly and interrelationships, even those that are imperceptible to humans. Anomalies can signal a possible account takeover or RAT attack, as well as detect zero-day and dynamic malware attacks. bugFraud protects against threats even when they do not match a known malware signature.

Financial institutions do not have to redesign detection systems or policy rules every time a new threat appears. buguroo bugFraud keeps them protected in the rapidly changing cybercrime landscape.

**PREVENT FRAUD DURING THE ENTIRE ONLINE BANKING SESSION**

Unlike other fraud detection solutions, buguroo bugFraud protects the institution, its users, and sessions from login to logout across the spectrum of potential attacks that target the user.
GAIN REAL-TIME VISIBILITY WITH ONGOING PROTECTION

bugFraud provides a holistic view of the user's session including device, network, channel, biometry, web content, and other data—together with its analysis—to provide institutions with comprehensive and accurate visibility. Institutions can see exactly how, when, and where fraud attempts are occurring and which customers are victimized.

ENHANCE THE USER EXPERIENCE WITH FRICTIONLESS PROTECTION

With bugFraud banks do not have to ask their customers to install nor update any software. Protection is completely invisible to the customer, yet they are protected with any device that they use for banking—PCs, laptops, tablets, or smartphones.

NO FALSE POSITIVES SAVE TIME FOR SECURITY TEAMS

A comprehensive classification system eliminates false positives and avoids false negatives so that the bank’s IT team is not continually reacting. Deep Learning profiles users’ biometric passive patterns to improve protection with every transaction. bugFraud saves time and enables bank IT teams to accurately identify real threats.
buguroo originated 15 years ago and today, global banks and financial institutions use buguroo to detect new online cyberattacks. The company’s Deep Learning and advanced neural networks together with world-class team of cybercrime experts makes buguroo a first-class product to reduce online banking fraud. Every month, the buguroo monitor more than 10 millions of users. As a result, buguroo was named a “Cool Vendor” in 2016 by Gartner, Inc. for its buguroo bugFraud solution.

**Security Expertise in Banking**

**DEFENSE**
- Phishing clones
- Man in the Browser
- WebInjects
- Adware

**ENVIRONMENT**
- Advanced device fingerprinting
- Networking profiler
- Threat Intelligence Analysis

**DETECTION**

**BIOMETRY**
- ATO Detection
- RAT Detection
- Man in the Middle
- Session Hijacking
- BOT Detection

**OMNI-CHANNEL**
- Server Cross Library

**MANAGEMENT**

**ALERT MANAGEMENT**
- Executive Dashboard, Alert Management, Event Classifier, Administration

**LOADERS**

**WEB**
- For web users

**MOBILE**
- For mobile users

**DETECTION PROVIDES COMPREHENSIVE PROTECTION AGAINST THE WIDEST RANGE OF THREATS, INCLUDING RATS.**
SEE A DEMONSTRATION

Learn more about buguroo bugFraud and request a demonstration.

Visit www.buguroo.com, or contact us at info@buguroo.com.