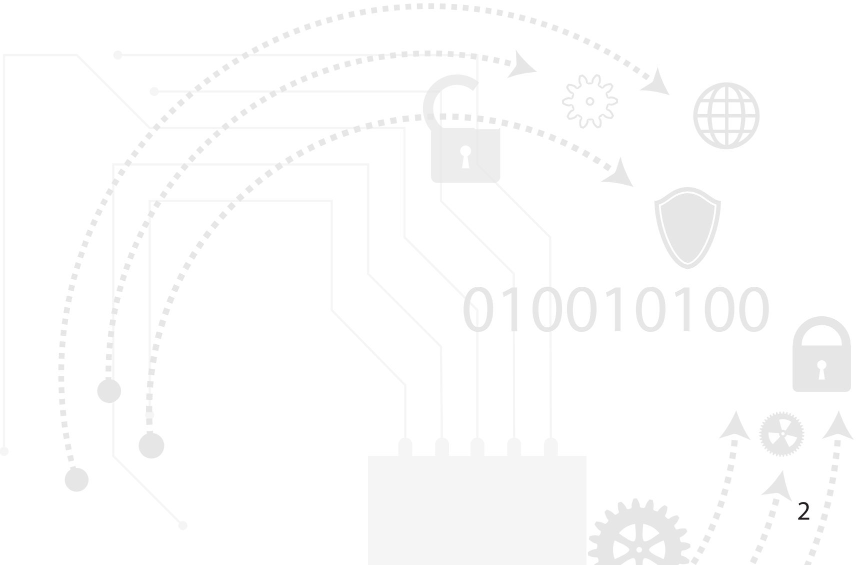
buguroo

Protect the Customer First

Next-generation bank fraud prevention with Buguroo bugFraud

> **“Today’s global cybercrime is big business. Attacks currently account for more than $400 billion in financial losses annually.”**

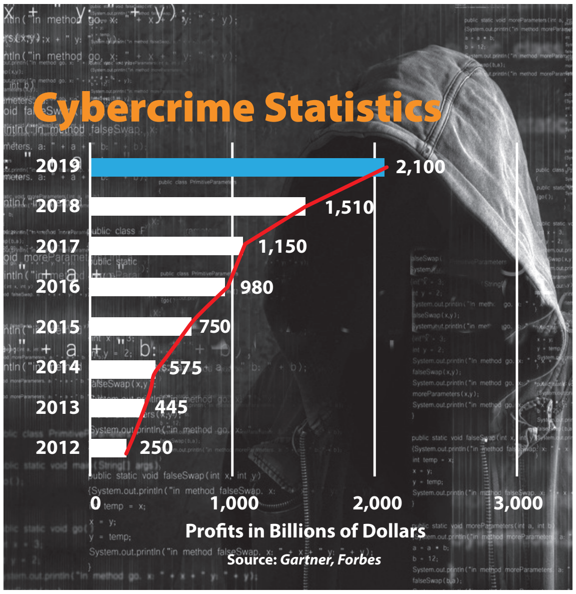
Table of Contents



From debilitating online attacks on major corporate websites to data breaches designed to influence elections, cybercrime has dominated the headlines in 2016. Threats and attacks are becoming more frequent, more sophisticated, and more effective every day. They are also becoming more profitable for the cybercriminals.

Today's global cybercrime is big business. Attacks currently account for more than $400 billion in financial losses annually.[1] In fact, cybercrime is now the second fastest growing global economic sector and is on track to be the most lucrative soon. From the perspective of organizations that are the victims, cybercrime results in huge losses. Experts predict that annual cybercrime costs will grow from $3 trillion in 2015 to $6 trillion annually by 2021.[2]

Faced with this increasingly powerful and malicious economic force, banks and other financial institutions are scrambling to stay one step ahead of attackers. Most are approaching this task by investing in cybersecurity solutions designed to combat each new threat, once it is identified. Let's begin by examining today's current cybercrime landscape and take a look at available solutions.



Source: *Gartner, Forbes*

Anatomy of a Bank Fraud Attack

There are two main ways cybercriminals are able to gather customer data. First, they can redirect customers to fraudulent bank sites. Second, they can inject malware into customers' systems which changes the behavior of the legitimate site to facilitate the cybercrime.

In the first type of attack, fraudsters will clone a legitimate bank site and create a fake one that directs customer traffic to the malicious servers. This is done through:

- Phishing schemes, where customers open up a malicious email that appears to be from a bank or business and click a link that directs them to a cloned impostor site.
- Pharming attacks that trick the domain name server to redirect a user (who has typed in the correct address) to the impostor site.

Once the customer reaches the cloned site, cybercriminals can either steal from them, copy their login credentials for future theft, or use them as "mules" to unwittingly transfer money or data from the bank to the malicious servers.

Other types of cybercrime, such as man-in-the-browser (MITB) attacks, infect a customer's device and are triggered when a particular site is visited through the browser. These attacks inject malware code designed to compromise interactions on the legitimate bank sites. Users believe they are safe because they are logged in to the legitimate bank's website, but the malware, which is sitting in the background, modifies the request presented by the browser. The malware intends to steal the user's valuable information and credentials or even hijack a user session to order automatic fraudulent transactions.

Going After Gozi

In late 2012 and early 2013, financial malware called Gozi infected more than 1 million computers globally and caused millions of dollars in losses and damages. In August of 2016, researchers at Buguroo Labs discovered new Gozi campaigns aimed primarily at banks and financial services in Japan, Poland, and Spain, with the intention of later launching in the U.S. and Western Europe. These new threats are using dynamic web injection and automation to choose "mules" (individuals who unwittingly transfer data and funds to malicious servers). The selection of the mules has become more sophisticated, based on the victim's vulnerability and value to the cybercriminal (for example, level of access credentials).

Through its ongoing cyber intelligence efforts, Buguroo researchers successfully detected Gozi and analyzed the behavior of these new Gozi attacks. Buguroo Labs alerted the public so that financial institutions globally would be prepared to defend themselves and their customers against Gozi and its variants.

Types of Cybercrime Attacks	
Zero-day malware	An unknown virus or other malware for which a victim or visited site has no protections.
RAT in the browser	A Remote Access Trojan that is unknowingly installed on a victim's computer, giving cybercriminals complete access to the victim's data.
Man in the middle	Attackers who insinuate themselves between two parties in an online conversation, impersonating one of the parties and copying or changing the conversation in an effort to steal information or do other damage.
Man in the browser	Malware that infects an end user's device, which allows it to inject malicious code into a site the user visits, create a false request for credentials on that site, and steal data.
Targeted malware	Threats designed for a specific organization or industry.
Form grabbers	Malware that can steal credentials, like IDs and passwords, from browser forms.
Session hijacking	Taking control of a victim's valid computer session to gain access to its information and services.
Adware	Software that displays (usually unwanted) advertising when a person is online.
ClickFraud	The practice of repeatedly clicking on an ad to drive up the cost for the advertiser while increasing profits for the host site.
Spyware	Malware that secretly gathers and steals information from a user's computer.
BOTs	A type of malware that infects a victim's computer and executes whatever type of activity a cybercriminal commands.
Website defacements	Attacks that break into a web server and change a website's visual appearance, usually by replacing the site with one of its own (for example, a fake version).

Small Investment, Big Returns

Investing in cybercrime can be relatively cheap, yet profitable. A malware campaign with an advanced system of cybercrime behind it can be launched for an investment as low as $3,000.[3] This modest sum can reap a return averaging $12,000 per campaign, a 300% ROI. Those making these investments need no knowledge of how to run the campaigns due to the large supply of highly skilled cybercriminals ready and eager to sell their skills on the black market.

Compliance and Liability

The motives for today's banks to protect their customers from data or financial theft have extended beyond measures of goodwill, positive public relations, and retention of customer loyalty. In many countries, banks are legally responsible for recouping a customer's losses. For instance, in a recent case in Spain, a bank customer's computer was infected with malware that caused her to lose more than $70,000. The customer took the case to court, charging the bank with the loss, and won.

Each country is different in terms of its liability and insurance requirements. In the United States, banks are required to guarantee the authentication and transaction process and to carry insurance against theft. In any case, a bank's viability depends on its ability to ensure its customers' holdings are safe, in spite of the advanced and changing threats intent on compromising that security.

To provide this assurance, today's financial institutions and other businesses should consider revisiting their approach to cybersecurity, moving toward solutions that are:

- **Customer-focused** to protect those who currently are not protected, and take into account the billions of devices that can serve as launchpads for malware.
- **Signature-less** and able to protect against zero-day and dynamic attacks without needing to know exactly what they are.
- **Agent-less**, so as not to inconvenience customers and erode their trust in the banks.
- **Intelligent** and able to learn from each attack as a way of strengthening protections for both new and returning online customers.

Signature-Based Security Solutions

Most bank fraud prevention solutions available today are based on signatures that aim to match and stop each type of attack. But this strategy has its limitations because malware is constantly changing, with malicious hackers developing new ways to evade detection mechanisms. In some cases, malware injections are dynamically calculated and impact victims in the post-login phase, making signature-based protections ineffective. Banks, e-commerce companies, and other businesses are challenged to ensure online protection for their organizations and customers amidst a fast-changing cybercrime landscape.

Some solutions on the market aim to safeguard banks, but they lose sight of the customer. For example, the customer may be asked to install a software agent for protection during transactions. Often, the agent conflicts with the customer's operating system, and the customer is unable to complete the task. Even customers who can successfully install the agent are likely to feel inconvenienced by this extra step and remain unsure about their level of security on the bank's site. Furthermore, many of today's agent-based solutions are not able to gather intelligence and learn from attacks in order to strengthen protection over time.

A Customer-First Approach

Many cybersecurity measures currently on the market are designed to safeguard banks and businesses, but not necessarily their customers. Banks, in particular, offer few protections for customers who are sharing data and making financial transactions on the banks' websites. This not only makes customers vulnerable to identity and financial theft, it also leaves much of the attack surface unprotected. Malware can reach banks through potentially billions of personally owned endpoints, including desktops, laptops, tablets, mobile phones, and a host of other devices.

Some solutions are designed to protect customers from attacks, but they usually:

- Rely on signatures to find matching threats, making them ineffective for zero-day and other dynamic attacks.
- Require customers to download protective software agents, which undermines the customer's assumption that the bank site is already secure.
- Interrupt the customer in the middle of the transaction to stop the attack, which inconveniences the customer, and again, erodes trust in the bank's online security.

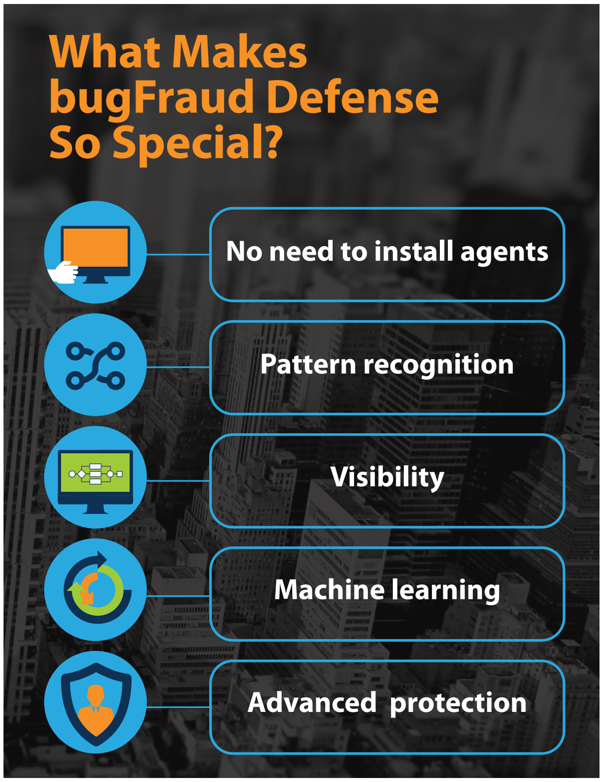
Buguroo® bugFraud Defense takes a different approach. It is the most effective customer-focused solution on the market, using signature-less and agent-less technology. It can also derive intelligence from each attack and strengthen its effectiveness. As a result, this solution is well positioned to counter the new types of malicious schemes that are infiltrating financial sites and to keep customer data and funds in the right hands.

Transparent protection

bugFraud Defense's protective operations operate in the background, foiling attempts to redirect users to malicious sites or to compromise their data on legitimate ones. With bugFraud on the bank site, it's business as usual for the customer.

No need for signatures

Instead, bugFraud Defense needs only to detect unusual site or traffic behavior to become aware of threats. It can home in on zero-day and dynamic attacks in a way that signature-based solutions can't. As a result of its signature-less approach, bugFraud Defense can successfully identify and stop threats that evade the protections of other solutions.



What Makes bugFraud Defense So Special?

No need to install agents

Pattern recognition

Visibility

Machine learning

Advanced protection

An agent-less approach

Customers don't need to download any software or undergo any other online security procedure to ensure they will be protected on a bank site.

The more it's used, the better it protects

bugFraud Defense uses artificial intelligence, or machine learning, to gather data and learn from the attack. That way, it can safeguard not just frequent users, but also infrequent or new users from malware attempts.

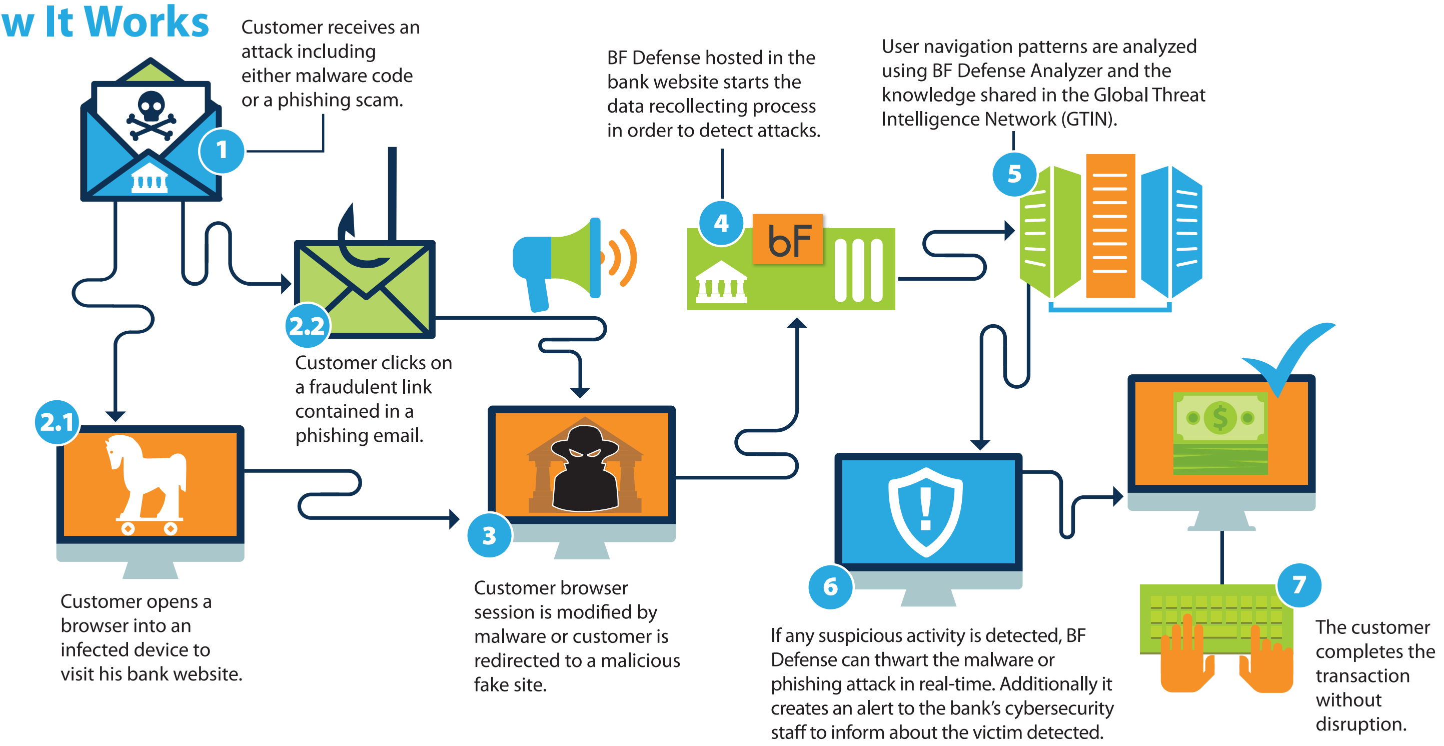
Next-Generation Fraud Defense

Most current defenses are focused on combating common viruses, but advanced threats, such as zero-day attacks or ad-hoc, targeted malware injections, can't be detected by traditional antivirus technology. In addition, most solutions available today have difficulty keeping up with the rapid evolution of malware. Malware-as-a-Service allows attackers to develop new threats much faster than security vendors can develop protection.

The key to fully protecting customers and organizations from these fast-changing threats is a comprehensive, adaptive, and multi-faceted approach to online security. This requires a system that keeps customers, data, and money safe; prevents next-generation threats from compromising your network; and gets stronger with every attempted attack.

bugFraud Defense focuses on the initial phase of compromise at the endpoint, which often begins with phishing attacks on customers. The goal of these attacks is to steal or misuse credentials and redirect users through their browsers to simulated, malicious banking websites. Advanced malware can modify navigation through the browser, compromising credentials or even hijacking the session to transfer stolen funds from financial institutions to malicious servers.

How It Works



1 Customer receives an attack including either malware code or a phishing scam.

2.1 Customer opens a browser into an infected device to visit his bank website.

2.2 Customer clicks on a fraudulent link contained in a phishing email.

3 Customer browser session is modified by malware or customer is redirected to a malicious fake site.

4 BF Defense hosted in the bank website starts the data recollecting process in order to detect attacks.

5 User navigation patterns are analyzed using BF Defense Analyzer and the knowledge shared in the Global Threat Intelligence Network (GTIN).

6 If any suspicious activity is detected, BF Defense can thwart the malware or phishing attack in real-time. Additionally it creates an alert to the bank's cybersecurity staff to inform about the victim detected.

7 The customer completes the transaction without disruption.

bugFraud Defense identifies attack behavior in real time before the attack can gain a foothold. When bugFraud Defense is deployed on a bank's server, it can detect the fraudster's attempts to clone the bank site, take full control of the user's path, and redirect the customer to the legitimate site, preventing cybercriminals from achieving their malicious objectives. In the case of MITB attacks, bugFraud Defense sees that there is some illegitimate code being injected into the bank site, and overrides it. It prevents the malware from capturing and transmitting the customer data, and once again, protects the customer and the bank.

> **"The more bugFraud Defense is used globally, the more it knows, and the better it protects all customers."**

bugFraud Defense relies on advanced, automated machine learning to analyze every transaction and gather threat intelligence. The solution incorporates this information into rules for preventing fraud against future bank transactions conducted by all the bank's customers, not just the current victim. Protection improves with every transaction, saving organizations time and helping them identify real threats more accurately. The more bugFraud Defense is used globally, the more it knows, and the better it protects *all* customers.

Conclusion

As malicious hackers become increasingly savvy and greedy, it's more important than ever for banks and other organizations to reassure customers that their data and assets are safe. Most banks have sought to do so by focusing on their institutions and by attempting to identify and combat every new threat, but this strategy has proven impractical and ineffective in such a fast-changing attack environment.

By contrast, the bugFraud Defense approach focuses on the security and convenience of the customer, needs only to recognize unusual endpoint and site behavior (rather than specific threats), and becomes more effective each time it's used. This is the strategy that can turn the tide against cybercriminals and provide the security that banks and customers need and expect.

For More Information

To learn more about bugFraud Defense and how it can protect your customers and your organization from transaction fraud, visit our website at www.buguroo.com, or contact us at info@buguroo.com.

[1] https://www.lloyds.com

[2] buguroo Labs and Kaspersky Labs (https://business.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/2930/)

[3] Ibid.

SILICON VALLEY
1370 Willow Road
Suite 200
Menlo Park, CA 94025
United States
(650) 285-2408
info@buguroo.com

MIAMI
1395 Brickell Avenue
Suite 800
Miami, FL 33131
United States
(305) 351-7396
info@buguroo.com

MADRID
Calle Anabel Segura,
16 Edificio 3 Planta 1
Alcobendas, 28108
Madrid, Spain
(+34) 91 229 43 49
info@buguroo.com