FRAUDSTER HUNTER: DELIVERING A STRATEGIC ADVANTAGE TO FINANCIAL ORGANISATIONS TO STOP FRAUD AT THE SOURCE

buguroo

INTRODUCTION

Global financial institutions have been engaged in an arms race with fraud and cybercrime gangs for the best part of two decades. **During this time, banks have largely been playing in defence, seemingly one step behind the fraudsters.**

First it was phishing and early banking trojans, then dynamic malware featuring polymorphic and domain generation algorithm (DGA) techniques. As behaviour-based defences were developed to tackle these threats, bots, remote access trojans (RATs) and emulators emerged to cause more chaos.

Today a cybercrime economy potentially worth as much as $1.5 trillion annually supports **a vast underworld marketplace for breached identity and financial data** as well as for automated fraud tools and know-how.

The current pandemic is spurring a new wave of digital transformation in the industry as banks and lenders scramble to support mass remote working and customers who are reluctant to set foot inside branches.

According to Deloitte, 35% of US customers have increased their use of online banking during the crisis. As this growth continues so will the level of online fraud: even last year, over 60% of respondents to KPMG's Global Banking Fraud Survey reported an increase in fraud volume and over 50% experienced an increase in fraud losses.

As fraudsters take advantage of readily available identity data, anonymising tools, automated bots and willing mules, the odds continue to stack up against financial institutions.

Fortunately, new ways are emerging to spot increasingly sophisticated fraud patterns. These include **AI-powered behavioural biometrics** – which profile how individual users interact with mobile devices, keyboards, touchscreens and mice – along with device fingerprinting, network data and zero-day malware analysis in order to alert when activity deviates from the norm.

There's just one problem: while these tools are great at providing assurances that a user is who they say they are, and flagging when sessions are hijacked by fraudsters, **that's where they stop.**

An additional approach is needed to reveal the bigger picture of malicious activity; **one that is capable of improving banks' resilience going forward, and leads to the discovery of much larger and systematic fraud campaigns.** This is where buguroo's **Fraudster Hunter** tool comes in.

THE BIGGER PICTURE

Buguroo uses a **highly granular approach to fraud prevention**, combining behavioural biometrics such as cadence, typing rhythm, finger size, pressure, mouse velocity and clicking frequency with other elements including network and threat intelligence, device profiling data, malware inspection, and behavioural analytics.

This creates a unique BionicID for every banking user that can be used to generate a risk score in real-time for each interaction at all points during a transaction, from login to signoff.

While this technology works effectively to provide visibility into customer behaviour and block fraud, there's another use case which could empower banks to get even more proactive about stopping malicious activity.

Powered by the right algorithms, it could help to **identify and link potentially much wider fraudulent activity**, whilst providing intelligence to help **block future attacks at the source.**

It's the fraud equivalent of tracing an individual droplet of water falling on a garden back to the sprinkler it came from.

This is Fraudster Hunter

INTRODUCING FRAUDSTER HUNTER

Fraudster Hunter is an innovative capability of the buguroo platform that alerts banks' in-house teams of any suspicious behaviour and enables them to **build unique BionicIDs for each criminal attempting to target their systems.**

Via a highly intuitive user interface, fraud teams can double click on users, devices, IP addresses or sessions to discover the hidden relationships between them – and in so doing uncover major fraud campaigns in the planning or execution phases.

Once fraudsters are actively identified by their BionicID, their identifiers can be used to create rules and actions to recognise additional fraudulent activity. **This flexible capability provides fraud prevention teams with the ability to create customisable fraud detection and prevention rules.** Once identified, all subsequent suspicious activity will generate alerts to the financial institution allowing it to take appropriate action ranging from stepping up authentication to terminating the transaction.

Fraudster Hunter delivers a closed loop discovery and proactive mitigation capability **allowing financial institutions to dramatically improve fraud prevention team efficiency and fraud detection rates.**

In essence, **Fraudster Hunter** gives banks a competitive advantage by allowing them to get in front of emerging fraud threats. Furthermore, it enables them to **quickly respond to the unique fraud threats that they are experiencing** – allowing them to swiftly stop new fraud schemes and maintain customer trust and brand reputation.

Additionally, **Fraudster Hunter** allows banks to catalogue and cross reference user BionicID information with customer data, so fraud teams can **trace malicious activity back to individual actors in a highly effective manner**. It helps these teams pinpoint accounts that have been set up or compromised by the fraudster – including linked mule accounts – **allowing the bank to block any future fraud attempts – cutting fraud off at the root.**

This capability can be used to stop **New Account Fraud (NAF)**, **Account Takeover (ATO)**, **Card Not Present (CNP) fraud** and **uncover money mule activity**.

DIGGING AND LINKING

In the physical world, successful bank robbers would usually scope out a target bank for weeks or months before formulating their plan. They may pose as customers or cleaners to better understand how security works inside, where the CCTV cameras are and where the gaps are located that they can exploit. It's not so different in the virtual world.

Online fraudsters will usually need to perform detailed reconnaissance on a victim organisation prior to striking. They'll register an account and maybe carry out some simple transactions to check how authentication is performed and what measures the bank has in place to mitigate malicious activity.

What they don't know is that for buguroo clients, their users' every move is being recorded and analysed – all without using personally identifiable information. Using the same techniques described above, **a "digital DNA" is compiled for every customer, including those hidden fraudsters.**

This BionicID is impossible to mimic and will indelibly tie a malicious banking user to their activity. **Fraudster Hunter** effectively allows banking teams to intelligently mine compiled data in this way to efficiently determine the source of fraud. Once identified, fraudster **BionicIDs can be utilised as actionable data to stop new and in-progress fraudulent activity.**

How are hidden patterns discovered? With link analysis, which helps fraud teams visualise both legitimate and malicious connections to discover accounts being used to commit fraud and those at high risk of being used for future crimes.

Here's an example:

A single device is found to be linked to multiple accounts and is being used by seemingly unrelated people, raising a red flag for a bank's fraud teams.

They can use Fraudster Hunter to see what other connections that device has within the bank. It's possible the same device is linked to other IP addresses, that are in turn linked to other devices and other accounts —so it goes on, like a family tree.

A single discovery could therefore uncover hundreds of potential dangers. Using this link analysis, a bank can pinpoint the "brain of brains" — the central controller of multiple fraudulent accounts, potentially bringing a whole crime ring down in one go.

UNCOVERING A NETWORK OF 400+ MULE ACCOUNTS

One of Europe's top three biggest digital banks, with over 1.2 million clients and $10 billion incustomer assets, **contacted buguroo to help detect what it suspected to be a large number of mule accounts.**

A cybercrime group had tricked consumers into buying products that didn't exist, directing them to pay into mule accounts with the bank. The lender was able to detect some fraudulent activity due to suspicious behaviour patterns but found it difficult to identify all the fraudsters. **Fraudster Hunter** was able to profile the malicious actors through their behavioural biometrics, associated BionicIDs and geolocation information, before linking this activity to identify other fraudulently created accounts.

In total, **the bank uncovered a network of 425 mule accounts registered using stolen or synthetic identities.**

The bank was able to freeze these accounts and halt the campaign in real-time, notify the police to help with their investigation, and now has information to detect any future activity by these same fraudsters.

EARLY DETECTION IS KEY

Suspicious activity that **Fraudster Hunter** helps identify includes:

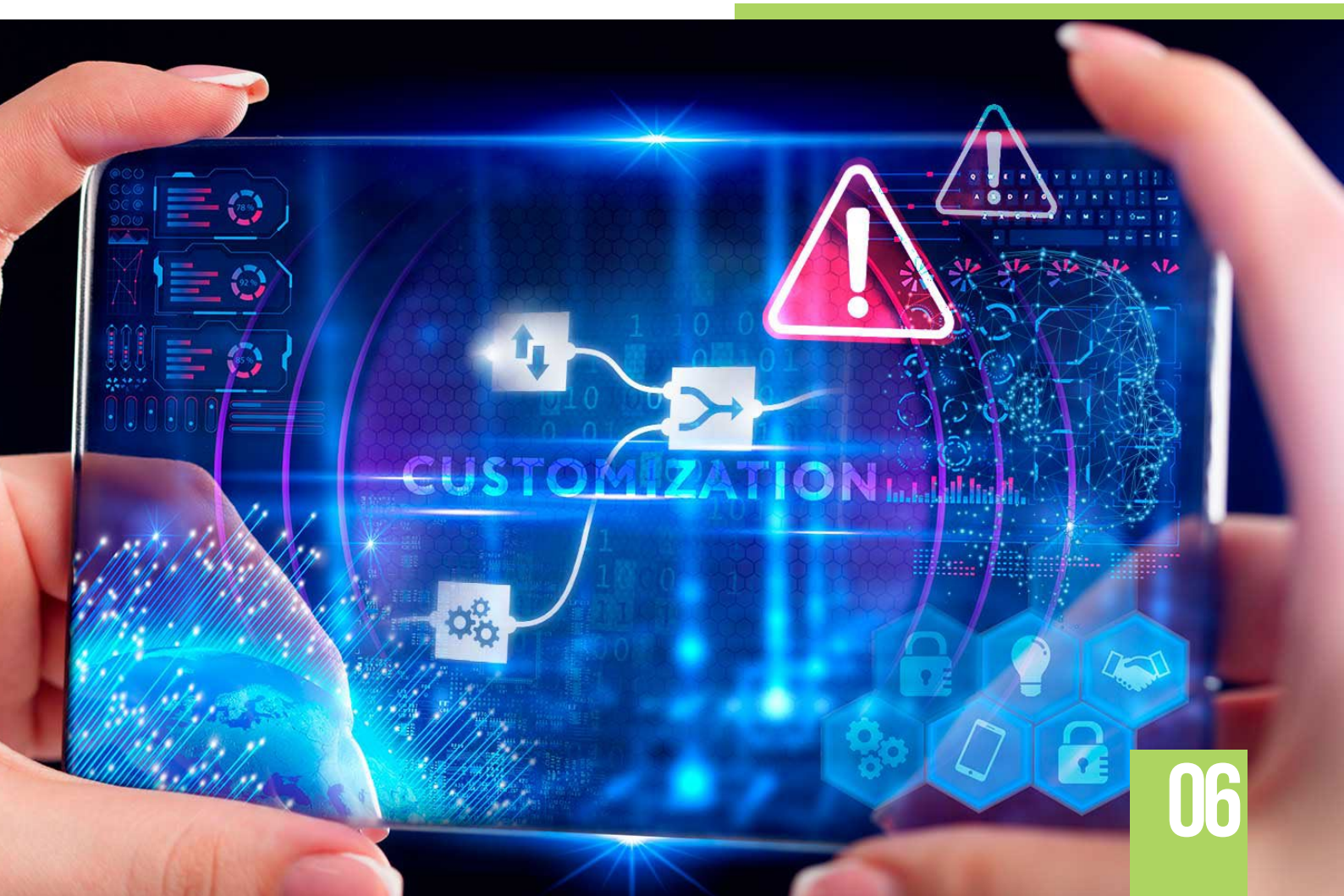
1. Dozens of individuals using the same infrastructure on the same day and in the same timeframe. This could suggest **an attacker is stealing from several victims in a single working day.**

2. One device, multiple unrelated accounts being accessed at rapid speeds, which could indicate **a bot testing stolen credentials** obtained through a phishing campaign or purchased online.

3. **One account, multiple BionicIDs:** Each account holder should have unique biometric identifiers, but what if you see more than one biometric behaviour pattern in them? It could be a couple sharing the account, or it could be an attacker impersonating the account holder using stolen credentials.

4. **One BionicID, multiple accounts:** Here the bank would see the same bionic profile appear in several accounts, i.e. the same individual has accessed all of them. This may be legitimate if they are corporate accounts managed by an external agency. But it could also be a clue that the same attacker is accessing multiple victim accounts. Some of these accounts may even be the attacker's own — registered to help them with reconnaissance. By locating this account, the bank could unmask the attacker.

As we've seen, individual cases might not always reveal fraud, but they can at least **generate a transaction risk score indicating a bank should take action.** This could be in the form of extra ID checks, further investigations or even account suspension. It's all about improving transparency at a more strategic level to better mitigate fraud risk.



THE NETWORK EFFECT

The value of **Fraudster Hunter and BionicIDs** go way beyond helping individual financial institutions eliminate professional fraudsters.

The challenge for the industry as a whole is that fraud gangs will focus on a single institution, drain it of as much cash as possible before they are discovered, and then simply move on to the next one.

To break this vicious cycle, the financial services industry must enhance global collaborative efforts with improved information sharing.

This has historically been a challenge: commercial entities loath to give their rivals a potential competitive advantage by admitting fraud losses and sharing potentially sensitive proprietary information.

However, BionicID data without any associated and problematic personally identifiable information offers a real opportunity for banks to benefit from a more open approach.

By sharing and utilising this data it then can be used to proactively stop fraudsters from moving unimpeded from one institution to another.

Using **Fraudster Hunter**'s active fraud alerting capability loaded with shared fraudster BionicID data there's no way a fraud operator can shake their permanent digital DNA imprint, so forewarned and forearmed with this information, banks could:

1. Minimise the impact of fraud on legitimate customers.
2. Reduce their own digital attack surface.
3. Act pre-emptively to block fraud from day zero.
4. Set honeytraps that can be used to detect and counteract fraudsters' reconnaissance efforts and attacks against other banking customers.
5. Share account registration details, identities and locations with international police to show there are real world consequences to online fraud.
6. Make fraud less profitable and riskier for the perpetrators, potentially deterring some of them.

This is just the beginning. BionicIDs and **Fraudster Hunter** could be applied in a range of scenarios outside of the banking fraud space, from e-commerce CNP transactions to policing account access across a range of online services. It's time to gain a strategic advantage over fraudsters and stop playing in defence.

To find out more about **Fraudster Hunter** and buguroo's comprehensive range of banking fraud detection solutions, please visit our website.

www.buguroo.com

EUROPE OFFICES

MADRID
CALLE ANABEL SEGURA, 16
EDIFICIO 3 PLANTA 4ª
ALCOBENDAS, 28108
(+34) 91 229 43 49
SPAIN

LONDON
6 HAYS LANE
LONDON · GREATER LONDON
LONDON BRIDGE · SE1 2HB
(+44) 20 3300 1606
UNITED KINGDOM

KATOWICE
UL. UNIWERSYTECKA 20
4TH FLOOR · 40-007
POLAND

LATAM OFFICES

MEXICO CITY
AV. RÍO MISISIPI, 49 06500
(+52) 41600149
MEXICO

BOGOTA DC
CARRERA 12A #78-40110221
COLOMBIA

SAO PAULO
AV. PAULISTA, 37 - 4º ANDAR01310-100
BRAZIL

NORTH AMERICA OFFICES

MIAMI
7950 NW 53RD STREET
FLORIDA, 33166
US