NORSE

SOLUTION BRIEF

Account Origination Fraud: A Growing Threat to Institutions and Consumers

Live Attack Intelligence Defends Against Fraudulent New Accounts

New account fraud increasingly threatens financial institutions and consumer banking customers. According to Javelin's 2013 Identity Fraud Report, this type of fraud has risen by 50%, with $9.8 billion in losses.

On the Rise and Difficult to Detect

One of the fastest-growing areas of fraud is account origination fraud. Defined as the use of stolen or fake identities to create new accounts, account origination fraud is difficult to detect.

Relying on the anonymity of the financial services institution's Internet channel, fraudsters use stolen and fake identities to create new bank or credit card accounts, submit applications or request quotes for loans, insurance or other virtual products that can be quickly turned into cash. As soon as fraudsters create a set of new fraudulent accounts, they move quickly to exploit them, making detection and recovery of assets difficult.

While many companies turn to verification tools to respond to the threat of account origination fraud, many of these tools involve labor-intensive processes. As ever-faster-moving techniques for monetizing fraud emerge, these processes can no longer keep pace. What companies need is a system that can identify patterns of fraud and respond, in real-time, to indicators of account creation that pose real risk—all while allowing legitimate users to seamlessly access services.

The damage from new account fraud is not limited to just the stolen funds, goods, and lost revenue. The theft itself and the inconvenience it creates for legitimate users can result in loss of consumer confidence and trust. The resulting consequences, including damage to brands and to organizations' reputations, can have lasting impact.

Geolocation – Knowing Your Enemy

Knowing your enemy is the start to fighting any battle. As a result, it has become increasingly important for online businesses to know where their web visitors are located in order to make real-time decisions to prevent fraud by allowing or denying new account registrations.

Geolocation - the technique of determining the actual location of a particular IP address - has been increasingly used to combat new account fraud. Geolocation calculates the distance between a physical billing address and the IP address where a transaction is initiated to determine whether it is likely to be fraudulent. The greater the distance, the greater the likelihood of fraud.

For example, if a request to open an account under the name of a customer living in Charlotte, North Carolina is initiated from Romania, a typical geolocation solution would indicate the transaction as having a higher likelihood of fraud than one initiated from Charlotte. The geolocation calculation returns a risk score or rating to the bank that can then be used to allow or deny the new account.Norse live attack intelligence enables organizations to instantly assess the risk level and threat profiles of any IP address visiting a web page, attempting an account log-in, originating a new account application, or initiating an online transaction. The Norse DarkMatter live attack intelligence platform continuously detects millions of in-the-wild IP risk factors. Within 5 seconds each risk factor is systematically analyzed, categorized, added to an IP's timeline and history, and available as IP Intelligence.

The end result is a trail of information and history for any given IP address to reveal negative, unethical, or illegal behavior. Up to 1,500 data points are compiled by Norse per IP address and can be used to identify threats in near real-time, giving financial organizations a new layer to their security and anti-fraud controls that proactively adapts to the evolving threat landscape to enhance existing perimeter security, website security, fraud prevention, and zero-day threat migration.

Stopping New Account Fraud Requires Live Intelligence

Today, cyber criminals rapidly change the origin of their attacks and hide their true location and identity using virtualized servers, on-demand public cloud infrastructure, and anonymizing proxies such as the Tor network. Needing only minutes to register a new

account, cyber criminals quickly set up accounts to orchestrate fraudulent transactions, and just as quickly bring them down — making it nearly impossible to accurately trace the fraud back to its actual source.

Effectively detecting and stopping sophisticated account origination fraud therefore requires a live, threat intelligence-based approach that empowers financial services organizations to assess the risk level of any transaction in milliseconds.

Norse Live Attack Intelligence – The Missing Layer of Security

While existing technologies and solutions are in many cases a good foundation for a layered fraud prevention program, one critical element is missing: live attack intelligence.

Norse live attack intelligence enables organizations to instantly assess the risk level and threat profile of any IP address visiting a web page, attempting an account log-in, originating a new account application, or initiating an online transaction – adding a new layer to their security and anti-fraud controls that proactively adapts to the evolving threat landscape. Using criteria as simple as the Norse IPQ score, or multiple risk factors and geolocation, organizations can build granular policies and rules to assess and mitigate fraud and security risks.

Key Features of Norse Solutions

- SaaS-based solution delivers live threat and fraud intelligence
- Configurable IPQ Risk Score allows easy implementation of risk-weighted decisions and controls
- Contextual risk categories enable creation of rules and polices unique to your business
- Geofilter and GeoMatch scoring identifies fraud by geographical attributes
- Flexible REST API enables rapid, light-weight integration and deployment
- Powerful analytics provide rich and comprehensive reporting data

Key Benefits for Financial Services Organizations

- Prevents fraudulent account registrations from stolen customer identities
- Reduces direct fraud losses
- Reduces the indirect costs of fraud such as: customer service, fraud investigation, customer litigation, risk of regulatory fines, and damage to brand image and reputation

How to Buy

DarkList is available as an annual subscription based on company size. Call Norse sales at +1 972.333.0622 for a demonstration or quote, or email us at sales@norse-corp.com

DarkViking is available as an annual subscription based on company size. Call Norse sales at +1 972.333.0622 for a demonstration or quote, or email us at sales@norse-corp.com

DarkWatch is available as a bundled 1U hardware and virtual appliance, and volume discounts are available. Call Norse sales at +1 972.333.0622 for a demonstration or quote, or email us a sales@norse-corp.com

Silicon Valley
1825 South Grant Street, Suite 635
San Mateo, CA 94402 | 650.513.2881

Saint Louis
101 South Hanley Road, Suite 1300
St. Louis, MO 63105 | 314.480.6450

ABOUT NORSE

Norse is the global leader in live attack intelligence. Norse delivers continuously-updated and unique Internet and darknet intel that helps organizations detect and block attacks that other systems miss. The superior Norse DarkMatter™ platform detects new threats and tags nascent hazards long before they're spotted by traditional "threat intelligence" tools. Norse's globally distributed "distant early warning" grid of millions of sensors, honeypots, crawlers and agents deliver unique visibility into the Internet – especially the darknets, where bad actors operate. The Norse DarkMatter™ network processes hundreds of terabytes daily and computes over 1,500 distinct risk factors, live, for millions of IP addresses every day. Norse products tightly integrate with popular SIEM, IPS and next-generation Firewall products to dramatically improve the performance, catch-rate and security return-on-investment of your existing infrastructure.

© 2014, Norse Corporation. All rights reserved.