NORSE

SOLUTION BRIEF

eCommerce Fraud: Growing in Scale, Sophistication, Cost

Live Attack Intelligence Empowers eRetailers to Fight eCommerce Fraud

According to Cyber Source's 2013 Online Payment Fraud Trends report, the estimated fraud cost for online retailers increased over the past two years to reach an estimated $3.5 billion, representing 0.9% of total online revenue and an average fraud rate by order of 0.8%.

Rise in eCommerce Gives Rise to Fraud

ECommerce sales continue to grow at a rapid pace and US sales are expected to reach $262 billion in 2013 and $370 billion by 2017. Meanwhile, eCommerce sales in Western Europe are expected to grow even faster.[1]

The rise in eCommerce and the introduction of mobile payment technologies presents immense growth opportunities for online merchants worldwide, as it is becoming easier for consumers to spend their money anywhere, at any time. Unfortunately, as eCommerce grows, so does fraud.

Growing in Scale, Sophistication

The rise in the sophistication of fraud is cause for alarm. Fraudsters have evolved their efforts by increasing automation and creating malnets. With their immense distributed power, malnets pose a significant threat to eCommerce. Leveraging these technologies, fraudsters are able to rapidly change locations to avoid being traced and initiate transactions from locations that seem to be legitimate or may even be the cardholder's actual compromised computer – a type of fraud known as Clean Fraud. The end result is that many fraudulent eCommerce transactions appear to be legitimate and circumvent traditional anti-fraud methods.

Mobile Fraud an Emerging Threat

Mobile Fraud is an emerging threat as many mobile devices are vulnerable to malware that can steal credit card account data and other confidential information.

Validation tools available through the web are not as effective for mobile and most merchants have not yet established stronger user-authentication for their customers' mobile devices. Because less consumer payment and personal information, which can be analyzed to ensure it correlates with a genuine customer, is required for a payment to occur, mobile can be an easier channel for fraudsters to exploit.

Traditional Defenses Fall Short

Determining whether a transaction is legitimate or fraudulent and deciding whether to approve or reject a transaction is a critical moment in eCommerce. Overly stringent measures may trap fraudulent transactions, but may also block and alienate genuine customers.

Merchants use a variety of automated fraud management techniques, such as fraud-scoring calculators, device fingerprinting, order velocity, multi-merchant data, and analysis of anonymous or free email accounts. In addition, most merchants manually review orders. Yet despite these efforts, they remain challenged in their abilities to protect against fraud attacks, maintain a positive customer experience, and keep costs in line.

Combating eCommerce Fraud Requires Live Intelligence

Today, cyber criminals rapidly change the origin of their attacks and hide their true location and identity using virtualized servers, public cloud infrastructure, and anonymizing proxies such as the Tor network. Needing only minutes, fraudsters quickly set up connections to shop and place orders, and just as quickly bring them down — making it nearly impossible to accurately trace the activity back to its actual source. Effectively detecting and stopping eCommerce fraud therefore requires a live, threat intelligence-based approach that empowers online merchants to assess the risk level of any transaction in milliseconds.

SOLUTION BRIEF

Norse Live Attack Intelligence – The Missing Layer of Security

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

The most effective way to reduce eCommerce fraud is to leverage Norse live attack intelligence. Using a custom integration via the DarkViking API, online merchants obtain a highly accurate live risk assessment of any eCommerce transaction within milliseconds.

Norse's ability to identify and block anonymized IP addresses and dozens of other fraud risk factors protects merchants and processors from the most advanced online fraud techniques.

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 eCommerce Organizations

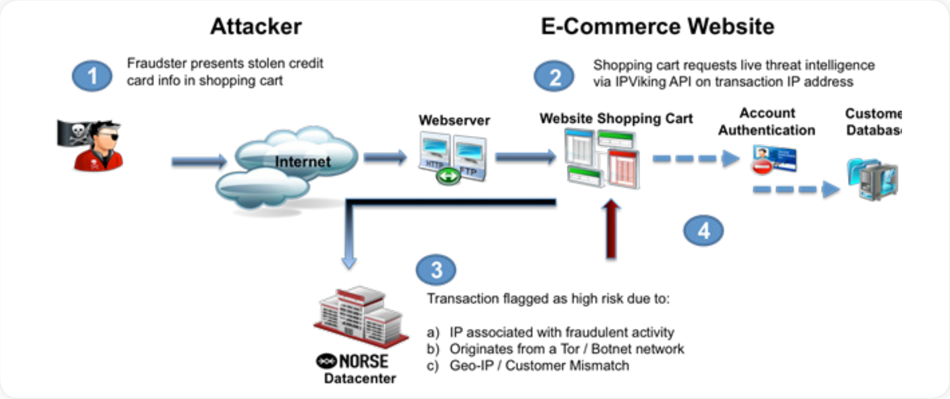
- Prevents fraudulent account registrations from stolen customer identities
- Reduces direct fraud losses
- Reduces the indirect costs of fraud such as; customer service, fraud investigation, customer litigation, risk of regulatory fines, and damage to brand image and reputation.

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


Attacker
E-Commerce Website
1
Fraudster presents stolen credit card info in shopping cart
2
Shopping cart requests live threat intelligence via IPViking API on transaction IP address
Internet
Webserver
HTTP
FTP
Website Shopping Cart
Account Authentication
Custome Databas
4
3
Transaction flagged as high risk due to:
a) IP associated with fraudulent activity
b) Originates from a Tor / Botnet network
c) Geo-IP / Customer Mismatch
NORSE Datacenter

Norse IPViking can be easily integrated into any merchant's payment flow via its simple, flexible REST API.

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

norse-corp.com

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.