NORSE

SOLUTION BRIEF

Account Takeover: A Complex and Growing Problem

Live Attack Intelligence enables new solutions for fighting online fraud

A recent Javelin study estimated losses from account takeover fraud to be over $4.9 billion in 2012, representing a 69 percent increase over 2011. In addition to financial damages, account takeover fraud can lead to loss of consumer trust, damage brand reputation and jeopardize compliance with industry regulations.

Refined Techniques of Attack

Account takeover attempts are on the rise and the increased diversity and sophistication of tactics has in many cases overwhelmed legacy security and anti-fraud technologies. Efforts to prevent losses associated with account takeover and online fraud have proved temporary as cyber criminals adapt quickly to new anti-fraud measures and security controls. Although there are several methods being employed to steal credentials, the most prevalent involves malware that is commonly distributed via email links, social networking sites and malicious websites. Using the power of malware-based botnets, cyber criminals compromise customer's computers, enterprise networks, websites, and applications to steal consumers' usernames, passwords, and private information. Many actually buy and sell usernames, passwords, and credit card information with other criminals in a thriving black market.

Using the stolen credentials, cyber criminals hijack email, social media, financial, and other accounts to launch their attacks anonymously through zombie computers behind proxy networks – or even from the customer's own compromised computer. Because the access attempts use the right username and password, include other valid account details that make the request seem legitimate, and appear to be coming from the right device, businesses are challenged in their ability to ensure the true party is accessing the account.

Bypassing Traditional Defenses

Financial institutions employ a variety of techniques to hamper the efforts of cyber criminals. Customer-facing solutions include security tokens and "one time password" technology. Because some 40 percent of personal computers are infected, "out of band verification" in the form of a phone call or text message is viewed as the most secure way to authenticate a user and has become an industry best practice for verifying access. Several types of advanced malware have already been shown to bypass multifactor authentication however. These out of band authenticaions also add additional steps to the login process often frustrating users and degrading the customer experience.

Other anti-fraud technologies such as device identification and web session analysis can be used to detect login attempts from unknown or suspicious devices and anomolies in the user's web browsing patterns. Unfortunately, these techniques all have limitations that enable today's more sophisticated threats to regularly bypass them. Consequently, despite these anti-fraud initiatives, too many organizations are falling short of truly effective protection against account takeover and other financial fraud.

Combating Account Takeover 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, anonymizing proxies such as the Tor network. Needing only hours or even minutes to carry out an attack, cyber criminals quickly set up attacks to orchestrate fraudulent transactions, and just as quickly bring them down — making it nearly impossible to accurately trace the attack back to its actual source. Effectively detecting and stopping sophisticated account takeover 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

SOLUTION BRIEF

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, today one critical element is missing: live threat 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 geo-location, organizations can build granular policies and rules to assess and mitigate fraud and security risks.

Key Features of Norse Solutions

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

Key Benefits for Financial Services Organizations

- Reduced customer account takeover fraud via stolen credentials
- Lowers the cost of direct fraud, customer service, and fraud investigation
- Reduced costs from fraudulent account creations
- Improved customer experience by minimizing out of band authentications

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.