NORSE

CASE STUDY

DARKVIKING™ Live Attack Intelligence Stops Tor-based Financial Cyber Attack Saving Political Campaign over $400K in Fraud.

Quick Facts:

- Duration of Attack: **4 months**
- Unique Accounts Used: **3,374**
- Frauds Attempted: **3,446**
- Frauds Detected by DarkViking: **3,446**
- Unique Tor Exit Nodes Used: **109**
- $ At Risk: **$403,000**
- $ At Risk Saved: **$403,000**

In 2012, a political campaign's fund-raising web site became the target of a sophisticated, automated attack that continued for months. The attack co-opted global published and non-published Tor exit nodes to seed the campaign's donation system with fraudulent transactions using stolen and otherwise compromised credit and debit card data. Significant losses accrued from more than 1,500 fraudulent transactions in April 2012 before campaign staff identified DarkViking as a solution.

The attack illustrates a new, alarming trend. While the perpetrators of this long term, concerted attack might never be identified, it is possible that this represents the emergence organized financial cyber crime as a tactic for groups wanting to make political statements or punish politicians for their actions.

The Challenge

The attack against the political fund raising site used sophisticated, automated scripts that were specifically designed to workwith the target site's financial system.In addition to gathering key information about how the target site worked, the attack was also characterized by:

- Thousands of unique credit and debit card details. The attack was distinguished by the use of credit card account information that looked legitimate enough to spoof some typical forms of fraud detection.
- Numerous unique Tor exit nodes. 109 unique and undocumented Tor exit nodes provided attack launch points from which the attackers could not be traced.
- Strategically placed botnet command and control points. While specific points oforigin were obfuscated with Tor anonymization, the pattern of attack required a distributed, orchestrated effort.

Tor (The Onion Router)

Maintained by global volunteers, Tor is a distributed network of relays that provides anonymity to users. Created for legitimate privacy protection, Tor has anonymizing capacity that has become a popular tool with anti-censorship activists and dissidents in countries that monitor and censor Internet activities.

In spite of Tor's legitimate uses, unregistered Tor exit nodes can be

exploited as a “back door” in accessing zombies to create botnets and orchestrating seemingly legitimate (but malicious) connections to servers using port 80. Known as the darknet or dark web, the use of such schemes pose an increasing threat to Internet commerce.

The Solution

The DarkMatter live attack intelligence network includes millions of physical and virtual agents around the globe to gather live security intelligence on malicious and high-risk netw traffic. Norse continuously analyzes live traffic and attack data using powerful algorithms that assess 1,500 different risk factors, calculating Norse’s proprietary IPQ risk score within microseconds, enabling a live risk assessment to be calculated within microseconds.

With its network providing instantaneous cyber threat and risk intelligence, Norse is unique in its ability to provide an extremely accurate, live risk assessment of any ecommerce transaction via the IP address, identifying in seconds addresses being anonymized via Tor exit nodes and other proxy servers, in addition to dozens of other fraud risk factors.

Norse live attack intelligence is easy to integrate into an online payment flow. Within hours, the campaign was able to seamlessly implement it and eliminate the threat to its fundraising efforts. DarkViking’s extremely flexible implmentation options enable it to be quickly integrated into websites, e-commerce and payment systems, web logon forms and authentication systems, as well as programable network devices and appliances.

Results:

After embedding DarkViking into the payment gateway, financial losses fell to zero out of 3,446 fraudulent transaction attempts. By blocking these fraudulent attempts, DarkViking prevented more that $317,000 in direct losses, plus more than $86,000 in indirect losses through chargeback fees and fines from June to October 2012.

How to Buy

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

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.