NORSE

INDUSTRY BRIEF

Reducing the Risk of Cyber Attacks to Transportation & Logistics Organizations with Live Attack Intelligence

Transportation & logistics organizations must look beyond traditional defenses to protect against advanced attacks and data breaches.

The Stuxnet worm is perhaps the most well known supply chain digital attack, designed to attack industrial Programmable Logic Controllers (PLCs) in nuclear centrifuges. Since the PLCs themselves weren't connected to the Internet, the attackers instead focused on several points of the supply chain. It is believed that a maintenance worker was able to insert the worm, which is believed to have destroyed one fifth of Iran's nuclear centrifuges.

Transportation and Logistics is an Increasingly Valuable Target for Attackers

While financial services, retail, and government organizations generate most of the media headlines, transportation and logistics are increasingly targets for cyberattacks. It's not surprising, as the transportation & logistics sector is integral to the world's economies, and cyberattacks could have disruptive, unpredictable, devastating effects:

» **Direct financial costs** of incident response, IT forensics, remediation, and services provided to victims

» **Theft** of research and intellectual property

» **Loss of reputation**

Attackers always look for the weakest points of entry, and increasingly those points are in the supply chain. Organizations in the transportation and logistics sector are particularly critical, because successful cyberattacks could lead to physical damage. According to a Price Waterhouse Coopers report, "Cyber attacks inducing physical damage are an increasing threat for the transportation and logistics industry."[1]

Rapidly Changing Attacks Add To Defense Complexity

Transportation & logistics are prime targets for a variety of bad actors each with different motivations and attack vectors including:

» **Cybercriminals** motivated by financial gain targeting valuable personal and financial information

» **Hacktivists** motivated by political and social causes

» **Industry and nation state** sponsored actors targeting confidential research and intellectual property.

With multiple new attack vectors and a rapidly evolving threat landscape, bad actors now use advanced malware and highly targeted attack techniques such as:

» **Targeting** known and zero day vulnerabilities in organizations' website

» **Breaching** perimeter security defenses to directly access critical servers and systems

» **Compromising** user accounts through phishing and credential-stealing malware

Cybercriminals today use a combination of advanced and targeted attacks such as spear-phishing, Trojans, Man-in-the-Browser attacks, and the use of anonymous proxies such as TOR to mask the true origin of an attack and the locations of botnet command and control servers.

Traditional Controls Not Keeping Up

Traditional security controls used in a layered security strategy have not fully protected transportation and logistics organizations and have proven to be static in their defense. They lack the adaptability to proactively defend against the speed and sophistication of new advanced malware, insider and zero-day threats, and the use of Tor and anonymous proxies to hide and anonymize malicious network activity.

[1] http://www.pwc.com/en_GX/gx/transportation-logistics/pdf/TL2030_vol.4_web.pdf

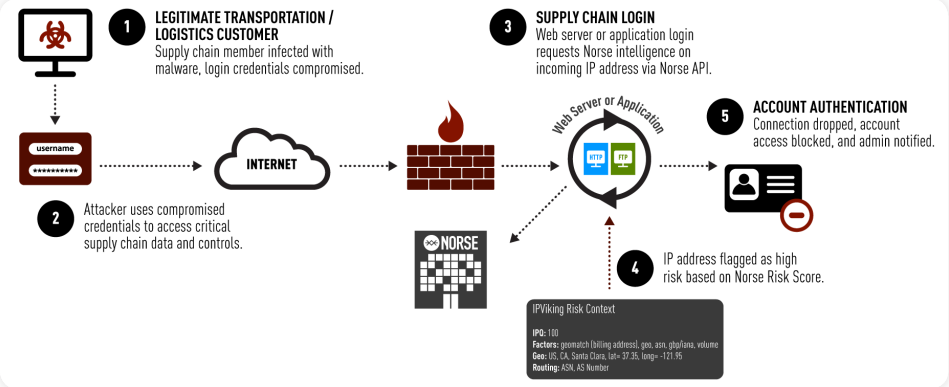
IP reputation-based technology are sometimes utilized as a means to identify and block connections from known bad IP addresses, however, these solutions have a binary approach to blocking risky IPs and are rarely up to date, causing false positives. Security intelligence traditionally collected by vendors via customer logs and aggregation of open source blocking lists prevents them from keeping pace with the multitude of attack vectors or the speed with which IP address risk levels and threat characteristics can change.

Threat Intelligence to Accurately Assess True Risk

To effectively combat this ever-changing threat landscape requires security intelligence beyond static rules and policies and traditional IP and URL blocklists. It requires threat and attack intelligence that is live, contextual, and that provides visibility into network traffic from darknets and anonymous proxy services such as Tor – identifying the sources of threats and malicious attacks as they happen.

The Norse DarkMatter™ live attack intelligence platform continuously detects millions of in-the-wild IP risk factors from the Internet's darknets and the deep web. Up to 1,500 data points are used by Norse to identify threats in as they happen. Within 5 seconds this data is analyzed, processed and available to organizations via a RESTful API.

The end result is a new proactive layer in the security stack that proactively adapts to the evolving threat landscape, enhancing existing perimeter, web, and authentication security controls. When integrated with a SIEM or big data security analytics system Norse enables the correlation of internal network events with external threats to rapidly detect advanced malware and threats missed by conventional signature-based anti-malware solutions.



Use Case:
Account Takeover Protection

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.