The Evolution of the Threat Landscape and the Need for a Live Intelligence-based Approach to Security

IPVIKING™

WHITE PAPER

Executive Summary

While there is little debate that enterprise networks are in a constant state of growth and change, arguably the most significant transformations have occurred in just the past five to seven years. While just a few years ago the network was comprised of primarily corporate-owned devices connecting to corporate servers accessing corporate applications inside a well-defined and secured network perimeter, today it is hard to tell where a corporate network starts and where it ends. Today's highly mobile and remote workforces demand worldwide round-the-clock connectivity to corporate email, applications, and data from a wide variety of corporate and increasingly personally owned devices. These devices also access myriad web, mobile, and social applications, most of which are hosted and delivered from servers in the cloud, outside the corporate network.

While these recent trends have improved network efficiency and worker productivity, they have also significantly increased network complexity and vulnerability, putting network administrators in a daily struggle to balance accessibility with security. Capitalizing on trends like cloud computing, the social web, mobile computing, BYOD, and the resulting collapse of the network perimeter, hackers and cyber criminals are increasingly exploiting new attack vectors using highly sophisticated and automated techniques. Using virtualized servers, cloud hosting, and botnets they rapidly change their network location, unleashing drive-by and targeted zero-day attacks from virtually anywhere in the world. The consequence is that traditional signature and policy-based defenses such as firewall, IPS-IDS, anti-malware, and authentication systems have become less and less effective, allowing hackers to gain unauthorized access to corporate networks, resources, and data — at times seemingly at will.

In this paper we examine some of the major enterprise technology trends of the last 10 years and how they have changed the cyber-threat landscape, reducing the efficacy of traditional security solutions and driving the need for a new more intelligence-based approach to security. Finally, we explore some of the new criteria enterprises must use to evaluate threat intelligence providers and ways in which enterprises can begin to implement intelligence-based security strategies today using Norse Live Threat Intelligence.

The New Actors and Their Motivations

In the not so distant past, "cyber attacks" and "computer viruses" were largely the work of teens and young adults, whose motivations were often simply the challenge, the thrill of making news headlines, and perhaps impressing their friends. Today, organizations are being attacked by and must protect against several types of different actors with more varied, complex, and less obvious motivations than usually associated with the mainstream image of a "hacker."

Cyber Criminals

As quickly as broadband Internet, eCommerce, and online banking have evolved over the last decade, so has cyber-crime and online fraud. Cyber criminals have traditionally been purely profit-motivated, often associated with organized crime, and engaged primarily in eCommerce and bank fraud. While nefarious, their motivations were relatively simple and easy to understand. This enabled information security and anti-fraud professionals and technology solutions providers to focus their efforts on securing the attack vectors specific to eCommerce and financial transactions. While the industry was unsuccessful in preventing all fraud, a few years ago it was a manageable problem.

The Rise of Hacktivism

Today, many of the most damaging and high profile attacks are launched by what are known as "hacktivist" organizations. These are loosely defined groups of individuals, many of whom possess exceptional software engineering skills. They use their hacking and malware writing abilities to make political and social statements; supports causes; and harass or punish corporations, governments, politicians, and individuals. This more recent phenomenon has added a new level of complexity and nuance to the possible motivations for and objectives of an attack and gives corporations and high-profile individuals a new set of concerns with regard to their public statements and policies. While there is no easy answer for how to protect against hacktivist attacks, it is clear that high profile organizations must take this new threat seriously. Specifically C-suites and boards should review their communication and approval processes with regard to decisions and public statements with the potential to provoke an attack.

State-sponsored Attackers

Lastly, many organizations now have to worry about cyber attacks sponsored by nation states. Here the motivations are varied but are most often associated with intellectual property theft and corporate, government, and military espionage. State-sponsored attacks are especially troublesome since the hackers are well funded, able to operate with immunity within their country, and able to carry out very targeted attacks over long periods of time to meet their objectives. Aside from the target organizations themselves, the vendors and suppliers to these organizations are increasingly being targeted as another way to penetrate the target organization. Large organizations at risk of state-sponsored attacks should therefore create and enforce security policies and procedures for employees, partners, and supplier vendors to reduce the risk of compromise through extranet and social engineering based attack vectors.

Understanding the "New Threats"

Much like traditional warfare, protecting against conventional Internet threats has usually been relatively clear-cut, with obvious, known players; malware or hackers on one side, and individuals or business networks on the other. In most cases, we had known "good guys" and "bad guys," and as a result, even when threats became more complex, at least IT knew who and what they were up against. But fighting today's threats is far more difficult. Today's threats are stealthy by design, and can be launched from anywhere, including legitimate, well-known applications and websites that have been compromised. For these reasons it's usually not clear who the enemy is or from where they might launch their next attack.

Traditional attacks have historically been levied through vectors such as email attachments, downloaded software, browser vulnerabilities, and fraudulent websites. Though these could certainly be complex and have at times proven to be problematic for IT administrators, each could be identified as a bad actor, website, or malware using policy, signature, and black list-based defenses.

In contrast, many of today's attacks come from legitimate, well-known sites including banks, established retailers, and large corporations -- rendering traditional IP reputation and blacklists useless. By compromising and controlling the networks of these unsuspecting companies, hackers can leverage trusted networks to launch attacks and penetrate other organizations, all while evading detection. Other attacks employ IP proxies and anonymizers such as the Tor network to conceal their location and identity and easily circumvent many legacy security and fraud mechanisms.

Myriad Techniques

In addition to the increased volume, intensity, and complexity of modern-day attacks, the diversity of tactics has overwhelmed legacy security. Ranging from moderate nuisance to severe security threat, these are just some of the attacks that are infiltrating corporate networks today:

- **Cross-site Scripting.** Using vulnerabilities in web applications, hackers can compromise a trusted site. Since the client's browser already trusts the site, all content originating from it is deemed reliable, enabling malicious content to be sent undetected in the legitimate traffic stream.

- **SQL and Code Injections.** Attackers enter partial SQL commands into web-based entry fields in an attempt to either change the content of the database, or send the attacker sensitive database information such as credit card data or passwords.

- **Watering Hole Attacks.** In this increasingly popular technique a hacker uses a well known and trusted website as a vector to refer and redirect visitors to another untrusted, malicious website. The malicious website then exploits existing or zero-day vulnerabilities in the visitors' web-browser to inject or download malware onto the computer before re-directing the visitor back to the original site.

- **Login Attacks.** Using advanced scripts, hackers can discover account user names, detect code flaws, or gain access to accounts by performing brute force or dictionary-style attacks that try the most common password/ID combinations.

- **Registration Spamming.** Wiki and blog sites are most susceptible to this growing problem, in which bots or spammers register profiles on the site, effectively "joining the community." Those profiles are then used for a variety of purposes, including posting advertising spam messages and spreading malware.

• **Contact Form or Comment Spam.** Similar to registration spamming, bots or spammers use web contact or comment forms to send or post spam or carry out exploits.

Hacking and Cybercrime Transformed

Virtualization; social, mobile, and cloud computing; open source software; and the declining costs of CPU power and bandwidth have transformed IT over the last 10 years and resulted in substantial productivity gains and cost savings for businesses. Unfortunately, hackers and cyber criminals have also benefited from and been empowered by these same innovations and trends. Virtualized servers, infrastructure as a service (IaaS), on-demand cloud hosting, free open source software, malware exploit kits, and botnets for rent have all changed the face of hacking and cybercrime.

Today most attacks are automated, and cyber criminals can rapidly setup and change their online locations, remotely launching attacks from virtually anywhere in the world. The net effect has been that the costs of cybercrime have been greatly reduced, while access to the knowledge, skills, tools, and resources to commit cybercrime has increased dramatically. This, combined with the sheer increase in the number of young well-educated and skilled software engineers in developing countries has created the "perfect storm" of cybercrime we see today.

Traditional Security

Traditional approaches to cyber security originally focused on vulnerability and threat detection and protection. Firewalls, authentication systems, anti-virus and other types of anti-malware products are examples of the first generation of IT security products developed during the late 1980s and 1990s in response to the vulnerabilities created by the mainstream adoption of the PC, enterprise networks, and the Internet. These approaches were fairly effective against the first generation of slow to evolve malware and cyber threats, but fundamentally reactive to new vulnerabilities and threats.

With the mainstream adoption of the Internet, web, and eCommerce in the late 90s and early 2000s, enterprise networks became more complex, more distributed, more difficult to maintain, and harder to defend against new emerging cyber threats. In response, security vendors developed network-based monitoring solutions such as intrusion detection and prevention systems designed to detect and prevent attacks in real-time. Additionally, security event monitoring systems were developed that collected, stored, and analyzed security event logs and other data, alerting IT personnel to suspicious events, producing security reports, executing pre-defined policy scripts. These systems were the precursors to today's advanced SIEM and big data security analytics solutions. While these systems did produce value for organizations, it tended to be in the form of policy management, compliance reporting, incident response, and forensics, rather than proactive detection and prevention of cyber threats.

The rise of mobile computing, the social web, and access to broadband and mobile Internet has become almost ubiquitous throughout even the developing world. This has enabled continuous digital communication with employees, customers, partners, and other stakeholders to become an absolute requirement of organizations wishing to participate in the 24X7 global business environment. These same channels used to deliver efficient, streamlined global communications have also provided cybercriminals with many of the new attack vectors and vulnerabilities that have enabled today's advanced cyber threats. This has transformed hacking, cybercrime, and the cyber threat landscape in the process and helped usher in the third wave of security innovation that is occurring today.

Intelligence-based Security - The Next Wave of Security Innovation

As noted earlier, the collapse of the network perimeter and the ability of new advanced threats to regularly by-pass traditional security solutions have fueled the need for a new security model, one that provides organizations with context-aware and risk-weighted security intelligence from which they can design automated systems capable of making accurate and effective decisions.

An intelligence-based approach to security provides enterprises greater flexibility in designing their security and anti-fraud strategies and enables solutions to be more tailored to a business' unique needs. Instead of being limited to the innate capabilities of traditional security products, intelligence-based security marries many different internal and external sources of threat data with big data analytics to produce, among other things, more accurate assessment of risk; more effective identification of anomalous behavior; more rapid detection and mitigation of compromise and breach; and security systems and business processes that are more intelligent, automated, and adaptive to the threat landscape than what is possible today.

While offering many seemingly obvious benefits over traditional security, the factors that will determine the efficacy and performance of intelligence-based security strategies may not be obvious or apparent to security teams trained in a traditional security mindset. With a plethora of security and threat feeds and solutions available, the challenge will be vetting and identifying the best vendors and solutions, and specifically the ones that best support an enterprise's specific uses cases and requirements.

Consequently, security professionals need to consider different factors and criteria when evaluating threat intelligence vendors and solutions. Among other factors, enterprises should consider:

- What percentage of data is directly acquired in the wild by the vendor and what percentage comes from external and third party sources?
- How are those external sources vetted in terms of quality control and data consistency?
- What is the depth and breadth of the data sets used to create the "intelligence?"
- What is the average amount of threat data analyzed per day?
- Is the data analyzed in real-time or batched?
- What is the latency between a threat/risk indicator being observed in the wild and it being available to customers?
- How is the intelligence consumed and made actionable and what integration options are available?

The Need for Live Intelligence

While security and threat intelligence feeds have been available for quite some time, the traditional tactics of "whitelisting" (allowing access to or from known trusted IP addresses, domains, URLs) and "blacklisting" (preventing traffic to or from IP addresses, domains and URLs known to be bad) have become increasingly ineffective. Blacklists and reputation feeds, usually created by aggregating log file data from service providers, enterprise network appliances, and security vendor's products, provide coverage of only a small part of the Internet, become out of date quickly, and provide little to no context about why an IP address, domain, or URL is "bad" or "good." Lack of context is one of the primary factors that has prevented these lists and feeds from being of more than marginal use and value to security professionals. Without context they get data but not intelligence that is actionable and which can be used to produce better decisions and business outcomes.

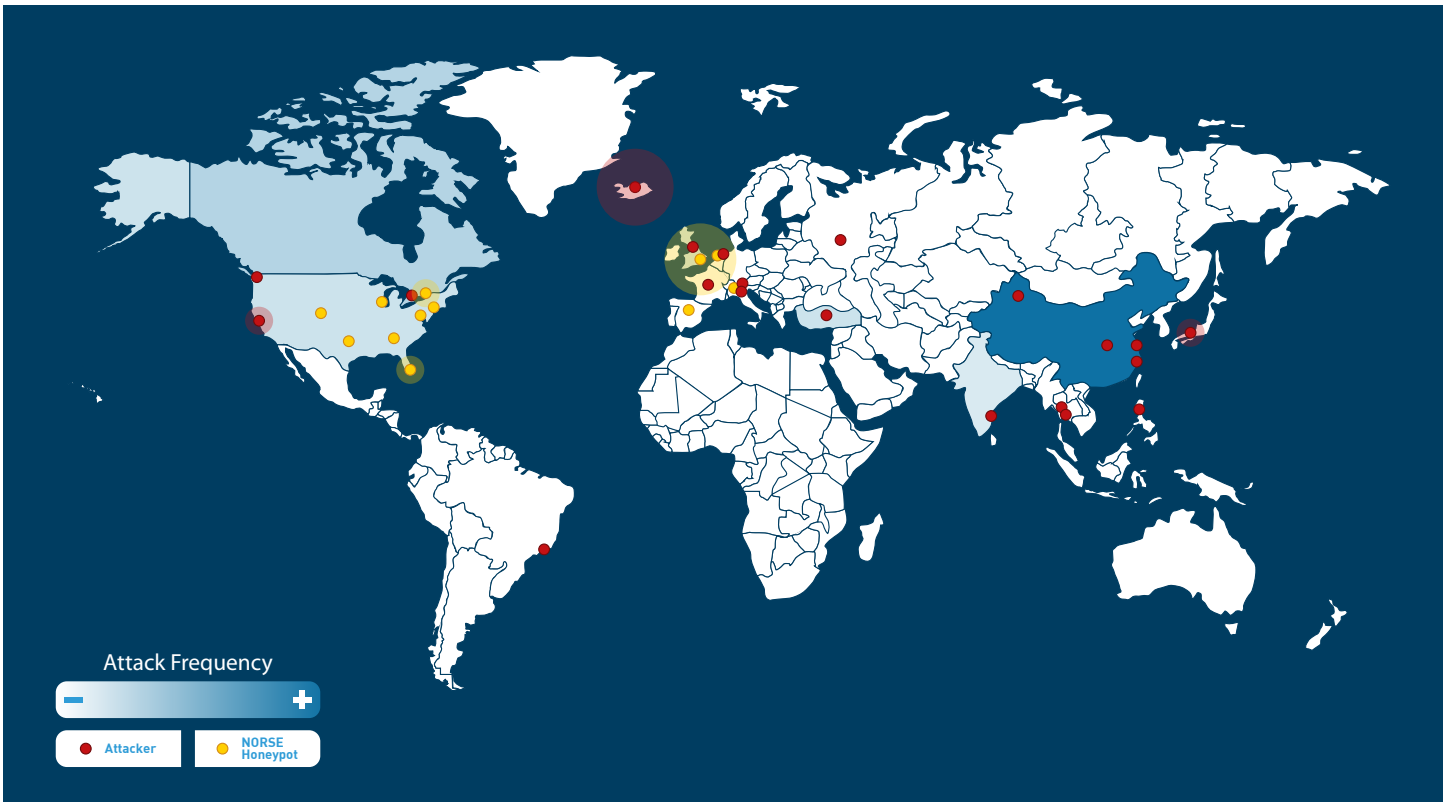
Over the last 5-7 years, bad actors have also learned to leverage technologies like virtualized servers, public cloud infrastructure, anonymizing proxies like the TOR network, and rentable botnets to rapidly change their IP address and obfuscate their true location and identity. Needing only hours or even minutes to carry out an attack, sophisticated cybercriminals change the origin of their attacks quickly, avoiding detection and making it nearly impossible to accurately trace an attack back to its actual source. Consequently, an IP address can go from good to bad, then back to good again in a matter of hours or even minutes. With over a billion active public IP addresses in use on a typical day, it becomes readily apparent how difficult it is to assess the risk and threat characteristics of real-time network connections on a global scale.

To provide global threat intelligence that is reliable, accurate, and fast enough to effectively block today's zero-day exploits and advanced threats requires a new approach. It's an approach that moves security beyond the points of attack, beyond the network hosts and websites, and beyond the traditional network perimeter. It moves security to the far reaches of the Internet; identifying live cyber attacks at their source, before they arrive at your network.

Given that, it begs the question, "Even with lots of data and powerful big data analytics, how can intelligence-based security solutions reliably protect against today's advanced threats, given the vast nature of the global Internet and the speed with which the cyber threat landscape evolves?" To quote an old adage "The devil is in the details." In the case of big data analytics and threat intelligence, "the devil is in the data."

Norse Live Threat Intelligence Platform

The Norse Live Threat Intelligence platform is a patent-pending infrastructure-based technology that continuously collects and analyzes vast amounts of live high-risk Internet traffic to identify compromised hosts, botnets, APTs, and other sources of cyber attack and online fraud. Using Norse's proprietary big data analytics platform, over 1,500 different threat and risk factors are used to provide a live risk score and deep contextual information providing visibility into the threat profile of any public IP address. Delivered in milliseconds via Norse's global high-speed delivery platform, the IPQ score and threat factor data enable highly effective solutions for online fraud prevention and protection from cyber attacks including zero-day exploits and Advanced Persistent Threats. In this section we examine the high level architecture and design considerations of the Norse platform and how it enables the delivery of threat intelligence that is live, contextual, and actionable.



The Norse platform continuously collects and analyzes live high risk Internet traffic identifying the sources of cyber attacks and fraud.

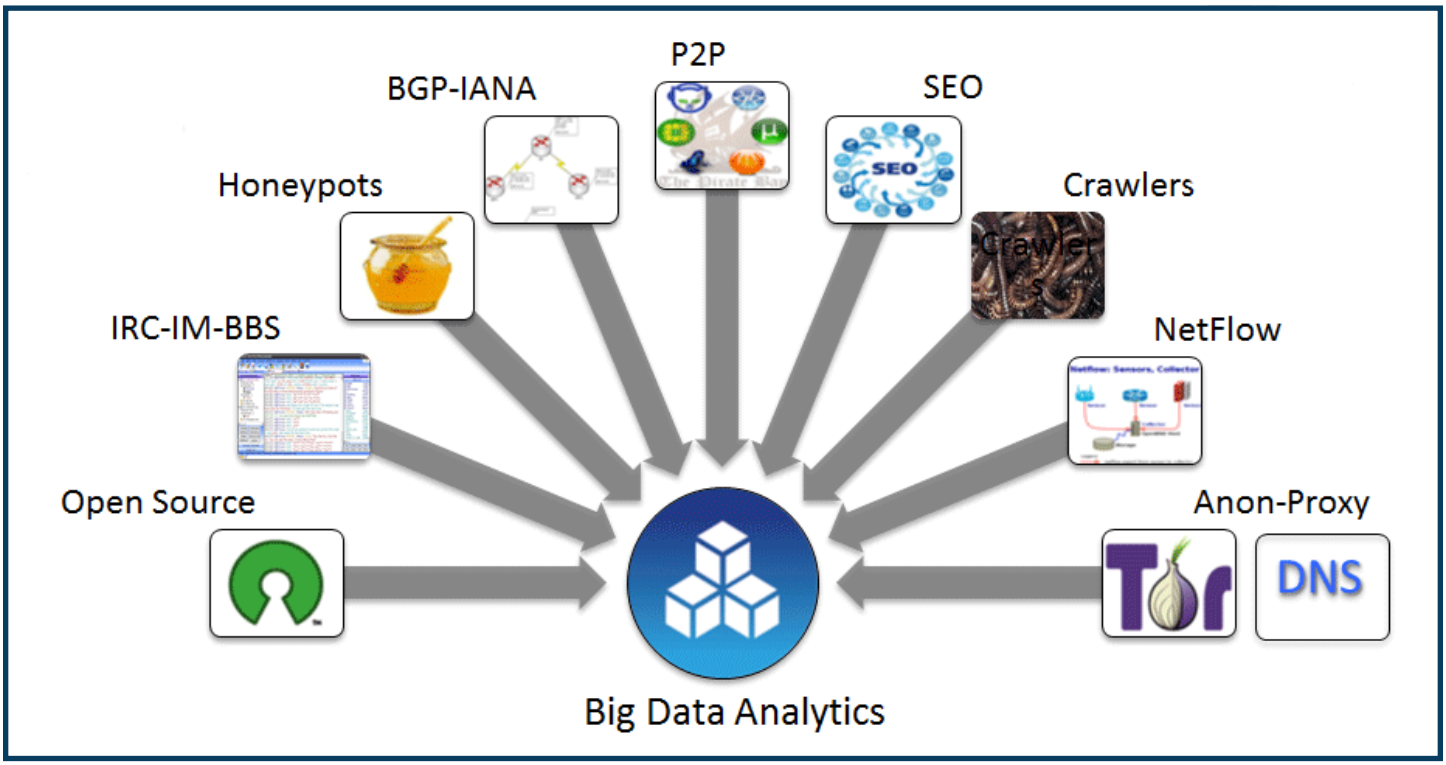
Global Coverage and Sample Rate

Gaining live contextual insight into the activity of bad actors on the Internet with the ability to provide full global IP space coverage is dependent on attaining broad Internet coverage and sample rates. Essentially this means how much geographically representative threat data is the platform able to collect and how fast is it able to process and analyze the data in order to make it available to customers as intelligence. To achieve this requires a massive globally distributed network infrastructure capable of continuously collecting and analyzing many terabytes of live cyber attack and high-risk network traffic every day. Not all data is created equal however. Equally important is what types of data are being collected and from where. Simply analyzing large amounts of data is not particularly valuable for providing threat intelligence if the data is largely "good" data. The Norse platform is therefore designed specifically to find and collect the Internet's "bad" or high-risk data and traffic.

Strategically Located Infrastructure

At the heart of the Norse platform are 16 core routers that sit on Tier 1 long haul fiber network rings. Norse owned infrastructure in over 140 strategically located data centers in more than 40 countries is used to collect the widest possible breadth of high risk data types and network traffic. This platform uses up to 16 Million IP addresses with coverage in every /8 aspect of the IPV4 space. Threat data is then fed to GPU calculation clusters in 40 global NOCs spread across 36 different countries.

This unique approach and platform architecture achieves massive global coverage and sample rate including the places where much of the new malware is born and first detected. The platform currently detects greater than 80% of the Internet's bad traffic and re-samples the entire IP range every few minutes.



The Norse platform is architected to maximize data breadth and depth providing a live contextual view into the Internet threat landscape.

Breadth and Depth of Data Collection

As stated earlier, for threat intelligence to be actionable and valuable requires big context, not just big data. To achieve big context and reduce the chances of false positives requires a high degree of data breadth as well as depth. The Norse platform was architected to enable the collection of many different types and sources of threat data. This comprehensive approach to breadth and depth of data enables Norse to provide enterprises with a highly accurate and effective risk score as well as the rich contextual data needed to design more granular polices and business processes.

The following are descriptions of the major data types and collection methods used by the Norse platform to achieve its objectives.

Honeypots
Norse Honeypots support the emulation of thousands of applications that appear as desirable targets for malware, bots, and hackers. Supporting both server and client configurations, Norse honeypots are continually accessed and attacked by compromised hosts, networks, and network connected devices. Client-based honeypots emulate browser-based actions causing compromised websites to reveal their malware. Emulating many different types of network infrastructure, protocols, and services, the platform creates 6-7 million concurrent transactions at any given time.

IRC
Internet Relay Chat is a popular method for exchanging ideas and plans among bad actors. By participating in these chats, the Norse platform is able to quickly gain intelligence on new and modified attack vectors.

BGP-IANA
Border Gateway Protocol is the routing protocol of the Internet. The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. By maintaining current copies of this information the Norse platform detects if an IP address is valid or bogus (bogon) or if a valid IP address has been hijacked or is being spoofed—all clear indicators of risk.

P2P
Peer-to-Peer connections are created without the need for a central server. P2P networks can be set up within the home, a business, or over the Internet. Participants who are interested in communicating without detection often set these up between interested parties. The Norse platform gains valuable information through its active participation in these networks.

SEO
Search Engine Optimization is a technique to gain rankings for specific criteria. By managing websites that score highly when people are looking for bad things, they expose themselves as bad actors to the Norse platform.

Crawlers
A crawler is a bot that systematically browses the web, typically for the purpose of indexing. Focusing on text-based documents, Norse's proprietary dark-net crawlers search for a wide range of text-based language that indicates potential malicious behavior.

NetFlow
The NetFlow protocol enables the Norse platform to see who is talking to whom across a network. By checking the IPQ score of the IP addresses at both ends of the connection, it is possible to identify bad actors and compromised hosts.

Anon-Proxy
Anonymous proxies are used to hide the identity of the participant. While originally designed to protect the innocent, they are now widely used to launch and mask cyber attacks. By understanding where all of the Tor exit nodes are at any given time, the Norse platform can assign a higher risk score to IP addresses anonymizing themselves. Also by offering free DNS services that do not log, the Norse platform is able to attract users who obviously do not want to be detected. When bad actors use these Norse hosted services, they add to our live intelligence.

Open source
By running popular open source applications within the Norse platform's Honeypot network, it is possible to emulate applications that are used by many and secured by none. This attracts bad actors that end up divulging their tools and techniques.

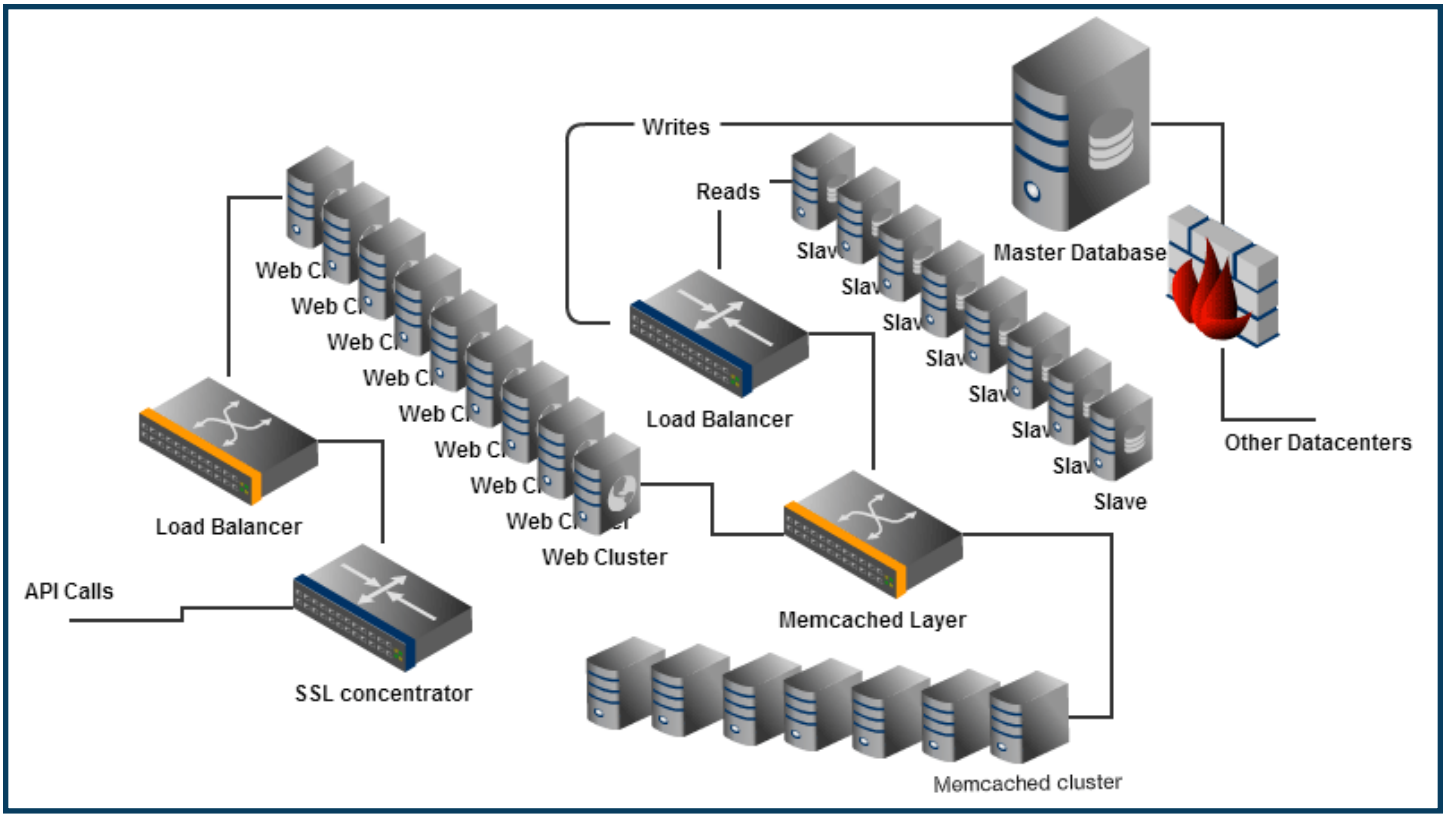
Big Data Analytics

Enterprises are struggling to manage the ever-growing size and complexity of their network infrastructure, security systems, and operations. The objective of the Norse platform is to provide IT security departments with truly actionable live intelligence that enables more accurate and automated decisions, reducing the strain on understaffed IT security departments and improving business outcomes with regard to the reduction of online fraud and network compromise and breach.

The Norse platform does the heavy lifting; analyzing enormous amounts of threat data collected every second through its massive, globally distributed network of honeypots and sensors. This data is analyzed in real-time against over 1500 risk criteria to calculate an easy to understand IPQ risk score (0-100). The higher the IPQ score, the greater the risk associated with that IP address.

Some factors and criteria used to calculate the IPQ score include:

- Geo-location risk assessment
- Network related risk assessment
- IP ownership changes throughout value chain
- Official IP assignment and other record assessment
- ISP behavior and profiling assessments
- Volume/velocity/recidivism profiling assessments
- Enterprise network behavior and vulnerability profiling



A scalable high-speed delivery infrastructure ensures extremely fast and reliable delivery of data.

Norse Global High-speed Delivery Platform

Designed to be integrated with high volume network infrastructure and critical business processes such as routers, firewalls, load balancers, websites, customer login forms, and eCommerce systems, the Norse platform is architected with a highly redundant and scalable high-speed delivery infrastructure that ensures extremely fast and reliable delivery of data with no latency from calculations. Response time against the Norse Delivery Platform is measured in microseconds with the ability to support hundreds of thousands of queries per second. Dynamic DNS ensures that customers connect to the geographically closest resource to minimize network latency.

REST API Integration

Integrating with the Norse platform is both simple and elegant. With just a few lines of code an enterprise or developer can begin to integrate Live Threat Intelligence into the IT infrastructure, websites, account login-forms, and business processes. From a simple curl command one can quickly see how the information is displayed:

curl -d apikey=YOURAPIKEY -d ip=208.74.76.5 -d method=ipq http://beta.ipviking.com/api/

For more examples and community code go to our github: https://github.com/norsecorp

Conclusion

Mobile, social, cloud, virtual – all innovations that have transformed the way we live and do business in recent years – have also empowered cybercriminals with automated tools, new attack vectors, and a seemingly never-ending supply of zero-day vulnerabilities to exploit.

Despite a plethora of available solutions, the fundamental architectures of traditional signature and policy-based security solutions lack the intelligence and proactive adaptability needed to effectively protect against today's advanced attacks, APTs, and zero-day exploits. While some promising new intelligence-based security offerings have started to emerge, the complexity of today's attacks and the ability of cybercriminals to rapidly change the IP addresses from where their attacks are launched have highlighted the need for big context, not just big data, and truly live data vs. the dubious "real-time" claims of many solutions.

It's clear the rules of the cyber security game have changed. The time is now for security vendors and IT security professionals to rise to this challenge together with new intelligence-based solutions and deployment strategies. Making this transition will take time and won't necessarily be easy. The inherent business risks of today's rapidly evolving threat landscape are too great, however, for organizations to take a wait and see attitude.

Fortunately, innovative cloud-based solutions like Norse Live Threat Intelligence enable organizations to transition to an intelligence-based strategy incrementally, prioritizing resources and efforts based on the organization's specific risk profile and attack surface. Using flexible REST APIs, organizations can quickly and cost effectively integrate live actionable threat intelligence at virtually any point in their IT infrastructure and web-based business processes, thereby raising their overall security posture and lowering business risk.

For specific case examples illustrating some of ways live threat intelligence can be deployed within an enterprise please refer to Appendix 1: Live Threat Intelligence Use Cases.

Appendix 1: Live Threat Intelligence Use Cases

Norse Live Threat Intelligence opens up many new possibilities for organizations in designing effective cyber security and fraud reduction strategies. With direct integrations to third-party solutions or simple integration via the flexible REST API, organizations can now add actionable threat intelligence virtually anywhere within their IT infrastructure and online business processes, enabling more informed and accurate decisions about what to block, what to allow, and what is should be routed for additional analysis or verification. The following use case examples illustrate just some of the potential ways live threat intelligence can be deployed to help organizations better manage the risk and overcome difficult fraud and cyber security challenges.

Web Security

For many enterprises the website is the primary channel for communicating and transacting with prospects, customers, partners, suppliers, etc. Consequently, it is also one of the primary attack vectors used by cyber criminals when targeting an organization. For companies that engage in eCommerce and store confidential personally identifiable customer information, the website represents an even greater source of potential business risk that must be managed.

Consider the 2011 hacking of the Sony PlayStation Network, which resulted in compromising upwards of 77 million users' private information. Aside from tarnishing Sony's brand and reputation, the incident is reported to have cost the company approximately $170 million USD in direct losses and incurred costs. While we may never know for sure exactly how the attack was carried out, the hacktivist group LulzSec claimed credit for the website attack, noting, "from a single injection, we accessed EVERYTHING." This statement, while unverifiable, simply highlights how large and multi-faceted of an attack vector a corporate website can be and, thus, the importance of effective web security.

While there's no shortage of available solutions for web security, in general they all suffer from a similar problem -- the inability to effectively detect and block zero-day threats and attacks. Norse Live Threat Intelligence is an effective solution for protecting against the most common and malicious website attacks such attacks as SQL injection, cross-site scripting, etc. Because it does not rely on threat signatures and constantly adapts to the changing threat landscape, it is also uniquely suited for protecting websites from unknown threats and zero-day exploits. With a flexible REST API, organizations can easily create custom integrations with any website or web application. Unlike many web security solutions, no hardware or DNS redirect is required. Norse IPVenger also offers plug and play with several content management systems such as WordPress.

In addition to enabling live, cloud-based web security, Norse Live Threat Intelligence empowers organizations to deliver an improved user experience. Because organizations have the ability to determine if a human or botnet is controlling the IP address, if it is coming from a compromised host or high-risk location, they can reduce the use of annoying CAPTCHAS and other challenge-response methods typically used on websites today to validate a user on login forms.

eCommerce Fraud Prevention

With the rise in eCommerce over the past decade, fraudsters have evolved their efforts by increasing automation and creating botnets. Over the past few years, botnets morphed into ever-larger malnets. With their immense distributed power, malnets pose an increasing threat on the eCommerce landscape. In addition, the increasing use and popularity of Tor and other Internet anonymizing services has created a new security and fraud challenge for businesses and organizations that conduct business and process transactions online. 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. The end result is that many fraudulent eCommerce transactions appear to be legitimate and circumvent traditional anti-fraud methods.

While closing known loopholes and performing out of band verification on obvious high-risk transactions yields some positive results, the most effective way to reduce eCommerce fraud is to leverage Norse Live Threat Intelligence. Using a

secure payment gateway solution such as Norse nGate, or a custom integration via the IPViking API, online merchants get a highly accurate live risk assessment of any eCommerce transaction within milliseconds. Norse's ability to identify and block IP addresses being anonymized via unpublished Tor exit nodes and other proxy servers, as well as dozens of other fraud risk factors protects merchants and processors from the most advanced online fraud techniques.

Account Takeover Fraud Prevention

Using the power of malware-based botnets, cyber-criminals have refined techniques of discovering and exploiting network and application layer-based vulnerabilities through which they steal consumers' usernames, passwords, and private information. Using the stolen credentials and supporting information, cyber criminals hijack email, social media, banking, and other financial accounts. Armed with such information, they are then able to launch their attacks anonymously through zombie computers from behind proxy networks including Tor – or even the customer's own compromised computer. Because the access attempts use the correct username and password, include other valid account details that make the request seem legitimate, and appear to be coming from the right device, organizations are challenged in their ability to ensure the true party is accessing the account.

With Norse Live Threat Intelligence, organizations can instantly assess the risk level and threat profile of the IP address of the web visitor initiating an account login. Using the powerful Norse IPQ score, and multiple risk factors such as whether the IP address is being spoofed or hijacked, whether it is a human or botnet, and the geo-location among others, organizations can build sophisticated and granular policies and rules that accurately identify fraudulent and high-risk logon attempts and block account takeover fraud before it can impact the business.

Account Origination Fraud

Another chapter from the online fraudsters' playbook is account origination fraud. Defined as the cyber criminal's use of stolen or fake identities to create new accounts, account origination fraud is difficult to detect. Fraudsters use stolen and fake identities for a wide variety of exploits. These include the creation of new bank or credit card accounts and acquisition of leased server and hosting services from which to launch attacks – all with the intent of gaining access to proprietary programs and data and obtaining virtual products online. As soon as cyber criminals create a set of new fraudulent accounts, they move quickly to exploit them, making detection and recovery of assets difficult. The damage from new account fraud is not limited to just the stolen funds, goods, and lost revenue. In the case of stolen identities, the negative experience and inconvenience it creates for legitimate users can result in loss of consumer confidence and trust.

Integrating Norse Live Threat Intelligence into a company's web based account sign-up forms via the IPViking API gives companies the ability to identify account originations from high-risk site visitors. Armed with information about the risk level associated with an account origination request, businesses can better understand their potential customers and make decisions in real time to allow account access for legitimate requests while denying fraudulent transactions.

Social Media Account Authentication

Why do you occasionally get annoying messages and wall postings from your Facebook friends that seem strange and link to dubious looking websites? Social web users have their account credentials stolen every day, which are then used to send out spam and phishing messages or worse to their friends' accounts. If that's not bad enough, all one needs to do is look at the national news reports to see that virtually all of the most popular social sites on the Internet have experienced a security breach of some kind over the last 18 months. Most recently, the micro-blogging site Twitter was hacked with approximately 250K user accounts compromised, with Facebook, Apple, LinkedIn, and others having all reportedly been breached to different degrees as well. [include recent AP Hack]

Social media sites and their customers' accounts are prime targets for hackers and cybercriminals because of the richness of the personal data contained in most user accounts, the trusted relationships between online friends, and the myriad ways in which stolen accounts can be exploited for financial gain. Hijacked Facebook accounts, for example, are

used to deliver spam, steal users' online and offline identity, perpetrate scams against users' friends, clone accounts, and simply sell them for cash in online hacker forums.

Online social networks are built on trust - the trust between users and their online friends, and the trust between the social website-platform and its users. Users need to be confident that the "friends" with whom they are communicating are actually who they think they are and not hackers or fraudsters. Lastly users need to have confidence in and trust that the social network platform can safely store and protect their personal information. Without this trust social networks cannot grow and thrive. Integrated into web logon forms, Norse Live Threat Intelligence is a simple flexible way for large and small social sites to protect their users' accounts from takeover and hijacking with stolen credentials. By leveraging live threat intelligence, social media organizations can validate the risk associated with account creation, helping ensure that cyber stalkers and other potentially suspicious actors are identified before they are allowed to interact with existing members.

Network Perimeter Security

Security at the network perimeter has been one of the backbones of the traditional IT security model. Among other systems, firewall, intrusion detection and prevention, authentication, VPN, and gateway anti-malware have most commonly been used to implement a layered security strategy. The conventional wisdom is that if an attack is not detected or blocked at the first layer, there are several other opportunities for it to be blocked by different solutions at other layers of the stack. When implemented and maintained properly this approach was fairly effective and served organizations well. As noted earlier in this document however, recent technology innovations have radically changed the threat landscape and enabled hackers and their malware to bypass these traditional systems with increasing regularity.

Norse Live Threat Intelligence, integrated with perimeter and edge network devices such as routers, firewalls, and load-balancers, and UTM appliances, helps organizations identify, manage, and mitigate incoming high-risk connections. By leveraging live threat intelligence, organizations can stop unknown and zero-day attacks at the perimeter before they enter the enterprise network.

Web and Data and Hosting Security

Web and server hosting providers are attractive targets for cybercriminals and hackers due to their rich stores of data, large number of companies and websites hosted, and their attractive CPU bandwidth resources. Often the goal is stealing financial information, hijacking website hosting servers to launch DDoS and other attacks, or redirecting site traffic to other, malicious sites. Hackers may also make use of hosting accounts using stolen credit cards to set up malicious websites, or inject malware onto a web server by exploiting vulnerabilities in a legitimate website. Once a site is compromised, it becomes a danger to all of the other legitimate sites hosted on that server.

At their core, hosting businesses are predicated on trust. If customers can't trust a provider to protect their network, customer websites, servers, and data from cyber attacks, they will choose a different provider. Consequently, the compromise of a hosting provider's network can be catastrophic for its business. Norse Live Threat Intelligence can be implemented via the IPViking REST API as a secure web gateway providing website owners and operators a more effective defense against zero-day vulnerabilities and threats by identifying and blocking website attacks before they can enter a site and do damage. Hosting providers can build this capability right into their service offering, thereby transparently helping customers keep their servers and data secure while also improving the security and efficiency of the datacenter's network as a whole. Depending on the provider's business model, the service can also be offered as an optional value-add to generate additional revenue.

Appendix 2: Case Study: TOR-based Financial Cyber Attack

To better understand the power and value of live threat intelligence, it is helpful to examine real-world examples of organizations using it to reduce fraud and improve their security posture.

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.

The Challenge

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

- 109 unique and undocumented TOR exit nodes that provided attack launch points from which the attackers could not be traced.

- Strategically placed botnet command and control points. While the specific origination points of the attack were obfuscated by the TOR network, it was determined that the complex attack pattern could only have been achieved through a highly distributed, orchestrated effort.

The Solution

Within hours of making the decision to use Norse Live Threat Intelligence, the campaign was able to seamlessly implement it and eliminate the threat to its fundraising efforts. The extremely flexible REST API enables it to be quickly integrated into websites, eCommerce and payment systems, web logon forms and authentication systems, as well as programmable network devices and appliances.

The Results

After embedding Norse live threat intelligence into the payment gateway, financial losses fell to zero out of 3,446 fraudulent transaction attempts. By blocking these fraudulent attempts, the solution prevented more than $317,000 in direct losses, plus more than $86,000 in indirect losses through chargeback fees and fines.

Bottom Line

The unique ability of the Norse Global Live Threat Intelligence platform to detect and identify the IP addresses of unpublished TOR exit nodes within seconds enables online merchants, payment gateways, payment processors, and other organizations to dramatically reduce their risk exposure to ecommerce fraud and drive significant ROI through the reduction of direct losses and chargebacks.

Norse Corporation
1825 S Grant St Ste 400
San Mateo, Ca 94402

www.norse-corp.com
inquiry@norse-corp.com
+1-650-513-2881

ABOUT NORSE CORPORATION

Norse is the leading innovator in the live threat intelligence security market with the goal of transforming the traditionally reactive IT security industry with proactive intelligence-based security solutions designed to enable organizations to defend against the advanced cyber threats of today and tomorrow. Norse's live global threat intelligence platform is a patent-pending infrastructure-based technology that continuously collects and analyzes live high risk Internet traffic identifying the sources of cyber attacks and fraud. Norse is the only provider of live, actionable, cyber threat intelligence that enables organizations to prevent financial fraud and proactively defend against today's most advanced cyber threats including zero day and advanced persistent threats. Norse is headquartered in St. Louis, Missouri, with offices in Atlanta and Silicon Valley. Visit us online at norse-corp.com.