How Advanced Attacks Get Past Traditional Controls

Five intelligence-based strategies for bolstering existing defenses.

NORSE

WHITE PAPER

Contents

Introduction

The cyber threat landscape has changed dramatically in just the last few years. Zero-day threats, advanced persistent threats (APTs), and web, mobile, and application level attacks and exploits often bypass traditional security defenses such as firewalls, anti-malware, intrusion detection, and user authentication systems. While these traditional security technologies are necessary and form the foundation of a comprehensive IT security strategy, they are no longer enough to effectively defend an organization's IT infrastructure from compromise.

Not long ago, corporate-owned devices connected to corporate servers accessing corporate applications inside a well-defined and secured network perimeter were the norm. Today, highly mobile and remote workforces demand round-the-clock connectivity to email, applications, and data from a wide variety of corporate and personally owned devices. These devices also access myriad web, mobile, and social applications, most of which are hosted and delivered from servers outside the corporate network. While these recent trends have improved network efficiency and worker productivity, they have also significantly increased network complexity and vulnerability.

According to the "Global State of Information Security Survey 2013"1, as mobile devices, social media, and the cloud become commonplace both inside the enterprise and out, technology adoption is moving faster than security. The survey found that 88 percent of consumers use a personal mobile device for both personal and work purposes, yet just 45 percent of corporations have a security strategy to address personal devices in the workplace, and only 37 percent have malware protection for mobile devices.

Capitalizing on this trend, hackers and cyber criminals are increasingly exploiting new attack vectors using sophisticated and automated techniques to launch targeted 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 effective, allowing hackers to gain unauthorized access to corporate networks, resources, and data.

Protection against these advanced threats requires new intelligence-based approaches and strategies. This white paper examines how advanced attacks get past traditional controls and therefore mandate the need for a new intelligence-based approach to security.

How Advanced Attacks Are Getting Past Traditional Controls

In the past, conventional Internet threats were relatively clear-cut, levied through email attachments, downloaded software, browser vulnerabilities, and fraudulent websites. Even when threats became more complex, they could easily be identified using policy, signature, and black list-based defenses.

Today's threats are stealthy by design and can be launched from legitimate, well-known applications and websites including banks, retailers, and large corporations that have been compromised. No longer is it clear who the enemy is or from where they might launch their next attack. According to "The Evolving Threat Landscape," a report by Juniper Networks2, "the prototypical cybercriminal is no longer the student defacing a website from a personal computer for amusement and notoriety. Today's stakes and spoils are greater, attracting highly paid professionals working within a web of technology suppliers, career hackers, and legacy crime organizations."

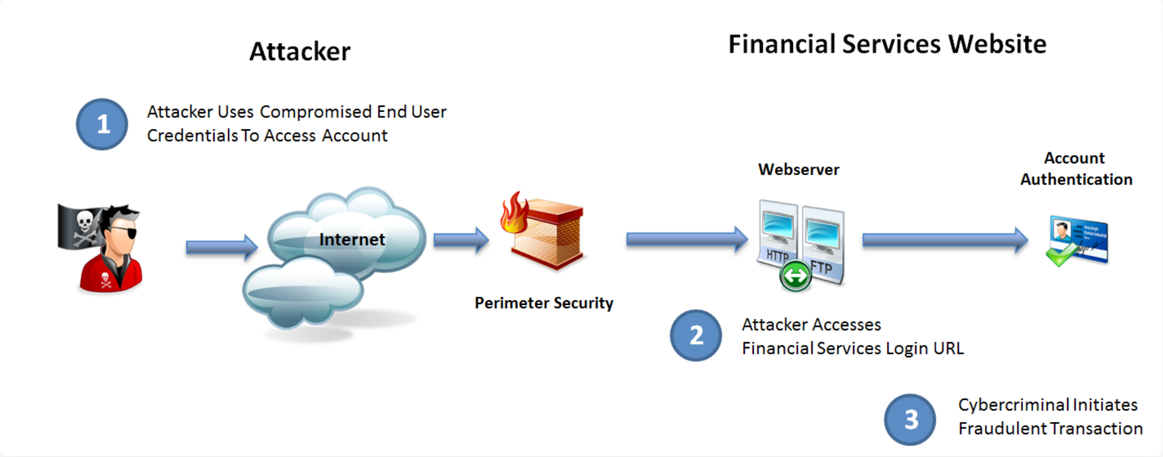
By compromising and controlling the networks of unsuspecting companies, hackers can leverage trusted networks to launch attacks and penetrate other organizations. Other attacks employ IP proxies, peer-to-peer communications, and anonymizers such as the Tor network to conceal their location and identity and easily circumvent many legacy security and fraud mechanisms. The number of malware samples using peer-to-peer communications alone has increased dramatically in just the past 12 months. The largest contributors to this increase are advanced threats like ZeroAccess, Zeus version 3, and TDL4.

The following are four examples of advanced threats that are using new techniques to get past traditional security controls:

1. Bypassing User Account Authentication Systems Using Stolen Account Credentials.

Account takeover fraud occurs when a cybercriminal obtains and uses a victim's account authentication details to take control of existing bank or credit card accounts and carry out unauthorized transactions. According to survey results from the Financial Services Information Sharing and Analysis Center, the total number of account takeover attempts reported by financial institutions has tripled since 2009. [3]

Perimeter and Website Security Can Be Compromised By Attackers Exploiting Internet Facing IP Addresses


Attacker
Financial Services Website
1
Attacker Uses Compromised End User Credentials To Access Account
Internet
Perimeter Security
Webserver
HTTP
FTP
Account Authentication
2
Attacker Accesses Financial Services Login URL
3
Cybercriminal Initiates Fraudulent Transaction

Using malware-based botnets, cyber-criminals have refined techniques of discovering and exploiting network and application layer-based vulnerabilities, using techniques such as SQL injection or binary code injection, 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. They are then able to launch attacks anonymously through zombie computers from behind proxy networks. Because the access attempts use the correct username and password, include other valid account details that make the request seem legitimate, organizations are challenged in their ability to ensure the true party is accessing the account.

Once the end user is infected, Trojans can work in many ways – all leading to the loss of money for the banking organization and customers.

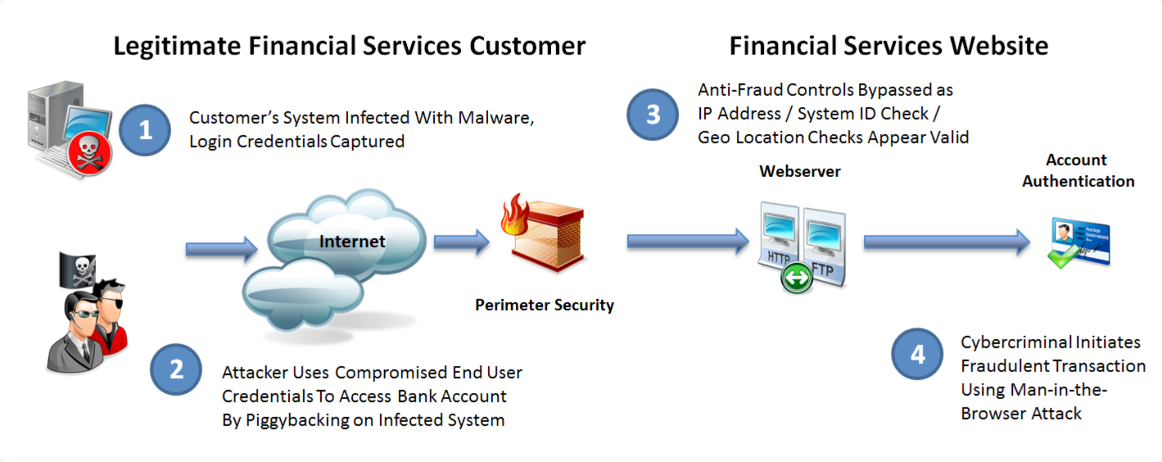
2. Bypassing Device Identification Anti-Fraud Technologies Using Mitb Malware Attacks.

The banking industry often employs two-step security measures as an added layer of protection against password theft and fraud. But several new Man in the browser (Mitb) style attacks have recently been shown to be able to defeat even two-factor authentication systems. Using the Mitb method, a cybercriminal constructs a fake bank website and entices the user to that website. The user then inputs their credentials and the cybercriminal in turn uses the credentials to access the bank's real website. When executed well, the victim never realizes they are not actually at the legitimate bank's website. The cybercriminal then has the option to either abruptly disconnect the victim and initiate fraudulent transactions themselves, or pass along the victim's banking transactions to minimize suspicion while making their own transactions in the background.

Advanced account takeover attacks can be very sophisticated and complicated to execute which is reflective of the fact that they are created by motivated, coordinated, and well funded organized cyber-crime syndicates. In many cases, the malware must be custom-made for each bank website, which involves extensive coding on the part of the malware authors. Destination accounts must also be created at the targeted bank so that the malware has a place to deposit the stolen money. Access to the stolen funds is achieved by a network of money mules, which must be recruited to access the destination accounts and move the money out of the bank.

Luckily, the attacker is only able to infiltrate the site once with the user-supplied pass code. But, once in, the attacker can hide records of money transfers, spoof balances, and change payment details.

Account Takeover Using a Man-in-the-Browser Attack That Circumvents Traditional Anti-Fraud Checks


Legitimate Financial Services Customer
Financial Services Website
1
Customer's System Infected With Malware, Login Credentials Captured
3
Anti-Fraud Controls Bypassed as IP Address / System ID Check / Geo Location Checks Appear Valid
Webserver
Account Authentication
Internet
Perimeter Security
HTTP
FTP
2
Attacker Uses Compromised End User Credentials To Access Bank Account By Piggybacking on Infected System
4
Cybercriminal Initiates Fraudulent Transaction Using Man-in-the-Browser Attack

3. Bypassing Endpoint and Gateway Anti-Malware via Botnet Command Servers Hidden in Tor.

Tor is a software-based tool originally developed by the U.S. Naval Research Laboratory for legitimate privacy reasons. Unfortunately, Tor has evolved into a tool used by cybercriminals to control botnets, access online accounts, and use fraudulent financial information to purchase legitimate online goods or services.

Tor enables the creation of network servers used to send traffic over many different routes, masking the original source of the traffic using layers of packet encryption. Distributed relays help to conceal a user's location or usage and protects against traffic analysis and data snooping. Tor also encrypts the traffic between each relay, so it cannot be blocked by security controls such as Intrusion Detection Systems and other Deep Packet Inspection solutions.

Although some organizations have started to block Tor traffic from the published list of known exit nodes, unpublished Tor exit nodes (the last encryption node in the chain of network relays) can be quickly setup and taken down to perpetrate an attack, masking the true origin of the source and rendering them almost untraceable.

4. Bypassing Ecommerce Fraud Detection Systems Using Tor and Proxy Hidden Attacks.

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 ecommerce fraud as well as security compromise and breach. For companies that engage in ecommerce and store confidential personally identifiable customer information, the website represents an even greater source of potential business risk.

Tor is a public peer-to-peer network, but unlike other peer-to-peer networks, its main function is anonymization of network traffic. 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 result is that many fraudulent ecommerce transactions appear to be legitimate and circumvent traditional anti-fraud methods.

In 2012, a political campaign 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 attack against the political fund raising site used sophisticated, automated scripts that were specifically designed to work with the target site's financial system. The attack was distinguished by the use of credit card account information that looked legitimate enough to spoof some typical forms of fraud detection. It also used 109 unique and undocumented Tor exit nodes to provide attack launch points from which the attackers could not be traced. Finally, the attackers use strategically placed botnet command and control points. While specific points of origin were obfuscated with Tor anonymization, the pattern of attack required a distributed, orchestrated effort.

Five Live Attack Intelligence-based Approaches for Bolstering Existing Defenses

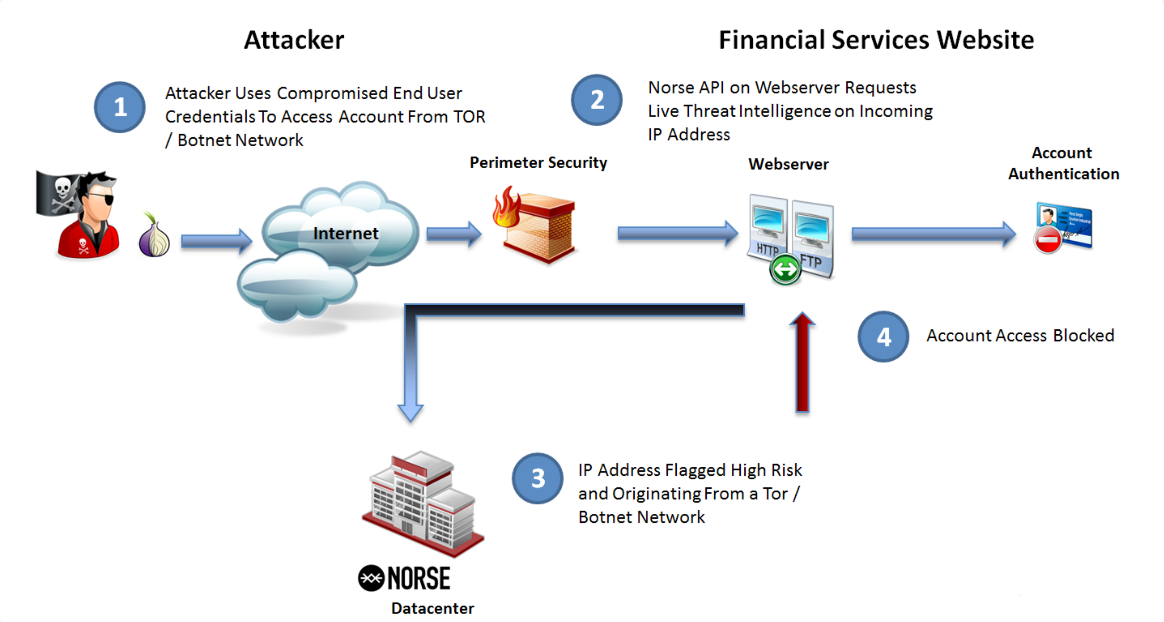
Today, traditional security controls and defenses, while necessary, are not enough to combat advanced cyber threats. As a result, some companies are starting to adopt new intelligence-based strategies. An example is Norse Live attack intelligence. Norse is the only provider of truly live attack intelligence that is able to detect changes in the threat landscape in real-time and fast enough to effectively protect organizations from these types of advanced attacks. When integrated at strategic points in an organization's IT infrastructure and business processes, Norse Live attack intelligence can dramatically reduce ecommerce fraud and increase overall security posture. Live attack intelligence can also increase the efficacy of traditional security systems, enabling companies to leverage their existing security investments for greater efficiency and ROI. Because the threat intelligence is live and requires no signatures, data is never out of date and constantly adapts to the Internet's changing threat landscape.

The following are five live attack intelligence-based approaches companies can use to bolster their existing defenses:

1. Integrate Live Attack Intelligence into the User Authentication Web Page.

Using a RESTful API and approximately 20 lines of HTML/Javascript code, Live attack intelligence can be added to a user authentication web page. This code then checks the IP address of a web page visitor before login is allowed to determine the risk/threat factor. An aggregated risk score, geo-location/geo-match, and live risk/threat factor information is returned. Based on this live intelligence, the connection can then either be blocked/dropped, allowed, or sent for secondary/out of band authentication.

Account Access Using Compromised Credentials Can Be Eliminated Using Live attack Intelligence to Identify and Block Rogue IP Addresses


Attacker
Financial Services Website
1
Attacker Uses Compromised End User Credentials To Access Account From TOR / Botnet Network
2
Norse API on Webserver Requests Live Threat Intelligence on Incoming IP Address
Perimeter Security
Webserver
Account Authentication
Internet
HTTP
FTP
4
Account Access Blocked
3
IP Address Flagged High Risk and Originating From a Tor / Botnet Network
NORSE
Datacenter

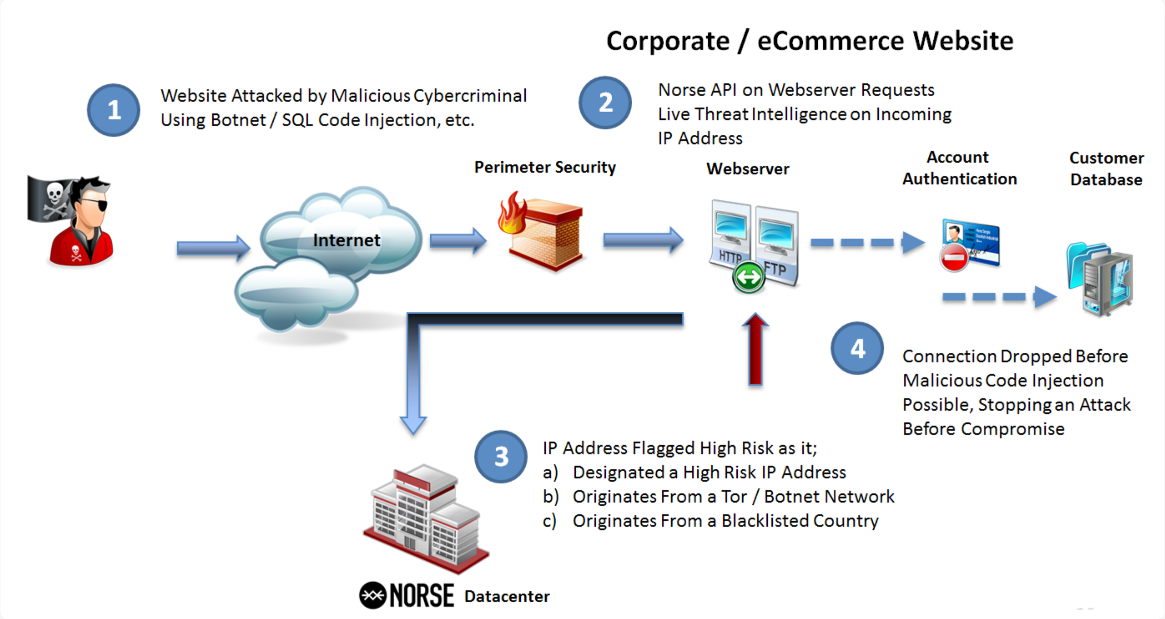
2. Integrate Live Attack Intelligence at the Web Server Level.

To more proactively protect an organization from the broader range of web-based security attacks, Live attack intelligence can be easily integrated at the web-server level. In this scenario a script in the webserver automatically checks the IP address of every incoming connection request to determine the risk/threat factor before they enter the site and can launch an attack. Based on live intelligence, the connection can then either be blocked/dropped, allowed, or sent to captcha or another method of determining whether the visitor is a bot versus a human. This method is extremely effective in blocking the most common website attacks such as SQL injection, binary code injection, cross-site scripting attacks, as well as unknown and zero day attacks.

3. Integrate Live Attack Intelligence into Perimeter Security.

In addition to web-based attacks, organizations can also use Live attack intelligence to stop unknown and zero-day attacks at the perimeter before they even enter the network. Integrating Live attack intelligence with common perimeter and edge network devices such as routers, firewalls, load-balancers, and UTM appliances enables protection against a wide breadth of network-based attacks. With Live attack intelligence these network layer security appliances and devices can instantly assess the risk level of every incoming and outgoing network connection enabling the blocking malicious traffic before it enters the network and routing higher risk or suspicious traffic for additional analysis or sandboxing by IDS and DPI systems.

Identifying Rogue IP Addresses at the Perimeter or Website Can Significantly Improve the Integrity of the Network



1 Website Attacked by Malicious Cybercriminal Using Botnet / SQL Code Injection, etc.

2 Norse API on Webserver Requests Live Threat Intelligence on Incoming IP Address

3 IP Address Flagged High Risk as it;
a) Designated a High Risk IP Address
b) Originates From a Tor / Botnet Network
c) Originates From a Blacklisted Country

4 Connection Dropped Before Malicious Code Injection Possible, Stopping an Attack Before Compromise

4. Integrate Live Attack Intelligence into Website Payment Flow to Detect and Block Fraudulent Transactions.

Even a small percentage of disputed purchases or fraudulent chargebacks can significantly erode a Merchant or Service Provider's profit margin. Therefore, reducing online fraud transaction processing is critical to reducing the costs and risk associated with accepting online payments.

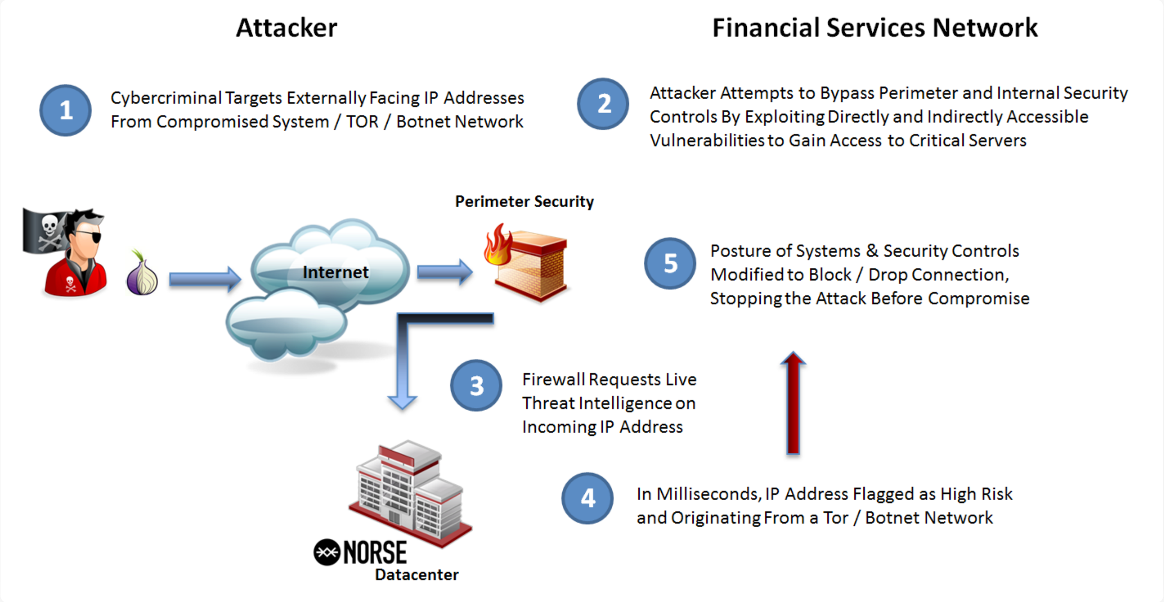
Integration of Live attack intelligence into a company's website payment flow helps financial services organizations automate the detection and blocking of fraudulent transactions as they happen and automatically stay current with the latest tactics of fraud perpetrators to reduce risk of attack by Tor and Proxy based threats. Live attack intelligence tools can instantly accept or deny most orders based on easily defined rules and thresholds – helping merchants and service providers reduce the time spent on reviews of suspicious transactions by costly, manual processes traditionally used to thwart fraud.

5. Integrate Live Attack Intelligence with the SIEM System.

Integrating the SIEM system with Live attack intelligence can help identify and remediate unknown and zero day threats. A company can correlate external Live attack intelligence with internal intelligence data to uncover signs of compromise and breach.

According to security firm McAfee, the integration of SIEM and Live attack intelligence is vital to a successful security strategy. “The ability of SIEM to collect, analyze, and generate actionable output has tagged SIEM as a ‘must have’ security technology,” the firm stated in a recent report on threat intelligence SIEM requirements.4 “Similarly, threat intelligence has become indispensable for its ability to identify bad actors. These two solutions working in tandem become part of a proven strategy. This strategy yields a highly optimized solution that provides improved threat identification and remediation and also has a positive impact on business priorities.”

Identifying Rogue IP Addresses at the Perimeter or Website Can Significantly Improve the Integrity of the Network


Attacker
Financial Services Network
1
Cybercriminal Targets Externally Facing IP Addresses From Compromised System / TOR / Botnet Network
2
Attacker Attempts to Bypass Perimeter and Internal Security Controls By Exploiting Directly and Indirectly Accessible Vulnerabilities to Gain Access to Critical Servers
Perimeter Security
Internet
5
Posture of Systems & Security Controls Modified to Block / Drop Connection, Stopping the Attack Before Compromise
3
Firewall Requests Live Threat Intelligence on Incoming IP Address
4
In Milliseconds, IP Address Flagged as High Risk and Originating From a Tor / Botnet Network
NORSE
Datacenter

Conclusion

Today's cybercriminals have automated tools, new attack vectors, and a seemingly never-ending supply of zeroday vulnerabilities to exploit. Despite a wide range of available security and anti-fraud solutions, the fundamental architectures of traditional signature and policy-based solutions lack the intelligence and proactive adaptability needed to effectively protect against today's advanced attacks, APTs, and zero-day exploits.

Given today's elevated threat environment, "businesses can no longer afford to play a game of chance. They must prepare to play a new game, one that requires advanced levels of skill and strategy to win."5 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.

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

About Norse Live Attack Intelligence

Norse Live attack intelligence opens up 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 RESTful 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 should be routed for additional analysis or verification.

Designed to support the requirements of high volume network infrastructure such as routers, firewalls, and load balancers, and to enable easy integration into critical business processes, websites, customer login forms, and ecommerce systems, the Norse Live attack Intelligence platform is features a highly redundant and scalable global 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.

DarkViking Overview

DarkViking is a Live attack intelligence service that provides enterprises with actionable Live attack intelligence, enabling them to dramatically reduce ecommerce fraud and increase their overall security posture. Integrated via a flexible RESTful API or direct solution level integration, DarkViking increases the efficacy of traditional security systems enabling them to identify and intelligently block today's most advanced cyber threats. And because Norse's threat intelligence is live and requires no signatures, the data is never out of date and constantly adapts to the Internet's changing threat landscape.

DarkViking Benefits:

» Reduces risk of security breaches, website hacks, and the associated loss of reputation, and revenue.

» Prevents account takeover fraud due to stolen credentials.

» Reduces fraud and chargeback related costs.

» Protects your brand and improves user experience when integrated into sign-up and login screens.

» Provides security analysts with contextual threat intelligence for improved forensics and investigations.

» Supports FFIEC and other compliance requirements for layered security.

[1] "Changing the Game - Key findings from the Global State of Information Security Survey 2013," PwC, 2013, http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf

[2] "The Evolving Threat Landscape - Where the Key Security Battles Are Taking Place Today—and Essential Strategies for Winning Them," Juniper Networks, 2012, http://www.juniper.net/us/en/local/pdf/whitepapers/2000371-en.pdf

[3] FS-ISAC ANNOUNCES the Results of Account Takeover Survey, Financial Services Information Sharing and Analysis Center, June 14, 2012, http://www.aba.com/Solutions/Fraud/Documents/FSISACPressRelease62012.pdf

[4] "Focus on Five Threat Intelligence SIEM Requirements," McAfee, 2012, http://www.mcafee.com/us/resources/brochures/br-focus-on-five-threat-intelligence.pdf

[5] "Changing the Game - Key findings from the Global State of Information Security Survey 2013," PwC, 2013, http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf

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 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.

© 2014, Norse Corporation. All rights reserved.

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 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.

© 2014, Norse Corporation. All rights reserved.