Meeting Updated FFIEC Requirements and Strengthening Security and Fraud Controls with Live Attack Intelligence

Increasing the Efficacy of Security and Fraud Prevention Systems to Minimize Risks to Financial Business Operations

Edited by Jeff Harrell | August 2014

NORSE

WHITE PAPER

Contents

Executive Summary

This white paper clarifies the updated FFIEC guidelines and identifies some of the potential threats and explores various attack mitigation strategies that can be leveraged by financial service institutions such as commercial banks, credit unions, and investment services to benefit their customer base and reduce the risk of compromise.

In 2011, the Federal Financial Institutions Examination Council (FFIEC) issued a supplement to the "Authentication in an Internet Banking Environment" guidance document, originally released in October 2005. The supplement emphasizes the need to promote security in electronic banking with formal assessments of financial institutions beginning in January 2012. The changes reinforce the risk-management framework and stress the need for performing regular assessments and the subsequent adjustment of customer authentication controls in response to new threats. Further recommendations include the implementation of effective strategies for risk mitigation and raising the overall customer awareness of threats associated with electronic banking.

Financial Institutions are under constant attack from malware, botnets, and advanced persistent threats, which continue to grow exponentially. As signature and policy-based defenses have become less effective and are now regularly bypassed by advanced and unknown threats, comprehensive security intelligence is essential for financial institutions to safeguard customer information, reduce fraud stemming from the theft of sensitive customer data, and promote the legal enforceability of electronic customer agreements and transactions. Reputation Services have emerged as part of the existing layered security architecture and provides a basic level of threat intelligence to identify known threats and improve an organizations' overall security posture and response to active threats.

A next generation of Reputation Services has started to emerge in the form of live attack Intelligence, providing richer context, greater accuracy, faster threat response times and highly effective protection against known, unknown, and zero day threats generally missed by legacy security controls. Stopping malicious and high-risk traffic at the network edge can provide a clear and dramatic improvement in security efficiency, in addition to the authentication of IP addresses when used to reduce online fraud transaction processing.

FFIEC Supplemental Guidance Explained

With the continued growth of electronic banking and greater sophistication of transaction and account related threats, financial institutions and their customers have seen a significant increase in risk and experienced substantial losses from direct institutional attacks, online account takeovers, account origination fraud, as well as ACH and wire transfer fraud. To address these new threats, financial institutions and their customers should adopt technologies and implement processes to combat an increasingly hostile online environment, including:

Perform Regular Risk Assessments:

Financial institutions are required to perform regular risk assessments and update these assessments to identify new risks as information becomes available. A risk assessment is recommended to be performed prior to implementing new financial services or as new threats and attack vectors emerge.

These technologies may include:

» Customer profiling using historical and behavioral data

» The use of debit blocks and other techniques to limit the transactional use of the account

» Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels

Additional Controls for Business Banking:

To combat ACH or wire fraud, financial institutions are required to establish higher-level controls for high-risk activities and transactions. In particular, more stringent controls over commercial banking are required given higher account balances and transaction amounts.

These technologies may include:

» Additional controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows

Implementation of a Layered Security Program:

Layered security involves different types of controls at multiple points within a network or transaction process. They must include the ability to detect and respond to suspicious activity and have improved control of the administrative functions that are frequently manipulated in fraud attacks. Financial institutions are required to implement additional controls as dictated by the results of each risk assessment.

These technologies may include:

» Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud.

» Internet protocol (IP) reputation-based tools to block connections to banking servers from IP addresses known or suspected to be associated with fraudulent activities.

Further Enhance Customer Awareness and Education:

Increase awareness of the fraud risk and effective techniques that account holders can use to mitigate the risk.

These technologies may include:

» The use of multi-channel authorization or out-of-band verification for business transactions

Financial institutions risk regulatory non-compliance penalties and customer defections from online services if they fail to deploy solutions that meet these FFIEC guidelines.

Understanding the Financial Threat Landscape

The nature of institution and transaction attacks has rapidly changed over the last decade. Originally, threats were passive and performed by individuals or small groups of hackers: eavesdropping and offline password guessing. A decade later, the threats targeting financial services and their customer base are automated, more invasive, and often crafted by international crime rings. Cybercriminals today use a combination of tried and true advanced techniques such as phishing, Trojans, Man-in-the-Browser attacks, and the use of anonymizing proxies such as TOR (The Onion Router) to help mask the true origin of attacks and the locations of botnet command and control servers.

Cybercriminals are continually creating sophisticated malware and network based-attacks designed to specifically target financial institutions. At a basic level, these threats can be broken down into 3 categories based on the intended targets, which are:

» Business Banking Customers

» Consumer Banking Customers

» Financial Institutions' Systems and Infrastructure

Threats Targeting the Financial Institution

Attacks against financial institutions typically involve the penetration of the perimeter network, websites, and other bank systems to steal internal bank and customer account data. Direct attacks against externally facing IP addresses of any Internet-based business are well understood but unfortunately still continue to be a major source of compromise. Even when best practices are followed and standard security controls are implemented, the dynamic nature of business networks makes constant monitoring and frequent configuration changes necessary to adapt to changing business needs.

In a recent network breach, cybercriminals compromised a banking system to obtain account information. Once the account data was obtained, the cybercriminals erased internal fraud control data to remove enforceable withdrawal limits on prepaid debit cards. Crime ring members in twenty-seven countries then repurposed old hotel key cards or expired credit cards by running them through handheld magnetic stripe encoders. Easily obtained online for approximately $300, these inexpensive encoders allow cybercriminals to change information on the magnetic stripes and write new cards with a simple swipe - instantly transforming them into prepaid debit cards with no daily ATM withdrawal limit.

With over $45 Million dollars of fraud committed from the stolen card data in just a few days, this incident serves as a painful reminder that financial organizations using static and somewhat insecure perimeter and website security controls will continue to fall victim to these types of fraud attacks.

Among others, the active threats targeting financial institutions today are:

» **Spear Phishing.** Spear Phishing is a targeted attack that attempts to compromise key individuals within an organization using a known, trustworthy entity in an electronic communication. These attacks can appear to be from fellow employees or business partners but can lead to the download of a malware payload, but with the ultimate goal of compromising an administrator's system to gain administrative level access and passwords to business critical systems.

» **Perimeter Security Control and Website Compromise.** These attacks typically target Internet facing IP addresses to exploit vulnerabilities in external services or misconfigurations in perimeter security controls. Once the attacks succeed, the cybercriminal can gain a foothold within the internal network and further compromise critical business systems.

Using a risk-based approach, organizations can apply a structured process designed to optimize each security control based on the criticality of the banking system and the data residing on it. Once each of these controls is identified, the financial institution can further develop a methodology to measure the effectiveness of those controls and ultimately determine the residual risks to the organization's assets.

Actively monitoring the externally facing IP addresses for attacks using live attack Intelligence to identify and block potentially malicious activity and the automatic implementation of mitigating controls before the perimeter is compromised could go a long way in reducing the overall attack surface of financial institutions.

Threats Targeting the Business Banking Customer

A growing trend in cybercrime is Automated Clearing House (ACH) Fraud, which can be very costly for the businesses that fall victim to it. Under current law, business fraud recovery is much more difficult than it is for consumers; consumers need to alert their bank within 60 days of a fraudulent transaction in order to recover funds, but businesses sometimes have as little as one or two business days.

In addition to the lost funds, businesses may also have to invest in legal costs and fees to recapture their lost funds if the financial institution is unwilling to reimburse them - in addition to the lost productivity and soft costs associated with fraud investigations. There are numerous court cases pending regarding business customers suing financial institutions for fund reimbursement due to this type of fraud. Most businesses hold the bank responsible for the security of their account, even though the vast majority of these banking relationships include an agreement where the customer promises to indemnify the bank should a fraudulent wire transfer happen.

Automated Clearing House (ACH) Fraud

ACH fraud uses the Automated Clearing House funds-transfer system that provides transfers between banks and other financial institutions nationwide and is considered a form of account takeover fraud. This type of fraud is becoming more popular with cybercriminals because it is very easy to perpetrate.

Active threats targeting business-banking customers are:

» **Phishing.** Phishing is the act of masquerading as a trustworthy party (such as the business users bank) in an electronic communication with forged links to a fake website to order to obtain login credential information.

» **Trojan Attack.** Banking Trojans either infect Web browsers via a drive-by download (visiting a legitimate, but compromised, website) or piggybacking as an attachment on a phishing email. After banking Trojans infect a Web browser, they will lie dormant and undetected until the end user to visit his or her online banking website. When the business user logs into his bank's legitimate website, the cybercriminal captures the account authentication data and then uses that data to transfer funds from the account, often masked as goods or services purchased online or by telephone.

The targets of ACH fraud are characteristically small to medium size businesses that use community banks or credit union type services as they typically do not use updated anti-virus software or have dual control over accounts. Once the cybercriminal has a business customer's account and bank routing number, they can initiate ACH payments or withdrawals.

Threats Targeting the Consumer Banking Customer

Attacks against banking and financial service consumer customers are much more varied but ultimately all lead to account origination or account takeover fraud.

Account Origination Fraud

Account Origination fraud is one of two basic forms of financial identity theft and occurs when a cybercriminal establishes new accounts under the victim's name using their Social Security number and other available personal information.

Cybercriminals employ a variety of techniques to obtain the personal and financial information typically needed to take control of existing accounts. Obtaining such information can involve low-tech social engineering techniques such as mailbox theft or scam calls. Account origination fraud is most often associated with traditional Identity Theft.

Account Takeover

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 against them. Cybercriminals typically use more technology-reliant methods, such as phishing, SMiShing and Trojans, and invest a substantial amount of time and effort to establish fake websites in order to perpetrate the fraud, collecting account and payment details without the victim's knowledge.

Active threats targeting consumer-banking customers are:

» **Phishing & SMiShing.** Phishing is the act of attempting to acquire personal information such as passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. SMS (Short Message Service) phishing (also called SMiShing) uses cell phone text messages to deliver the bait to induce people to divulge their personal information.

» **Trojan Attack.** Banking Trojans are among the stealthiest of all Trojans and are the most common form of malware used in account takeover attacks. Once installed on a victim's computer, the Trojan lies in wait until the end user visits their bank website, silently stealing the bank-account username and password information and forwarding the authentication data to a system controlled by cybercriminals. The cybercriminals then log into the account themselves, and transfer available funds to their previously created accounts – sometimes held at the same bank. Within days or even hours, money mules (untraceable and anonymous participants to the fraud) withdraw cash from the accounts and send the funds overseas via Western Union or similar wire transfer services.

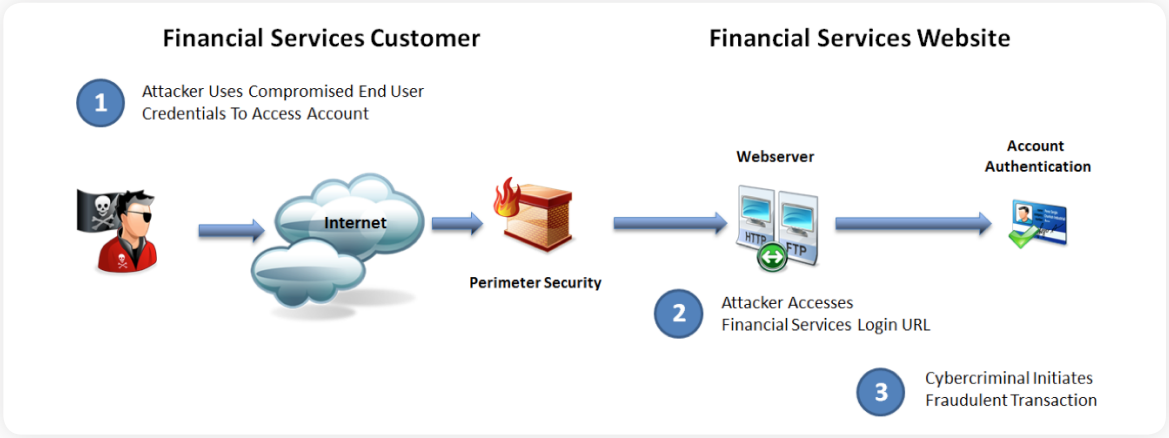
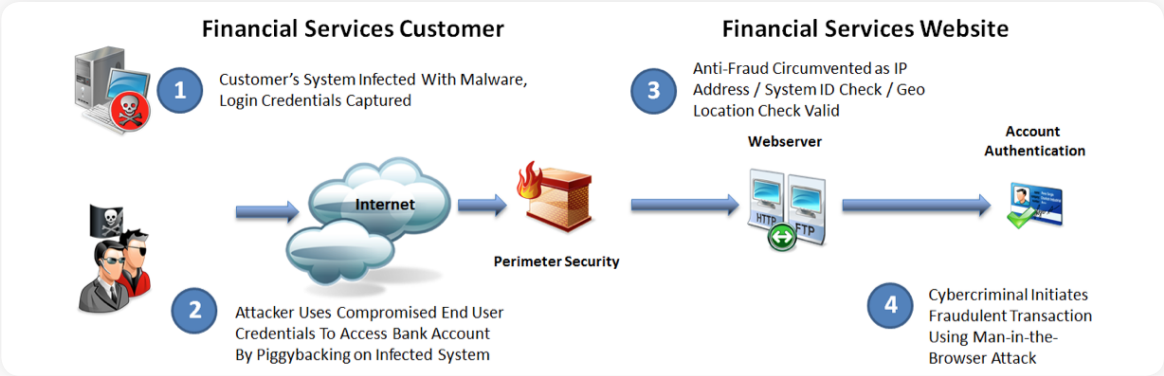


Fig 1. Account takeover after a customer's computer system has been compromised by a banking trojan

» **Man-in-the-Browser Attack.** 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 it to access the bank's real website. When executed correctly, the victim will never realize that they are not actually at the legitimate bank's website. The cybercriminal 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.

Fig 2. Account takeover using a man-in-the-browser attack, circumventing traditional anti-fraud checks

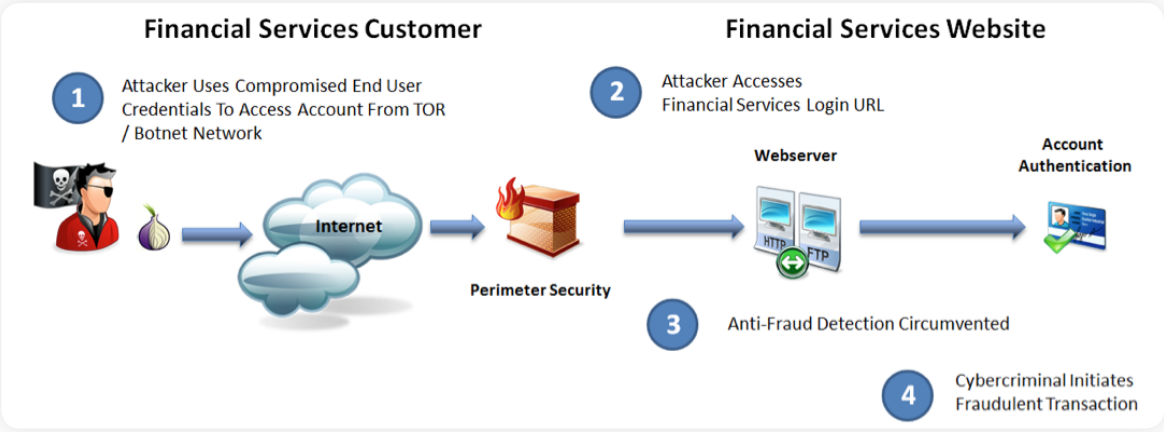


Account takeover attacks can be extremely complicated to execute. In many cases the malware must be custom-made for each bank website, which involves further research and coding on the part of the malware authors. Destination accounts must also be created at the targeted bank so that the malware has a place to deposit the stolen money. Access to the stolen funds is often achieved using a network of local "money mules," to access the destination accounts and move the money out of the bank.

» **Tor-based attacks.** Tor (also known as The Onion Router) is an open source (P2P peer to peer) network that enables users to send their Internet traffic through many different proxy servers, masking the original source of the traffic using layers of packet encryption. With a worldwide network, the distributed relays help to conceal a user's location and protects against traffic analysis and data snooping.

Developed for legitimate privacy reasons, Tor has evolved into a dark world of nefarious and illegal activity primarily used by cybercriminals to control botnets, access online accounts and use stolen financial information (such as credit card information) to perform fraudulent online transactions for goods or services. Unpublished Tor exit nodes (the last encryption node in the chain of network servers) can be quickly setup and taken down to perpetrate an attack, masking the true origin of the source and bypassing security and anti-fraud controls that use IP block lists based Tor's official published list of exit node servers.

Fig 3. Compromised credentials provide account access with attacher utilizing Tor Network to Mask Source IP of Attack



Strengthening FFIEC Compliance Using Live Attack Intelligence

Layered security is defined as the use of different controls at different points of a transaction process. This layered approach addresses the inherent weaknesses found in one type of security control by balancing it with the strengths of a different and separate security control. Layered security has proven to be a successful strategy for the overall security of Internet-based commerce and effective in reducing fraud based financial losses.

The FFIEC supplemental guidance specifically identifies Internet protocol (IP) reputation-based technology as a primary recommendation in the layered security model as a means to identify and block connections to critical banking servers from IP addresses known or suspected to be associated with fraudulent activities. IP Reputation services were initially effective in this role but have become less effective over the last few years, unable to keep up with the speed with which IP addresses can change their risk, threat characteristics and profile.

In response, a next generation service has evolved beyond the stagnant, days, weeks, or month old blacklists into a fully-fledged, contextual IP intelligence service using a multi-factor risk score and geo-location information to block the sources of threats and fraudulent transactions as they happen. With millisecond response times and contextualized risk data that proactively adapts to the Internet's evolving threat landscape, financial service organizations with perimeter and website security – as well as transaction fraud processing – finally have live, actionable threat intelligence with which to make automated decisions on critical business processes and strengthen their existing security defenses.

The Evolution of IP Reputation Services to Live Attack Intelligence

The origins of IP reputation services began in the early days of SPAM filtering using IP and DNS blacklists and whitelists. These lists were maintained by volunteer netizens, traded back and forth with weekly or monthly updates and circulated to an ever-widening group of network administrators. These lists contained IP addresses and IP address ranges of known spammers and worked by correlating the incoming source IP address (when a connection attempt was made) to the blacklist and dropped the connection if there was a match. Unfortunately, the updates to the blacklist and whitelists were sporadic, often inaccurate, and increasingly large in volume – making it difficult for a committed, but loosely coordinated group of volunteers to maintain. A number of organizations formed to provide a professional level of service to these blacklist and whitelist "customers" and commercial IP Reputation Services were born.

The next level of evolution of IP Reputation Services sought to identify IP addresses that were the source of web attacks, phishing activity, port scanning, centrally managed and automated botnets to block DDoS attacks and other malicious activity. This IP threat data is often derived from a security vendor's customer endpoint, server, or gateway log files, aggregated and either sold or provided for free to customers as IP Reputation or Threat Intelligence data as well as being aggregated with data feeds from other reputation service providers.

Typically, IP Reputation Services rely on updates from multiple data sources and providers to form the core of their intelligence, which must be normalized across widely differing formats before it can be delivered to and utilized by customers. This data normalization process can introduce significant data latency - especially if any one-vendor changes their data set format without warning – leaving the customer exposed. Additionally, the quality and accuracy of aggregated data sets is difficult to assess and monitor and often cannot be relied upon for real-time automated decisions for ecommerce transactions, customer account logins, and detection of malicious and high-risk network connections.

Another shortfall found in IP Reputation Services is the lack of overall Internet coverage these aggregated, log-file based Reputation Services provide. If a customer does not wish to make their logs available to a vendor, a potential void in coverage exists. If the customer base is

limited, only a minor sampling of threats in relation to IP addresses are exposed, leading to an incorrect threat assessment and a false sense of security. Even when aggregated across multiple sources by a market leading Security Vendor, IP Reputation Services that use log file aggregation may only cover, at most, 1-5% of the actual malicious traffic.

The next generation of IP Reputation Services has evolved beyond out-of-date and inconsistent updates from multiple, disparate data sources into a single, definitive source of live attack intelligence. With a global infrastructure-based threat collection platform, Norse provides unmatched visibility into the darkest corners of the Internet with the accuracy, context, and speed of delivery required to automate business and security decisions that are effective in dramatically reducing online fraud and the risk of security breaches.

Using 6-7 Million active Internet connections at any given time, Norse collects millions of IP-based risk factors per minute. Each risk factor is systematically compared to a timeline and history, automatically analyzed, categorized, cataloged and stored for future reference. The end result is a trail of information and history for any given IP address to reveal negative, unethical, or illegal behavior. These 1,500 data points can be used to identify threats in near real-time, giving financial organizations the edge when dealing directly with Perimeter Security, Website Security, eCommerce Fraud prevention, and Zero Day Threat mitigation.

Using Live Attack Intelligence to Enhance Existing Layered Security Defenses

The Norse live attack 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. This section describes some of the most common use case scenarios for financial institutions using live attack intelligence.

Norse Live Attack Intelligence for Perimeter Security:

Organizations needing to defend against advanced threat that target the enterprise network to compromise confidential financial customer data can integrate Norse live attack intelligence into perimeter and edge network devices such as routers, firewalls, load-balancers, and UTM appliances. This integration enables organizations to instantly assess the risk level of every inbound network connection before it enters the network to stop known, unknown and zero-day attacks at the perimeter - and drop any network connection deemed malicious or too high a risk.

Norse Live Attack Intelligence for Website Security:

One of the most high profile targets used to compromise financial customer account data is the banking or financial services website itself. Typically, Website security can be bypassed using multiple techniques including Cross Site Scripting and Request Forgery, SQL injection, Binary Code Injection, poison cookies, bypassing the authentication schema with direct page requests and Session ID prediction, in addition to hacking toolkits, Distributed Denial of Service (DDOS) attacks via Botnets and stealth banking Trojans. All of these attack techniques and tools mentioned above can be sourced or found freely available on the World Wide Web. Many of these toolkits and attacks succeed due to (but not limited to) perimeter security device or software misconfigurations, known or unknown vulnerabilities that are directly accessible from the internet, web server administration errors or poor application programming skills.

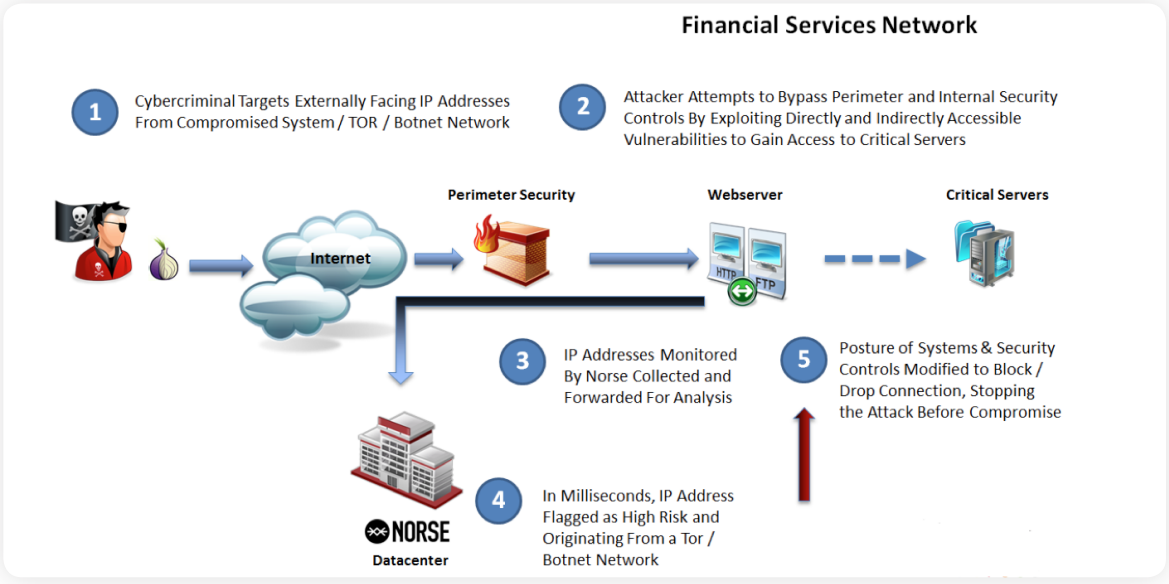


Fig. 4. Identifying Rogue IP Addresses and Attacks at the Perimeter or Website Can Significantly Improve the Integrity of the Network

Integrating Norse's live attack intelligence at the web server level helps organizations to identify Website visitors and validate their IP risk score or threat factor before they can enter the site and launch a potentially malicious attack. Based on the results of the live attack intelligence, the Website can automate the decision process needed to drop the connection, permanently block the connection, allow the connection, or send the session to CAPTCHA (a type of challenge-response test used to determine whether or not the user is human) or other method of determining whether the user is a bot or human.

Norse Live Attack Intelligence to Prevent Customer Account Takeover:

User Account Authentication systems can be easily bypassed using stolen account credentials often obtained through Phishing schemes, or malware Trojans infecting the account holder's PC directly. Once infected, Trojans can evade antivirus detection using stealth malware tactics to gather login credentials from unsuspecting users. In turn, these legitimate credentials can be used to initiate fraudulent transactions from the victim's account – all leading to the loss of money for the financial services organization and its customers.

Unfortunately, Man-in the Browser and other types of attacks launched from the customer's system have been show to be able defeat and bypass traditional Device Identification based anti-fraud and Two Factor Authentication solutions.

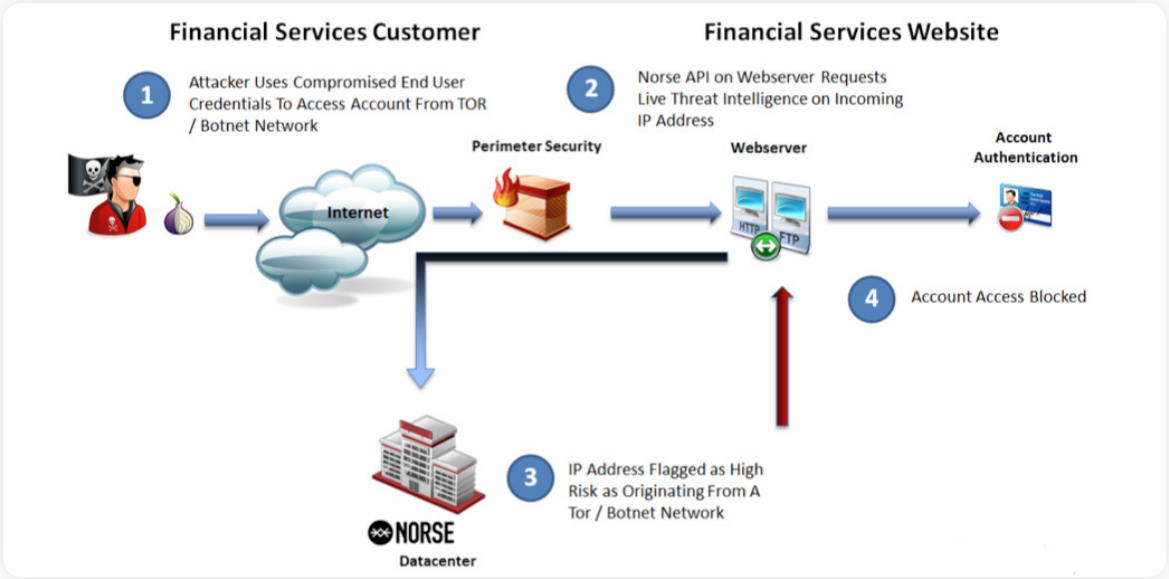


Fig 5. Blocking account access using Norse as customer endpoint identified as high risk due to Trojan infection

The integration of live attack intelligence into the financial services Website at the point of user authentication can help determine the risk or threat factor to automate the decision process needed to drop the connection, permanently block the connection, allow the connection, or elevate the session requirement to include a secondary or alternative "out of band" authentication.

Norse Live Attack Intelligence for eCommerce Fraud Prevention

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 benefits Financial Services organizations by automating the real-time detection and blocking of fraudulent transactions, proactively adapting to cyber criminals new techniques, and mitigating risks of TOR and Proxy based threats. Using Norse's proprietary IPQ risk score and easily defined rules and thresholds, Norse enables merchants and payment gateways to instantly accept or deny most orders before it is submitted for approval - helping merchants and service providers to reduce chargebacks and the time and cost of manual transaction fraud reviews.

Conclusions

The FFIEC supplemental guidelines highlight the need of Financial Services organizations such as Banks, Online Trading Services, and Credit Unions to:

» Enhance existing anti-fraud solutions with formal risk assessments

» Adjust customer authentication controls in response to new online account threats

» Implement effective strategies for mitigating risk

» Raise customers' awareness of threats associated with electronic banking

Traditional Security and Fraud Controls were not Designed for Today's Advanced Threats

With multiple attack vectors and a rapidly evolving threat landscape, cybercriminals are increasingly able to use advanced techniques and attacks to perpetrate fraud by targeting the financial institution's website, breaching perimeter security to directly access critical systems, or compromising the consumer or business customer directly. While traditional security controls used in a layered security strategy have largely met the needs of financial institutions, they have proven to be virtually static in their defense, and lack the flexibility to proactively defend against the speed and sophistication of new advanced and zero day threats.

IP Blacklist Services Lack the Required Coverage, Context, Speed, and Accuracy

As with all technology, each generation has perceived limitations - from the basic first generation SPAM Blacklists and Whitelists to the limitations of second generation Reputation Services – organizations are often overwhelmed by the speed at which the threat landscape evolves and the demands put on IT to defend against new threats using existing security technologies. Internet protocol (IP) reputation is one technology specifically recommended in the FFIEC supplemental guidance as a means to directly address targeted attacks and add an additional, complementary layer to the existing layered security approach. As described earlier in this document however, there are many issues associated with current IP Blacklist and feed services that make them incomplete and unreliable solutions for blocking advanced attacks.

Live Attack Intelligence Provides the Missing Layer

What is missing in these existing defenses is the ability to make accurate automated decisions based on live attack intelligence provides the next evolutionary step in IP reputation technology with services that easily integrate with websites, applications, and network edge devices, often strengthening existing security and fraud controls. Beyond simple IP blocking, Norse's breadth and depth of threat intelligence collection, 1,500+ risk factors, speed of analysis and delivery provides organizations with the global coverage, context, accuracy, and performance missing from today's IP blacklist and reputation services. Armed with live attack intelligence organizations can quickly implement automated, intelligence-based security and fraud prevention strategies that dramatically reduce an organization's cost of fraud and risk of compromise and breach.

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.

NORSE norse-corp.com