

WHITEPAPER

Cybercrime Battle Basics

Online Account, Transaction and Device Protection

ThreatMetrix™ Cybercrime Defender Platform



Contents

You Can't Fight the Fire from Behind the Firewall	3
Traditional Device Identification Has Become Obsolete	4
IP Addresses Cannot Be Trusted	4
Cookies Can Be Copied and Sessions Hijacked	4
You Can't Stake Your Business on Your Customer's Antivirus	5
Man-In-The-Browser	5
Man-In-The-Mobile	6
Rootkits	6
Requirements for Integrated Device and Transaction Security	7
Introducing ThreatMetrix™ Cybercrime Prevention Platform	8
Conclusion	9

You Can't Fight the Fire from Behind the Firewall

The cybersecurity war is fought on the new frontier of unregulated and insufficiently protected computers belonging to customers, contractors, business partners and the web applications with which they transact, login, consume and share. The unstoppable consumerization of the enterprise means the front has expanded to include employee smartphones and laptops that roam between private and public networks.

In this battle, no networks need to be breached when the keys to the front door lie on phishing sites, unprotected consumer devices, social networks and compromised credit cards. The artificial division between corporate data and assets and those belonging to their customers and employees is convenient for existing enterprise security vendors but does not stand up to the hard reality of an embedded and amorphous foe that is better equipped, highly connected and immune from retribution.

The actual task of stemming the torrent of money, customer satisfaction and shareholder value that gushes to the tune of tens of billions a year out the Internet front door falls at the feet of the irregular army of the fraud department. This group is loosely organized into silos depending on whether they are internal or external focused, or by specialization depending on whether fraud is associated with an online credit card payment, a new account enrolment or compromised account.

To the same degree that their security cousins are focused on endpoints and perimeters but largely ignorant of anything that happens after the submit button, today's fraud fighters attempt the equivalent of taking on tanks with sticks while blindfolded as their transaction processing systems, locked behind the firewall knowledge gap, have zero knowledge as to true identity, integrity and reputation of the anonymous device behind the transaction. On the Internet they say no one knows you're a dog, but enterprises are spending hundreds of millions of dollars on technology that can count dogs.

The problem lies not with either discipline; the fact is that fraud and security are just two sides of the same cybercrime coin. Effective enterprise cybercrime prevention requires an integrated and layered approach to device and transaction security for the entire customer acquisition lifecycle. To achieve this, enterprises need two core capabilities:

- Device identification: The ability to instantly differentiate between valuable customers and employees, and cybercriminals using stolen identities and credentials
- Malware protection: Once identified as a valued customer or employee device, the ability to validate that the device is in a safe and secure state to guarantee transaction integrity

Traditional Device Identification Has Become Obsolete

First generation device identification methods that relied primarily on cookies and IP address intelligence have proven to be completely ineffective against modern cybercriminals. For evidence, consider the fact that new FFIEC Online Banking Authentication guidance requires an upgrade to next generation “complex device identification” technologies in response to two key threats.

IP Addresses Cannot Be Trusted

Every cybercriminal worth their salt knows that the weakest link in any authentication method is the enrollment. When opening a bank or trading account with stolen credentials, the preferred method is to use the online equivalent of a patsy, an intermediate computer or so-called proxy, to disguise the true originating device and location. In the first evolution of crime on the Internet, spam and click fraud were routed through poorly configured web servers that would relay incoming traffic onto a new IP address.

ThreatMetrix' own tests in 2008 demonstrated that it took approximately 10-15 minutes for a misconfigured server to be found by scanners, with the first malicious traffic being routed within 20 minutes. Lists of these open proxies were shared by hackers, but were also eventually added to IP proxy lists by whitehats. This drove criminals to use malware that installed backdoor proxies that listened on random ports known only to the botnet controller and hence were invisible to whitehats and competitive bot herder port scanners alike. The newest botnets have now migrated to Virtual Private Networks (VPNs) that are immune to attempts to get clients to leak their true IP information.

Likewise, relying on IP address to authenticate a returning customer is problematic for corporate networks and ISPs alike that pool large numbers of devices behind a single external IP address.

Cookies Can Be Copied and Sessions Hijacked

As trivial as it is for a fraudster to delete a cookie to try and evade detection, it is even more problematic if a fraudster is able to hijack customer privileges by hijacking sessions and authentication cookies. Wi-fi networks make it trivial for fraudsters to eavesdrop on traffic and implement Ethernet Address Resolution Protocol (ARP) attacks to sniff traffic from a target device.

Using an ARP attack, the cybercrime doesn't have to compromise the target device, it merely intercepts all traffic between it and the router/gateway. For remote attacks, DNS Spoofing and Cross-Site Scripting (XSS) have also proven to be successful at stealing sessions. As sophisticated as they may sound, most popular commercial intrusion prevention tools such as Metasploit, Burp Suite and BugTrack implement many session hijack techniques as routine tests.

You Can't Stake Your Business on Your Customer's Antivirus

Since 2006 ThreatMetrix has tracked the reputation of billions of compromised computers. Anywhere between 10-15 million are active at any given time, being used as a launch platform for a multitude of illegal activities. Originally used to send spam and phishing emails, the use of compromised computers expanded to include click fraud, affiliate fraud, credit card fraud and more recently banking fraud.

This last evolution was a response to online banks deploying device identification and out-of-band authentication technologies. Customer Device Identification made it much more difficult for phished credentials to be replayed from a remote computer while out-of-band authentication used One-Time-Passwords (OTPs) delivered either via SMS or hard token as additional assurance that the transaction was being initiated by the true owner of the account. The following section describes how on-device attacks have evolved to cause newer multi-factor authentication defense systems to start firing blanks.

Man-In-The-Browser

So called man-in-the-browser (MitB) attacks typically leverage browser plugins to inject JavaScript directly into the online banking page before or during a valid login by the remote user. Controlled through configuration files, MitB Trojans have been shown to completely incapacitate multi-factor authentication schemes through a number of techniques, depending on what it is instructed to do:

- **Form Field Injection:** The MitB injects form fields into the login page requesting the user for additional authentication information such as mother's maiden-name, social security number or OTP received via SMS or hard token. Personal data is normally used to answer challenge questions when the attacker attempts to enroll a new device, or to answer security questions when calling in via phone.
- **Data Theft:** The MitB uploads captured credentials and information such as cash balances to a drop-zone site for immediate or later use or sale.
- **Content Insertion:** If a OTP is intercepted, a MitB can be instructed to present a message to the user that the service is down or delayed while the hacker uses the stolen information to steal money.
- **Automatic Posting:** In the example above, the MitB posts a transaction in the background from the user's browser, typically using JavaScript.
- **Form Field Overwrite:** In this attack the MitB piggybacks on an existing money transfer by changing the payee account and post amount immediately when the submit button is pressed. The Trojan also overwrites the confirmation response so that the user is unaware the transaction has changed. Account balances are overridden to hide the attack.

Man-In-The-Mobile

In 2011 both Zeus and SpyEye also started targeting smartphones directly. The attack vector is essentially the same in both variants; a computer already infected will trick a user to key in a URL into their mobile device which when downloaded forwards One-Time-Passwords to the attacker. It is expected that hackers will soon evolve to automating downloads by exploiting mobile browser vulnerabilities when visiting compromised websites.

Rootkits

Installed deep in the operating system, rootkits give Trojans unfettered access to the entire OS, not just the browser, including the ability to sniff keystrokes for passwords and bank details, capture screenshots of virtual keyboards, disable firewalls and anti-viruses, turn off Windows updates, sniff packets on a network for vulnerabilities or infecting other machines. Rootkits are so effective at evading detection and removal that often the only remediation is to reinstall the operating system from scratch.

Requirements for Integrated Device and Transaction Security

Criteria	Requirement
Cookieless Device Fingerprinting	Passively collected device attributes to identity devices without requiring software or hardware tokens provides a first layer of defense across all website interactions. Unfortunately malware and fraudsters routinely delete, steal and tamper with browser and flash cookies and attributes. Cross correlating device fingerprint attributes and behavior with session and browser cookies provides an additional layer of authentication.
Man-In-The-Middle and True Origin Detection	Based on browser and packet fingerprint interrogation, automatically detects and classifies MitM attacks and bypasses hidden proxies to reveal the true IP Address, geo-location and origin of the transaction.
Compromised Device and Man-In-The-Middle Protection	Organizations not only need to identify a customer's device, they also need to know whether that device is now compromised and infected. Subscribing to IP reputation feeds is not enough if the botnet intelligence cannot be acted on while the customer is on the page.
Global Recognition	Ability to re-identify customer devices across sites, with proactive protection against known fraudulent devices and identities across the reputation network.
Integrated Contextual Risk Scoring and Decisioning	A risk decision based on device intelligence needs to be made in context based on the organization and transaction type requirements.

Introducing ThreatMetrix™ Cybercrime Prevention Platform

The ThreatMetrix™ Cybercrime Defender Platform goes beyond combining malware protection and device identification – it supplements the combined solution with real-time transaction intelligence and analysis across the enterprise and throughout a global network of sites sharing fraud information. Integrated into a single ThreatMetrix Cybercrime Control Center, the ThreatMetrix Cybercrime Defender Platform includes the following products:

- **TrustDefender™ ID:** TrustDefender ID is a cloud-based, real-time cookieless device identification solution that protects companies against cybercriminals and helps validate valuable returning customers. TrustDefender ID provides integrated shared reputation intelligence and identity verification to provide businesses with a crucial first perimeter of defense to protect online transactions, including account creation, login authentication and payment authorization.
- **TrustDefender™ Cloud:** TrustDefender Cloud is a cloud-based, real-time solution that helps companies protect customer data and defend against fraud, malware, MitB and Trojan attacks, and data breaches. It mitigates the risk of hidden malware compromising authenticated sessions to steal data, identities or money, the first time, every time.
- **TrustDefender™ Client:** TrustDefender Client provides malware protection without the performance hit. A small client component installed on end-user computers identifies and isolates malware, verifies legitimate websites, protects the online session with the business, and communicates with the business to identify potential fraud.
- **TrustDefender™ Mobile:** TrustDefender Mobile is an embeddable SDK for smartphone applications that creates cross-validating device fingerprints based on hardware, operating system and application parameters normally hidden from remote servers. In conjunction with TrustDefender ID's cloud-based device identification technology, TrustDefender Mobile provides bulletproof cross-platform authentication and fraud prevention without leaking personal information.

The ThreatMetrix Cybercrime Prevention Platform includes all of these technologies – that's the starting point. But it goes beyond simply offering best-of-breed solutions. The ThreatMetrix Cybercrime Control Center, part of the integrated platform, creates layered defenses by sharing information between these solutions and throughout the ThreatMetrix network, a global consortium of sites sharing fraud and cybercrime information.

With these solutions working in concert, businesses have new and powerful defenses against a fast-evolving threat environment. For example:

- Identify potential malware on a customer device and, in real-time, offer them client-software to lock down the transaction
- Identify new devices on your site that are active and suspicious across the global ThreatMetrix network
- Identify devices known globally to be participating in botnets when they visit your site and apply real-time fraud defenses
- Expose new MitB attacks that threaten customer transactions
- Look beyond apparent IP address and geolocation to find where devices are truly connecting from

And, as the threat environment evolves, the layered defenses keep pace with global intelligence that learns in real time. For the first time, online businesses have the ability to protect the integrity of an entire transaction, from the endpoint to the site.

Conclusion

As cybercrime exploits become more sophisticated, defending against them requires new, integrated approaches that look beyond the firewall and beyond single technology defenses. While human organizational structures may encourage segmented defenses, with different teams having different responsibilities, cybercriminals can exploit gaps and lack of communication for financial gain.

The only way to defend against online crime and fraud in this new environment is to work with layered, integrated defenses that share intelligence between them. And the best way to do that today is using the ThreatMetrix™ Cybercrime Defender Platform.

Contact Us

USA Corporate Headquarters:

ThreatMetrix Inc.
160 West Santa Clara Street
Suite 1400
San Jose, CA, 95113
Telephone: +1.408.200.5755
Fax: +1.408.200.5799

EMEA Headquarters:

ThreatMetrix B.V.
Laan van Vredenoord 33-39
2289 DA Rijswijk
The Netherlands
Telephone: +31 (0)70 8200 508

www.threatmetrix.com

www.threatmetrix.com/fraudsandends