ThreatMetrix®
BUILDING TRUST ON THE INTERNET™

WHITEPAPER

Advanced Cybercrime Tactics

Threats translate into crime. How do you stop them?

Cybercrime Can't Be Ignored

With data breach headlines appearing daily, it's well known that computer-related fraud and cybercrimes are significant, growing problems. On any given day, the news is filled with crime-ridden tales of company after company suffering online system breaches. In fact, a recent Ponemon study found that over the past four years, cybercrime-related costs have climbed an average of 78%, averaging a whopping $11.6 million dollars per company studied during 2013; moreover, the time required to recover from such a breach has increased by 130%[1]. Meanwhile, in Cisco Systems' 2014 annual security report, the company warned that the risk of cyber-attack and systems vulnerability is at its highest level since the year 2000[2]. Fraud due to credit card losses alone totals in the billions of dollars each year[3].

The problem is so severe that all IT professionals and managers, regardless of level, need to understand the basics of cybercrime—and how to implement appropriate defense mechanisms. This paper provides an overview of 10 common cyberthreats, with their corresponding ThreatMetrix™ safeguards.

Threats Translate To Crime And Compromise

The methods and technologies cybercriminals use to commit their crimes are innumerable, and continue to grow each year in both number and sophistication. With every new device, operating system, or application, new security holes and implications appear. Cybercrime fighters have to deal, not only with the security vulnerabilities of the past, but with an exponential number of new exposures each year.

Cybercriminals use various technologies or threats to attack these security holes. Much like vulnerabilities, these too are constantly growing in number and sophistication. Here is a short list of some of today's top threats:

- Malware
- Social engineering
- Phishing, vishing & smishing
- Stolen credentials
- Data center breaches

1 Fourth Annual Cost of Cybercrime Study, Ponemon Institute, Oct 2013
2 http://www.abc.net.au/news/2014-01-17/cisco-report-reveals-malware-posing- huge-hacking-threat/5205492
3 LexisNexis® 2013 True Cost of Retail Fraud Study

Without protection from vulnerabilities and threats, it's only a matter of time until attackers successfully breach even the latest websites and online applications, resulting in cybercrime.
The most common and damaging crimes involve:

- **Payment Fraud:** It's been estimated that credit card fraud accounts for roughly 40% of all financial fraud, with losses exceeding $5 billion dollars annually. Fraudsters commit payment fraud through a variety of methods, but most often by hacking merchant customer databases to steal credit card data, or by planting spyware in consumer devices to capture legitimate consumers' online session credential—then using this data either to commit "card not present" fraud or to create counterfeit credit cards.
- **Account Takeover/Data Security Breach:** This occurs when a victim's bank, online shopping, system administration, or other account is used by an unauthorized individual or process. Financial account takeover often involves removing funds by direct debit, making purchases or payments, or executing fund transfers, all without the victim's consent. In particular, taking over a privileged root or system administrator account can result in staggering losses, including denial of service, and theft of IP or millions of credit card records.

  Account Takeover is accomplished by obtaining user logon credentials through direct observation, network sniffing, password cracking tools, spyware, user visits to compromised or hacked web sites, session hijacking, phishing, social engineering, and many other techniques. Passwords alone are not sufficient to protect against these sophisticated schemes to obtain account credentials.
- **Fraudulent Account Creation:** Criminals create fraudulent accounts by using stolen or fake identities. Once created, these bogus accounts are used to commit payment fraud or launch additional attacks.
- **Multi-Channel Web Fraud:** When fraudsters use multiple, coordinated methodologies and components to commit their crimes, it's known as multi-channel web fraud. Hackers and fraudsters understand that large enterprise cybercrime defenses are often "stove-piped." Different business units frequently deploy standalone solutions that do not communicate well with each other. Criminals exploit this weakness by spreading their attacks across multiple applications or business units in order to avoid detection. Once they establish a beachhead within one application, they use it to launch costly attacks on other business units.

Cybercrime fighters must be ever diligent in their battle against threats. Failure to do so will result in costs that far outweigh the price of protection. As an example, studies show that costs associated with stolen credit card data amount to over $175 dollars for every record[4]. The losses of just 100,000 records can be over $17 million dollars. Unfortunately, it's all too common to hear of companies losing millions of records and tens of millions of dollars.

4 2013 Cost of Data Breach Study, Symantec and Ponemon Institute, May 2013

Cybercrime Detection and Prevention

The various technologies, products, and solutions to battle cybercrime can be broken into two broad areas: passive defenses and active defenses. While the detection features of passive defenses can be useful, the preventative power of active defenses makes them your most effective choice.

Passive Defenses: Detection

Passive defenses scrutinize cyber-events at session, transaction, log, and network levels. They look for anomalies, log them, and raise alerts, but take no other action. Passive defenses detect and record what has happened, but they themselves don't alter traffic, or reject connection attempts, or deny transactions. Passive defenses are not effective in stopping crime in real time. Primarily forensic tools, they are most useful in analyzing an incident after the fact.

Active Defenses: Prevention

Active defenses, available from ThreatMetrix, are tightly integrated into protection systems and processes. They're capable of altering results in real time, and can terminate or deny suspicious sessions and transactions, enabling them to prevent crimes before they occur. Active defenses can also take steps to proactively analyze behavior and collect intelligence well in advance of future actions or transactions, thus setting up defenses and protection mechanisms before they are needed.

Examples of ThreatMetrix active defenses:

- **Pre-site Intelligence:** Billions of global intelligence data points are collected from thousands of cooperating entities, providing information about users long before they connect to a protected website. User devices, logon names, email and physical addresses, geolocations, typical online behaviors, and other attributes are known in advance. Additionally, ThreatMetrix solutions can certify the level of user trust or risk by applying "Trust Tags," greatly accelerating the process of identifying trusted as well as untrusted users.
- **Visitor and Device ID:** Desktops, laptops, tablets, smart phones, or other devices are uniquely and individually identified across the globe, and are associated with one or more users or owners. Individuals are also identified, and are associated with user names, accounts, addresses, geolocations, devices, and more. Devices and users may be tagged as trusted or untrusted.
- **Botnet and Malware Detection:** A significant amount of fraud occurs from malware that exists on the devices of legitimate users. Advanced ThreatMetrix authentication and fraud prevention systems proactively look for and identify malicious code on devices before they are allowed to log on or execute a transaction. Not only are devices examined for malicious threats at connection time, they are—if infected—tagged as such in ThreatMetrix's Global Trust Intelligence Network, as a future warning to all cooperating organizations worldwide.

- **Behavior Screening:** A real-time user persona, which establishes typical user behaviors, is created as part of ThreatMetrix's advanced authentication. Home, work, or other common geolocations may be identified; frequency and times of logins, associated accounts, and other behavioral data are gathered in advance; and the resulting information is used to detect anomalies or suspicious behavior—all with the goal of establishing levels of trust or risk.

ThreatMetrix Cybercrime Protection Platform

The ThreatMetrix TrustDefender™ Cybercrime Protection Platform is a cloud based, active defense solution designed to reduce friction during transactions and access, and quickly establish trust with legitimate users, while at the same time guarding against fraud and unauthorized access. TrustDefender maximizes revenue, protects digital assets, and safeguards brands.

The system leverages the collective, shared power of the Global Trust Intelligence Network comprised of user and device attributes, to deliver context-based authentication. This next-generation, advanced authentication process is used to authorize payments and transactions, prevent the use of stolen or fake IDs during account creation, and protect access to established logon accounts.

Advanced context-based authentication from ThreatMetrix:

- Profiles end-user devices of all types to validate their identity and assess potential threats
- Identifies malware threats in the device or compromising the session
- Examines the user's identity, behaviors, and other attributes
- Configures business rules to accept, reject, or otherwise handle each situation
- Validates the effectiveness of business policies using real-time data
- Enables detailed analysis through visualizations and reports
- Creates and assigns Trust Tags to users based on various attribute combinations, to certify levels of trust or risk associated with any give user

Common Cybercrime Threats and ThreatMetrix Solutions

Here's a list of 10 common threats that can lead to fraud or unauthorized access, and sample ThreatMetrix solutions for each. Of course, individual applications will vary, and not all possible solutions are shown, but these examples illustrate several ways in which threats can be brought under control.

Threat #1: IP Address and Geolocation Spoofing

Protection systems often use end users' locations as one way to authenticate their identities. Locations can be determined by an end user's IP address and geolocation. But attackers with even limited skills can easily change both IP address and geolocation to make it appear as though they are in a different location. Moreover, scripts or human attackers can use a VPN, proxy or TOR network, or botnets to hide their true IP address and geolocation.

ThreatMetrix solutions can actively authenticate and assign levels of risk to a transaction based on:

- ☑ Direct detection of VPN based on packet fingerprinting
- ☑ Direct detection proxy using proxy piercing and packet fingerprinting
- ☑ Detection of known proxy IP Address
- ☑ Detection of known hosted server providers
- ☑ Cookieless device identification to detect IP Address with multiple time zones/zip codes/ devices/identities across network

Threat #2: Botnets and Scripting Attacks

Attackers like to launch their crimes from someone else's computers or devices to help cover their tracks; and, by using lots of computers, attackers gain additional advantages such as added sophistication, performance, redundancy, and subterfuge. Botnets are networks of individual, often private computers which have been infected with malicious software and controlled as a group, without the owner's knowledge. Attackers use botnets to spread Trojan horses and other viruses, and to plant spyware for the purposes of capturing and stealing payment card data and account credentials.

A typical attack involves a fraudster using botnets and proxy networks to automate password guess attempts, and to capture and post content.

ThreatMetrix solutions can defeat these types of well-organized attacks by:

- ☑ Detecting a high-velocity sequence of password attempts, or a high frequency of such attempts, using cookieless device identification
- ☑ Detecting short time-on-page
- ☑ Detecting VPN/proxy usage
- ☑ Detecting browser and device anomalies
  - Screen size and resolution anomalies
  - Images/Flash/JavaScript turned off
  - Virtual machine detected
  - Unusual packet fingerprint (e.g. bare-bone Linux)

Threat #3: Stolen and Spoofed Identities and Payment Card Fraud

Narrowly defined, stolen identities are equivalent to stolen credentials, and equip attackers with everything they need to assume the identity of another person, at least on a specific account. Attackers, however, prefer to obtain as much information about their victims as possible, including credentials for numerous accounts, as well as personal information that will allow them to answer challenge questions, receive shipments, and more. Identities may include logon credentials, credit card data, Social Security number, address, phone numbers, date and place of birth, and even answers to specific and personal challenge questions.

In a typical stolen identity attack, human fraudsters or botnets register for an account using stolen or spoofed identities, or use stolen credit card information to steal goods.

ThreatMetrix solutions can identify the use of stolen credentials by:

- ☑ Detecting multiple identities using the same device
- ☑ Detecting private browsing or excessive cookie deletion
- ☑ Detecting use of Proxies or VPNs
- ☑ Detecting frequent or rapid account registrations, or transactions from the same device
- ☑ Detecting computer-generated names and emails
- ☑ Recognizing both high-risk and trusted devices and users within the network

Threat #4: Stolen Credentials and Breached Accounts

In the fraud and cyber community, credentials refer to the information required to gain access to a wide rage of accounts and systems. Typically, they consist of a logon username and a password. Using stolen credentials is by far the most common method for gaining access to accounts, including privileged administration and financial accounts. A large percentage of the most damaging cybercrimes of all time have been, and continue to be, committed with stolen credentials.

ThreatMetrix advanced cybercrime protection systems use two-factor authentication and other technologies to significantly strengthen the security of credentials and detect their theft.

ThreatMetrix solutions:

- ☑ Utilize two-factor authentication to prevent account takeover
- ☑ Recognize both high-risk and trusted devices and users within the network
- ☑ Detect access from new locations or new devices
- ☑ Detect login attempts whose geolocations are suspiciously far from recent previous ones
- ☑ Detect devices accessing multiple unrelated accounts
- ☑ Track mobile devices accessing “honey-pot” accounts specifically designed to attract and contain criminals.
- ☑ Provide step-up authentication as needed

Threat #5: Crime Rings and Collusion

The axiom “There’s strength in numbers” is frighteningly true where cybercriminals are concerned. “Collusion” refers to multiple fraudsters working together. It may be as simple as the utilization of an insider, or as sophisticated as a full system of fraud rings—each performing elaborate steps to obtain an element essential to the intended crime.

A typical collusion attack involves groups of devices and criminals, acting in concert, using pooled identities, passwords or credit cards.

ThreatMetrix solutions actively provide a defense against these coordinated attacks through:

- ☑ Real-time detection of related transactions linked by devices, identities or attributes
- ☑ Detection of identities being used across different geographies, IP addresses, time zones, and languages in short periods of time
- ☑ Powerful custom-match capabilities, to flag transactions with related attributes

Threat #6: Session Hijacks, Man-In-The-Browser, Man-in-the-Middle

If criminals can insert themselves into a session between a website and a user, they can alter the conversation and commit fraud. There are a number of techniques criminals use to get inside a session, including man-in-the-browser (MITB), man-in-the-middle (MITM), and server-side malware injections.

MITB attacks typically take the form of a proxy Trojan horse that infects web browsers. Unseen by the website or user, the malware may capture user names, passwords, credit card numbers, and other data, sending it to the hacker. The malware may also commit fraud by modifying web pages submitted by the user, and may even make purchases or transfer funds to the hacker's account.

MITM attacks are a form of active eavesdropping where the attacker makes independent connections with the victims and their intended web site, and relays messages between the two. It appears to both the user and the web application that they are communicating directly with each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker may wait until the user is successfully authenticated, then capture cookies and credentials—or even modify web pages to execute unauthorized transactions.

Server-side malware injections occur when hacked websites are infected with malware that, in turn, infects the browsers or devices that connect to them. This malicious code may capture user logon credentials or credit card data, launch man-in-the browser attacks to alter web pages, or execute a number of other fraudulent actions.

ThreatMetrix solutions can detect MITB attacks by utilizing:

- ☑ Page fingerprinting to ensure pages have not been altered
- ☑ Botnet or malware detection, through analyzing actions and settings such as
  - Time-on-page unusually fast
  - Screen resolution anomalies

ThreatMetrix solutions can detect MITM attacks by detecting:

- ☑ Device profile changes between login and transaction
- ☑ Unrecognized device for this account
- ☑ Cookie copying detected

ThreatMetrix solutions can identify server-side malware injection though the use of:

- ☑ Page Fingerprinting to detect server-side page injections
  - Differences in page content delivered to visitors vs fraud and security administrators are immediately detected

Threat #7: Phishing Attacks

Phishing attacks lure victims into connecting with a fraudulent web site posing as the intended legitimate site. Victims interact with the imposter site, where they are asked to submit their logon credentials such as user names, passwords, or other sensitive data.

Phishing "lures" come in many forms, but most frequently, potential victims receive emails asking them to connect to what appears to be their legitimate bank site, e-commerce site, or other online service provider.

ThreatMetrix solutions can alert when the following conditions exist:

- ☑ Phishing site detected
  - Use regular expression pattern matching to detect when referrer to login page looks similar to customer domain
- ☑ Page copying detected
  - Detect when page content has been copied to a non-customer domain
- ☑ Mutual authentication with client-server, via downloadable client

Threat #8: Pharming Attacks

Pharming is the evil twin of phishing, and has been called "phishing without the lure". Like phishing attacks, pharming directs victims to bogus websites that look legitimate. These imposter sites ask victims to submit user and account credentials including user names, passwords, and credit or debit card numbers. Unlike phishing, which sends a lure (such as an email) to victims, pharming uses malware to automatically redirect users to bogus sites, without their knowledge.

In one form of pharming attack, malware modifies local host files on a personal computer, converting URLs into the addresses that the computer uses to access Web sites. A computer with a compromised host file will go to the fake website even if a user types in the correct URL or clicks on an affected bookmark.

ThreatMetrix solutions can detect these attacks by identifying and alerting on:

- ☑ Operating system anomalies
- ☑ Operating system or client's browser differs from OS detected by packet fingerprinting

Threat #9: Spyware and Keyloggers

In this scenario, attackers infect victims' desktop, laptop, tablet, or phone with malware that steals their credentials. A typical approach captures the user's keystrokes, enabling the attacker to steal anything typed or entered, including user names, passwords, credit card numbers, and more.

ThreatMetrix solutions protect users by detecting spyware or keyloggers with:

- ☑ Downloadable client that protects against all zero-day malware
  - Kernel and memory forensics
  - OS patch and anti-virus update checking
  - Suppression of unknown or untrusted processes
  - Lock-down of non-trusted Internet connections

Threat #10: DNS Spoofing

In this attack, the authentic IP address for a legitimate site, such as the user's bank, is replaced with an address for an attacker's bogus site, which mimics the intended site. The victim types or selects the correct domain, such as www.mybank.com, but connects instead to an imposter site. This attack can be carried out by malware that alters the hostname file on the victim's device, replacing valid IP addresses with the attacker's address, or by compromising the DNS server used by the victim's device.

ThreatMetrix solutions provide protection from DNS spoofing by:

- ☑ DNS Hardening
  - Downloadable client provides mutual client-server device authentication
  - IP Address access is locked down to site's SSL certificate
  - Optional toolbar provides visual cue that customer is logged onto a valid and protected site

ThreatMetrix®
BUILDING TRUST ON THE INTERNET™

Summary and Conclusion

Most websites are attacked multiple times each day, with many sites experiencing thousands of probes daily as attackers look for vulnerabilities. With attacks becoming so frequent and growing ever more sophisticated, it's imperative for website and web application owners to take immediate, effective precautions.

When searching for protection from cybercrime, decision makers need to carefully weigh the advantages of the various solutions, keeping in mind the fundamental differences between passive and active defenses. Active defenses offer more protection, with the best solutions leveraging global intelligence to proactively prepare against cyber threats.

In spite of all the challenges, there is some good news. ThreatMetrix provides the most effective fraud prevention and user authentication platform for businesses looking to protect online and mobile access to high value applications. ThreatMetrix can help your business stop fraud, maximize revenue, and protect digital assets and brands.

For more information about fraud prevention and context-based authentication solutions, please visit
www.threatmetrix.com