ThreatMetrix™

WHITEPAPER

Five Trends to Track in E-Commerce Fraud

Fraud is nothing new if you're in the e-commerce business – you probably have a baseline level of fraud losses due to stolen credit cards, return fraud and other tactics. But with the rapid changes to the online fraud environment, those losses are going to escalate unless you alter your fraud prevention tactics to keep pace.

Several new trends should make businesses that do online sales and commerce sit up and take notice. Taken individually, each trend may seem manageable. But when you put them all together, they paint an increasingly threatening picture for businesses that sell goods and services through online websites.

This paper outlines five troubling trends in e-commerce fraud, and offers some guidance on how you can mitigate the risk they present to your business.

Trend #1:

E-Commerce is the new “low hanging fruit” for online fraud.

For years, cybercriminals have focused their efforts on online financial services – in particular online banking, trading and payment processors. As a result, financial institutions have had to defend themselves against a constantly evolving body of malware targeting banking credentials and transactions. Regulatory requirements have changed to address this new risk environment.

As financial institutions put layered defenses in place, e-commerce sites remain relatively unguarded in comparison. Recent months have seen malware starting to target e-commerce sites. Online shopping sites are attractive targets for attackers, for several reasons:

- There’s a lot of money changing hands online. Acccording to Comscore[1], total online spending from November 1 to December 2 of 2012 totaled $21.3 billion - the entire gross domestic product of many small countries.
- Retailers have access to customer credit card information and deliver tangible goods or instant, digital goods that criminals can resell.
- Most e-commerce sites lack the layers of fraud and theft protection that financial institutions have put in place.

Cybercriminals are increasingly taking the techniques refined in financial services fraud and turning them to e-commerce sites. For example, a new variant of the Zeus virus is targeting online shopping sites, while other malware targets a common online commerce platform used by many sites.

At ThreatMetrix, we expect that the steady growth in online spending will be accompanied by a significant, potentially steeper increase in e-commerce fraud and theft.

[1] ComScore press release December 5, 2012; www.comscore.com/insights/Press_Releaes/2012

Trend #2:
Account takeover and identity theft are on the rise.

Research by the Merchant Risk Council identifies identity theft and account takeover as two of the top concerns for e-commerce providers. In research the Aite Group conducted with e-commerce merchants in spring of 2012, 50% of the surveyed merchants noted a "significant increase" in account takeover.

Obviously, the concerns are closely related. If a criminal has a legitimate user's credentials, they can then hijack that customer's account (account takeover fraud). Once they have control of the account, they might simply execute a one time fraudulent transaction – such as making a purchase. Or they could try to disguise their tracks and prolong the takeover. Signs of an account takeover might include:

- Changing shipping addresses
- Adding themselves as a registered user on the account
- Changing the email and password associated with the account

In these cases, the criminal hopes to extend the duration of the fraud, potentially increasing the financial losses for you or your customer.

According to the Aite Group, 50% of malware strains in the wild are designed to compromise credentials (identity theft)

According to the Aite Group, 50% of malware strains in the wild are designed to compromise credentials (identity theft)

Trend #3:
Mobile is the new desktop.

Another factor in the e-commerce threat environment is the growing use of mobile devices. Smart phone usage is increasing rapidly – but the growth in mobility doesn't end there. For many people, tablets are replacing laptops, and laptops replacing desktop systems.

People are using those mobile devices for online shopping. According to the 2012 Internet Trends report[2] mobile devices accounted for 24% of all online shopping traffic on Black Friday of 2012.

This growing mobility has important ramifications for traditional defenses against fraud and malware:

- Many device-oriented defenses don't work well with smartphones and tablets. These devices don't provide the same kind of device information as traditional Windows or Apple-based laptops and desktop systems.
- It's harder to use location as a factor when devices are mobile.
- Mobile devices are a 'green field' opportunity for many attackers, as most lack the anti-virus and anti-malware defenses now well established on desktop systems.

Criminals will continue to target mobile devices, including tablets, particularly as consumers increasingly use them for online shopping.

[2] Mary Meeker, Kleiner Perkins Caulfield Byers, Internet Trends 2012 (Website www.kpcb.com/insights/2012-internet-trends-update

According to the 2012 Internet Trends report by Mary Meeker of Kleiner Perkins Caulfield Byers, there are 1.1 billion smartphones around the globe.

Trend #4:
Malware is everywhere.

E-commerce sites are familiar with traditional, human-powered fraud schemes, such as price scraping, returns abuse and reshipping. But non-human malware is a much more difficult target, as it is constantly evolving and reshaping itself.

Mobile devices offer cybercriminals new, often unprotected platforms for delivering their malicious code. For example, on the Android platform there is a widespread category of malware called OpFake that disguises itself as the OperaMini browser or otherwise uses the browser download as an attack vector.

Once you could protect yourself by simply being careful about sites visited and software downloaded. As cybercriminals get more creative in finding ways to implant malware, it's increasingly difficult for people to protect their devices, whether laptops, desktops, tablets or smartphones.

According to Aite Group, the best strategy is to assume that any endpoint can be compromised.

Aite Group estimates that there are 111,111 unique strains of malware deployed each day.

Trend #5:
Even your trusted customers cannot be trusted.

Malware puts both you and your customers at risk of payment fraud, in which thieves make fraudulent purchases using stolen credentials or hijacked accounts.

Many traditional fraud measures look at the user's device to help make sure that the user is who they claim to be. If a device is connecting from Africa, for example, when the customer resides in Maryland, then that's a red flag. They assume that the person with the trusted device is the trusted user, and is therefore safe. Malware breaks this model.

When a user's computer is infected with malware, the legitimate user and legitimate device are both on the other end of the transaction. The customer is entering into a transaction with your business in good faith. They are generally unaware that their device harbors malware.

Man-in-the-Browser (MITB) and Man-in-the-Middle (MITM) malware can intercept the transaction with your business and manipulate it for various reasons.

For example:

- The "OddJob" malware keeps a session open, behind the scenes, after the user thinks that they have logged out – enabling the malware to then make transactions on the authenticated session.

- MITB attacks can subtly alter the authentication page for your e-commerce site, asking for personal or payment information.

With malware so pervasive, you can no longer trust that a legitimate user connecting to your site is free from these exploits.

Adjusting to the new reality

Today's environment requires a fundamental shift in how you look for fraud. While existing fraud methods are not going away, they must evolve to confront new methods and sophisticated malware.

In adjusting to this evolving threat environment, financial services organizations can serve as a guide. They have been the leading target of financially motivated fraud and malware, and are taking steps to mitigate the risk.

FFIEC guidelines state that financial institutions must adopt a layered approach to fraud prevention. More specifically, they recommend that financial institutions use complex device identification, a layered security approach and effective malware protection to safeguard assets.

Today, online banking and financial services sites are adopting layered and integrated fraud defenses, at the urging of FFIEC guidelines. They are using multiple technologies to catch a broader range of fraud and increasingly sophisticated attacks. By following their example, you can keep on pace with the best practices in an industry focused on mitigating risk and protecting profitability.

Specifically, here are some suggestions for building your own layered fraud defenses:

- Don't abandon existing methods and strategies. There is still value in using cookies, for example, as well as behavior profiling, if you integrate this data with advanced device identification technologies.
- Add malware detection technologies to help you spot malware that is manipulating your session for transaction fraud or account takeover.
- Combine behavior and device profiling to look for stolen credentials and account takeover, as well as devices that may be compromised by malware.
- Connect with a global fraud database to spot new trends and exploits as they develop, before they can do serious damage to your business.

ThreatMetrix For Malware Detection

ThreatMetrix Cybercrime Defender Platform includes the TrustDefender Cloud, Client and Mobile products for protection against malware. These malware protection products detect malicious software present on online retail customer machines, and prevents the malware from stealing customer credentials and committing online transaction fraud on your ecommerce website.

TrustDefender Cloud is a completely transparent, SaaS solution designed to prevent account takeover and protect online transactions from the most sophisticated web-based attacks including web session manipulation, cookie hijacking and Man-in-the-Browser attacks. TrustDefender Cloud can detect web attacks from any device including PCs, Macs or the various mobile devices common today.

TrustDefender Client extents the protection offered by TrustDefender Cloud to include machine resident malware that cannot be detected by web-based JavaScript alone. TrustDefender Client is a lightweight client program that scans the machine initiating online transactions at an extremely comprehensive level, including scanning the kernel, OS, applications, network and the transaction for any suspicious activity. Using this methodology TrustDefender Client can discover many hidden malware items that are not detected by the leading anti-virus products including Trojans, viruses, key-loggers, rootkits and spyware. This capability ultimately protects your customers' accounts from account takeover, and prevents compromised accounts from being used for fraudulent purchases on your website.

TrustDefender Mobile extends fraud prevention to mobile platforms and devices, by providing a light-weight embeddable SDK that can be integrated into your mobile app on iOS, Android, BlackBerry and Symbian. The TrustDefender Mobile SDK, once integrated into your dedicated online shopping app performs the same malware prevention functions for mobile devices as the Cloud and Client products do for the web-based platform.

Summary

The trends highlighted in this whitepaper combine to create a threatening picture for e-commerce sites. While consumers are connecting with your site using mobile devices, cybercriminals are targeting those users, compromising their credentials and taking over their accounts. It's clear that account takeover and the resulting fraud will escalate unless online merchants take measures to prevent it. The best strategy is to adopt the strategy online financial institutions have used to strengthen their defenses against hackers, fraudsters and malware, and implement layered account takeover prevention and payment fraud detection solutions.

About ThreatMetrix

ThreatMetrix is the fastest-growing provider of integrated cybercrime prevention solutions. The ThreatMetrix™ Cybercrime Defender Platform helps companies protect customer data and secure transactions against fraud, malware, data breaches, as well as man-in-the browser (MitB) and Trojan attacks. The platform consists of advanced cybersecurity technologies, including TrustDefender™ ID, which is cloud-based, real-time device identification, malware protection with TrustDefender™ Cloud and TrustDefender™ Client, as well as TrustDefender™ Mobile for smartphone applications.

Recently named to the Wall Street Journal's "Next Big Thing" listing of the top 50 start-ups in the U.S., the company serves a rapidly growing global customer base across a variety of industries, including financial services, e-commerce, payments, social networks, government, and healthcare. For more information, visit www.threatmetrix.com.

For more information, please visit us at:

www.threatmetrix.com

V1.10.2013