EASYSOLUTIONS

DETECT MONITORING SERVICES AND DETECT SAFE BROWSING:

Empowering Tools to Prevent Account Takeovers

SUMMARY

The Federal Financial Institutions Examination Council (FFIEC) is planning to update online transaction authentication guidelines for the first time since 2005. This regulatory oversight plans to put greater responsibility on the banks and credit unions to enhance their security and prevent fraud. Easy Solutions Detect Monitoring Services and Detect Safe Browsing are two state of the art tools that will surpass the security requirements set forth by the FFIEC and can help detect fraud before it happens.

TABLE OF CONTENTS

THE GROWING PROBLEM

1

Emerging Phishing Attacks and Financially Motivated Malware

It is no hidden secret that financial institutions have always been handicapped when it comes to protecting their customers from their own, ill-advised actions. Online fraudsters are well aware of this reality and are constantly launching sophisticated and organized attacks that obtain sensitive account information such as usernames, passwords, and challenge question answers. This information then leads to corporate account takeover and ensuing ACH/wire fraud that amounts to millions of dollars in losses annually.

Cybercriminals have various methods to steal credentials, but the most prevalent involve phishing attacks and malware that infect computer desktops and laptops of small and medium sized businesses. With phishing attacks, the fraudsters masquerade themselves as a trustworthy entity in an electronic communication such as an email. The carefully designed emails can imitate a variety of legitimate sources including social websites, business partners, financial institutions, and IT administrators.

The emails often direct the unsuspecting users to a fraudulent website where they provide sensitive account information that is captured by the criminals.

As for malware, a business employee’s computer can become compromised by opening a corrupt document that is attached to an email or by clicking on a link that connects to a malicious site. USB flash drives and legitimate social networking web sites also serve as vectors for spreading malware. For example, viruses and Trojans can be downloaded by clicking on an infected video or photo.

In recent attacks, criminals have combined phishing and malware. First, the criminals send out expertly engineered emails that mimic a reputable organization. The highly sophisticated emails look and feel so real that even the most cautious individuals are tricked into clicking malicious content. The links take the unsuspecting employees to fake websites that also appear authentic. Another click on the fraudulent website leads to downloading malware, and the computer is now infected.

THE GROWING PROBLEM

Financial Institution	Organization Attacked	Estimated Money Lost
Comerica Bank	Experi-Metal Inc.	$550K
Professional Business Bank	Village View Escrow	$465K
BankcorpSouth	Choice Escrow	$440K
PlainsCapital Bank	Hillary Machinery	$800K
Bankers Trust	Catholic Diocese of Des Moines	$600K
Ocean Bank	Patco	$500K

The malware installs key logging software that can capture the account credentials as soon as the user enters the login information at the online banking site. With this information now in hand, the criminal has complete access to the account, and thus has the power to initiate fund transfers. Ultimately, the funds are usually sent overseas via over-the-counter wire transfers, and the money is lost forever.

A major obstacle is that the financial institution has to assume that the banking sessions and subsequent transfers committed by the criminal are legitimate. By the time the affected business discovers there has been a breach, it is often too late to recover the money. Moreover, when commercial businesses and individuals fall victim to account takeovers, the associated financial institution bears the brunt of the economic loss. Countless investigation hours, irreparable reputation damage, and legal disputes that almost never favor the institution only compound the situation.

The current business model is not going to change in the foreseeable future. Businesses and individuals alike will continue to perform online banking on their computers because their day to day activities require it. Sophisticated, socially engineered attacks will without a doubt continue to target businesses, and they will have success at directly stealing credentials or installing malware that can do it later. Therefore, financial institutions have two options: continue reimbursing the corporate account takeover victims or start deploying new, proactive solutions than can prevent the takeover in the first place.

Easy Solutions has developed two powerful, proactive, and collaborative technologies that protect both the financial institution and its customers from phishing, pharming, and malware attacks.

DETECT MONITORING SERVICES

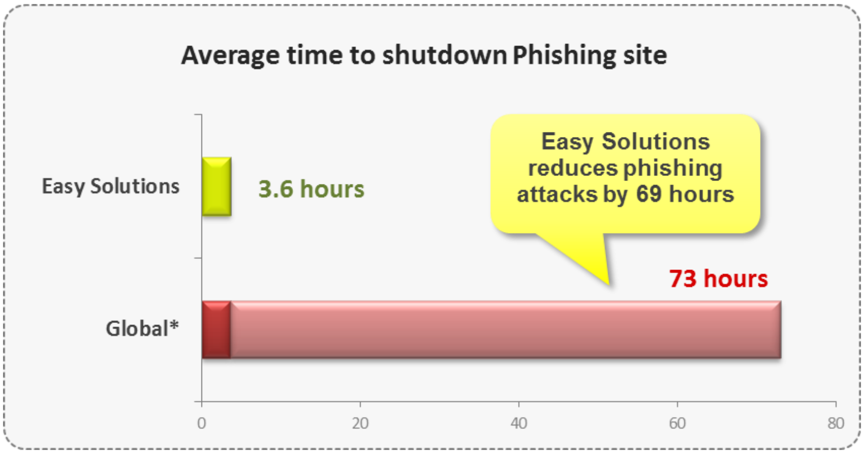
2

Proactive Anti-Phishing Protection

Detect Monitoring Services (DMS) is a dominant layer of security that detects and removes malicious users who are visiting a financial institution's website. DMS utilizes technology that collects high level user connection information in real-time such as the associated geolocation of the IP address, Internet service provider, visitation history of the user, time of day, type of operating system used, and additional relevant data. This captured information then feeds into a correlation engine that identifies a malicious user.

At this point, the Easy Solutions security analyst team that monitors the website connections on a 24/7/365 basis is immediately alerted and tracks the user's online activity.

The security analyst observes and investigates the actions of the user. For example, is the user simply exploring the website, copying the website, or injecting harmful code that exploits a security vulnerability of an application on the website? If there is any unauthorized malicious activity by the user, the security analyst notifies the financial institution and then deactivates any fraudulent phishing websites that were created. In short, DMS protects all online entities of the protected financial institution.



*Anti-Phishing Working Group, 2H 2010

More than ever financial institutions need to proactively protect their online banking channels. Cybercriminals are actively looking to exploit vulnerable websites. DMS is an intelligent technology and service that empowers financial institutions to work in the proactive zone of detecting malicious activity and phishing attacks and stops them before they can even be launched.

DETECT SAFE BROWSING

3

End User Level Protection

Easy Solutions has recognized this major void at the end user level and has created Detect Safe Browsing (DSB) to overcome it. DSB is a powerful yet simple application that protects end users from modalities of online banking fraud, such as phishing or pharming where antivirus and spyware removal software are not effective. DSB provides real-time malware protection and is installed and runs on the end user's computer(s) that performs online banking.

The Hosts file represents a serious attack vector for malicious software because its job is to map hostnames to IP addresses. If the Hosts file is hijacked and poisoned by financially motivated viruses or Trojans, the user is redirected from the intended destination to fraudulent sites. These socially engineered web sites appear authentic and capture sensitive information from unsuspecting users.

DSB works in the following manner: Before the user can connect to the online banking website, DSB will quickly scan the Hosts file and the processes running on the end user's computer. If DSB detects a malicious process that is poisoning the Domain Name System (DNS) server or Hosts file, BOTH the end user and financial institution are instantly notified.

The user will be warned that his or her computer is infected and that it is strongly recommended against conducting an online banking session. The financial institution can carefully monitor the user's transactions until the malicious process is stopped and deleted by the user.

DSB also verifies the IP address that the end user wishes to visit with the protected IP address listed on the Easy Solutions server. This IP validation is real-time pharming protection and prevents the user from redirection to counterfeit web pages where personal information can be stolen. The cyber criminals fail to infect the computer with malware and thus cannot obtain the account information.

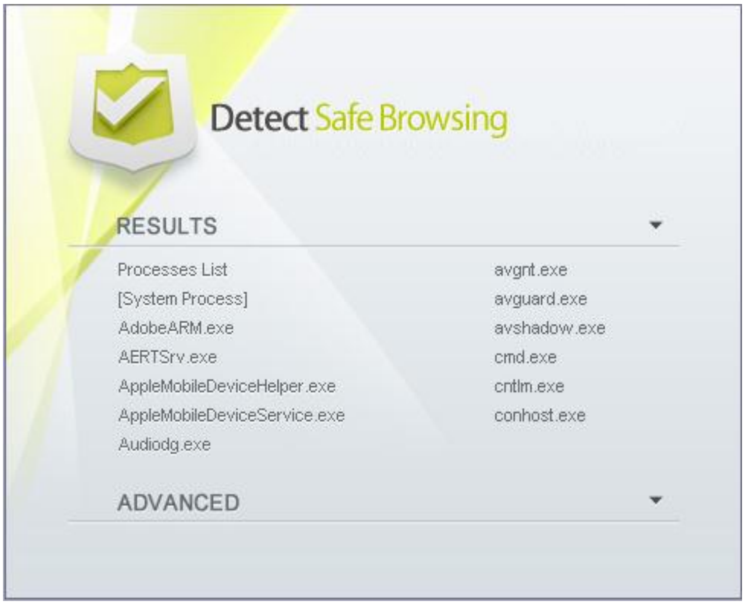
DETECT SAFE BROWSING

Key Features of Detect Safe Browsing

DSB can be customized to meet the branding needs of any financial institution. It is designed to be non-intrusive, effective, and fast. The entire scan takes milliseconds. The application is a one-time installation, and there are no end user updates; only the Easy Solutions server is updated. As new malware processes develop and evolve, Easy Solutions adds them to a blacklist that is continually updated. The malicious activity is also logged and history reports are provided. This summary information keeps financial institutions well connected and aware of the threats affecting them and their customers.

DSB detects and protects against the following:

- Hosts file poisoning
- Pharming attacks
- Malware attacks that include:
  - Key logging and screen logging
  - Financially motivated malware
  - Man in the middle (Proxy)
  - Man in the middle (ARP Poisoning)
  - Man in the middle (SSL Weakness)



Processes List
[System Process]
AdobeARM.exe
AERTSrv.exe
AppleMobileDeviceHelper.exe
AppleMobileDeviceService.exe
Audiodg.exe

avgnt.exe
avguard.exe
avshadow.exe
cmd.exe
cntlm.exe
conhost.exe

DMS AND DSB OPERATING TOGETHER

4

True Game Changers

It is important to note and understand that DMS and DSB feed off of each other. For example, when DSB detects malicious activity on an end user device, it's highly likely that additional users are also affected. In this case, the DMS team receives the information and initiates the deactivation process. All users benefit from this real-time, collaborative protection, and it is a unique differentiator in the industry.

Also noteworthy is that, in light of the recent lawsuits businesses are filing against their financial institutions for inadequately offering "commercially reasonable security solutions", both DMS and DSB can offer banks and credit unions much needed relief in the courtrooms. When a financial institution offers DSB to their customers, the businesses that fall victim to malware cannot make the argument that they were never offered an end user level security solution. The institutions can also point out that DMS is proactively protecting their online banking channels.

DMS and DSB also help financial institutions to comply with regulations. Regulators require that institutions conduct regular security and IT assessments. When vulnerabilities are discovered, the regulators want to see what actions the institution has undertaken to mitigate the problem. DMS and DSB are solutions that help mitigate online banking fraud by stopping phishing, pharming, and malware.

Financial institutions understand that the online fraud war is not ending anytime soon, and that they must deploy proactive solutions that effectively fight back. They also know that there is a growing list of regulations they must follow. DMS and DSB offer the financial institution an affordable, non-intrusive security layer that protects both the online banking website and the highly risky end user device.

START PROTECTING YOUR FINANCIAL INSTITUTION AND CUSTOMERS WITH DETECT MONITORING SERVICES AND DETECT SAFE BROWSING

For additional information including DMS and DSB demonstrations, please contact David Sylvester or visit the Easy Solutions website.

David Sylvester

dsylvester@easysol.net,

Business Development Manager

Tels: (206) 452-5613, (866) 524-4782 ext. 103

ABOUT EASY SOLUTIONS

5

Easy Solutions is the only security vendor focused exclusively on fraud prevention, providing anti-phishing services, multifactor authentication and anomaly transaction detection.

Easy Solutions delivers an integrated and comprehensive approach to multichannel fraud prevention and works in alliance with industry leaders in other security disciplines supporting a wide range of heterogeneous platforms.

EASYSOLUTIONS

Headquarters:
1401 Sawgrass Corporate Parkway, Sunrise, FL 33323 – Tel. +1-866-5244782

Latin America:
Cra. 13A No. 98 – 21 Of. 401 Bogota, Colombia – Tel. +57 1- 7425570.

www.easysol.net