PhishWall Remittance Fraud Countermeasures Solutions for Financial Institutions

PhishWall Premium/PhishWall Clientless White Paper

www.securebrain.co.jp

CONTENTS

The threat of cyber attacks targeting Internet banking

In recent years, cyber attacks targeting Internet banking with a view to financial gain have become increasingly sophisticated, involving scenarios devised by engineers with professional skills, and have become difficult to counter using conventional security measures. Malware attacks targeting Internet banking are particularly difficult to detect using conventional antivirus software. For this reason, the damage caused by remittance fraud through cyber attacks on Internet banking is growing every year.

One of the best known attacks in Europe and the United States is Operation High Roller, which in 2012 caused €2 billion of remittance fraud damages through Man-in-the-Browser (MITB) malware attack *1). In 2014, the threat came from GameOver ZeuS, which is thought to have infected between half a million to one million PCs worldwide and to have caused losses estimated by the FBI at more than $100 million *2). The most prevalent method of remittance fraud is shifting from phishing to malware but conventional phishing continues to cause damages. According to RSA, worldwide losses due to phishing in the month of November 2014 alone totaled $594 million *3).

SecureBrain is a Japanese security vendor that develops in-house countermeasure solutions against Internet crime. Highly skilled and experienced engineers in SecureBrain investigate and research increasingly complex net crime, respond swiftly to new threats and provide feedback to SecureBrain’s products. SecureBrain coordinates with Japan’s Metropolitan Police Department (MPD) to prevent net crime and limit the damage it causes. In 2015, the company provided technical cooperation to the MPD’s Net Banking Virus Neutralization Operation and played a part in preventing remittance fraud damage.

SecureBrain offers two remittance fraud countermeasures solutions — PhishWall Premium and PhishWall Clientless — in which if used together can provide stronger protection against MITB and MITM attacks.

Sources:

*1) Report by McAfee and Guardian Analytics;

http://www.mcafee.com/uk/resources/reports/rp-operation-high-roller.pdf

*2) US Department of Justice press release;

https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

*3) RSA report; http://www.emc.com/collateral/fraud-report/online-fraud-report-1214.pdf

PhishWall Premium (countermeasures against diversion to fake websites and MITB attacks)

PhishWall Premium is to be installed on PCs. It uses “authentication files” uploaded to the web servers of financial institutions that have deployed this solution to verify if the user is accessing its genuine website or not. When an Internet banking user accesses the website of a financial institution that has deployed this solution, PhishWall Premium could detect unauthorized behavior of MITB attacks and alert the user of malware infection.

Deploying PhishWall Premium

PhishWall Premium carries out authentication over HTTP/HTTPS. Deployment does not require additional dedicated servers. It simply involves uploading an authentication file set onto the existing web servers, and the system can be operational within a short timeframe. PhishWall Premium’s authentication file set are also not dependent on any specific OS environment. Network traffic during authentication by PhishWall Premium is very small compared to typical HTTP communications network, and the increase in traffic load on web servers due to the deployment of PhishWall Premium is kept to a minimum.

About authentication file sets

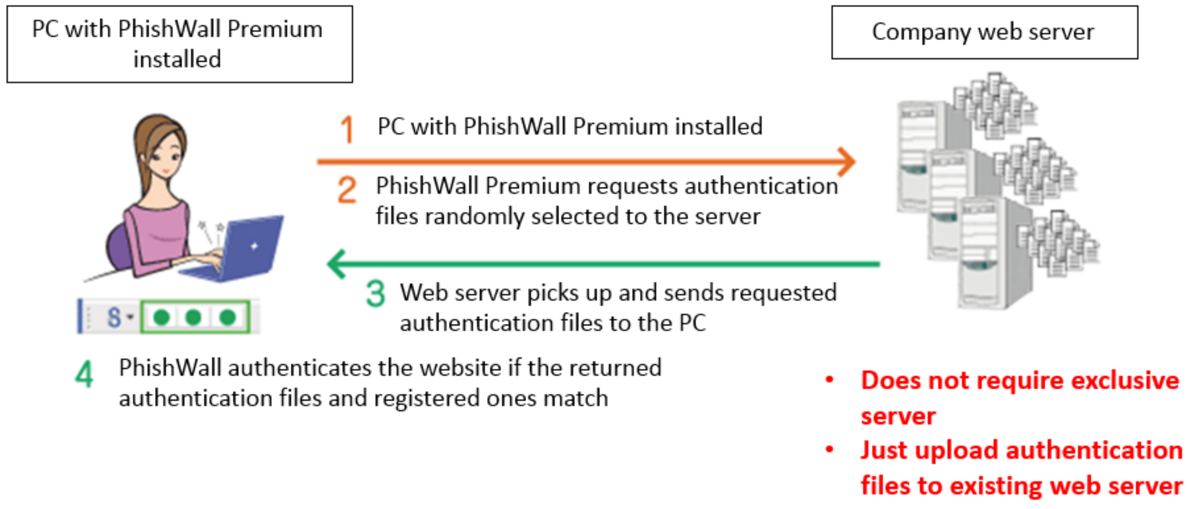
Authentication file sets consist of multiple text files and one html file (index html). They typically contain several tens of thousands of text files (approximately 300 MB in total size).

Authentication file sets need to be replaced annually.

PhishWall authentication (verifying that the website being accessed is genuine)

If PhishWall Premium is able to verify the three elements of the URL, IP addresses registered with SecureBrain, and the authentication files uploaded to the servers of the financial institution, it lets the PC user know by displaying a green signal indicating that the website being accessed is genuine and has not been falsified. Showing that the website is genuine at first glance prevents users from being diverted to a phishing website.

If the user accesses a genuine website, but is then diverted to a different website in an MITM (Man-in-the-Middle) attack, the green signal is not shown to warn the user of the anomaly.



PC with PhishWall Premium installed

Company web server

1 PC with PhishWall Premium installed

2 PhishWall Premium requests authentication files randomly selected to the server

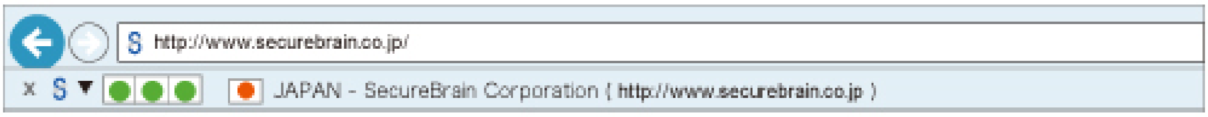
3 Web server picks up and sends requested authentication files to the PC

4 PhishWall authenticates the website if the returned authentication files and registered ones match

- **Does not require exclusive server**
- **Just upload authentication files to existing web server**

PhishWall Premium authentication signals

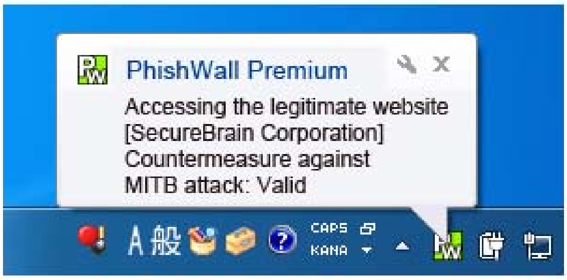
Internet Explorer edition



http://www.securebrain.co.jp/

JAPAN - SecureBrain Corporation (http://www.securebrain.co.jp)

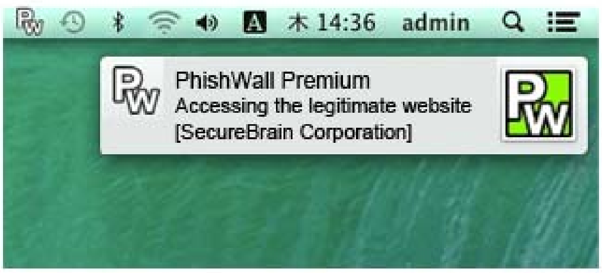
Firefox and Chrome editions



PhishWall Premium

Accessing the legitimate website [SecureBrain Corporation] Countermeasure against MITB attack: Valid

Mac edition



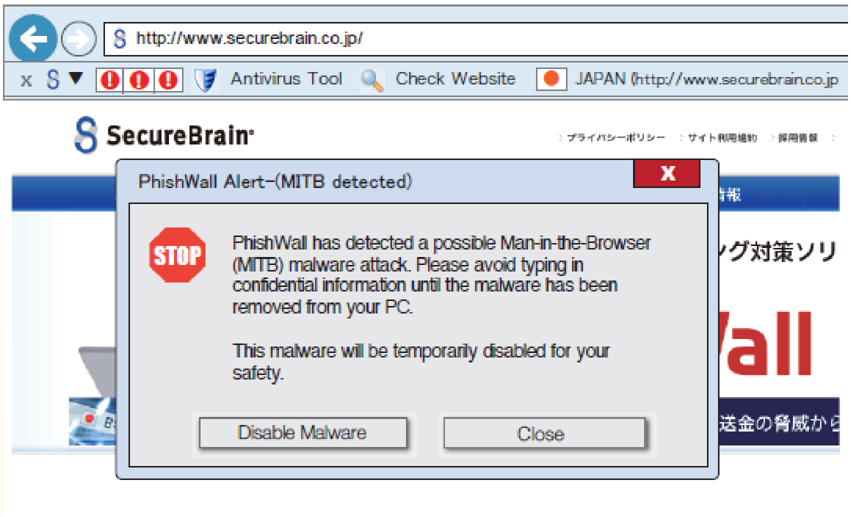
PhishWall Premium

Accessing the legitimate website [SecureBrain Corporation]

Detection and warning of MITB attacks

Attacks that use fraudulent pop-ups or other means to steal sensitive information such as usernames and PIN numbers are caused by malware infection of the user's PC. When a PC user browses the website of a financial institution that has deployed PhishWall Premium, PhishWall Premium would check to make sure that the user's PC is not infected with any MITB attack-type malware. If signs of infection are detected, a red signal and a warning message are displayed to prevent the user from typing sensitive information into a fraudulent screen. PhishWall Premium is also capable of disabling or removing certain malware. Disabling or removing the malware allows the user to avoid the risk of an MITB attack even with the infection.

Warning screen when PhishWall Premium detects an MITB attack



PhishWall Alert–(MITB detected)

PhishWall has detected a possible Man-in-the-Browser (MITB) malware attack. Please avoid typing in confidential information until the malware has been removed from your PC.

This malware will be temporarily disabled for your safety.

PhishWall Premium MITB attack detection logic

In recent years, tools that make it easy to write malware have become available on the market. Because it is now possible to write malware without sophisticated knowledge, new species of malware are appearing faster than signature-based antivirus software is able to counter them.

MITB attacks are able to circumvent two-factor authentication such as one-time passwords. Thus, financial institutions have been under pressure to provide solutions specialized in the prevention of remittance fraud.

SecureBrain had analyzed in detail the behavior of financial malware with web injection and MITB attack functions, and has succeeded in developing an engine that detects malware on the basis of that behavior. The analysis covered not only Zeus and SpyEye malware that attacked Japanese banks in October 2012, but also covered malware that caused damages in other countries. SecureBrain added functions that monitor and detect malware behavior and launched this service under the name PhishWall Premium in December 2012.

PhishWall Premium not only detects the file component of malware but also detects the “behavior” of an MITB attack taking over browser communications. This enables PhishWall to detect new variants of malware which other antivirus products may not be able to detect since new variants may not match their detection signatures. PhishWall Premium is able to detect even financial malware known to be difficult to detect, such as Rovnix, URLZone and Dridex that are currently wreaking havoc worldwide.

PhishWall Clientless (server layer remittance fraud countermeasures)

PhishWall Premium is a client-facing solution. When installed on a client PC, it can monitor the behavior of a wide range of malware, but its disadvantage is that users must install it on their PCs. SecureBrain realized that this called for security measures where the bank's Internet banking server checks the user's browser automatically. Based on this concept, SecureBrain developed PhishWall Clientless. When the user accesses the Internet banking login page, the Internet banking server checks that no fraudulent screen is displayed on the browser to prevent damage due to remittance fraud. Its greatest merit is that it allows the bank to automatically implement security checks for all of its users.

PhishWall Clientless MITB attach detection logic

Whitelist approach

Because judging whether or not the malware has tampered with genuine content is more effective against unknown attacks, PhishWall Clientless uses a whitelist approach. A whitelist of the HTML content of Internet banking websites is created, and this data is kept on the PhishWall Clientless inspection server.

Content tampering detected using JavaScript

When a user accesses an Internet banking site, ~~is~~ PhishWall Clientless sends the website contents to the inspection server. PhishWall Clientless compares the contents with the whitelist held on the inspection server and issues a detection report.

PhishWall Clientless action after tampering is detected

Internet banking user

PhishWall Clientless displays a warning screen on the browser to inform the user of a possible MITB infection. The user is advised to close the browser.

Financial institution

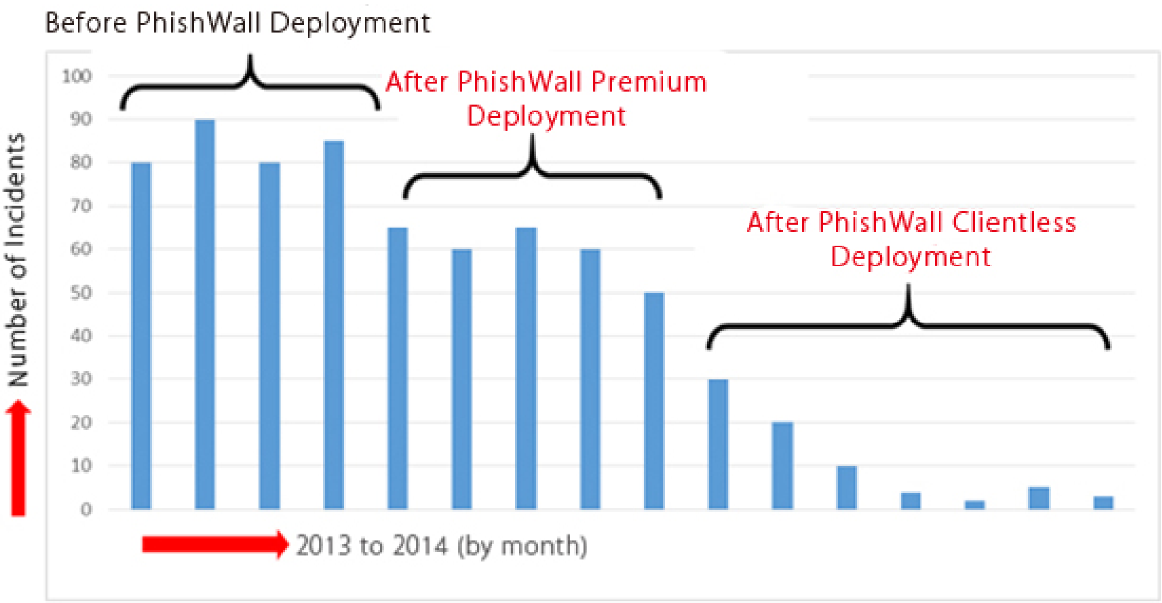
The financial institution receives information by email about the user whose PC a possible attack has been detected on.

Benefits of PhishWall series solutions

PhishWall is in use by more than 170 financial institutions in Japan. In recent years, the number of attacks by foreign perpetrators targeting Japanese financial institutions has risen sharply.

SecureBrain. At the time of the Rovnix attack on Japanese financial institutions in December 2015, there were even cases where banks that had originally been targeted were left aside when it was discovered that they already had deployed PhishWall.

PhishWall Clientless does not require any software installation but carries out security checks in the server layer. For this reason, it is not able to detect all malware attacks. But using PhishWall Clientless in conjunction with PhishWall Premium, which is resident on the client, makes for strong MITB attack countermeasures. The chart below shows the case of a bank that has successively deployed PhishWall Premium and PhishWall Clientless. Whereas the bank had been recording several dozen incidents of remittance fraud each month, the number of incidents subsequently fell to single digits. The number of incidents fell by around 30% following the deployment of PhishWall Premium and by around 84% following the deployment of PhishWall Clientless. In comparison with the situation before the deployment of PhishWall, the overall reduction was 88%.



Conclusions

In recent years, remittance fraud malware based on sophisticated technology has become widespread and is incorporating new techniques every year. Financial institutions are increasingly aware of the importance of taking action to prevent remittance fraud involving such malware, but very few have implemented adequate countermeasures.

Today, the use of PhishWall Premium in conjunction with PhishWall Clientless is considered to be highly effective, and the deployment of both solutions is increasing at an accelerating rate. In 2015, a number of major Japanese banks have deployed both PhishWall solutions, and in 2016, this trend is expected to spread to other countries.

SecureBrain will continue studying and implementing countermeasures against malware that evolves year by year, working to improve the functions of PhishWall solutions to enhance security, and promoting their wider use with a view to establish the PhishWall series as the standard remittance fraud countermeasures solutions for financial institutions.

SecureBrain Corporation

http://www.securebrain.co.jp/

Tel: 03-3234-3001 (switchboard)

7F, Kioicho Building, 3-12 Kioicho, Chiyoda-ku, Tokyo 〒102-0094

*Product specifications and prices are subject to change without notice. The information in this document was correct as of March 2016.