MRG Effitas

Efficacy Assessment & Assurance

Efficiency assessment of

SecureBrain Phishwall Safe Browser

Table of Contents

Executive summary 3

Analysis boundaries.. 4

Detailed test results 5

Real-time protection test 5

Phishing detection test.. 7

Botnet test... 8

Conclusion... 9

Executive summary

The purpose of this report is to document our comprehensive efficacy assessment of SecureBrain Phishwall safe browser.

In the assessment, we measured levels of In-the-wild Protection, Botnet test and Phishing test.

In-the-Wild Real Financial Malware Test

In total, 79 live ITW samples were used. The tests were performed using financial malware only, including, *inter alia*, the following: ZeuS clones, Ursnif, Banbra.

Phishing Protection test

Phishing Protection tests used a set of newly discovered Phishing URLs, which carry a huge risk for home and business users to face day by day. As most of the users' data are stored on online services nowadays, access to these data can be financially rewarding for criminals.

Botnet Test

MRG Effitas is proud to present the world's first real botnet test. In this test, we acquired leaked builders from real financial malware (Zeus, PowerZeus/KINS, ZeusVM, Citadel, SpyEye, Modified Zeus, Tinba), created the droppers and configured the C&C servers in the safe SoftLayer environment. Because this test uses real financial malware, where data exfiltration can be tested as it happens in the wild, the test efficiently maps the real-world threats users face today. These builders and droppers are available to everyone for free, thus the threats provide an entry level for criminals and are common threats in the wild.

SecureBrain Phishwall passed all three tests, thus it is eligible to receive the MRG Effitas Online banking Certification.

Analysis boundaries

The objective of the evaluation was to measure the efficacy of SecureBrain Phishwall.

The used test-cases (threats\botnets\phishing) are verified against their ability to cause danger to a user's system. All tests were done in virtualized environments, on a fully patched Windows 7 64-bit. Internet Explorer 11, Chrome 54 and Firefox 49 was used as the browser.

The test was carried out between 27 September 2016 and 11 November 2016.

Hitachi Europe Ltd. commissioned MRG Effitas for an efficiency analysis of the SecureBrain Phishwall product. The tested version was SecureBrain Phishwall 3.8.7.5.

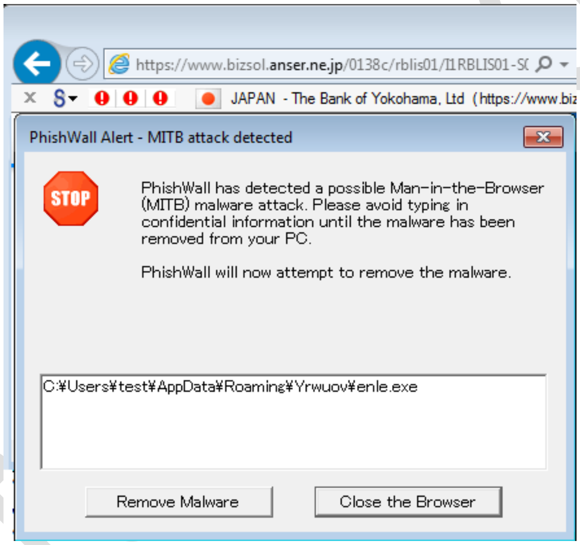
When conducting the tests, we tried to simulate normal user behavior. We are aware that a "Real World" test cannot be conducted by a team of professionals inside a lab because we understand how financial malware works, how it attacks and how such attacks could be prevented. Simulating normal user behavior means that we paid special attention to all alerts given by security applications. A pass was given only when alerts were straightforward and clearly suggested that malicious action should be blocked.

Detailed test results

Real-time protection test

Sample selection is of fundamental importance to this and all similar tests. All samples used are "live" and "in the wild", by which we mean that they reside at the URLs, selected or created by cybercriminals, and not from a time lagged ITW list. As these are live ITW samples, they represent current zero day-threats that can present an issue with sample verification. There is no effective and reliable way to verify samples before testing that does not introduce possible artificial sample submission or delay, so all verification is conducted after testing. Tests performed using samples that are later proven invalid are excluded from the results. The type of samples used is selected by MRG Effitas on the basis of a mixture of criteria:

1. Prevalence – they are widespread and so represent the most common threats.
2. Growth – they may be few now, but our research shows they are rapidly expanding.
3. Innovation – they employ innovative techniques to counter security measures.
4. It is malware with financial motives, which steals login credentials, initiates transactions, or does web injects.



https://www.bizsol.anser.ne.jp/0138c/rblis01/I1RBLIS01-S(
JAPAN - The Bank of Yokohama, Ltd (https://www.biz
STOP
Remove Malware
Close the Browser

PhishWall Alert - MITB attack detected

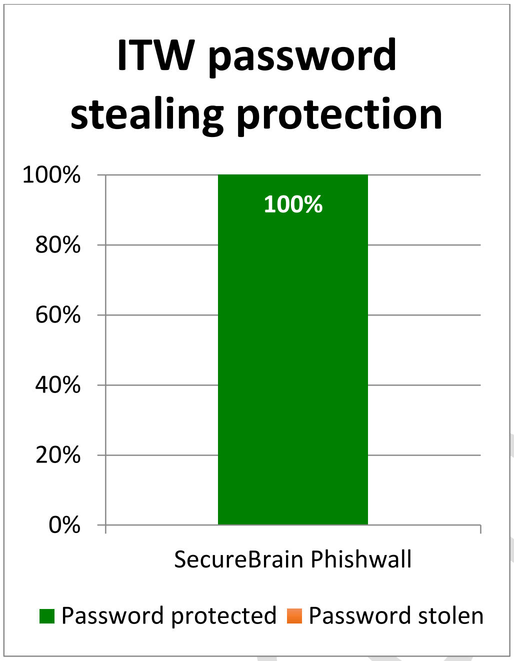
PhishWall has detected a possible Man-in-the-Browser (MITB) malware attack. Please avoid typing in confidential information until the malware has been removed from your PC.

PhishWall will now attempt to remove the malware.

C:¥Users¥test¥AppData¥Roaming¥Yrwuov¥enle.exe

Figure 1 - Zeus MiTB detected by Phishwall

Shown below are the results for 79 live ITW malware:



Phishing detection test

We carefully selected 100 phishing pages that worked at the time of the test. We opened all of the webpages in Internet Explorer 11 and checked whether the product identifies the website as a valid, trusted website.

Test results

Phishwall protection differs from traditional phishing protection, where bad websites are marked as malicious. In the case of Phishwall, it only marks valid, trusted websites as trusted, which are registered with Phishwall.

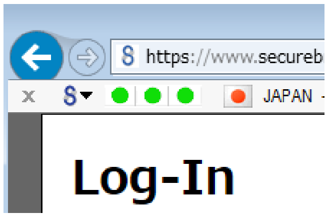


Figure 2 – Valid, trusted, registered website

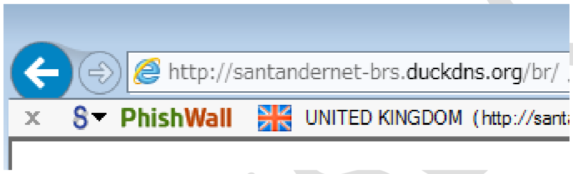
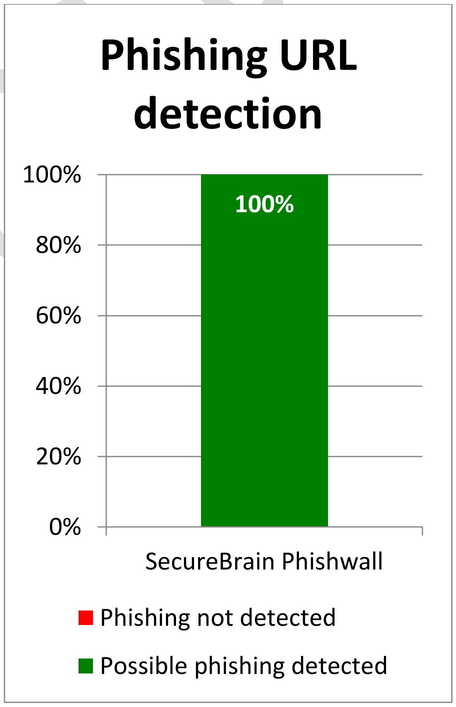

http://santandernet-brs.duckdns.org/br/
PhishWall
UNITED KINGDOM (http://sant

Figure 3 - Unknown website, possible phishing

Shown below are the results for 100 phishing webpages:



Botnet test

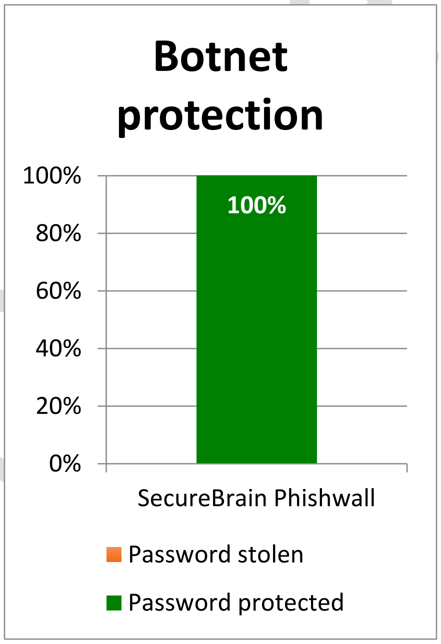
Builders and webserver components of the financial malware ZeuS, Citadel, SpyEye and Powerzeus have been leaked in previous years. We used these leaked builders to build our in-house C&C malware network. The C&C servers are operated at the cloud provider SoftLayer in a safe environment, thus the whole infrastructure is as close to real financial malware as possible, simulating attackers by either buying resources at cloud providers or hacking legitimate websites and placing the C&C server there.

We used the following malware versions:

- ZeuS 2.0.8.9
- Citadel 1.3.4.5
- SpyEye 1.3.48
- PowerZeus 1.0.2.0
- ZeusVM
- Modified Zeus 2.0.8.9
- Tinba

Test results

Shown below are the results for 7 botnet tests:



The original Phishwall version tested failed on one old variant of SpyEye that is no longer actively developed in the wild but was tested for completeness. After consulting with the SecureBrain engineers, the newly released version now protects against all tested SpyEye malware.

Conclusion

SecureBrain Phishwall passed all three tests (In-the-wild, botnet, and phishing), thus it is eligible to receive the MRG Effitas Online Banking Certification.