

westcoast labs

May 2009

SentryBay

PhishLock and EntryProtect for Web Applications

SentryBay – Custom Test

Vendor Details

Vendor:

SentryBay, 1 Northumberland Avenue, Trafalgar Square, London WC2N 5BW
Tel: +44 (0) 207 872 5512

Products:

PhishLock 3.2 and EntryProtect for Web Applications 4.10

Test Laboratory Details

US Headquarters and Test Facility

West Coast Labs, 16842 Von Karman Avenue, Suite 125
Irvine, CA 92606, U.S.A., Tel: +1 (949) 870 3250, Fax: +1 (949) 251 1586

European Headquarters and Test Facility

West Coast Labs, Unit 9 Oak Tree Court, Mulberry Drive, Cardiff Gate Business
Park, Cardiff, CF23 8RS, UK, Tel: +44 (0) 29 2054 8400, Fax: +44 (0) 29 2054 8401

Test Facilities also in Delhi, Hong Kong and Sydney, Australia.

Authors: Richard Thomas, Chris Elias

Tel : +44 (0)2920 548 400

Date: 27th May 2009

Issue: 1.4

SentryBay – Custom Test

Contents

Introduction	4
Test Outline	7
Test Suites	9
Test Methodology	10
Test Results	12
Conclusion	29
Vendor Statement	30
References	31
Appendix A	32
Disclaimer	33

SentryBay – Custom Test

Introduction

West Coast Labs were commissioned by SentryBay to test their browser plug-ins PhishLock and EntryProtect for Web Applications.

These technologies are aimed at protecting end users when online – in the case of PhishLock by ensuring that attempts at Phishing against sites known and fingerprinted by SentryBay are detected and intercepted, and for EntryProtect for Web Applications to counter the effects of software keyloggers.

Given the risks posed by keyloggers and phishing sites, especially along with the fluid nature of the latter, it is important not only for end users to be aware of the hazards associated with entering their personal data online and to develop a cautionary approach to potential scams, but also for corporations and businesses to be seen to be doing everything possible in order to protect their brand and the personal and private data of their customers.

Industry bodies such as the AntiPhishing Working Group [1], as well as various individual security companies regularly publish reports showing the extent both of proliferation of Phishing websites and of sites which install malicious software specifically to facilitate financial fraud such as keyloggers.

To illustrate the extent of the potential threat, consider some statistics from the AntiPhishing Working Group and the UK Payments Association APACS [2], along with numbers from a report recently published by IT security vendor Symantec [3]:

SentryBay – Custom Test

Introduction (Cont)

- In Q1 of 2009, Phishing attacks were up by 200% on the same period in 2008. (APWG)
- Almost 20% of recipients do not delete or ignore phishing emails (APACS)
- In the latter half of 2008, the number of unique brands that were reported as having been targeted varied between 229 per month and 271 per month (APWG)
- The industry sectors targeted by fraudsters in 2008 were shown with the following breakdown: Financial services 46%, payment services 38%, Auction services 11%, Retail 1%, Other 4%. (APWG)
- Symantec's EMEA Internet Security Threat Report showed that the UK was ranked second overall for malicious activity, just behind Germany, being the primary source of malicious code and the secondary source for Phishing website hosting.

SentryBay offer a different approach to the conventional route of solving some of these issues.

The PhishLock solution does not attempt to use blacklisting to control phishing websites, as this is a method that relies on being able to identify, block, and roll out updates quickly. Instead they will fingerprint and train upon specific sites and then use a series of rules based upon what is known about those sites to ascertain if the visited URL is genuine or illicit. The solution can be deployed to protect either an individual company's brand or to protect a wide range of brands. The version of Phishlock tested by West Coast Labs had

SentryBay – Custom Test

Introduction (Cont)

been trained on 80 brands, and SentryBay have informed West Coast Labs that full release versions typically cover approximately 500 brands.

There are four release versions of EntryProtect, including the version tested by West Coast Labs, EntryProtect for Web Applications.

The other offerings are EntryProtect Enterprise, which includes EntryProtect for Web Applications with additional Client and Server side components providing extra protection, EntryProtect for PC Applications, which may be integrated into software applications to protect against keylogging for application fields, and EntryProtect Inject which covers any Windows application.

The EntryProtect solution secures a user's details by protecting data being entered into the common fields found within online forms. Due to the employment of this method, the protection offered is not dependent on the detection of malware such as keyloggers.

SentryBay – Custom Test

Test Outline

In order to evaluate the technologies offered by SentryBay, West Coast Labs performed a wide range of testing including attempting to access known Phishing sites, and using various keyloggers (both publicly available and proprietary keyloggers) to demonstrate that the protection offered by SentryBay was valid.

West Coast Labs also performed a number of CPU and memory usage tests against a browser both with the SentryBay product installed and without to gauge system impact.

All testing was conducted using the two most widespread browsers [4,5], Internet Explorer and Firefox. These were tested on the versions supported by SentryBay and most appropriate to three different installations of Operating Systems - a base installation of Windows XP (Internet Explorer 6), Windows XP with Service Pack 3 installed (Internet Explorer 7, Firefox 3), and Windows Vista Home Premium edition (Internet Explorer 7, Firefox 3).

Both solutions were also scanned using a wide range of common home Anti-Malware applications chosen by SentryBay – McAfee [6], Symantec Norton [7], Kaspersky [8], Grisoft AVG [9], and Trend Micro [10] - to ensure that they did not identify either EntryProtect for Web Applications or PhishLock as malicious code. Scanning was carried out using the latest definitions on the day of testing and was conducted on Windows XP Service Pack 3 and Windows Vista only, as none of the AntiMalware products would install on Windows without at least Service Pack 2 installed.

SentryBay – Custom Test

Test Outline (Cont.)

Further, when testing PhishLock, West Coast Labs were asked to compare the anti-phishing block rates (if appropriate) of each of these products to those provided by PhishLock, results can be seen later in this report.

West Coast Labs have also been asked to comment specifically on the following features of SentryBay's solutions.

- Confirming correct installation into each browser / Operating System combination
- Confirming that without the protection afforded by the solutions, data could potentially have been stolen at each site tested
- Confirming that an update provided at a pre-agreed time is implemented without any user interaction.

SentryBay – Custom Test

Test Suites

Phishing sites were drawn from known sites that publish phishing information, as well as sites received during the testing period from West Coast Labs' numerous spam feeds and external honeypot email accounts. Further to this, West Coast Labs set up a number of "dummy" phishing sites by copying pages of sites known to be protected by SentryBay, and constructed a series of tests against live URLs on a web server on a separate network to the test network to confirm that these were also blocked. Naturally, West Coast Labs also tested against the known good sites to confirm that these were not blocked.

In order to test the range of SentryBay's EntryProtect for Web Applications' coverage, West Coast Labs utilised a number of free and publicly available keylogging software applications along with proprietary software that registers keystrokes.

Publicly available software included the popular Perfect Keylogger, Powered Keylogger, KGB Keylogger and Home and Family Keyloggers. Proprietary software included samples provided by SentryBay and samples from West Coast Labs that have not been released.

SentryBay – Custom Test

Test Methodology

Testing was conducted on both Firefox and Internet Explorer on the various Operating Systems in the combinations mentioned in the Testing Outline section.

For each Operating System, West Coast Labs created multiple forensic images with each of the commercial antimalware software installations installed. Further to this, there was a host with only SentryBay installed as browser protection, and a “sacrificial” host with no protection installed.

Onto each of these images, the appropriate SentryBay solution was installed, and it was determined that the AntiMalware solutions did not identify the SentryBay solutions as malicious. This was tested not only during installation (an On-Access test), but also via a system-wide scan (On-Demand). Following each of these tests, the original image was restored, so that the SentryBay solution was not installed during the functional testing on the same host as an anti-malware solution.

In order to test the main functionality of PhishLock, West Coast Labs visited a number of sites as detailed in the Test Suites section from each of the hosts protected by the antimalware solutions, from the host protected only by SentryBay, and from the host with no protection. Results were recorded on a site by site basis as to whether the phishing sites were allowed or blocked at the browser level.

SentryBay – Custom Test

Test Methodology (Cont.)

The main functionality of EntryProtect for Web Applications was tested by installing the keyloggers as detailed in Test Suites, and then visiting a number of web sites with login pages to observe whether the solution correctly obscured the entered keystrokes. Further to this, the subset of keyloggers that took screenshots were configured to take screen grabs at appropriate intervals, and results for these were also analysed.

West Coast Labs were also asked to perform some basic testing against a server owned and controlled by SentryBay with the EntryProtect Enterprise server components installed to look at form grabbing prevention, clipboard protection, testing the encryption of the password field in transmission over a live network connection, and testing the replacement of real characters entered into a password field with fake characters.

SentryBay – Custom Test

Test Results

PhishLock – Operating System and Internet Browser Compatibility

West Coast Labs installed PhishLock to the following Operating Systems and browser combinations as shown in the table below with the aim of determining that the solution was fully compatible.

Operating System / Browser version	Compatibility
<i>Windows Vista Home Premium</i>	
Internet Explorer 7	Confirmed
Mozilla Firefox 3.0.8	Confirmed
<i>Windows XP with Service Pack 3</i>	
Internet Explorer 7	Confirmed
Mozilla Firefox 3.0.8	Confirmed
<i>Windows XP (base installation)</i>	
Internet Explorer 6	Confirmed

SentryBay – Custom Test

Test Results (Cont)

PhishLock – identification of solution by third party malware solutions

In order to demonstrate the ability of PhishLock to work alongside a selection of common anti malware solutions provided by household names, a cross-section of common vendors' products was used whilst PhishLock was installed. Following this test as to whether the solutions detected PhishLock as malicious during an "On Access" scan (i.e. during Installation), a further full system scan ("On Demand") was conducted. The exact version of products may be seen in the "References" section.

Anti Malware Solution provider / Scan type	Result
<i>Grisoft AVG</i>	
Installation	No malware detected
Standard System Scan	No malware detected
<i>Kaspersky</i>	
Installation	No malware detected
Standard System Scan	No malware detected
<i>Trend Micro</i>	
Installation	No malware detected ¹
Standard System Scan	No malware detected
<i>Symantec</i>	
Installation	No malware detected
Standard System Scan	No malware detected
<i>McAfee</i>	
Installation	No malware detected
Standard System Scan	No malware detected

¹ Trend Micro notified the user that an application was attempting to install a plugin, however this did not interfere with the operational status of PhishLock.

SentryBay – Custom Test

Test Results (Cont)

PhishLock – Phishing Website Detection Rates

Multiple tests were undertaken to test the functionality of PhishLock. Testing was conducted against copies of real life sites that were then set up on a domain wholly owned and controlled by West Coast Labs and then attempts were made to visit these sites on a separate and distinct network from the one onto which the solutions were installed.

Data for Grisoft AVG is not included in these results as the solution does not appear to cater directly for blocking phishing sites using this testing methodology, and acts as a search engine plug in only, without acting directly on the sites.

These tests were conducted against specific sites protected by the version of Phishlock as detailed in Appendix A: Amazon, AmericanAirlines, Barclays Global, Bloomberg, Chase, eBay, Facebook, LinkedIn, Lloyds, MySpace, National Rail, PayPal, Verizon. Where errors have been thrown these are ignored and the figures adjusted accordingly.

The format used in these live tests was as follows:

<http://barclaysglobal.domainname.com>

Solution Provider	XP SP3	Vista	XP base (IE6 only)
<i>SentryBay</i>	100%	100%	100%
<i>McAfee</i>	0%	0%	n/a
<i>Kaspersky</i>	0%	0%	n/a
<i>Symantec (Norton)</i>	44%	0%	n/a
<i>Trend Micro</i>	0%	0%	n/a

SentryBay – Custom Test

Test Results (Cont)

PhishLock – Phishing Website Detection Rates

Against live sites discovered during the test period that the instance of PhishLock provided had been specifically trained on, it was noted that where there was an exact match for a site in the list against the spoof site, SentryBay successfully blocked access to 100% of sites across all combinations tested.

Individual companies' figures for this subset are as below:

Solution provider	% of blocks across all combinations tested
<i>SentryBay</i>	100%
<i>Kaspersky</i>	29%
<i>McAfee</i>	75%
<i>Symantec</i>	88%
<i>Trend Micro</i>	63%

It has been noted that SentryBay are very specific regarding the sites they protect, for example it was observed that while PayPal UK was included as a protected site, some Paypal France phishing sites were not blocked, but these were not included in the initial list, so they were not covered. This relates to the specific functionality and approach of the product.

SentryBay – Custom Test

Test Results (Cont)

PhishLock - False Positive Testing

In order to confirm that PhishLock was able to correctly block phishing websites, without denying access to legitimate websites such as online banking and other financial pages, a series of known-good URLs were tested with PhishLock installed.

West Coast Labs browsed to a variety of pages linked from well known financial institution websites. A series of pages from less well known corporations were also browsed to.

Testing was conducted using a mix of proprietary scripts and manual browsing, with results being recorded on a site by site basis.

Throughout the course of testing, it was noted that PhishLock maintained a 0% False Positive rate, successfully allowing through all legitimate pages.

SentryBay – Custom Test

Test Results (Cont)

EntryProtect for Web Applications – Operating System and Internet Browser Compatibility

West Coast Labs installed EntryProtect for Web Applications to the following Operating Systems and browser combinations as shown in the table below with the aim of determining that the solution was fully compatible.

Operating System / Browser version	Compatibility
<i>Windows Vista Home Premium</i>	
Internet Explorer 7	Confirmed
Mozilla Firefox 3.0.8	Confirmed
<i>Windows XP with Service Pack 3</i>	
Internet Explorer 7	Confirmed
Mozilla Firefox 3.0.8	Confirmed
<i>Windows XP (base installation)</i>	
Internet Explorer 6	Confirmed

EntryProtect for Web Applications – identification of solution by third party malware solutions

In order to demonstrate the ability of EntryProtect for Web Applications to work alongside a selection of common anti malware solutions provided by household names, a cross-section of common vendors' products was used whilst EntryProtect for Web Applications was installed. Following this test as to whether the solutions detected EntryProtect for Web Applications as

SentryBay – Custom Test

Test Results (Cont)

malicious during an “On Access” scan (i.e. during Installation), a further full system scan (“On Demand”) was conducted. The exact version of products may be seen in the “References” section.

Anti Malware Solution provider / Scan type	Result
<i>Grisoft AVG</i>	
Installation	No malware detected
Standard System Scan	No malware detected
<i>Kaspersky</i>	
Installation	No malware detected
Standard System Scan	No malware detected
<i>Trend Micro</i>	
Installation	No malware detected ¹
Standard System Scan	No malware detected
<i>Symantec</i>	
Installation	No malware detected
Standard System Scan	No malware detected
<i>McAfee</i>	
Installation	No malware detected
Standard System Scan	No malware detected

¹ Trend Micro notified the user that an application was attempting to install a plugin, however this did not interfere with the operational status of EntryProtect for Web Applications.

SentryBay – Custom Test

Test Results (Cont)

EntryProtect for Web Applications - Keylogger Nullification and/or Detection

The following results show the ability of each company's solution to nullify or detect a series of keyloggers. The keyloggers were selected to have a wide range of functionality in terms of ability, both from the level at which they interacted with the system, to whether they could perform screen grabs or not.

Each keylogger sample was tested against both Microsoft's Internet Explorer and Mozilla Firefox as described earlier.

SentryBay – Custom Test

Test Results (Cont)

EntryProtect for Web Applications - Keylogger Detection and/or Partial Nullification

Windows XP Service Pack 3/Windows Vista Home Ultimate Edition

Solution Provider / Browser	Nullified	Detected
<i>SentryBay</i>		
Internet Explorer	100%	N/a
Firefox	100%	N/a
<i>Grisoft</i>		
Internet Explorer	N/a	86%
Firefox	N/a	86%
<i>Kaspersky*</i>		
Internet Explorer	N/a	100%
Firefox	N/a	100%
<i>McAfee</i>		
Internet Explorer	N/a	82%
Firefox	N/a	82%
<i>Symantec</i>		
Internet Explorer	N/a	77%
Firefox	N/a	77%
<i>Trend Micro</i>		
Internet Explorer	N/a	93%
Firefox	N/a	93%

* The above result for Kaspersky reflects Kaspersky's ability to detect the samples as riskware, with the user being presented with the opportunity to quarantine the sample.

SentryBay – Custom Test

Test Results (Cont)

Nullification in this case means that the samples did not record exactly what was typed in. It should be noted with one keylogging sample that SentryBay's solution altered the data rather than replacing it. In the opinion of West Coast Labs, with human intervention and interpretation, results could be extrapolated to provide personal data.

It was further noted that although EntryProtect prevents screen capture, on some occasions if the browser window is not the main window in focus, screen grabs may be taken.

SentryBay – Custom Test

Test Results (cont)

EntryProtect Enterprise Testing

West Coast Labs also verified that additional functionality to the basic EntryProtect for Web Applications was available by visiting a site owned and maintained by SentryBay with the EntryProtect server components installed.

It was demonstrated that the server component allows for the prevention of form grabbing by visiting the SentryBay demo site, using keyloggers that allow for form grabbing, and noting that the functionality did not appear to be operational in the keyloggers used.

Clipboard protection was demonstrated by showing that a simple copy and paste operation from another Windows application (for example notepad.exe or Microsoft Word) allowed the password to be entered into the form correctly, but then cleared the Windows clipboard so that it could not be pasted into any other window

The encryption of the password in its transmission over the network connection was also tested by running packet capture tools in the background and examining the traffic – it could be seen from the logs that the password was encrypted before the point of transmission, thus protecting against possible man-in-the-middle attacks.

It was also shown that the EntryProtect Server component transmitted the correct password but entered fake characters into the actual password field to show up behind the asterisks that are normally associated with a password field when the SentryBay client component was installed.

SentryBay – Custom Test

Test Results (cont)

General Testing – CPU and Memory Usage Figures

The tables and charts contained on the following pages record the difference in memory and CPU usage both with and without the SentryBay solutions installed.

Each table contains the minimum, maximum, and average (mean) RAM and CPU usage during a series of web operations. The figures were recorded for all Operating Systems as detailed in the Test Outline.

All figures are provided as a percentage of the overall resource available on the machine.

SentryBay – Custom Test

Test Results (Cont)

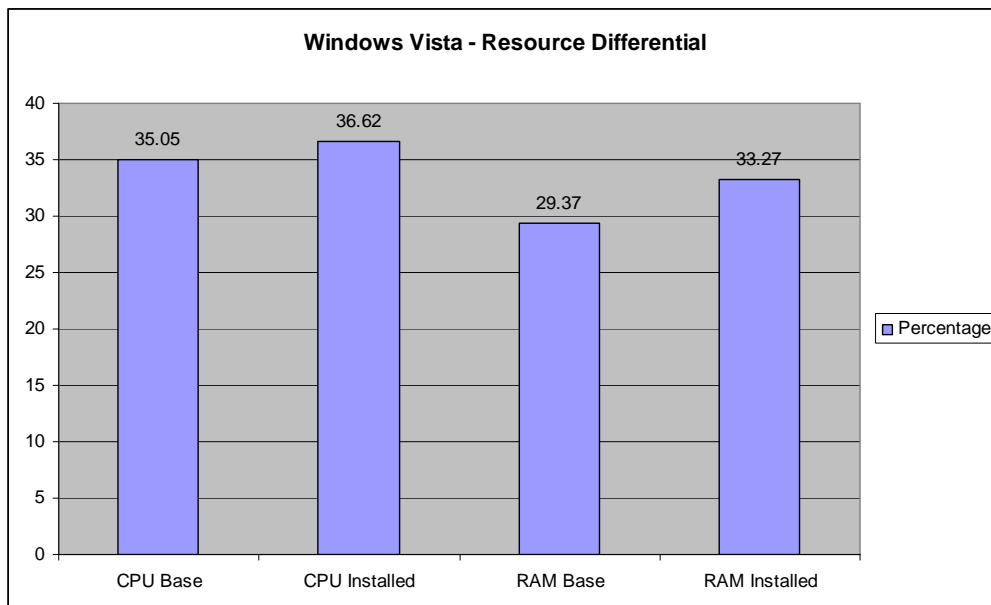
General Testing – CPU and Memory Usage Figures

Vista without PhishLock installed

	Minimum	Maximum	Average
CPU usage	12%	72%	35.05%
RAM usage	22.33%	42.14%	29.37%

Vista with PhishLock installed

	Minimum	Maximum	Average
CPU usage	27%	42%	36.62%
RAM usage	25.14%	49.77%	33.27%



SentryBay – Custom Test

Test Results (Cont)

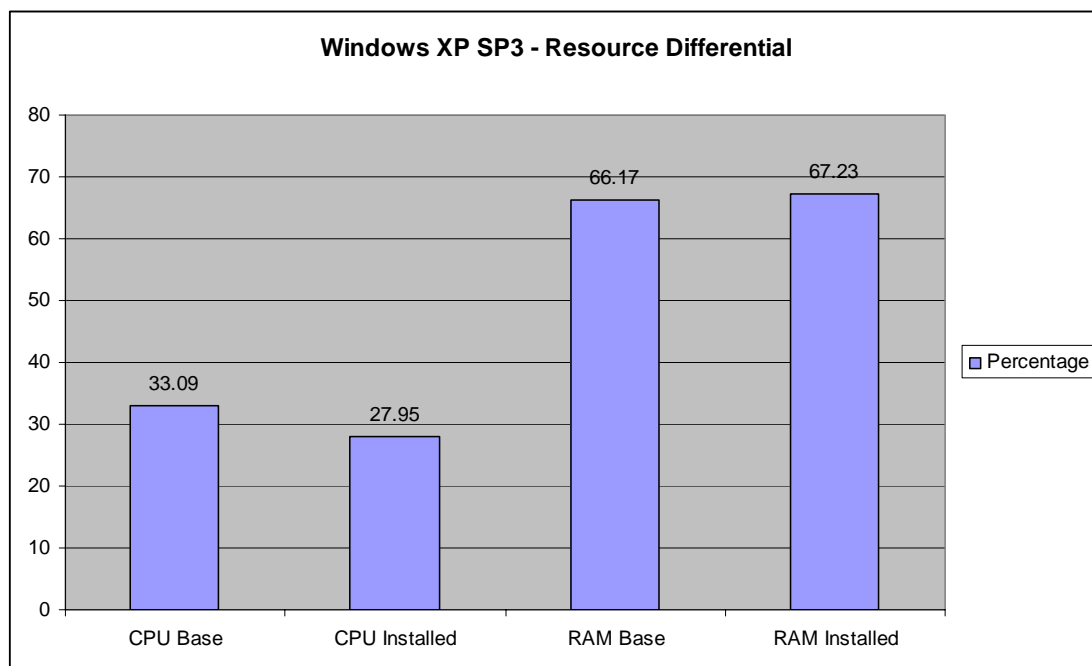
General Testing – CPU and Memory Usage Figures

XP SP3 without PhishLock installed

	Minimum	Maximum	Average
CPU usage	12%	91%	33.09%
RAM usage	62.78%	72.53%	66.17%

XP SP3 with PhishLock installed

	Minimum	Maximum	Average
CPU usage	12%	78%	27.95%
RAM usage	62.92%	76.01%	67.23%



SentryBay – Custom Test

Test Results (Cont)

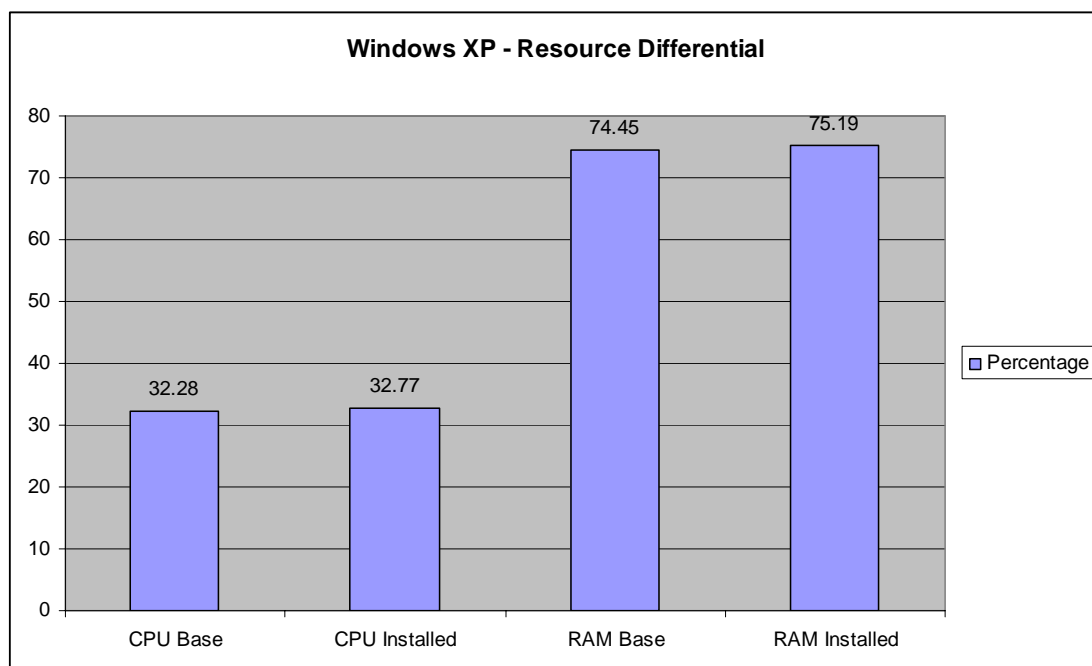
General Testing – CPU and Memory Usage Figures

XP without PhishLock installed

	Minimum	Maximum	Average
CPU usage	15%	91%	32.28%
RAM usage	71.23%	81.37%	74.45%

XP with PhishLock installed

	Minimum	Maximum	Average
CPU usage	15%	88%	32.77%
RAM usage	72.14%	81.46%	75.19%



SentryBay – Custom Test

Test Results (cont)

General Testing – CPU and Memory Usage Figures

From the above results, it is clear that the impact on system resources, caused by the solutions, is minimal. For example, while the Windows XP SP3 machine registered an increase of 1.06% in average RAM usage with PhishLock installed, this change is unlikely to impact on, or be noticed by, the average user.

Also worth noting is the natural fluctuation in memory and processor usage due to standard activity related to any installed applications, and indeed Windows itself.

SentryBay – Custom Test

Test Results (Cont)

General Test Remarks

For each Browser and Operating System combination tested both solutions installed without any issue – the Test Engineers reported that for each solution the installation routine consisted of only two clicks. However, it should be noted that any further customisation would increase this, and that the 2 clicks being reported are for the provided installation only.

For each Operating System and AntiMalware combination, it was noted that neither of the SentryBay solutions triggered a negative response from any of the AntiMalware installations. Only Trend Micro's solution offered any sort of interception, checking whether the user was aware that a browser plug-in was being installed and requesting authorisation to continue with the action.

Testing against the live sites on the host with no protection installed showed that, on each site, there was a potential for personal and private identifiable data to be stolen.

Updates performed as per the agreed time and date showed that no user interaction was required, and that the update process itself was transparent to the average user.

SentryBay – Custom Test

Conclusion

SentryBay have demonstrated that they have some innovative solutions to combating the problems of online identity and data theft. Their products are not designed to replace conventional antivirus and Internet security suites but to complement them, particularly in combating new threats.

The approach taken by PhishLock in learning about and fingerprinting specific sites, rather than maintaining a Blacklist, provides individualized proactive protection for companies' web pages and brands. This means that any lead-time between identifying a phishing site, adding it to a blacklist and rolling it out to a client-base in an update for those brands protected by the SentryBay solution is negated. Also of note is the zero percent False Positive rate observed over extensive testing.

Functional testing of EntryProtect for Web Applications has shown a high level of protection with a multitude of threats being neutralised. The approach taken here of blocking keylogging techniques at several Operating System levels, along with targeting common techniques used by this type of malware, has shown that even if a keylogger is undetected by a conventional anti-malware solution, SentryBay has the ability to offer protection against it.

The results of this testing along with the low system resources impact shows that, with these solutions, SentryBay are offering valuable incremental layers of protection to users attempting to protect their personal data.

SentryBay – Custom Test

Vendor Statement

“ [PhishLock] prevents phishing in real time due to SentryBay’s customized training on all major website brands. PhishLock is the most effective tool available to combat new phishing threats.”

“From an Enterprise viewpoint, [PhishLock] is an ideal way to provide protection for a corporate brand from a phishing attack.”

“ [EntryProtect is] a pro-active tool to combat Spyware and Trojans, particularly during the critical danger period of the first few days after a new attack is launched. This is the period during which conventional AV techniques are least effective, and most data is stolen.”

“EntryProtect Enterprise provides enterprise-strength protection for both client PC data entry and the data transmitted in order to secure a company’s web-based transactions. This can be set up in less than a day with only minor server-side modifications and can eliminate almost all online fraud.”

SentryBay – Custom Test

References

- 1 <http://www.antiphishing.org/phishReportsArchive.html>
- 2 http://www.apacs.org.uk/08_04_15.html
- 3 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_emea_internet_security_threat_report_04-2009.en-us.pdf
- 4 <http://marketshare.hitslink.com/browser-market-share.aspx?qprid=0>
- 5 http://en.wikipedia.org/wiki/Usage_share_of_web_browsers
- 6 McAfee Internet Security (VirusScan build 13.3.117)
<http://home.mcafee.com/store/package.aspx?pkgid=272>
- 7 Symantec Norton Internet Security Suite (16.5.0.135)
<http://www.symantec.com/norton/internet-security>
- 8 Kaspersky Internet Security (8.0.0.506)
http://www.kaspersky.co.uk/kaspersky_internet_security
- 9 Grisoft AVG Internet Security (8.5.287)
<http://www.avg.com/product-avg-internet-security>
- 10 Trend Micro Internet Security Pro (17.1.1250)
<http://us.trendmicro.com/us/products/personal/internet-security-pro/index.html>

SentryBay – Custom Test

Appendix A

Amazon:

<https://www.amazon.com/gp/css/homepage.html?ie=UTF8&ref%5F=topnav%5Fya%5Fgw>

AmericanAirlines:

<https://www.americanairlines.co.uk/aa/login/loginAccess.do?previousPage=%2Faa%2FhomePage.do&bookingPathStatelD=&marketId=&previousPage=/aa/homePage.do&marketId=>

Barclays Global:

<http://www.barclaysglobal.com/>

Bloomberg:

<http://www.bloomberg.com/subscriber/>

Chase:

www.chase.com

eBay:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&UsingSSL=1&pUserId=&co_partnerId=2&siteid=0&ru=http%3A%2F%2Fcgj5.ebay.com%2Fws%2FeBayISAPI.dll%3FSellItem%26hm%3Dnu.rundkoi347%26%26hc%3D1%26guest%3D1%26userid%3D&pageType=1144

Facebook:

<http://www.facebook.com/>

Google:

<https://www.google.com/accounts/Login?continue=http://www.google.co.uk/&hl=en>

LinkedIn:

https://www.linkedin.com/secure/login?trk=hb_signin

Lloyds:

<https://www.lloyds.com/ur/login.aspx>

MySpace:

www.myspace.com

National Rail:

<https://ojp.nationalrail.co.uk/en/p/secure/login>

PayPal:

https://www.paypal.com/uk/cgi-bin/webscr?cmd=_login-run

Verizon:

<http://www.verizon.net/central/vzc.portal>

SentryBay – Custom Test

West Coast Labs Disclaimer

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is not always possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and / or functionality of any particular product tested and / or guarantee that any particular product tested is fit for any given purpose.

Therefore, the test results published within any given report should not be taken and accepted in isolation. Potential customers interested in deploying any particular product tested by West Coast Labs are recommended to seek further confirmation that the said product will meet their individual requirements, technical infrastructure and specific security considerations.

All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability. West Coast Labs provide test results for any particular product tested, most relevant at the time of testing and within the specified scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools used during the specific test process.

West Coast Labs is unable to directly endorse or certify the overall worthiness and reliability of any particular product tested for any given situation or deployment.

Revision History

Issue	Description of Changes	Date Issued
1.0	SentryBay	15 th May 2009
1.1	First revision	21 st May 2009
1.2	Second Revision	22 nd May 2009
1.3	Third Revision	26 th May 2009
1.4	Fourth Revision	27 th May 2009

westcoast labs

US SALES

T +1 (949) 870 3250

EUROPE SALES

T +44 (0) 2920 548400

CHINA SALES

T +86 1 343 921 7464

CORPORATE OFFICES AND TEST FACILITIES

US Headquarters and Test Facility

West Coast Labs

16842 Von Karman Avenue, Suite 125,
Irvine, California, CA92606, USA

T +1 (949) 870 3250 , F +1 (949) 251 1586

European Headquarters and Test Facility

West Coast Labs

Unit 9, Oak Tree Court, Mulberry Drive
Cardiff Gate Business Park, Cardiff CF23 8RS, UK

T +44 (0) 2920 548400 , F +44 (0) 2920 548401

Test Facilities also in Delhi, Hong Kong and Sydney, Australia

E info@westcoast.com

W www.westcoastlabs.com