Comparative Efficacy Assessment of Wontok SafeCentral

February 2013

Contents:

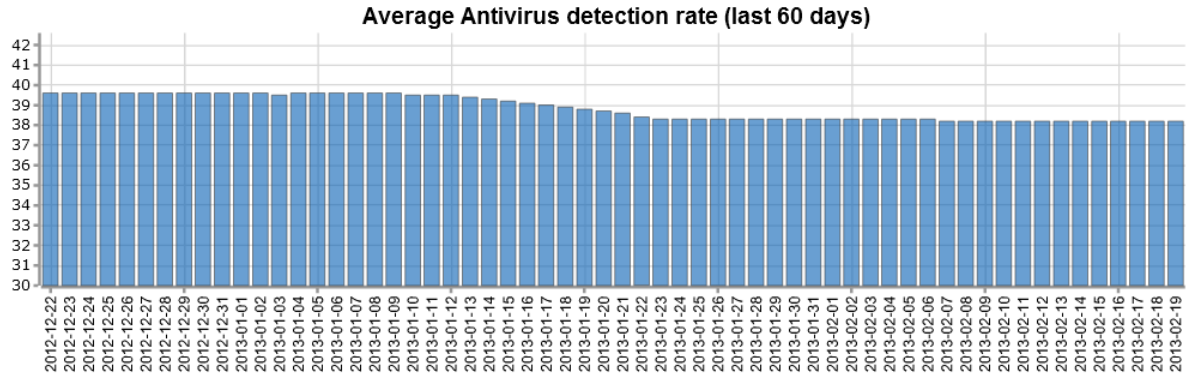
Introduction:

This report has been commissioned by Wontok Inc. with the objective of providing an independent efficacy assessment of a cohort of browser security and data capture prevention products, including SafeCentral.

This comparative assessment will measure each products efficacy against a range of attacks used by financial malware and advanced persistent threats (APT).

Modelling the Threat - Penetration Test Tools and Malware Simulators used:

The graph below shows the recent average detection of Zeus, the most prevalent financial malware threat:



Average detection of Zeus is currently below 40% and along with other financial malware, detection has consistently dropped over time.

The nature of the threats posed by these classes of malware are such that one needs to be able to determine if a data breach has occurred, not if they are detected or blocked, since evidence proves current solutions are unable to reliably prevent infection of systems.

Given that the key metric is the determination of prevention of data breach, testing was conducted using a range of simulators which model the attack types used by real financial malware and APTs.

The test tools used were as follows:

1. BBC Sim
    a. This is the simulator we created for the BBC for use in their news programme based on our research - http://www.youtube.com/watch?feature=player_embedded&v=EUGTIVSefeo which uses a man in the browser attack modelled on that employed by SpyEye
2. FM Simulator 02
    a. This simulator uses a bespoke malicious BHO as used in custom crimeware tools we have captured and analysed.
3. FM Simulator 03
    a. This simulator employs a function hooking technique gathered from reverse engineering an APT captured from one of our malware feeds.
4. PW Cap
    a. This simulator uses a malicious browser extension which employs in-house rootkit technology to capture user credentials entered in to SSL protected sites.
5. Br Manip
    a. This simulator uses malicious browser extension rootkit technology to perform browser manipulation (BM). BM technologies are used by criminals to alter what is displayed by the browser. Commonly, the alterations will be such that a banking login site will request a full password, rather than random elements etc.

6. CookSteal
    a. This simulator uses malicious browser extension rootkit technologies to steal session cookies from banking, e commerce, social networking and similar sites.[i]

Versions of the Applications Tested:

- Prevx with SafeOnline 3.0.5.220
- ThreatMetrix TrustDefender Pro V3.2.0.4958
- Trusteer Rapport Emerald Build 1208.24
- Webroot SecureAnywhere 8.0.2.109
- Wontok SafeCentral 3.0.2.3240

Methodology Used in the Test:

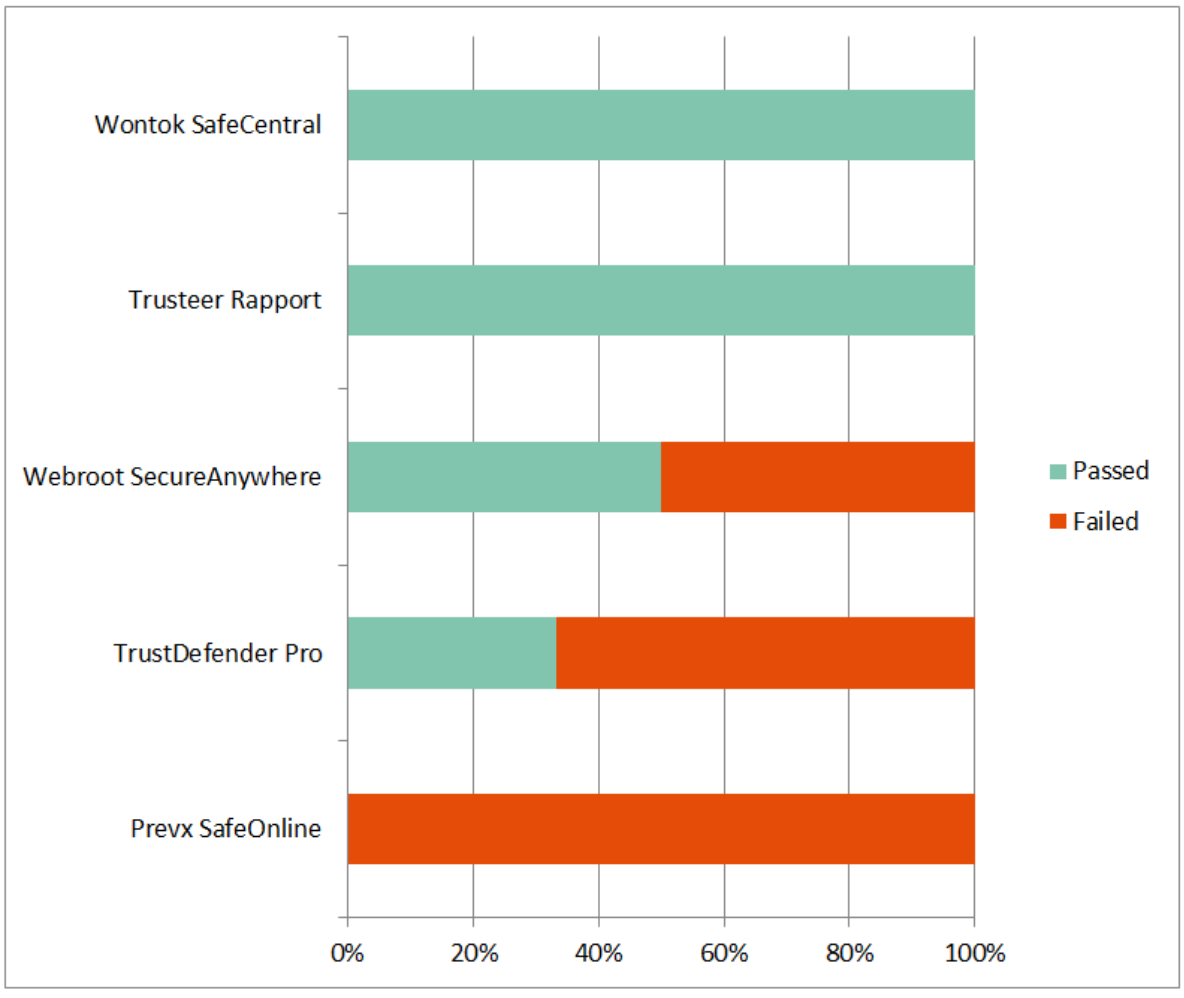
1. Windows 7 Ultimate Service Pack 1 64 bit operating system is installed on a virtual machine and all updates are applied.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the 5 security applications to be used in the test.
4. An individual security application is installed using default settings on each of the systems created in 3 and then, where applicable, is updated.
5. A clone of the system as it is at the end of 4 is created.
6. The BBC Simulator test is conducted by:
    a. Downloading the simulator using Internet Explorer to the desktop, closing Internet Explorer and then executing the simulator.
    b. Starting a new instance of Internet Explorer and navigating to www.paypal.com[ii]. Text is entered into the Account login page of www.paypal.com using the keyboard, or using a virtual keyboard if the application under test provides such functionality and then the "log in" button is pressed.
7. The test using FM Simulators 2 and 3 is conducted by:
    a. Performing steps 1-6 above with the exception of 6a, but infecting the system with the simulator via a USB flash drive.
8. The test using the PW Cap, Br Manip and CookSteal simulators is conducted by:
    a. Infecting (installing the simulators on) the system at 3 above and then performing the procedure detailed in 6b, but using FireFox.
9. A test is deemed to have been passed by the following criteria:
    a. The security application detects the simulator whilst it is being downloaded to the desktop, when the USB drive is inserted or when copied to the desktop.
    b. The security application detects the simulator when it is executed according to the following criteria:
        i. It identifies the simulator as being malicious and either automatically blocks it or postpones its execution and warns the user that the file is malicious and awaits user input.
        ii. It identifies the simulator as suspicious or unknown and gives the option to run in a sandbox or safe restricted mode and when run in this mode it meets the criteria c or d below.
    c. The security application prevents the simulator from capturing and sending the logon data to the MRG results page or local store location, whilst giving no alerts or informational alerts only.
    d. The security application intercepts the installation/action of the simulator and displays warnings and user action input requests that are clearly different to those displayed in response to legitimate applications, when they are executed or installed on that system.
10. A test is deemed to have been failed by the following criteria:

a. The security application fails to detect the simulator when it is executed and then:
    i. The security application fails to prevent the simulator from capturing and sending the logon data to the MRG results page or local store location and gives no, or informational alerts only.
    ii. The security application intercepts the installation/action of the simulator but displays warnings and user action input requests that are indistinguishable in meaning from those displayed in response to legitimate applications, when they are executed or installed on that system.
b. The security application identifies the simulator as suspicious or unknown and gives the option to run in a sandbox or safe restricted mode and when run in this mode it:
    i. Fails to prevent the simulator from capturing and sending the logon data to the MRG results page or local store and gives no, or informational alerts only.
    ii. Displays warnings and user action input requests that are indistinguishable in meaning from those displayed in response to legitimate applications, when they are executed or installed on that system.

11. Testing is conducted with all systems having internet access.
12. Each individual test for each security application is conducted from a unique IP address.
13. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.

Test results:

The chart below details ranking by product performance against the attacks.



The table below shows the results the five security applications achieved against each of the simulators / attack methods used.

Security Application:	BBC Sim	Sim 2	Sim 3	PW Cap	Br Manip	Cook Steal
Prevx SafeOnline	✗	✗	✗	✗	✗	✗
ThreatMetrix TrustDefender Pro	✓	✓	✗	✗	✗	✗
Trusteer Rapport	✓	✓	✓	✓	✓	✓
Webroot SecureAnywhere	✓	✓	✓	✗	✗	✗
Wontok SafeCentral	✓	✓	✓	✓	✓	✓

Conclusions:

Only Wontok SafeCentral and Trusteer Rapport were able to protect the system against all attack methods.

Webroot SecureAnywhere failed all three attacks which used the new browser extension / rootkit attacks. This product relies on heuristic analysis to determine the malicious nature of browser extensions, clearly, in this case, it was unable to make the correct determination.

TrustDefender was only able to block two of the MitB attacks and like Webroot, failed all the new browser extension attacks.

Prevx SafeOnline failed to protect the system against any of the attacks and therefore provided no security in this instance.

We have seen the same malicious browser extension technologies employed in our simulators used in an increasing number of ITW malware. Whilst the prevalence of this type of malware is currently low, we expect it to rise very quickly this year.

It is important that security vendors react to this threat now, before it becomes a more widespread and prevalent risk.[iii]

[i] All credit for researching and engineering the PW Cap, Br Manip and CookSteal simulators is greatfully given to our associate Zoltán Balázs, Senior IT Security expert at Deloitte Hungary.
[ii] Where applicable, all security applications under test are configured to provide their protection for this website.
[iii] MRG Effitas has contacted all vendors whose product are vulnerable to this attack and offered them free support in order that they can try to protect against it.