Online Banking Browser Security Project - June 2010

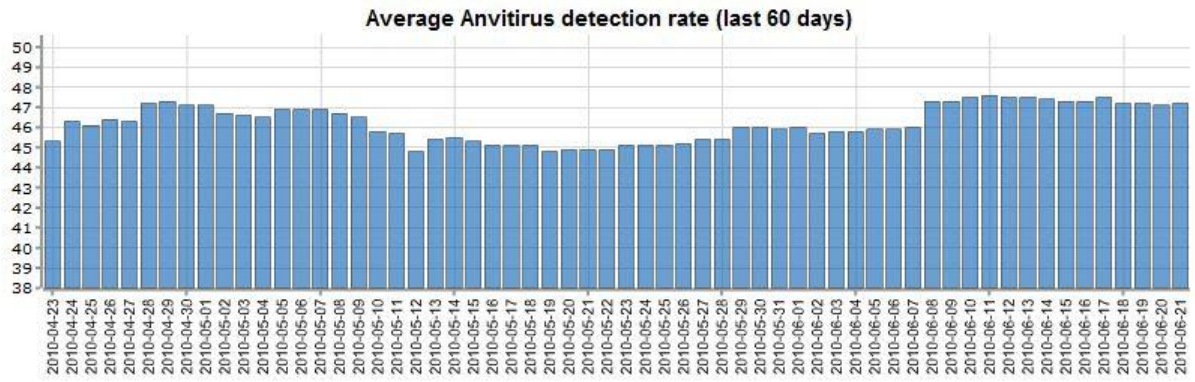
Day 30 / 30

Contents:

Introduction:

As we discussed before, in our previous tests, financial malware represents a significant threat to banks and their customers. An estimated 1% of PCs worldwide are infected with this malware and research shows, having an up to date antivirus only reduces the chance of infection by about 25%.

Financial malware is difficult to detect by design. It uses sophisticated techniques to evade detection, each type has thousands of unique variants and it is updated regularly. To illustrate this, the graph below shows the average detection rate of a cohort of antivirus applications for Zeus.



We have followed the overall detection rates for some time and generally, the overall trend is towards lower detection and rates are always below 50%. Based on these facts, it has been MRGs position for some time now that users should use additional measures to help increase the security of their online banking activities and not only rely on traditional antivirus products.

The purpose of this project is to simulate as accurately as possible a scenario where a new piece of financial malware is released in to the wild.

There have been various tests conducted to assess the efficacy of a number of security applications against financial malware threats. Commonly, these tests make use of various key logging, screen capture, clipboard monitoring simulators created by the vendors themselves. Whilst we accept there is value in these tests, we must point out that generally, they do not represent how financial malware works in the real world. This is for two main reasons:

Firstly, real financial malware commonly, will not use the same exploit / vector as a simulator. There are simulators available that we know of that use various screen capture techniques that are not used by any current financial malware. An application blocking these simulated attacks does not necessarily mean it will be effective against real malware.

Secondly, the tests do not use a control or means of assessing false positives. It would be easy to have an application which pops up an alert when any code runs; however, to be effective in the real world, an application should differentiate between malware which is trying to capture data and legitimate applications which require global hooks etc.

If an application alerts on the install of most software, the user will get used to these alerts and learn just to "allow" them. This will defeat the purpose of the application and make it ineffective in the real world.

MRG had developed a tool that simulates the behaviour of real financial malware. The tool once executed, permanently infects the system and is designed to capture data entered in to banking sites, bypass any firewall and send the captured data to our results page - www.browsersecurityproject.malwareresearchgroup.com.

The tool uses some sophisticated techniques, but has some built in weaknesses, so it should be possible for it to be detected by heuristics and behavioural analysis in time.

To reflect how financial malware infects, exists and operates on systems in the real world, we will run two tests in parallel.

1. Infection via Internet Explorer on a system already protected by a security application.
2. Security applications installed on a system which is already infected.

The results of the pre-infected system test will not be published publicly, but will be made available to vendors which have a support contract with MRG.

We conducted initial tests on 21 June 2010 and as of 23 June 2010 will re run the test every day for twenty nine days.

After this initial thirty day phase, we will start the test again using a more advanced test tool. Once this new tool is well detected, we will begin again with an even more sophisticated simulator. This process should represent the evolution and increase in sophistication exhibited by real malware.

This simulator is potentially very dangerous, therefore, we have included a safety feature which allows us to disable it instantly, should the need arise.

The simulator has never been exposed to any security applications, so accurately represents a zero day threat.

We will not provide any information about the simulator to the vendors whilst the first thirty day testing phase of the project is running. Vendors who have a support contract with MRG will be given feedback, along with a technical overview of the simulator and allowed remote access to it in our labs at the end of this first phase, however, we will not release the simulator itself.

Security Applications Tested:

We have chosen 31 applications made up of 18 full internet security suites and 13 dedicated identity / browser security utilities. Each of these purports to provide security for online activities, or is specifically designed to secure browsers for online banking.

The applications tested are as follows:

Browser Security / ID Protection Applications

1. Authentium SafeCentral
2. EMSI Mamutu 2.0.0.22
3. Global Information Technology Anti-Keylogger 9.2.1
4. Prevx SafeOnline 3.05.171
5. QFX Software KeyScrambler Professional 2.6.0
6. Quaresso Protect On Q
7. SentryBay Data Protection Suite 5.0.0.4493
8. SoftSphere DefenseWall 3.02
9. SpyShelter SpyShelter 4.17
10. Trusteer Raport 1003.9
11. Trustware BufferZone Pro 3.31-46
12. White Sky IDVault Free Edition
13. Zemana AntiLogger 1.9.2.206

System / Internet Security Applications

1. Acronis Internet Security Suite 2010

2. Agnitum Outpost Security Suite Pro 7.0.3373.514.1234
3. AVG Internet Security 9.0.819
4. Avira Premium Security Suite 10.0.0.542
5. BitDefender Internet Security 2010 13.0.21.347
6. Bluepoint Security 1.0.30.99
7. ESET Smart Security 4.2.40.0
8. F-Secure Internet Security 2010 246
9. G Data internetSecurity 2011 21.0.2.1
10. Kaspersky Internet Security 2010 9.0.0.736
11. McAfee Internet Security
12. Norman Security Suite
13. Norton 360 4.0.0.127
14. Panda Internet Security 2010 15.01.00
15. Sunbelt Software Vipre Antivirus Premium 4.0.3282
16. Tall Emu Online-Armor ++ 4.0.0.44
17. Trend Micro Internet Security 17.50.1647.0000
18. Webroot Internet Security Essentials 2010

Because of the "live" nature of the testing in this project, with captured data being sent directly to our test page in real time, we will identify the applications being tested by entering the application name as part of the login / password data on the banking site.

Methodology used in the Test:

1. Windows XP Professional Service Pack 3 is installed and updated with all important updates.
2. An image of the Operating System is created.
3. The "control" applications (Corbitek Antimalware, BluePoint Security & Trusteer rapport) installer files are copied to the system.
4. A clone of the Imaged system is made for each of the 30 security applications to be used in the test.
5. An individual security application is installed using default settings on each of the Cloned systems and then updated.
6. Four fresh clones of the clone created in 4 / 5 are used for each test. (one for the test application and three for the control applications)
7. The" infection via Internet Explorer on a system already protected by a security application test" is conducted by:
    a. Downloading the simulator using Internet Explorer to the desktop and executing it.
    b. Starting a new instance of Internet Explorer and navigating to the chosen banking site.
    c. The name of the application is entered in to the Account login page of www.paypal.com using the keyboard in the form of "[application name]fail@email.com" along with the password "password" and then the "log in" button is pressed.
8. The "Security applications installed on a system which is already infected" test is conducted by:
    a. Performing steps 1 – 6 above, but infecting the system with the simulator at step 2.
    b. Rebooting each of the unique systems created in 6.
9. A test is deemed to have been passed by the following criteria:
    a. The security application prevents the simulator from capturing and sending the logon data to the MRG results page, whilst giving no alerts or informational alerts only.
    b. 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 the installation / action of the legitimate control applications, which are executed on identical clones running at the same time as the test clone.
10. A test is deemed to have been failed by the following criteria:
    a. The security application fails to prevent the simulator from capturing and sending the logon data to the MRG results page and gives no, or informational alerts only.

b. 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 the installation / action of the legitimate control applications which are executed on identical clones running at the same time as the test clone.

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. The filename, creation date etc of the simulator will be changed for each test.
14. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG.

Test Results:

All live test results will be, at the directors discretion, published in real time here:

www.browsersecurityproject.malwareresearchgroup.com

Browser Security / ID Protection Applications:

Infection via Internet Explorer on a system already protected by a security application																													
Browser Security / ID Protection Applications	Day 01	Day 02	Day 03	Day 04	Day 05	Day 06	Day 07	Day 08	Day 09	Day 10	Day 11	Day 12	Day 13	Day 14	Day 15	Day 16	Day 17	Day 18	Day 19	Day 20	Day 21	Day 22	Day 23	Day 24	Day 25	Day 26	Day 27	Day 28	Day 29	Day 30	Pass / Fail
Authentium SafeCentral																															
EMSI Mamutu 2.0.0.22																															
Global Information Technology Anti-Keylogger 9.2.1																															
Prevx SafeOnline 3.05.171																															
QFX Software KeyScrambler Professional 2.6.0																															
Quaresso Protect On Q																															
SentryBay Data Protection Suite 5.0.0.4493																															
SoftSphere DefenseWall 3.02																															
SpyShelter SpyShelter 4.17																															
Trusteer Raport 1003.9																															
Trustware BufferZone Pro 3.31-46																															
White Sky IDVault Free Edition																															
Zemana AntiLogger 1.9.2.206																															

Security applications installed on a system which is already infected																															
Browser Security / ID Protection Applications	Day 01	Day 02	Day 03	Day 04	Day 05	Day 06	Day 07	Day 08	Day 09	Day 10	Day 11	Day 12	Day 13	Day 14	Day 15	Day 16	Day 17	Day 18	Day 19	Day 20	Day 21	Day 22	Day 23	Day 24	Day 25	Day 26	Day 27	Day 28	Day 29	Day 30	Pass / Fail
Authentium SafeCentral																															
EMSI Mamutu 2.0.0.22																															
Global Information Technology Anti-Keylogger 9.2.1																															
Prevx SafeOnline 3.05.171																															
QFX Software KeyScrambler Professional 2.6.0																															
Quaresso Protect On Q																															
SentryBay Data Protection Suite 5.0.0.4493																															
SoftSphere DefenseWall 3.02																															
SpyShelter SpyShelter 4.17																															
Trusteer Raport 1003.9																															
Trustware BufferZone Pro 3.31-46																															
White Sky IDVault Free Edition																															
Zemana AntiLogger 1.9.2.206																															

System / Internet Security Applications:

Infection via Internet Explorer on a system already protected by a security application

System / Internet Security Applications	Day 01	Day 02	Day 03	Day 04	Day 05	Day 06	Day 07	Day 08	Day 09	Day 10	Day 11	Day 12	Day 13	Day 14	Day 15	Day 16	Day 17	Day 18	Day 19	Day 20	Day 21	Day 22	Day 23	Day 24	Day 25	Day 26	Day 27	Day 28	Day 29	Day 30	Pass / Fail
Acronis Internet Security Suite 2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Agnitum Outpost Security Suite Pro 7.0.3373.514.1234	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	✗
AVG Internet Security 9.0.837	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Avira Premium Security Suite 10.0.0.542	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
BitDefender Internet Security 2010 13.0.21.347	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Bluepoint Security 1.0.31.99	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	✓
ESET Smart Security 4.2.40.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
F-Secure Internet Security 2010 246	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
G Data internetSecurity 2011 21.0.2.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Kaspersky Internet Security 2010 9.0.0.736	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	3	3	✓
McAfee Internet Security	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Norman Security Suite	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Norton 360 4.2.0.12	0	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	3	3	3	✓
Panda Internet Security 2010 15.01.00	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Sunbelt Software Vipre Antivirus Premium 4.0.3282	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	✓
Tall Emu Online-Armor ++ 4.0.0.44	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	✗
Trend Micro Internet Security 17.50.1647.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Webroot Internet Security Essentials 2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗

Security applications installed on a system which is already infected

System / Internet Security Applications	Day 01	Day 02	Day 03	Day 04	Day 05	Day 06	Day 07	Day 08	Day 09	Day 10	Day 11	Day 12	Day 13	Day 14	Day 15	Day 16	Day 17	Day 18	Day 19	Day 20	Day 21	Day 22	Day 23	Day 24	Day 25	Day 26	Day 27	Day 28	Day 29	Day 30	Pass / Fail
Acronis Internet Security Suite 2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Agnitum Outpost Security Suite Pro 7.0.3373.514.1234	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	✗
AVG Internet Security 9.0.837	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Avira Premium Security Suite 10.0.0.542	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
BitDefender Internet Security 2010 13.0.21.347	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Bluepoint Security 1.0.31.99	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	✓
ESET Smart Security 4.2.40.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
F-Secure Internet Security 2010 246	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
G Data internetSecurity 2011 21.0.2.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Kaspersky Internet Security 2010 9.0.0.736	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	✓
McAfee Internet Security	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Norman Security Suite	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Norton 360 4.0.0.127	0	0	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	3	3	3	3	✓
Panda Internet Security 2010 15.01.00	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Sunbelt Software Vipre Antivirus Premium 4.0.3282	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	✓
Tall Emu Online-Armor ++ 4.0.0.44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Trend Micro Internet Security 17.50.1647.0000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗
Webroot Internet Security Essentials 2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	✗

Key:

●	4	PASS - Security application achieves both levels 2 and 3. Simulator intercepted and user alerted, but also silently blocked if user overrides detection.
◕	3	PASS - Security application blocks the activity of the simulator automatically without user interaction
◑	2	PASS - Security application requests user intervention to block simulator and is able to differentiate its behavour from control application
◔	1	FAIL - Security application requests user intervention to block simulator but is unable to differentiate its behaviour from control application
○	0	FAIL - Security application fails to block the activity of the simulator and gives no alert

Preliminary conclusions: (Day 1)

From these early results, it is clear that as a group, the dedicated browser security / ID protection applications perform quite well. With 9 of the 13 passing the test, it is an affirmation that clear security benefits can be gained by their use.

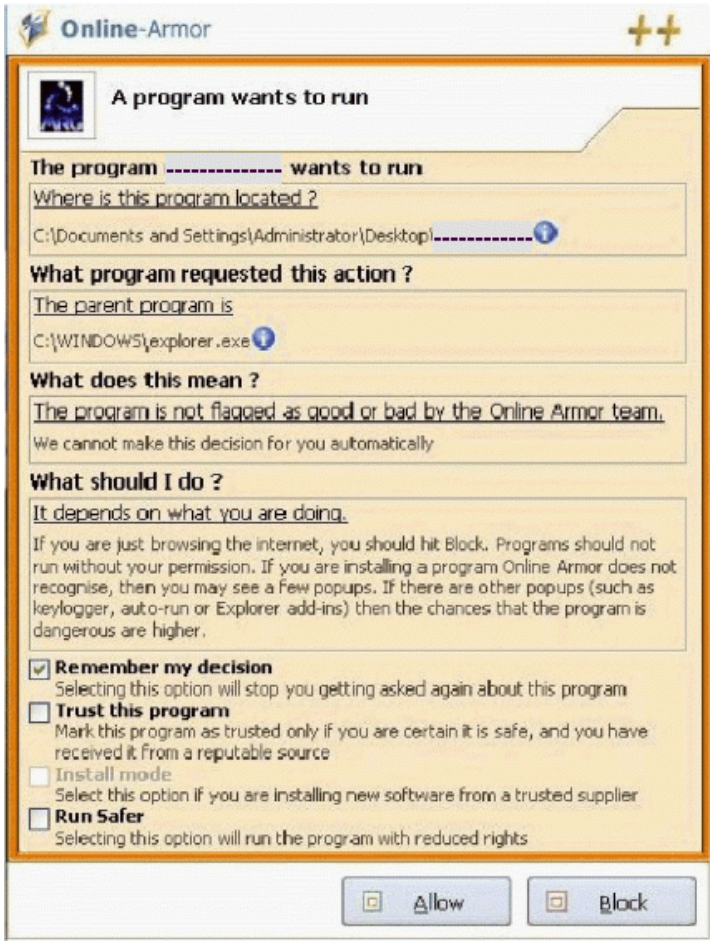
The System / Internet Security Applications have proved less effective with only BluePoint Security, Vipre Antivirus Premium and Kaspersky Internet Security being able to detect / block the simulator.

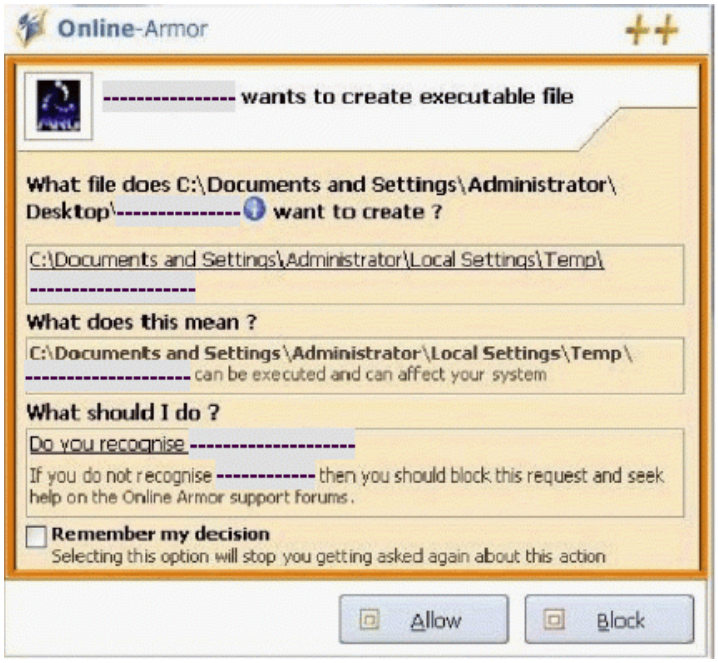
Clearly, we expect the Internet Security Application group to improve their detection as they should begin to pick the simulator up through heuristics and behavioural analysis over time. This said however, the poor detection is an accurate representation of a zero day threat.

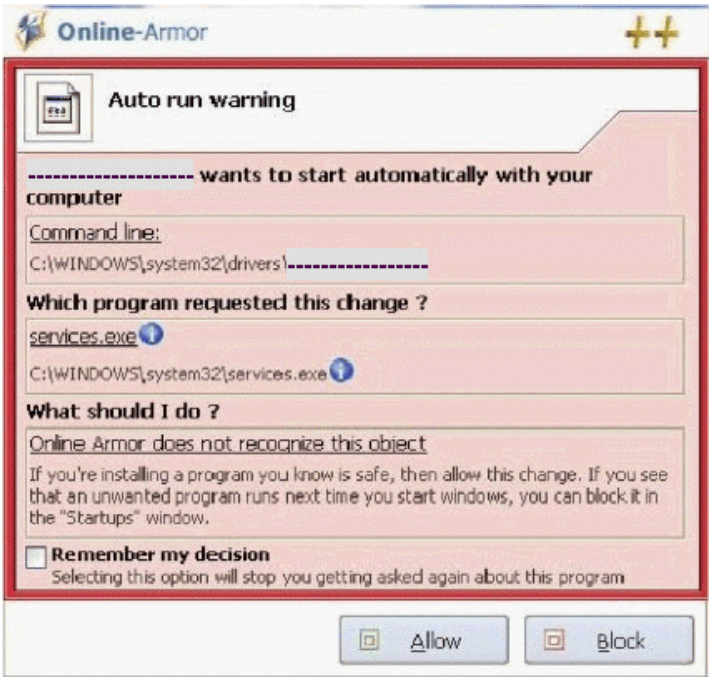
We found that the HIPS functionality against the simulator was generally poor, with most applications employing this functionality being unable to differentiate between its malicious behaviour and that of the legitimate control applications.

We have included screencaps of some of the alerts to demonstrate the above.

OA++ with the simulator:



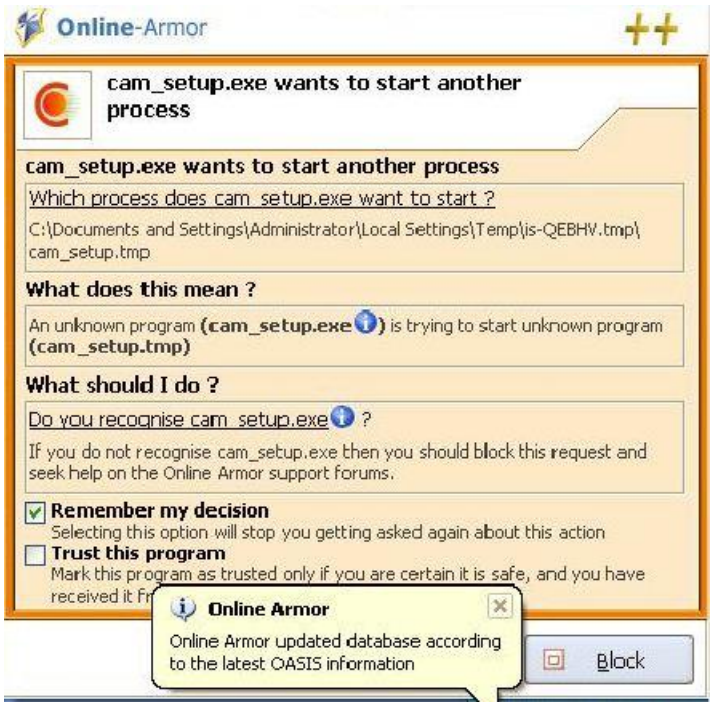


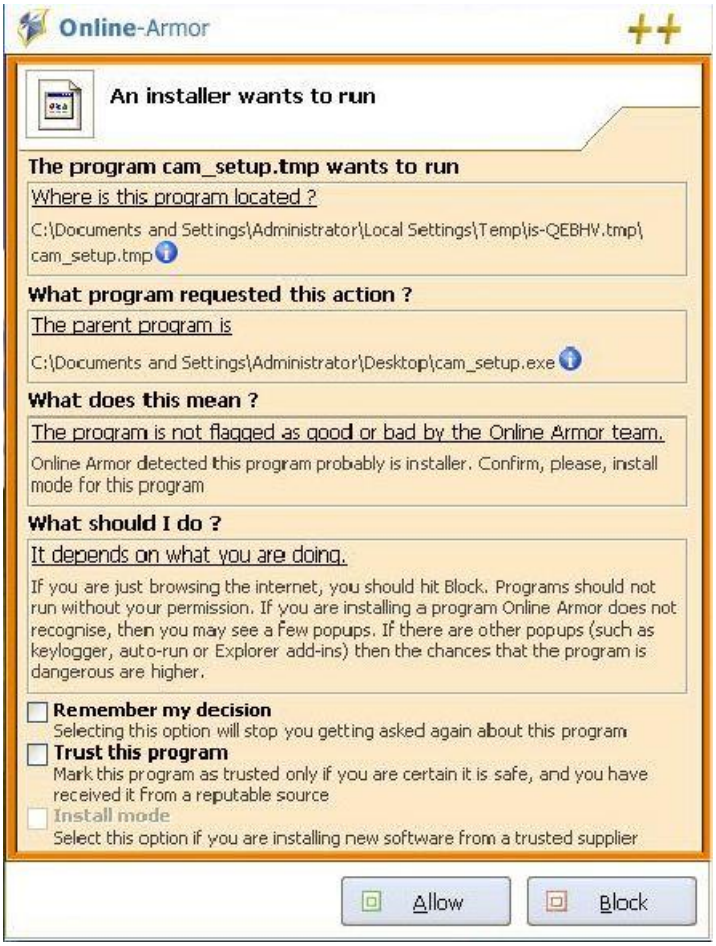


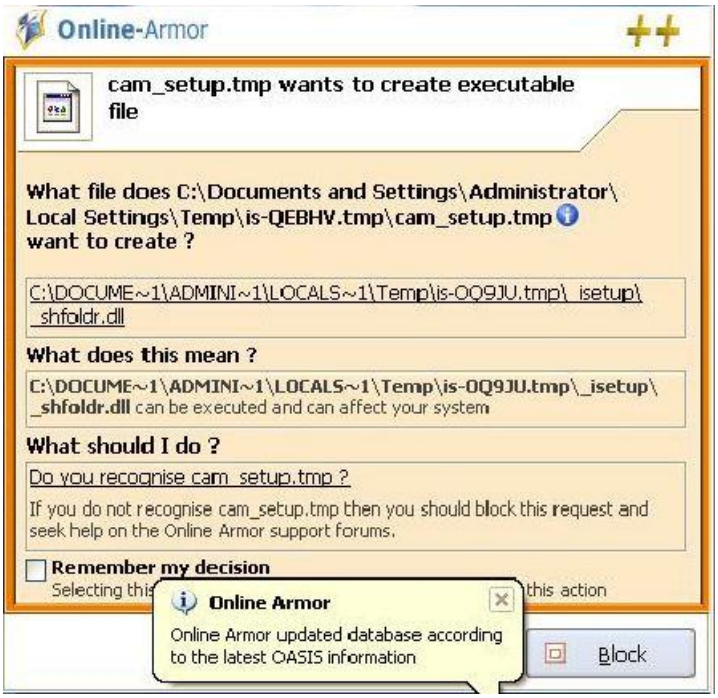
None of these alerts identifies malicious activity, instead, the simulator is simply "unknown" and the user is asked to decide if to allow it or not.

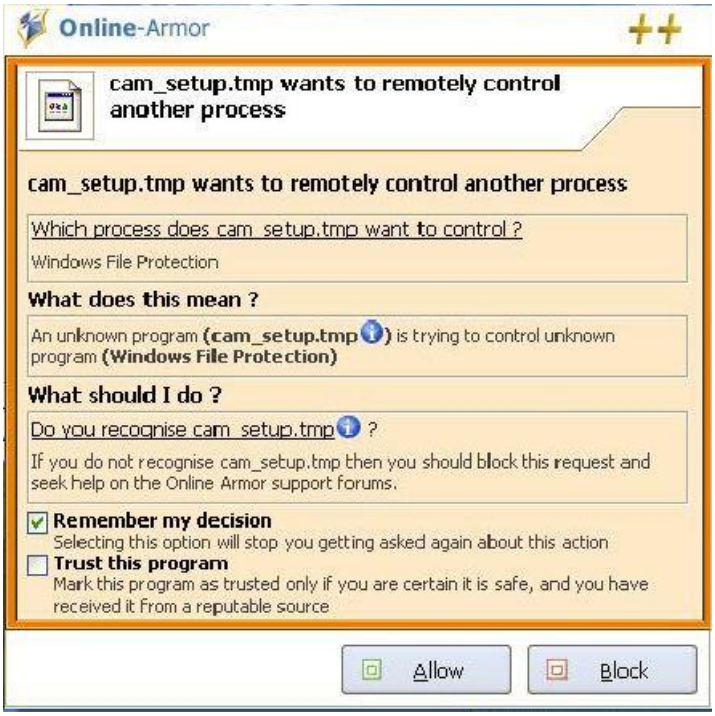
The final alert notifies that the simulator wants to auto run – which is not malicious in itself. Even if this activity is blocked, the system is already compromised and the simulator is able to capture the user data.

OA++ with Corbitek AntiMalware:



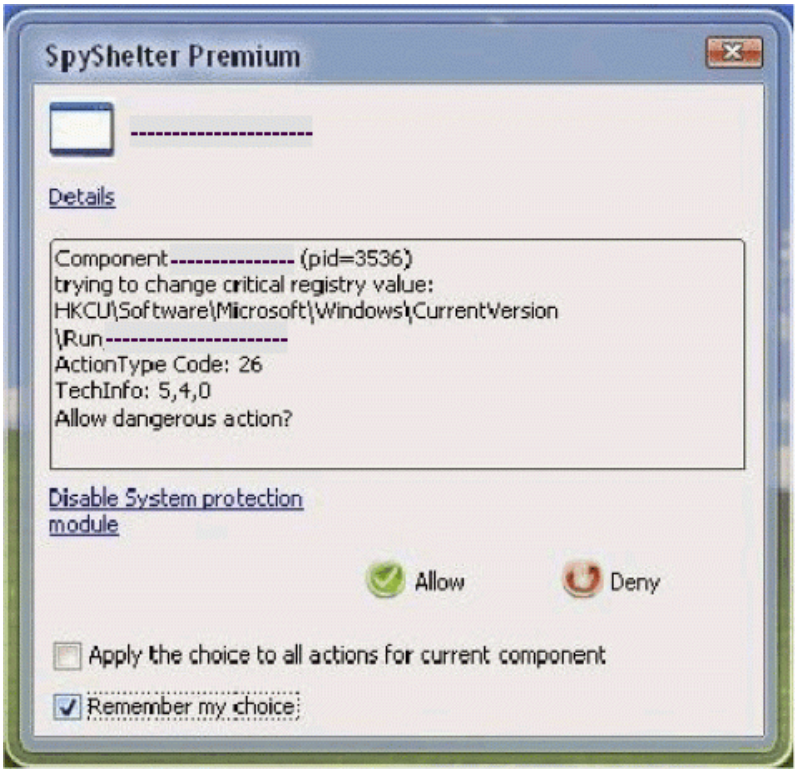


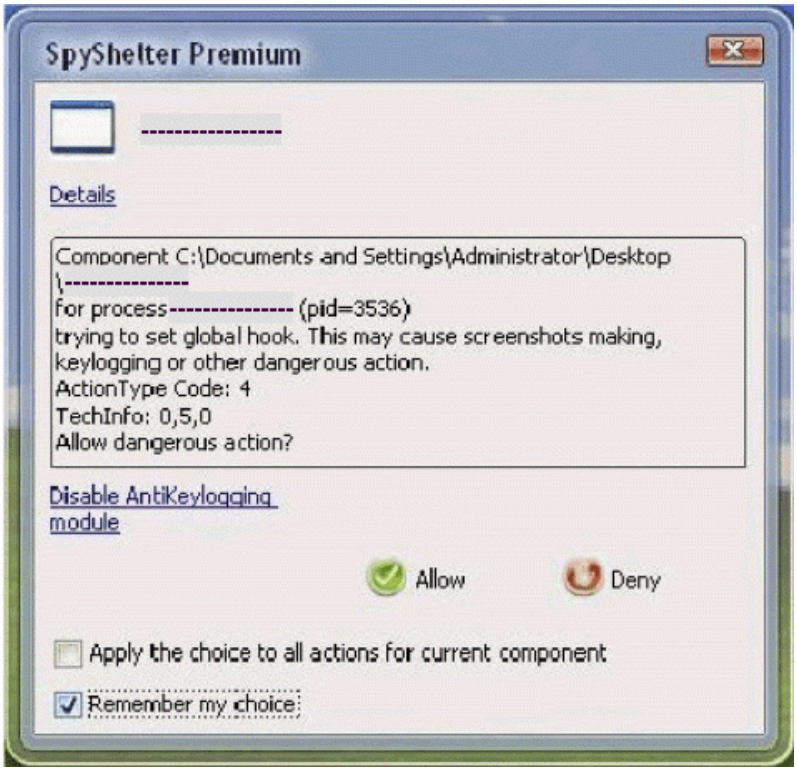




As these demonstrate, there is no meaningful difference between the alerts displayed when installing and activating a piece of malware which steals banking data and those displayed installing a legitimate application.

SpyShelter with the simulator:





SpyShelter with BluePoint Security & Corbitek Antimalware:

As these screencaps demonstrate, SpyShelter alerts on global hooks, however, these are used by many legitimate applications (including BluePoint as is demonstrated) and it is not an accurate indicator of intent to log keystrokes etc.

Every alert SpyShelter gave about the simulator was reproduced when installing the control applications, therefore, in this test, it was unable to differentiate between it and legitimate applications. It should also be noted that SpyShelter identified all activity as "dangerous action". If we had chosen to block every "dangerous action", none of the legitimate applications would have installed.

As mentioned earlier, users who have HIPS which are very "noisy" and alert on too many things, will simply get in the habit of selecting "allow", which negates the point of having the application in the first instance.

Zemana Antilogger and Kaspersky Internet Security were able to diferentiate between the simulator and control appliccations using HIPS / behavioural systems.

Authentium SafeCentral, Prevx SafeOnline, Quaresso MyProtect, SoftSphere DefenseWall, Trusteer Raport, Trustware BufferZone Pro, White Sky IDVault Free Edition, Bluepoint Security & Sunbelt Software Vipre Antivirus Premium were all able to protect the system without any user intervention and therefore, without presenting any opportunity of the data being captured by the simulator.

Preliminary conclusions: (Day 2)

The first observation we must make is that Mamutu now catches the simulator. This is an impressive result as it would appear it is the first application which has learned to protect against this specific threat. We will contact the vendor and discuss this matter with them, then detail any appropriate feedback in our forums.

We have been contacted by one of the vendors under test who took issue with our methodology, specifically, the way in which we use our control applications. In order to demonstrate how we use the control applications, we will post a video on YouTube contrasting the alerts generated by Zemana Antilogger, Kaspersky Internet Security and SpyShelter. We hope this will clarify the way in which we use this component of our methodology.

Preliminary conclusions: (Day 3)

The most notable developments are that Prevx SafeOnline now detects the simulator through its signature as opposed to blocking its functionality via the SafeOnline component which was the case previously.

Similarly, Norton Now automatically catches the simulator and blocks it via its Sonar technology.

These are both outstanding achievements, given the very limited exposure presented by the simulator. MRG congratulates both vendors.

Preliminary conclusions: (Day 4)

There have been no changes in the results today; however, we have changed the icon sets used to represent results. You will see from the new key that there is now a fifth condition to represent where an application is able to detect the simulator via signature AND also block its function if the detection is overridden by the user.

Given that there are now five conditions, we have added a pass or fail icon to the chart to make it easier to see which applications are able to block the simulator following the detailed methodology.

Preliminary conclusions: (Day 5)

As of today, we decided to include the results of the infected system test which we have been conducting in private. The purpose of this test is to see how the security applications perform against the simulator when it has been installed on a system before the security application was installed.

We believe this is a very valuable test as a good proportion of users install a new security application some time after the system was originally created. This is commonly as a result of a user switching security applications, or a user installing one after completing or creating a new system which includes third party applications and utilities etc.

In addition to the above, it is a fact that in reality, users take "calculated risks" when executing some types of software. MRG receives malware from several sources, including feeds from security vendors. In these feeds, we notice a significant proportion of samples which purport to be patches, loaders & keygens etc. The fact that this type of malware arrives in our labs through this route, is an indication that users ignore alerts and allow code to execute if they believe it is legitimate or purposeful in some way. Given this fact, the ability to block the action / effect of active malware is of equal importance to detecting or blocking its execution in the first instance.

Clearly, this test presents new challenges and the results reflect this. The most notable difference is that BluePoint Security does not block the simulator under these pre infection conditions. BluePoint focuses on infection prevention and, as can be seen from that test, performs perfectly at this, but it, along with the vast majority of others, has not yet detected the simulator by signature / behaviour.

Both DefenseWall and BufferZone Pro also fail the infected system test and unlike BluePoint, these applications do not have malware detection capabilities, so unless revised versions are released during the testing period, we don't expect these results to change.

The inclusion of the infected system test has highlighted an issue first raised by Prevx, this being the need for the fourth category / condition, where the application under test both detects the simulator but also prevents its action silently if the user ignores the initial alert and allows it to execute. We notice this condition applies to Zemana Antilogger also and apologise for the delay in highlighting this.

We have noticed that in some quarters there seems to be some difficulty in understanding what constitutes a pass or fail in this project, with some individuals insisting that if we had responded to alerts differently, then a particular application would have passed etc.

We have used control applications in order to determine if the application under test displays alerts which are different for the malicious simulator than displayed when installing the legitimate control applications. The reason for using this method is to assess whether the security application will, in real use, display alerts that convey enough information to the user to allow them to know what is a malicious application and what is harmless.

If the application being tested displays the same alerts for the simulator and control applications, it fails, as it is not meeting the above criteria.

Preliminary Conclusions: (Day 6)

There are no changes today, other than one confusing one, this being that Norton no longer detects the simulator. This strange result is the same for both the infected system test and infection prevention test. On day three Nortons Sonar technology caught the simulator and has done in each subsequent test – until today. We will contact the vendor and ask for a possible explanation.

Preliminary Conclusions: (Day 7)

Today's results remain unchanged from yesterday. In order to increase exposure of the simulator and thereby raise the probability of its detection, we will be running each infected VM for an hour each day and also conducting a user initiated system scan.

Preliminary Conclusions: (Days 8-11)

Despite increasing the exposure of the simulator, there has been no improvement in detection displayed by any of the applications under test.

One thing that struck us, is that this demonstrated how effective a targeted attack could be. A tool like the simulator could easily be used to compromise the systems of a company / agency / competitor or individual etc, and, based on these results, this may well go undetected by many of the major vendors aapplications.

It should be remembered that we designed this simulator to be easily detected by heuristics. We will release some specific details on how we did this in the next few days.

Preliminary Conclusions: (Days 12-20)

As is obvious from the charts, there has been no change in the detection exhibited by the applications under test since day six, which was an anomalous set of results for Norton.

The Issue with Norton has been resolved as we have established the reason for it detecting the simulator for three days and can confirm it was a glitch in the detail of the methodology. Norton does not detect the simulator, however, we will be contacting the vendor to highlight the phenomenon which caused the issue.

Given progress to date, it does not look likely that the applications under test are going to pick up the simulator in the remaining ten test days.

In an effort to increase the probability of detection, for the final ten days, we will, where the facility exists, set all detection and protection components of the applications to maximum and increase their exposure to the simulator by running the VMs 24 hours / day and performing the test six times each day.

Preliminary Conclusions: (Days 21-24)

Despite running the test applications with all their detection components set to maximum and increasing the exposure of the simulator, there has been no change in results.

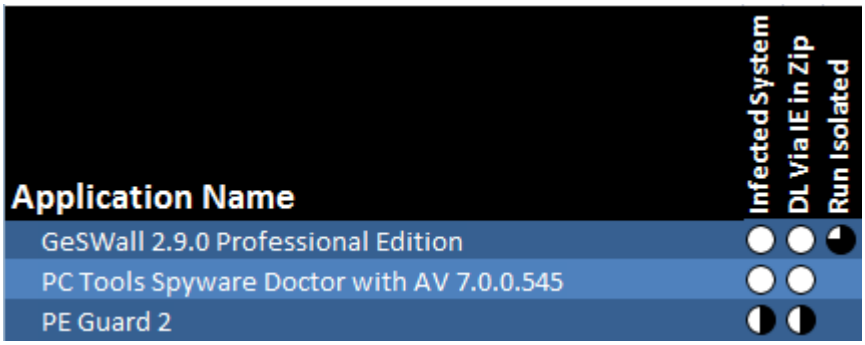
As detailed earlier in this report, we designed this simulator to be easily detectable by heuristics and expected, with behavioural analysis, the test applications to be able to detect in time.

As an example of the design features, the simulator contains strings as "paypal.com", "citibank.com", "login_password" etc. in unencrypted format and the executable nor any of it's modules are encrypted or packed. It is unsigned, makes several crucial changes to the registry and injects processes.

We will continue to test using the same methodology tomorrow, but for the final five days, we will run the test 12 times / day.

We have been asked to test PE Guard, GeSWall & ThreatFire against this simulator. The testing was conducted on 18/07/2010 using the same methodology as is used in the main project, other than only two control applications were used, Bluepoint Security and Trusteer Rapport to save time.

The results were as follows:



We were impressed with PE Guard and will be testing this application in greater detail shortly.

Preliminary Conclusions: (Days 25-30)

Increasing the exposure of the simulator seems to have paid off. On day 25, Norton began to detect the simulator again using its Sonar technology. Kaspersky began detecting the simulator on execution on day 26, but, does not detect it on the pre-infected system. Bluepoint Security began detecting the simulator on day 28 on the pre-infected system.

We will publish our final, overall conclusions for the project as a whole tomorrow.

In addition to this, we will be providing the simulator to selected vendors for analysis.