Online Banking and Endpoint Security Report

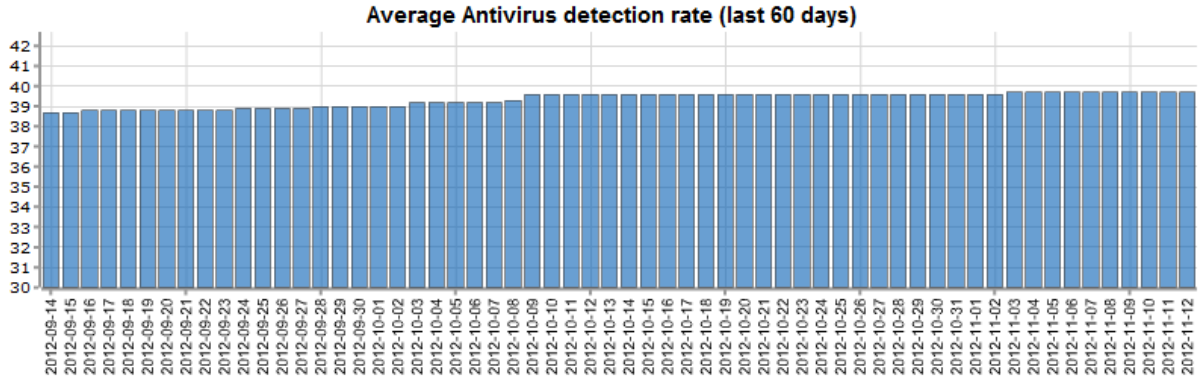
October 2012

Contents:

Introduction:

This is the fourth Online Banking Browser Security report we have published. These reports have all had the same core purpose, this being to assess the efficacy of a range of products against a man in the browser (MitB) attack, as used by real financial malware.

The stimulus for publishing these reports stems from the evidence we gain from our private research which suggests that most endpoint security solutions offer minimal to no protection against early life financial malware. In previous reports we have included graphs from Zeustracker[i], like the one below, to illustrate the poor detection of Zeus.



Our research has shown that detection of Zeus can be much lower and for binaries aged from zero to twelve hours varies between 5% to 20%[ii] , a statistic substantiated by research by our friends at NSS Labs, whose independent testing indicates detection being between 5% and 7%.The variation in detection rate can partly be explained by binary age. The older the binary, by which is meant, the longer it has been in the wild,[iii] the greater the likelihood is that vendors will have been able to capture it and create signatures to detect it.

The Purpose of this Report:

Whilst this report centres about the same theme as our previous reports, it differs in that it is designed to illustrate the difference between in the wild threats (ITW) and custom crimeware, which is <u>not</u> ITW.

Earlier this year, the BBC broadcast a programme[iv] we made with them based on our work on browser security and financial malware. The programme featured a test we conducted using one of our financial malware simulators which employed a verified[v] MitB attack as used by financial malware such as Zeus and SpyEye. We created the simulator to demonstrate the fact that very few security solutions had any dedicated protection against this type of attack and that relying on behavioural or blacklisting technology[vi] was ineffective against new threats.

The test used in the programme was representative of a targeted attack using custom crimeware, exactly the same kind of attack a well-funded, technically sophisticated criminal group could use against an individual or corporation.

To illustrate the difference between an attack using ITW crimeware and a custom engineered tool intended for a focused, targeted breach, we used three simulated attacks.

The first, which represents an ITW tool is conducted using a variant[vii] of the simulator we created for the BBC. As part of the BBCs policy, it offered the simulator to all the vendors featured in the programme, thus allowing them to analyse it. In addition to this, MRG Effitas anonymously submitted a further six variants to all the vendors over a six month period.[viii]

The BBC simulator uses a MitB attack to capture user credentials entered in to SSL protected sites such as PayPal, facebook and most banking sites. Once captured, the data is sent in real-time to an external URL where it can be viewed.

The second and third attacks are performed using custom crimeware tools[ix] created by our engineering team. Each of these tools, like the BBC simulator, employs a unique[x] MitB attack to capture user credentials entered in to SSL protected sites. These tools are designed to be installed on to systems locally via USB[xi] like Stuxnet, and store data captured from the browser on the local system, which can be retrieved by the attacker at a later date. These simulators were not exposed to any antimalware products during their development or testing and so were not ITW.

As the variants of the BBC simulator were submitted to vendors over a long period of time, we felt there would be a reasonable chance they would detect it in the test. This simulator is designed to be detectable after exposure as it contains unencrypted code which is clearly suspicious and performs highly malicious actions.

The second and third simulators were designed to be more stealthy and since they were effectively zero hour, we anticipated that most traditional endpoint protection technologies would not alert or block them.

MRG Effitas has conducted in-depth testing and research in to targeted attacks, looking at evidence from real world accounts such as Stuxnet and the private work conducted by our team. It is our position that any endpoint can be compromised and that for the technically proficient attacker, this can go undetected for months.[xiixiii]

Given the fact that it is possible to get malicious code to execute undetected on most protected endpoints, we believe a new set of testing metrics is needed to assess product efficacy in a way that maps meaningfully to real world scenarios. Simple "detection" tests, weather static or dynamic are not enough.

The metrics we suggest will serve us best in the future are as follows:

1. Time taken to detect malware or attack (How long does it take a solution to detect malware or an attack)
2. Time to remediate (How long does it take to remediate in cases where it is possible)
3. Determination of breach (Measure if a data breach has occurred – as the execution of malware on a system does not necessarily mean it has been able to effect a data breach)
4. Assessment of breach (Determine what was breached, for how long and possible assessment of impact)

In 2013, MRG Effitas will be conducting a number of on-going public projects based on the above, starting with a Time to Detect project which will run alongside our Flash Tests.

For the purposes of this report, our primary concern is metric 3, "determination of breach". We measure if the simulators are blocked from being executed, either by detection, hips (which may or may not involve a user input request) but our main focus is on measuring if the simulators are prevented from performing the data breach and the simulators allow us to do this.

Security Applications Tested:

Endpoint Financial Fraud Prevention and Anti-Keylogging Applications:

- Aplin Software Neo's SafeKeys 3
- Comitari Technologies Web Protector 1.5.21
- Global Information Technology PrivacyKeyboard 10.33
- Network Intercept Keystroke Interference 2.9
- Prevx SafeOnline 3.0
- QFX KeyScrambler 2.9.3.0
- Quarri Protect On Q 3.0
- Sandboxie 3.74
- Secure Banking Secure Banking 1.5.1
- SentryBay DataProtection Suite 5.6
- SoftSphere DefenseWall 3.19[xiv]
- StrikeForce Technologies GuardedID 3.01
- Threatmetrix TrustDefender Pro Gold Edition 3.0
- Trusteer Rapport 1207.31
- Trustware BufferZone Pro 4.02
- Webroot SecureAnywhere 8.0
- Zemana AntiLogger 1.9

Anti Malware and Internet Security Applications:

- avast! Internet Security 7.0
- Avira Internet Security 2013
- BullGuard Internet Security 2013
- Comodo Internet Security Pro 2012
- Emsisoft Anti-Malware 7.0
- ESET Smart Security 5.2
- F-Secure Internet Security 2013
- GFI Vipre Internet Security 2013
- Ikarus Virus Utilities 2.2
- Immunet Protect Plus 3.1
- Kaspersky Internet Security 2013
- McAfee Internet Security 2012
- Microsoft Security Essentials 4.1
- Norton Internet Security 2013
- Trend Micro Titanium Internet Security 2013

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 32 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 4 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.[xv]
   c. 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 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. 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.
9. 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.
10. Testing is conducted with all systems having internet access.
11. Each individual test for each security application is conducted from a unique IP address.
12. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.
13. All testing was conducted on the 28th of October 2012.

Test Results:

The table below shows the results for the Endpoint Financial Fraud Prevention and Anti-Keylogging Applications

Application Name	BBC Sim	Sim 2	Sim 3	Overall
Aplin Software Neo's SafeKeys	F	F	F	
Comitari Technologies Web Protector	F	P	F	
Global Information Technology PrivacyKeyboard	F	F	F	
Network Intercept Keystroke Interference	F	F	F	
Prevx SafeOnline	F	F	F	
QFX KeyScrambler	F	F	F	
Quarri Protect On Q	P	P	P	
Sandboxie	F	P	P	
Secure Banking Secure Banking	F	F	F	
SentryBay DataProtection Suite	F	F	F	
SoftSphere DefenseWall	P	P	P	
StrikeForce Technologies GuardedID	F	F	F	
Threatmetrix TrustDefender Pro Gold Edition	F	F	F	
Trusteer Rapport	P	P	P	
Trustware BufferZone Pro	F	P	P	
Webroot SecureAnywhere	P	F	F	
Zemana AntiLogger	P	U	U	

The table below shows the results for the Anti Malware and Internet Security Applications.

Application Name	BBC Sim	Sim 2	Sim 3	Overall
avast! Internet Security	P	P	P	
Avira Internet Security	D	F	F	
BullGuard Internet Security	D	F	F	
Comodo Internet Security Pro	D	D	U	
Emsisoft Anti-Malware	D	D	D	
ESET Smart Security	F	F	F	
F-Secure Internet Security	F	F	F	
GFI Vipre Internet Security 2013	D	F	F	
Ikarus Virus Utilities	D	F	F	
Immunet Protect	D	F	F	
Kaspersky Internet Security 2013	P	P	P	
McAfee Internet Security	D	F	F	
Microsoft Security Essentials	F	F	F	
Norton Internet Security	D	F	F	
Trend Micro Titanium Internet Security	D	F	F	

P	The application prevented the active simulator from capturing data
D	The application detected and automatically blocked the execution of the simulator
U	The application detected and intercepted the execution of the simulator and presented a user input request with guidance that the simulator was attempting to perform a potentially malicious action
F	The application did not detect the simulator or prevent it from capturing data

Analysis of the Results:

As mentioned at the start of this report, based on the evidence and data we have seen on targeted attacks, we expected the vast majority of applications to fail and the testing vindicates this.

We were surprised to see how badly the dedicated Endpoint Financial Fraud Prevention and Anti-Keylogging Applications performed, with only Quarri Protect On Q, SoftSphere DefenseWall, Trusteer Rapport and Zemana Antilogger fully protecting the system.

We were pleased to see that both Avast and Kaspersky have chosen to implement a secure browser functionality and that these proved effective against the MitB attacks.

Congratulations to Comodo Internet Security Pro and Emsisoft Anti-Malware for their excellent performance which was as a result of good detection and layered protection.

Conclusions:

We expected most applications in these tests to fail and it should be noted that many of those that did are just one element of protection provided by those vendors and We acknowledge that many vendors do have other product and technologies that would help detect these sorts of attacks in the real world – and this is what our work in 2013 will be focusing on.

We hope our tests in 2013 will assess in a meaningful way, the efficacy of a range of security technologies and help both the consumers and the vendors themselves.

[i] Reproduced with permission. See https://zeustracker.abuse.ch
[ii] Based on testing conducted over a three month period
[iii] The actual age as measured from when a binary is crated is largely irrelevant. For the purpose of testing and research, age is measuring the time binaries are in the wild
[iv] See http://www.youtube.com/watch?v=DUnZMwXCkyw
[v] The simulator and all testing was independently monitored and verified by S21sec www.s21sec.com
[vi] Blacklisting encompasses malicious URL lists and binary signatures
[vii] MRG Effitas does not weaponise its simulators, they rely on manual morphing, instigated by our engineering team.
[viii] This included vendors in this report which were not included in the BBC programme, but only those whose applications have the ability to detect malware or have telemetry functionality which would allow them to capture or submit unknown or suspicious code
[ix] All simulators are designed to be neutral. None are designed to bypass any specific vendor or product
[x] Whilst all three simulators use a MitB attack, each attack is unique and makes use of different mechanisms
[xi] Although they are effective when installed via any vector
[xii] We have conducted tests which involve compromising ten different systems with a malicious simulator. These systems were tested daily for a period of twelve months and none of them detected or blocked the malicious activity.
[xiii] It is also the position of the EU that all banks in the region should assume their customers PCs are compromised by financial malware
[xiv] This application operates on 32 bit OS only and was therefore tested on Windows 7 32
[xv] Where the security application offers a secured or dedicated banking browser, this is used