nProtect Online Security

Setting a New Standard in Web Fraud Detection & Prevention

User Manual

Copyright $\ensuremath{\textcircled{C}}$ 2014 nProtect, Inc. All Rights Reserved.

The software (including any accompanying functions and services) and documentation (including any product packaging) is the property of nProtect or its licensors, and is protected by copyright law. nProtect prohibits the partial or full copy, replication, translation or transformation into any form recognized by an electronic machine of the software or manual without nProtect's permission.

Contact Us

3003 N. First Street, Suite #301 San Jose, CA 95134 Website: http://www.nProtect.com TEL: 408-477-1742 / Toll Free: 855-466-7768 (1-855-GO-NPROT)

Table of Content

1. OVERVIEW	3
1.1. Product Description	3
1.2. Product Strengths	3
1.3. System Specification	3
2. INSTALLATION AND UNINSTALLATION	4
2.1. Installation	4
2.2. Uninstallation	9
3. NOS AGENT	10
3.1. Anti-Phising	
3.2. Hosts File Protection	
3.3. Auto-Start Setting	
3.4. Log	
4. NPROTECT ONLINE SECURITY	19
4.1. Real-Time Malware Monitoring	
4.2. Network Protection	
4.2.1. Automatic Process Authentication	
4.2.2. Manual Process Authentication	
4.2.3. Windows Default Programs Monitoring	
	27
4.2.4. Anti-Code Injection	
4.2.4. Anti-Code Injection	
4.2.4. Anti-Code Injection4.3. Keystroke Protection4.4. Anti-Screen Capture	28 29
 4.2.4. Anti-Code Injection 4.3. Keystroke Protection 4.4. Anti-Screen Capture	28
 4.2.4. Anti-Code Injection	27 28 29
 4.2.4. Anti-Code Injection	27 28 29 29 29 29 30
 4.2.4. Anti-Code Injection 4.3. Keystroke Protection 4.4. Anti-Screen Capture 4.4.1. Screen Capture by PrintScreen Key 4.4.2. Screen Capture by Screen Capturing Tools 4.5. DNS Monitoring 4.6. Log 	29
 4.2.4. Anti-Code Injection 4.3. Keystroke Protection. 4.4. Anti-Screen Capture 4.4.1. Screen Capture by PrintScreen Key 4.4.2. Screen Capture by Screen Capturing Tools 4.5. DNS Monitoring 4.6. Log 5. PROBLEM SOLVING 	29
 4.2.4. Anti-Code Injection 4.3. Keystroke Protection 4.4. Anti-Screen Capture 4.4.1. Screen Capture by PrintScreen Key 4.4.2. Screen Capture by Screen Capturing Tools 4.5. DNS Monitoring 4.6. Log 5. PROBLEM SOLVING 5.1. How to Collect Logs 	28 29 29 29 29 30 31 31 32 32

1. Overview

1.1. Product Description

nProtect Online Security (hereinafter **NOS**) is a total online security solution that secures online transactions on end-user's system with multi-layered protection such as **Malware Monitoring**, **Network Protection**, **Keystroke Protection**, **Anti-Phishing**, **Anti-Screen Capture**, and **DNS Monitoring**.

1.2. Product Strengths

Some of the key advantages of using NOS is:

- Multi-layered online security solution
- Top of the line kernel level technology
- Detects and repairs various financial malwares such as Zeus and SpyEye w/o cleaning utility
- Approximately 94% lighter file size compared to global anti-virus products and 50% lighter file size than competitor product.
- 24/7 proactive support from Response Center(ISARC)
- Coverage of malwares from all around the globe

1.3. System Specification

[Table 1-1] lists hardware and software specifications needed to operate NOS.

Item	Minimum requirements		
CPU: Intel Pentium IV 1.0Ghz or higher			
Hardware	Memory: RAM 512MB or higher		
	HDD: 150MB free space		
OS	Windows XP(x32), VISTA(x32/x64), 7(x32/x64), 8(x32/x64)		
	Internet Explorer 8, 9 and 10(Win 8)		
Browser	Firefox 17 and later		
	Chrome 23 and later		

[Table 1-1] System Specifications

2. Installation and Uninstallation

2.1. Installation

Download NOS setup file from NOS customer website. Or click the banner on the NOS sample trusted Financial Institute website.



[Image 2-1] Sample Trusted Financial Institute Website

When prompted, click 'Run' to begin the NOS installation.



[Image 2-2] Setup File Download

By clicking 'Save' or 'Save As', nProtectOnlineSecurity.exe file will be saved on the local system.



[Image 2-3] Setup File Icon

Once executed, Windows User Account Control will ask to allow NOS to be installed on the local system. Click 'Yes' to begin NOS Setup.

😌 User Accoun	t Control			
Do you want to allow the following program to make changes to this computer?				
	Program name: nProtect Online Security Installer Verified publisher: INCA Internet Co.,Ltd. File origin: Downloaded from the Internet			
Show det	ails Yes No Change when these notifications appear			

[Image 2-4] Windows User Account Control

Click 'Next' to continue installation



[Image 2-5] nProtect Online Security Setup

Please read the End User License Agreement and click 'I Agree' to continue installation.

RProtect Online Security Setup	<u> </u>			
License Agreement Please review the license terms before installing nProtect Online Security.				
Press Page Down to see the rest of the agreement.				
End User License Agreement				
IMPORTANT: THE FOLLOWING AGREEMENT ("AGREEMENT") SETS FORTH THE TERMS AND CONDITIONS UNDER WHICH NPROTECT INCORPORATED IS WILLING TO LICENSE THE "SOFTWARE" AND ACCOMPANYING "DOCUMENTATION" TO "YOU" AS AN INDIVIDUAL USER OR AN AUTHORIZED REPRESENTATIVE OF AN ENTITY. BY ACCEPTING THIS AGREEMENT, YOU ARE ENTERING INTO A BINDING LEGAL CONTRACT WITH NPROTECT. THE TERMS AND CONDITIONS OF THE	V			
If you accept the terms of the agreement, dick I Agree to continue. You must accept the agreement to install nProtect Online Security.				
INCA Internet Co.,Ltd. 	ncel			

[Image 2-6] End User License Agreement

Installation will not take more than few seconds, depending on user's system specifications.

Revealed the security Setup	
Installing Please wait while nProtect Online Security is being installed.	
Extract: npkfxsvc.exe	
Show details	
INCA Internet Co.,Ltd.	
< Back Next >	Cancel

[Image 2-7] Installing nProtect Online Security

Click 'Finish' to complete the installation.

🛜 nProtect Online Security Setup				
징nProtect	Completing the nProtect Online Security Setup			
NOS	nProtect Online Security has been installed on your computer.			
nProtect Online Security	Click Finish to close Setup.			
INCA Internet Co., Ltd				
	< Back Finish C	ancel		

[Image 2-8] Completing nProtect Online Security Installation

When the installation is complete, NOS icon will appear on the system tray as shown below.



[Image 2-9] nProtect Online Security Tray Icon

Once installation is complete, pop-up window ask to install Anti-Phishing add-on. To enable Anti-Phishing function, please click 'Yes' and install browser add-on.



[Image 2-10] Browser Add-ons

Once installation is complete, visit a Trusted Website (ex. bank.nProtect.com) and NOS will launch automatically.

The system tray icon will turn green to indicate that NOS is ON and website is secured.[Image 2-11]



[Image 2-11] Protection Status

Double click on the system tray icon and NOS mini UI will be shown as below.[Image 2-12]



[Image 2-12] nProtect Online Security UI

2.2. Uninstallation

Go to 'Programs and Features' on the Control Panel. (Start > Control Panel > Programs and Features)



[Image 2-13] Uninstalling nProtect Agent

Select NOS and click 'Uninstall' button. If a browser is open, uninstall will ask to close all running browsers. (Internet Explorer, Firefox, Chrome, etc) Click 'Yes', to remove NOS from the program list.

nProtect Online Security UnInstall	×
Exiting browser to normally perform remova	ıl.
Yes No	

[Image 2-14] Alert Message

Once uninstallation is complete, 'Uninstall Complete' message will be shown as below.

nProtect Online Security UnInstall	X
Uninstall Complete	
ОК	

[Image 2-15] Uninstall Complete

3. NOS Agent

Click the right-mouse button on the NOS tray icon and NOS Agent menu will be shown as below.



[Image 3-1] nProtect Online Security Agent Menu UI

The main functions are as follows.

Function	Description
	Move to menu window. User can turn on or turn off main functions of the
Agent Settings	nProtect Online Security such as Anti-Phishing, Hosts File Protection and Auto-
	start. User can also view all event logs of the Protect Agent.
Help	Moves to the Help page website.

[Table 3-1] nProtect Online Security Agent Menu Funtions

When 'Agent Settings' is selected, NOS agent UI will be displayed.[Image 3-2]

Function	Description			
	Anti-Phishing: Monitors the websites you visit and gives a warning upon			
Coourity Cottings	detection of a phishing site.			
Security Settings	Hosts File Protection: Prevents any modification or change of Host files in your			
	local system.			
nDrotoot Agont	Auto-start Setting: Using the ON/OFF option, users can decide whether			
nProtect Agent	nProtect Online Security is starts automatically when you visit a trusted website.			
Log	You can view all event logs of nProtect Agent.			

[Table 3-2] nProtect Online Security Agent Funtions

3.1. Anti-Phising

Security Settings nProtect Agent Log Anti-Phishing N OFF Monitors to identify phishing content contained in websites. Hosts File Protection Prevents any modification or changes to the system hosts file by	Protect Onlin	ne Security		_	
	Security Settings	nProtect Agent	Log		
ON OFF Monitors to identify phishing content contained in websites. Image: State of the system hosts file by the system host by the sys		Anti-Phishing			
Hosts File Protection	ON	OFF	Monitors to identify phis	hing content contai	ned in websites.
Prevents any modification or changes to the system hosts file by		Hosts File Protec	tion		
UFF malicious programs.					
	ON	OFF	Prevents any modificatio malicious programs.	n or changes to the	system hosts file by
	ON	OFF	Prevents any modificatio malicious programs.	n or changes to the	system hosts file by
		OFF	Prevents any modificatio malicious programs.	n or changes to the	system hosts file b

Anti-Phishing function can be turned off by moving the slide to 'OFF' and clicking 'OK' or 'Apply'.

[Image 3-2] Security Setting

When a suspicious website is visited, Anti-Phishing will alert users with the following warning message.



[Image 3-3] Anti-Phishing Warning

• Internet Explorer

After installing NOS, open Internet Explorer browser. An NOS pop-up window will show asking to install the Anti-Phishing add-on. Click "Yes" to install the add-on.

			_ 🗆 🗙
Attps://www.google.com/?gws_rd=cr&ei=n6KqUsP	FeahiAfL 🔎 マ 🔒 🖒 🚺 Google	×	☆ ☆ 🔅
		+You Gmail II	nages 🏭 Sign in
0 1	Protect Online Security	A fa	× ster way to browse the web
	nProtect Online Programinstallation		nstall Google Chrome
	Veb browsers' add-on needs be installed to use Inti-Phishing. Do you want to install the add-on of nProtect Inti-Phishing? Yes Xo		
Advertising Business About		New Privacy & Terms	Settings Google.co.kr

After the installation is complete, restart Internet Explorer. A message will appear on the bottom of the browser to enable 'PhishingBlockATLBHO Class'. Click Enable.

Advertising	The 'PhishingBlockATLBHO Class' add-on from 'INCA Internet Co.,Ltd.' is ready for use.	Enable Don't enable × Google.co.kr

Restart Internet Explorer and visit the sample phishing site (phishingdemo.nprotect.com) to see if Anti-Phishing feature is working properly.

Chrome

When Chrome browser is first started, NOS pop-up window will show asking to install the Anti-Phishing add-on. Click "Yes" to install the add-on.

Gaagla			_ _ X
← → C A https	s://www.google.com/?gws_rd=cr&ei=bUFWUrKyPMbJiAe36oH4Bg	9	£ २ ≡
		+You Gma	il Images III Sign in
	Protect Online Security Programinstallation Web browsers' add-on needs be installed to use Anti-Phishing. Do you want to install the add-on of nProtect Anti-Phishing? Yes	No	
Advertising Busin	ness About	Privacy & Terms	Settings Google.co.kr

After waiting about 10 seconds for the browser to install the add-on, close the Chrome browser and restart. When the browser is restarted, the menu button will be highlighted in orange.



8 Google ×	
← → C	숬 🔍 🔳
	New tab Ctrl+T
	New window Ctrl+N
	New incognito window Ctrl+Shift+N
	Bookmarks +
	Recent Tabs
	Edit Cut Copy Paste
	Zoom – 100% + []]
\mathbf{C} I	Save page as Ctrl+S
	Find Ctrl+F
GUUYIC	Print Ctrl+P
0	Tools 🕨
	History Ctrl+H
	Downloads Ctrl+J
Google Search I'm Feeling Lucky	Sign in to Chrome
	Settings
	About Google Chrome
	Help
Advertising Business About	Exit

Click the menu bar and select "New extension added(Chrome APS)"

When "New extension added(Chrome APS)" is selected, it will pop-up a message asking to "Enable extension".

gle.com				
	"Chrome APS" added	×	+You	G
	Another program on your computer added an extension that may change the way Chrome works.			
	It can:			
	Access all data on your computer and the websites you visit Enable extension Remove from Chrome]		
	Google			

After the installation is complete, visit the sample phishing site(phishingdemo.nprotect.com) to see if Anti-Phishing feature is working properly.

• Firefox

When Firefox browser is first started, NOS pop-up window will show asking to install the Anti-Phishing add-on. Click "Yes" to install the add-on.



"nProtect Online Security Setup" pop-up will show asking to restart Firefox. Click "OK" to continue.

	nProtect Online Security Setur
	Firefox is running. Please restart Firefox.
Google	OK Search

After restarting Firefox, "Install Add-on" tab will appear. Check "Allow this installation" and click "Continue".



Firefox will ask to restart Firefox to finish installation. Click "Restart Firefox" to finish installation.

follo	her program on your computer would like to modify Firefox with the wing add-on:
	nProtect AntiPhishing 2013 8 29 1
1	By INCA Internet Co.,Ltd
	Location: M:\Program Files (x86)\Common Files\nProtect Share
	☑ Allow this installation
You Man	can always change your mind at any time by going to the Add-ons ager.
	You must restart Firefox to finish installing this add-on. Restart Firefox Cancel

After the installation is complete, visit the sample phishing site(phishingdemo.nprotect.com) to see if

Anti-Phishing feature is working properly.

3.2. Hosts File Protection

Hosts File Protection can be turned off by moving the slide to 'OFF' and clicking 'OK' or 'Apply'.[Image 3-2] When Hosts File Protection is turned OFF, an alert message will be shown as below.[Image 3-4] Auto-Start function on nProtect Agent tab menu must be first turned OFF to turn OFF Hosts File Protection.



[Image 3-4] Hosts File Protection Alert Message

3.3. Auto-Start Setting

Auto-Start can be turned off by moving the slide to 'OFF' and clicking 'OK' or 'Apply'.[Image 3-5] When a trusted website is visited, Customer Name and Website URL will be added to the Auto-Start list.

n Protect Onlir	e Security				
Security Settings	nProtect Agent	Log			
	Auto-Start Setting	* This function allows nPro when visiting a Customer v * To use this function, Ho r	otect Online Securit website. sts File Protection I	y to start automatically must be ON.	у
Display Customer Customer Name NOS BANK	Websites Mebsites Mebsites	m	NOS Ma	anual Start	
* Customeris reg	ister automatically to the star	t list after nProtect Online	Security starts.		

[Image 3-5] Auto-Start Setting

3.4. Log

All event logs for agent update, phishing, hosts file protection can be seen on this tab.

Security Settings	nProtect Ager	n.	Lög
Log			
Date/Time	Туре	Status	Description
29-Apr-2013 - 11:45:10	Update		nProtect Online Security update is complete.
29-Apr-2013 - 11:44:45	Update		nProtect Online Security update is starting.
29-Apr-2013 - 11:36:52	Update		nProtect Online Security update is complete.
29-Apr-2013 - 11:36:48	Update		nProtect Online Security update is starting.
26-Apr-2013 - 18:20:59	Online Secu	Execute	nProtect Online Security has been started.
26-Apr-2013 - 18:20:59	Update		nProtect Online Security update is complete.
26-Apr-2013 - 18:20:58	Update		nProtect Online Security update is starting.
26-Apr-2013 - 18:20:56	Update		nProtect Online Security update is complete.
26-Apr-2013 - 18:20:56	Update		nProtect Online Security update is starting.
26-Apr-2013 - 18:20:39	Update		nProtect Online Security update is starting.
26-Apr-2013 - 18:19:56	Online Secu	Execute	nProtect Online Security has been started.
26-Apr-2013 - 18:19:56	Update		nProtect Online Security update is complete.
26-Apr-2013 - 18:19:42	Update		nProtect Online Security update is starting.
26-Apr-2013 - 18:19:06	Update		nProtect Online Security update is complete.
26-Apr-2013 - 18:19:04	Update		nProtect Online Security update is starting.
26-Apr-2013 - 18:18:45	Update		nProtect Online Security update is starting.

[Image 3-6] nProtect Agent Log

4. nProtect Online Security

When a user visits a trusted website, NOS will start automatically.



[Image 4-1] nProtect Online Security UI

Function	Mark	Description
Company	n Protect	On the top left, a company logo can be placed to be recognized
Logo	Online Security	where nProtect Online Security is running.
Settings	٥	Click this button to view the main menu UI.
Help	?	Click this button to open the help page.
Network	Network Protection	This quick option allows users to change the Network Protection
Protection	ON OFF	option without opening the main menu UI.
Keystroke	Keystroke Protection	This quick option allows users to change the Keystroke Protection
Protection	ON	option without opening the main menu UI.
DNS Monitoring	SAFE	Shows the security status of DNS Monitoring, showing whether URL address matches the IP address.

[Table 4-1] nProtect Online Security UI

When NOS tray icon is green, click with the right-mouse button to see that 'Advanced Settings' has been added to NOS menu.

Agent Settings	
Advanced Settings	
Help	
ко 🐶 🗛 📑	٠

[Image 4-2] nProtect Online Security Agent Menu UI

Click 'Advanced Settings' or the settings button (¹) in the UI to see the main menu UI.[Image 4-3]

٥n	nProtect Online Security							×
J	Protects	e Monitoring s system from malware thre	ats					
Ľ	Malware Monitoring	Network Protection	Keystroke &	Screen	Log	,		
	Real-Time Malware M	onitoring						
	Mor	nitoring Re	al-time monitoring	ofproces	ses and registry	/		
	🔲 Enable	e Auto-Repair Iow message after completi	ng Auto-repair					
				0	ĸ	Δr	vlv	

[Image 4-3] nProtect Online Security main menu

The features are as follows.

Function	Description				
Mahuara Manitaring	Monitors all running processes and registry in real-time. Can choose to enable				
Marware Monitoring	Auto-Repair.				
	Allows or blocks network access based on policies. Users can choose to turn				
Network Protection	ON and OFF Network Protection function. Also users can add or remove				
	programs to the list.				
Keystroke & Screen	Menu to turn ON and OFF Keystroke Protection and Anti-Screen Capture.				
Log	Shows all event logs of nProtect Online Security.				
	[Table 4-2] nProtect Online Security Functions				

4.1. Real-Time Malware Monitoring

When users open trusted websites, NOS will launch automatically and start scanning the user's system for malware. If a malware is detected, Real-Time Malware Monitoring will show an alert message as below.

Click 'Repair All' to repair the malwares.

nProtect Online Security						
	Real-time Malware Monitoring					
A suspicious malware is detected.						
Repair	Malware Name	Program Path				
✓	✓ Trojan/W32.Agent.12656 C:₩Users₩test₩Desktop₩s					
✓	Trojan/W32.Agent.12656	C:₩Users₩test₩AppData₩Roa				
	~	Repair All Repair Selected				

[Image 4-4] Repair All

To repair the malwares selectively, please select a specific malware name in the list and click 'Repair Selected'.

To change the Repair status, click the check mark (✓) in the Repair list and select 'Ignore' or 'Repair'.

Repair	Malware Na	me	Program Path	
O Trojan/W32.Ag		. Agent. 1265664.BA	C:\Users\test\Desktop\sha	
 Image: A second s	. Bonoir	Agent. 1265664.BA	C:\Users\test\AppData\Rc	
0	✓ nepair	V32.ZBot.93736.B	C:\Users\test\Desktop\sha	
	— Ignore			

[Image 4-5] Change Repair Status

If the 'Enable Auto-Repair' is checked, detected malwares will be repaired automatically without additional consent from the user.

To see the results of Auto-Repair, please check 'Show message after completing Auto-Repair'.

If a malware is repaired by Auto-Repair, the results will be shown as below.

In Protect Online Security					
Real-time Malware Monitoring ? Help					
Protect user's system from financial malwares.					
Detection Name : Trojan/W32.Agent.1265664.BA File Path : C:\Users\test\AppData\Roaming\windows.exe Result : Repaired					
05-Jun-2012 14:43:16 << < 1/2 >>> Do not show this message again.					

[Image 4-6] Auto-Repair Message

The user can choose to not show this message by checking 'Do not show this message again'.

4.2. Network Protection

4.2.1. Automatic Process Authentication

Network Protection allows or blocks network access based on policies. The default setting for Network Protection is ON. To disable the Network Protection function, move the slide bar to OFF.

Network Protection Monitors and blocks network intrusions		
Malware Monitoring Network Protection Keystroke & Screen Log		
Network Protection		
OFF Allow or block network activities based on policies	S	
Permit Program Check Hash Program Path		
	Þ	
i Details + Add to List - R	emove from List	
Monitor Windows default programs		

[Image 4-7] Network Protection ON/OFF

When Network Protection is enabled, all applications that access the network will be detected automatically as in **[Image 4-8]**. The user can choose to allow or block by clicking 'Allow' or 'Block'.

nProtect Online Security						
Network Protection Image: Constraint of the second se	Help					
Do you want to allow the network connection of below program?						
FacebookMessenger.exe Facebook Messenger						
Direction : IN -> OUT Protocol : TCP Connection Local Port : 51899						
Details						
O Allow 🔀 Blo	ock					

[Image 4-8] Process Authentication

<NOTE>

Windows default programs and trusted applications signed by 3rd party authorities(ex.Verisign) will not be blocked by Network Protection to enhance usability.

By clicking 'Allow' button in the above message box, the status of Permit will be displayed as " • .

Permit	Program	Check Hash	Program Path			
0	Smart NAC Patch Client	×	C:\Windows\Wsystem32\WSNPAge			
•	Smart NAC PClient	×	C:₩Windows₩system32₩AuthSer			
•	4 III II III					

[Image 4-9] 'Allow' network access of programs

By clicking 'Block' button in the above message box, the status of Permit will be displayed as "X".

	Permit	Program	Check Hash	Program Path
	X Smart NAC Patch Client		×	C:₩Windows₩system32₩SNPAge
	×	Smart NAC PClient	×	C:₩Windows₩system32₩AuthSer
•				

[Image 4-10] 'Block' network access of programs

To change the option of 'Permit' directly from the main UI, click " " or " " ifrom the list and a small menu will be displayed as below.

Permit Program	Check Hash	Program Path
× Smart NAC Patch Client	×	C:\Windows\%system32\%SNPAge
Allow Block	×	C:₩Windows₩system32₩AuthSe
•		•

[Image 4-11] Change of Process Authentication

To ensure whether an application is genuine or not, 'Check Hash' function can be used. Click " \checkmark " or " \times " to change the status as below.

Permit	Program		Check Hash	Program Pa	Program Path	
0	Smart NAC Patch Client		✓ C:₩		₩indows₩system32₩SNPAge	
0	Smart NAC PClient		× × ×	Enable Disable	s₩system32₩AuthSer	
•		111			•	

[Image 4-12] Change of the Check Hash

4.2.2. Manual Process Authentication

To manually add programs to the allowed list('White list"), click 'Add to List' button.

Permit	Program		Check Hash	Program Path
0	Smart NAC Patch Client		×	C:\Windows\%system32\%SNPAge
×	Gorealra3.0		×	C:₩Program Files₩SBS₩Gorealra3
0	Smart NAC PClient		×	C:₩Windows₩system32₩AuthSer
•				4
		Details	🕂 Add	to List — Remove from List
Mo	nitor Windows default programs			

[Image 4-13] Add to List

When a file explorer window is shown as below, select a program and click 'Open' to add to the White list.

🛜 Open						×
Look in:	952		•	G 🤌 🖡	🤊 🎹 -	
	Name 🔺		- Date	modified	- Type	
2	😵 g2mchat		5/21	/2012 10:43.	Application	
Recent Places	😵 g2mcomm		5/21	/2012 10:43.	Application	
	g2mfeedback		5/21	/2012 10:43.	Application	
	😵 g2mhost		5/21	/2012 10:43.	Application	
Desktop	G2MInstaller		5/21	/2012 10:43.	Application	
	G2MInstHigh		5/21	/2012 10:43.	Application	
	g2mlauncher		5/21	/2012 10:43.	Application	
Libraries	g2mmatchma	king	5/21	/2012 10:43.	Application	
	😵 g2mmaterials		5/21	/2012 10:43.	Application	
	😵 g2mpolling		5/21	/2012 10:43.	Application	
Computer	😵 g2mQandA		5/21	/2012 10:43.	Application	
- Computer	😵 g2mrecorder		5/21	/2012 10:43.	Application	
	g2msessionco	ntrol	5/21	/2012 10:43.	Application	
Network	😵 g2mstart		5/21	/2012 10:43.	Application	
INCLINOIR	Ra2mtestina		5/21	/2012 10:43.		_
	•					
	File name:	g2mlauncher		-	- 0	pen
	Files of type:	Window Application			• Ca	ancel

[Image 4-14] Select Application

To remove a program from the list, select the name of the program and click 'Remove from List' button and then click 'Apply'.

4.2.3. Windows Default Programs Monitoring

If the checkbox for 'Monitor Windows default programs' is checked, Network Protection will also check basic programs such as Internet Explorer or Outlook.

	Details	🕂 Add to List	- Remove from List
🖌 Monitor Windows default programs			

[Image 4-15] Enable to monitor Windows default programs

4.2.4. Anti-Code Injection

Zeus is a Trojan that steals banking information by injecting malicious thread into a running process. Periodically, the injected thread will send stolen personal data through the Internet to the hacker's server. nProtect Online Security provides an Anti-Code Injection(ACI) function under Network Protection. If any suspicious threads are detected by Anti-Code Injection, a warning message is shown as below. By clicking OK, the suspicious thread will be blocked from using the network.

C nProtect Online Security
Anti-Code Injection ? Help
ACI detected a suspicious thread.
A malicious thread has been detected. Will you block it?
05-Jun-2012 11:30:34 << < 1/1 > >>
🗸 ок

[Image 4-16] Anti-Code Injection

4.3. Keystroke Protection

Keystroke Protection protects user keystrokes from keyloggers. The default setting for Keystroke Protection is ON. To disable Keystroke Protection function, move the slide bar to OFF.

Image: Image	×
Keystroke & Screen Protection Protects personal information from keylogging and screen capture	
Malware Monitoring Network Protection Keystroke & Screen Log	
Keystroke Protection	
OFF Protects Keyboard Stroke(ID/Password/Typing Contents)	
Anti-Screen Capture	
ON OFF Blocks screen capturing and recording.	
	_
ОК	Apply

[Image 4-18] Keystroke Protection & Anti-Screen Capture Setting

When a keylogger(i.e. Bus Hound) attempting to steal user's keyboard input data in the kernel/driver level is detected in the system, Keystroke Protection will block all keyboard input.



[Image 4-19] Keystroke Protection Alert Message

4.4. Anti-Screen Capture

Anti-Screen Capture blocks all screen capture attempts while user is visiting a trusted website(bank.nProtect.com). The default setting for Anti-Screen Capture is ON. To disable Anti-Screen Capture function, move the slide bar to OFF.[Image 4-18]

4.4.1. Screen Capture by PrintScreen Key

Attempts to capture the screen with keyboard printscreen function will be blocked by Anti-Screen Capture. Captured screen image will be shown as an altenative nProtect image as shown below.



[Image 4-20] Protected image

4.4.2. Screen Capture by Screen Capturing Tools

Attempt to use screen capturing tools such as Easy Capture, ScreenshotCaptor, Gadwin PrintScreen, and other free tools to capture the screen will be blocked by Anti-Screen Capture. Captured screen image will be shown as an altenative nProtect image.

4.5. DNS Monitoring

DNS Monitoring prevents DNS hijacking and DNS changer by matching the Name Resolution with URL-IP records. To enable this function, customers need to provide the URL-IP information to nProtect first.

If the URL address and IP match, DNS Monitoring shows a "SAFE" message in green color as shown in the mini UI below.



[Image 4-21] DNS Monitoring status - SAFE

If the URL address and IP does not match, DNS Monitoring show a "WARNING" message in red color as shown in the mini UI below.



[Image 4-22] DNS Monitoring status - WARNING

4.6. Log

All NOS event logs can be seen on this tab.

nProtect Online	e Security					
Log Check n	Protect Online Secu	rity Log(s)				
Malware Monitoring	Network Protec	tion Key	stroke & Screen	Log		
Log (Maximum 1,0	00 logs)					
✓ Malware Monitoring	Network Pro	otection 🔽	User Information Pro	ti 📝 Event Log		
Date/Time	Type	Status	Description			Ľ
29-Apr-2013 - 13:14:52	Network Protect	Allow	C:\Windows\system3	32\SNPAgent.exe		
29-Apr-2013 - 13:14:29	Network Protect	Allow	C:\Windows\SysWOW64\AuthService.exe			
29-Apr-2013 - 13:13:06	Network Protect	Allow	C:\Windows\System32\sychost.exe			
29-Apr-2013 - 13:11:59	Network Protect	Allow	C:\Program Files (x86)\Common Files\Apple\Mobil		Mobil	
29-Apr-2013 - 13:11:38	Keystroke Screen	Anti-Screen	Anti-Screen capture has been stopped.			
29-Apr-2013 - 13:11:18	Keystroke Screen	Anti-Code I	Anti-Code Injection has been activated.			
29-Apr-2013 - 13:11:18	Anti-Screen Cap	Block	Received VK_SNAPSHOT event, launched EmptyC			
29-Apr-2013 - 13:11:17	Network Protect	DNS Monitor	DNS Monitoring has been started.			
29-Apr-2013 - 13:11:17	DNS Monitoring	Safe	yahoo		•	
			Oł	(Apply	

[Image 4-23] nProtect Online Security Log

To view the log according to each event, check or uncheck the checkboxes.

5. Problem Solving

5.1. How to Collect Logs

For any program errors or update failures, please send the log files to support@nprotect.com.

The log files of nProtect Online Security can be collected from the following paths:

- C:\Windows\System32\config\systemprofile\AppData\LocalLow\nProtect\Log
- C:\Users\[User Name]\AppData\LocalLow\nProtect\Log

🎍 Log			
GO⊽ 🌗 System 32₩config₩system	mprofile\#AppData\#LocalLow\#nProtect\#Log	Search Log	2
Organize 🔻 Include in library 🔻 Sha	re with 🔻 Burn New folder		:= 🕶 🔟 🔞
★ Favorites	Name ^	Date modified	Туре
🧾 Desktop	npen60.npe.npo	6/7/2012 1:07 AM	NPO File
Downloads	npen60.npe_bak.npo	6/5/2012 1:06 AM	NPO File
Recent Places	npestarter60.npe.npo	6/7/2012 7:01 PM	NPO File
Deskton	npestarter60.npe.npo_Dec.log	5/23/2012 9:34 PM	Text Document
	npestarter60.npe_bak.npo	6/7/2012 5:02 PM	NPO File
📕 test	inpesvc60.exe.npo	6/7/2012 6:15 PM	NPO File
🍌 AppData	npesvc60.exe.npo_Dec.log	5/23/2012 9:34 PM	Text Document
Application Data	npesvc60.exe_bak.npo	5/16/2012 5:35 PM	NPO File
E Contacts	npupdate.exe.log	6/7/2012 6:15 PM	Text Document
Cookies	npupdate.exe_bak.log	5/10/2012 5:20 AM	Text Document
	npupdate.log	6/7/2012 6:15 PM	Text Document
Pavorites	npupdate_bak.log	3/7/2012 4:05 PM	Text Document
🙀 Links			
👌 Local Settings 🗨 👻			F

[Image 6-1] C:\Windows\System32\config\systemprofile\AppData\LocalLow\nProtect\Log

🎴 Log					
🕤 🖓 🖓 🚺 C:\Users\Utest\App	Data	₩LocalLow₩nProtect₩Log	💌 🛃 Search	Log	2
Organize 🔻 Include in library 👻	Share	e with 🔻 Burn New folder			• 🔳 🔞
〕 Downloads		Name *		Date modified	Туре
🔄 Recent Places		20120524aps.npo		5/24/2012 1:14 AM	NPO File
E Desktop		firefox.exe.npo		6/3/2012 9:51 PM	NPO File
词 Libraries		iexplore.exe.npo		6/7/2012 6:50 PM	NPO File
🥦 test		npenUninstall5.exe.log		6/5/2012 1:01 AM	Text Docume
🍌 AppData		npesvc60.exe.npo		6/5/2012 1:03 AM	NPO File
Application Data		npeuseractor60.npe.npo		6/7/2012 1:06 AM	NPO File
tontacts					
📄 Cookies					
膧 Desktop					
🚺 Downloads					
Favorites	-	•			•

[Image 6-2] C:\Users\[User Name]\AppData\LocalLow\nProtect\Log

5.2. Customer Support

nProtect provides customer support for NOS users through website chat, email and telephone. For questions and technical support, please contact:

1) Website Chat

• http://www.nprotect.com

2) E-mail

- Business Inquiries: sales@nProtect.com
- Technical Support: support@nProtect.com

3) Telephone

- Office: 408-477-1742
- Toll Free: 855-466-7768 (1-855-GO-NPROT)