Casper: Invisible Windows Enumerator

SensePost Research

November 2004

Document Information

A project for:	**SensePost Research**
Project description:	**Casper: Invisible Windows Enumerator**
Partner:	**-**
Project completion date:	**2004/11/25**
Document number:	**CASPER_200411**
Issue:	**1.0 (Final)**
Last modified:	**2004-11-25**
Author:	**Haroon Meer**

SensePost Contact Details

Contact E-Mail Addresses

General:	info@sensepost.com	www.sensepost.com
Training:	training@sensepost.com	
Reseach:	research@sensepost.com	
HackRack:	info@hackrack.com	www.hackrack.com

Revision History

Document Version	Description	Date	Author
1.0	Final	2004/10/25	Haroon Meer

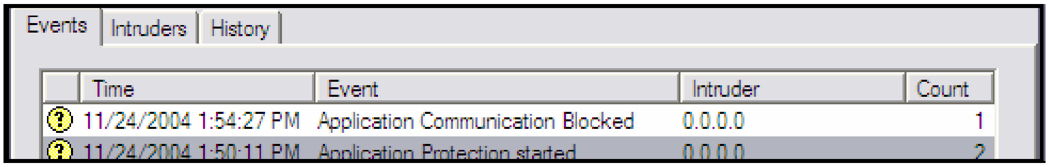
Table of Contents

1 Introduction

Early in 2002 SensePost revealed GATSLAG, a win32 Trojan that made use of (invisible) Internet Explorer sessions to tunnel information in and out of target networks. An amped up version called SETIRI was demonstrated at BlackHat Vegas 2002. While sizable snippets of Setiri code were given to anti-virus researchers in order to possibly detect Setiri derivatives, none of the personal firewall vendors (including Microsoft) appear to have clamped down on the actual problem. This (short!) paper and accompanying tool provides a simple antidote (or at least a recipe for one) to a problem that made lots of people write to us with tales of sleepless nights.

2 Setiri

Setiri made the headlines in 2002 when we demonstrated it at BlackHat / DefCon. Like most headlines on security / tech-related issues, some of the responses made us cringe and were blown a little out of proportion. However, the presentation definitely highlighted the existence of a serious potential problem. To combat the ever growing threat of call-home Trojans, most personal firewall vendors started adding “application white-lists”. The solution was simple and effectively cut down on the garden variety spy-ware / Trojans that tried to connect to a host / controller on the Internet.

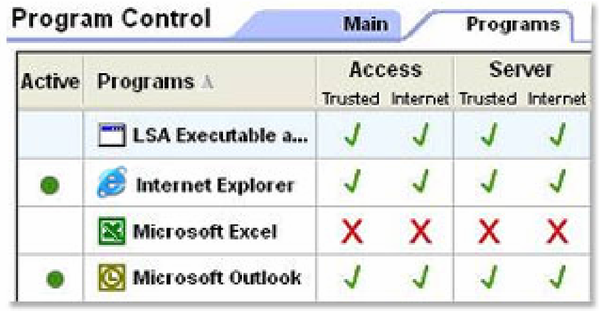


	Time	Event	Intruder	Count
?	11/24/2004 1:54:27 PM	Application Communication Blocked	0.0.0.0	1
?	11/24/2004 1:50:11 PM	Application Protection started	0.0.0.0	2

(Communication outbound blocked by default!)

The problems with this technique however, are immediately apparent:

1. Not all personal firewalls support it. (Microsoft’s built in firewall still makes no attempt to limit outgoing communication
2. The end user was now given an alert with a “Do you want to permit “XXX” to connect to the Internet” message, allowing Trojans with friendly names (or obscure ones) to sail through on user naivety.
3. Malware could now tunnel through these protection mechanisms by co-opting permitted applications to act as a communications broker.



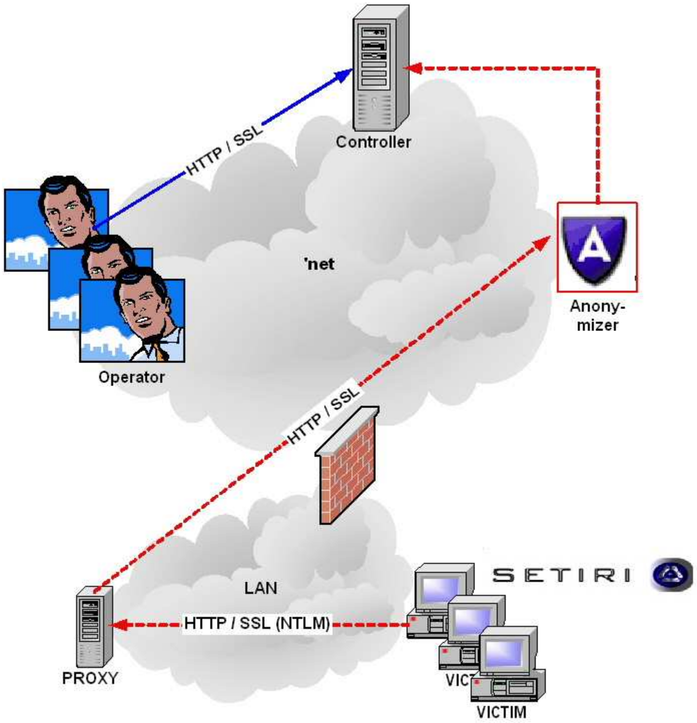
Active	Programs	Access		Server	
		Trusted	Internet	Trusted	Internet
	LSA Executable a...	✓	✓	✓	✓
●	Internet Explorer	✓	✓	✓	✓
	Microsoft Excel	✗	✗	✗	✗
●	Microsoft Outlook	✓	✓	✓	✓

(Internet Explorer allowed to browse the Internet)

Enter Setiri…

Without going into too much of Setiri's details (which is available from http://www.blackhat.com/ or http://www.sensepost.com/garage_portal.html), Setiri makes use of OLE automation to tunnel data through HTTP POST's.

This also buys the Trojan a great deal in terms of authentication. It is not uncommon these days to find users on internal networks being able to browse the Internet only once they have authenticated to an internal proxy server. Setiri therefore leverages the fact that the browser is both authenticated on the Proxy server and permitted through the host's personal firewall. Setiri also connected through anonymizer / anonymous proxies to add some measure of protection for the Trojan controller.



(Setiri overview)

3 Protection and Defense

To date most of the protection against Setiri-type Trojans have resided at the policy level aimed at preventing the compromise / preventing the Trojan from ever getting a foothold on your machine. This is an admirable goal since everyone knows “if a bad guy can run code on your machine, its not your machine anymore”, but falls horribly short when you consider the number of attack vectors open to attackers today.

Ed Skoudis (http://www.counterhack.com) in his chapter on Setiri (Malware – Fighting Malicious Code : ISBN 0131014056) recommends the following :

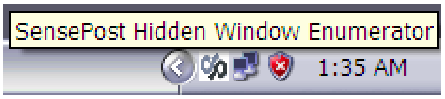
- Block access to sites like anonymizer
  - (He also mentions the futility of this)
- Keep an updated anti-virus signature database
  - (Invisible windows are so common place these days that the invisible Internet Explorer commands alone will generate far too many false positives if flagged as a possible Trojan snippet)
- Get the vendor to fix IE/Windows
  - (No comment!)

Most security officers also advise “safe surfing”, with the usual mantras of “Do not run un-trusted code” and “Do not double click that attachment” high up on their lists. Unfortunately with the mini-OS’s that are web browsers today, one could end up executing code by simply surfing to a carefully crafted JPEG. (http://www.microsoft.com/security/bulletins/200409_jpeg.mspx). It would not be difficult for an exploit to inject Setiri-like functionality into a running process, effectively calling-home to the attacker whilst whistling past the inline protection mechanisms.

Over the past 2 years very little has been done to combat the threat and while reports of this technique have surfaced in the wild, even more use has been made recently of “invisible window” functionality… digging the hole just a little bit deeper.

4 Introducing Casper (aka a few lines of ugly C#)

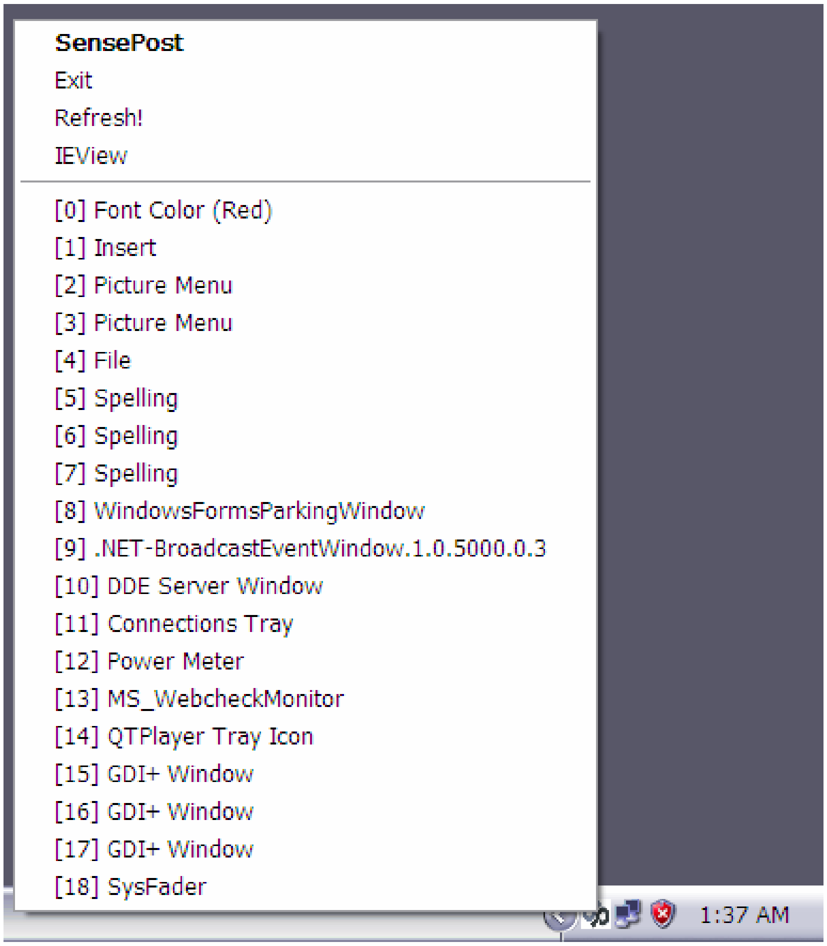
Casper is a tiny system tray application that can be used to view the invisible windows on your desktop.



Casper simply makes use of the following functions exposed through user32.dll

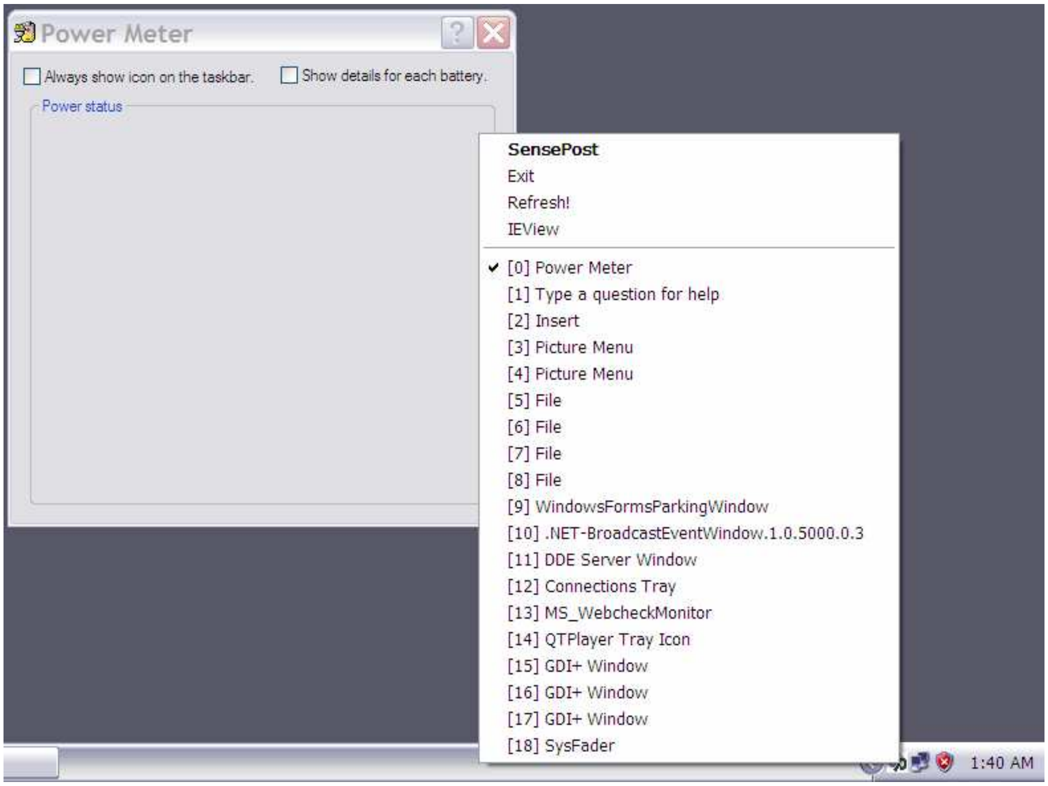
- `GetWindowText(int hWnd, StringBuilder title, int size)`
- `EnumWindows(EnumWindowsProc ewp, int lParam)`
- `IsWindowVisible(int hWnd)`
- `ShowWindowAsync(IntPtr hWnd, int nCmdShow)`

In its default mode Casper sits quietly on the taskbar doing very little. Right-clicking on Casper will raise the list of invisible windows currently available on the user's desktop.



(Casper + Invisible Windows)

Simply clicking on an entry in the context menu will make the selected window visible (and un-selecting it will return the window to its previous state).



(Power Meter Visible'ised)

While this does give us at least a few minutes of pointless fun (you know what they say about small things amusing small minds), we move on instead to the button labelled IEView.

Enabling this button, which is again disabled by de-selecting it, prompts Casper to make visible any instance of an invisible Internet Explorer.

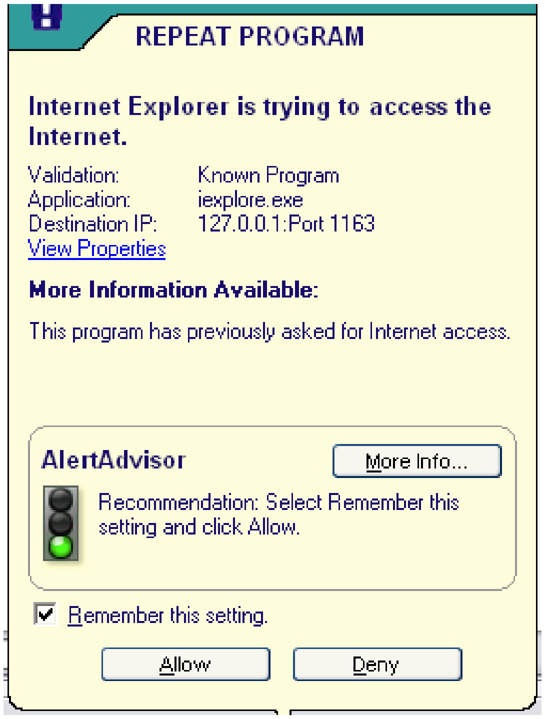
Casper implements this crudely by examining the desktop every 10 seconds looking for invisible browser instances.

5 The Bottom Line?

Casper, while possibly cute and mildly entertaining is not the right place for IEView functionality. This process is however one that would be incredibly valuable at the personal firewall / host IDS level. Most of these tools inspect outgoing services already and should now include an additional check for window visibility (possibly through the exposed user32.dll functionality mentioned earlier).

The bottom line is that a web browser is not the same as an invisible web browser. Personal firewalls and products providing similar functionality should start making this distinction. It could effectively change the alert messages from [A] to [B]:

Current Alert



REPEAT PROGRAM

Internet Explorer is trying to access the Internet.

Validation: Known Program
Application: iexplore.exe
Destination IP: 127.0.0.1:Port 1163
View Properties

More Information Available:

This program has previously asked for Internet access.

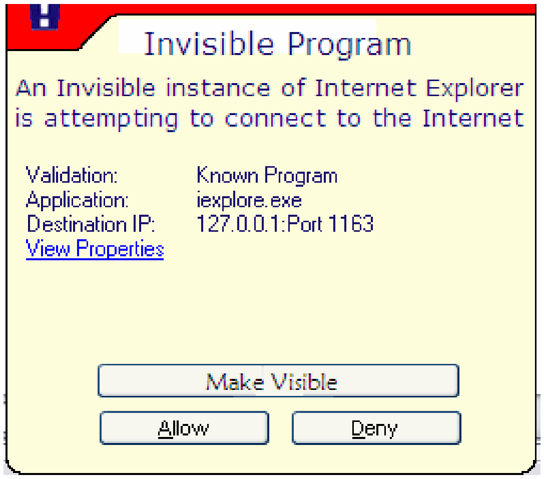
AlertAdvisor

Recommendation: Select Remember this setting and click Allow.

☑ Remember this setting.

[A]

(Fictional) Proposed Alert



Invisible Program

An Invisible instance of Internet Explorer is attempting to connect to the Internet

Validation: Known Program
Application: iexplore.exe
Destination IP: 127.0.0.1:Port 1163
View Properties

[B]

6 Conclusion

SensePost is releasing Casper as is, without any warrantees, guarantees… or even batteries included. The full source is available under the BSD licence to encourage people, especially personal firewall vendors, to use it as they wish.

We seriously hope that it will:

- Go a fair way towards mitigating the threat
- Cut down the number of requests we get every week for Setiri

-o0o-