security-assessment.com

Rage Against The Kiosk

BruCON 2009 – Belgium

Member of Datacraft Asia

Who The Heck Am I?

- **Paul Craig**
  - Principal Security Consultant – Security-Assessment.com
  - Based in New Zealand
  - I lead the Security-Assessment.com penetration testing teams.

  - Avid hacker and technology enthusiast.

- **Contact Me?**
  - paul@ha.cked.net
  - http://ha.cked.net

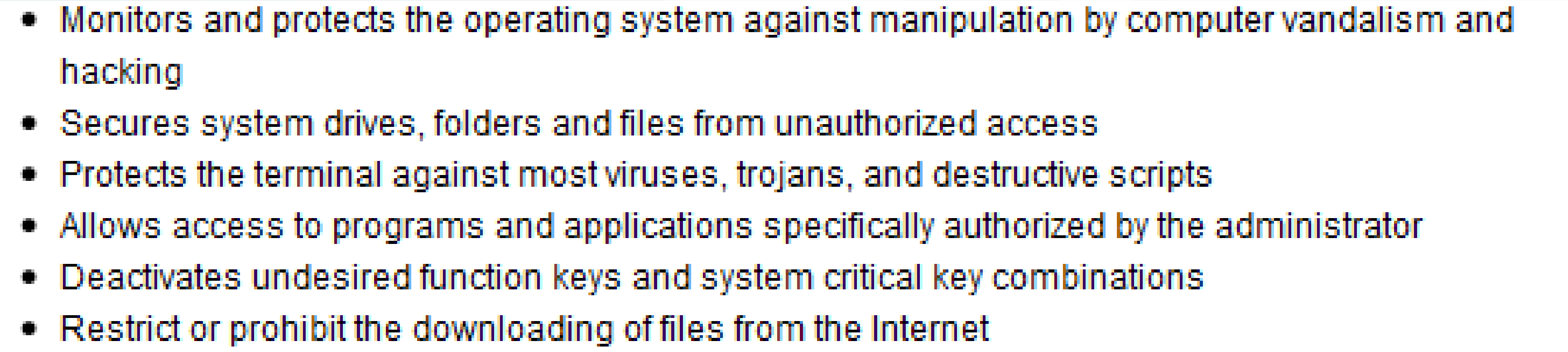
Agenda

- **Background**
  - My affair with Kiosks
- **Hacking Kiosks**
  - Objectives of Kiosk hacking.
  - How we do it.
  - What about Linux Kiosks?
- **Kiosk Hacking Demos**
  - Popping shells on the most popular Kiosks.
  - 5 Kiosks, as many shells as possible.

Kiosks, iKAT and Me

- **My affair with Kiosks began two years ago.**
  - “Damn those Airport Internet Kiosks are popular”
  - “Bet I could hack that….”
  - “Armed Asian police probably wouldn't like that”
- **16 months of hacking VM Kiosks at home later.**
  - Found common weaknesses in all Kiosk products.
  - Turns out, you can hack every internet Kiosk!
  - Its not even that hard.
  - 100% hackable.

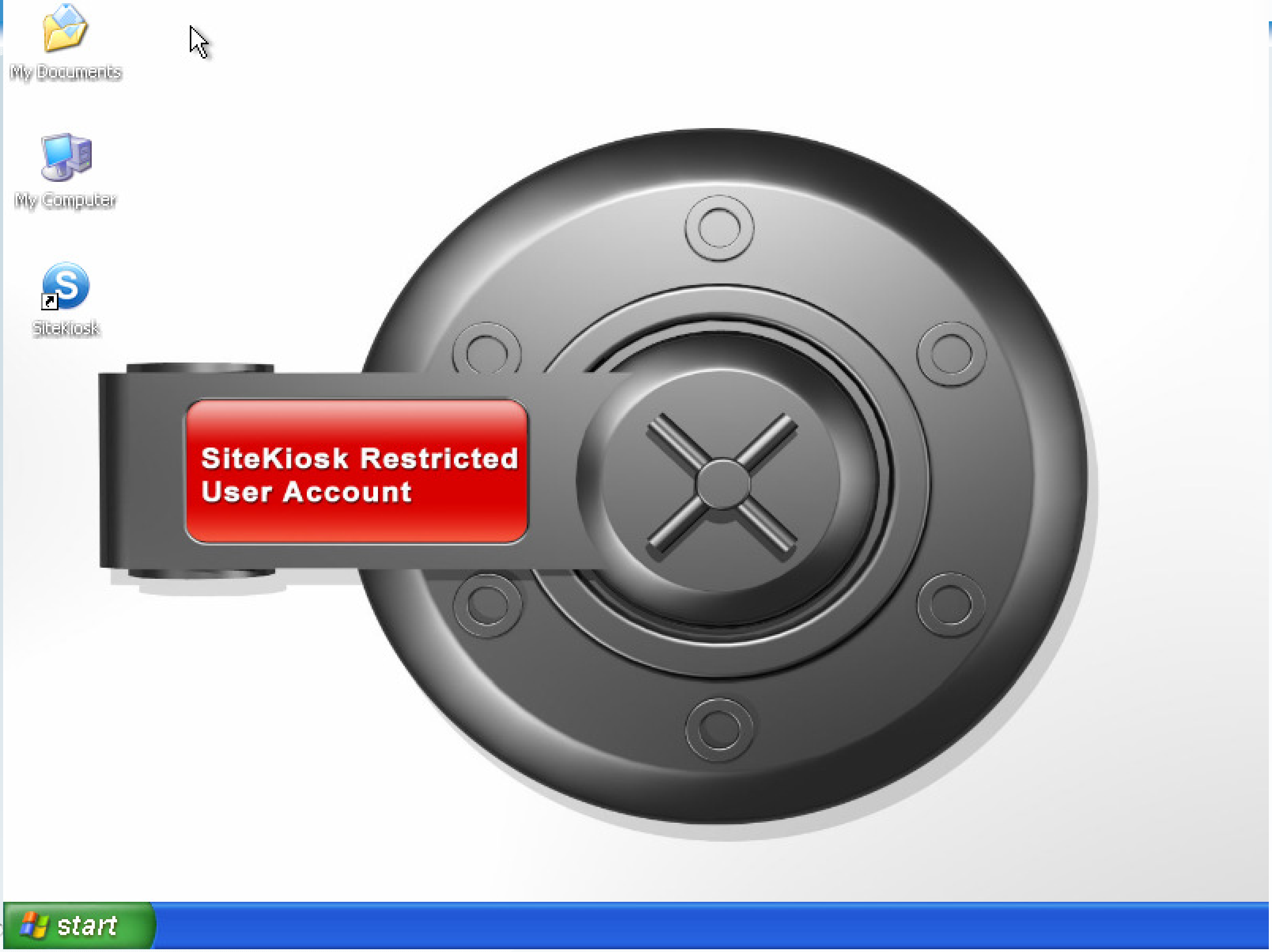
- **Kiosk vendors try to implement security features.**
  - Vendor websites tout security features.



- Monitors and protects the operating system against manipulation by computer vandalism and hacking
- Secures system drives, folders and files from unauthorized access
- Protects the terminal against most viruses, trojans, and destructive scripts
- Allows access to programs and applications specifically authorized by the administrator
- Deactivates undesired function keys and system critical key combinations
- Restrict or prohibit the downloading of files from the Internet

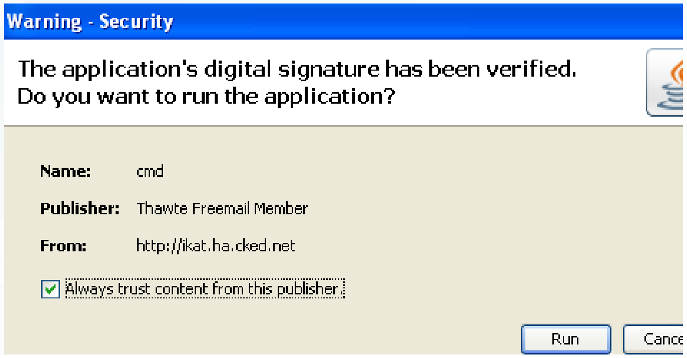
  - Security is also a functional requirement, and taken seriously.
  - Its also a selling point, “secure” Kiosks are not cheap kiosks.

- **Kiosks are designed with two types of security.**
  - User Interface Security
    - Graphically jailed into a Kiosk interface.
    - Cut-down/reduced functionality desktop.
    - Custom “Start” bar, full screen Kiosk application.
    - No way to get back to “Windows” or run explorer, cmd.exe
  - Activity Blacklist
    - Everything you do is monitored, unlawful activity is prohibited.
      - “Access to C:\ has been denied!”
    - Configurable blacklists set to monitor:
      - Windows/Buttons you click.
      - Processes running.
      - API’s being used.



My Documents
My Computer
SiteKiosk
SiteKiosk Restricted User Account
start

- I found three core security issues with all Kiosk vendors.
  - Blacklists don’t work.
    - 100 different ways to do anything on any OS!
    - A Kiosk blacklist must stop EVERY method, they don’t.
  - Websites visited from the Kiosk are not factored into the security model.
    - Kiosk rely on default browser security policy when dealing with remote sites.
    - This policy was not designed for a Kiosk/public environment.
  - Underlying browser technology implements security by “User Interaction”
    - Browser will trust the Kiosk user.
    - “Are you sure you want to run this?”
    - Don’t trust what I say!



Warning - Security

The application's digital signature has been verified.
Do you want to run the application?

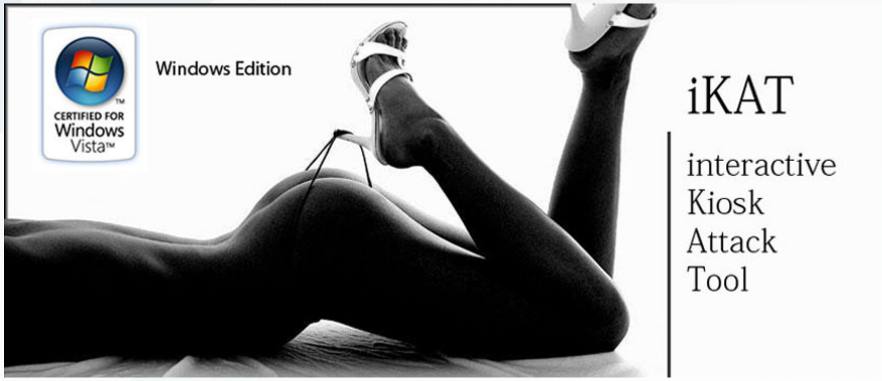
Name: cmd

Publisher: Thawte Freemail Member

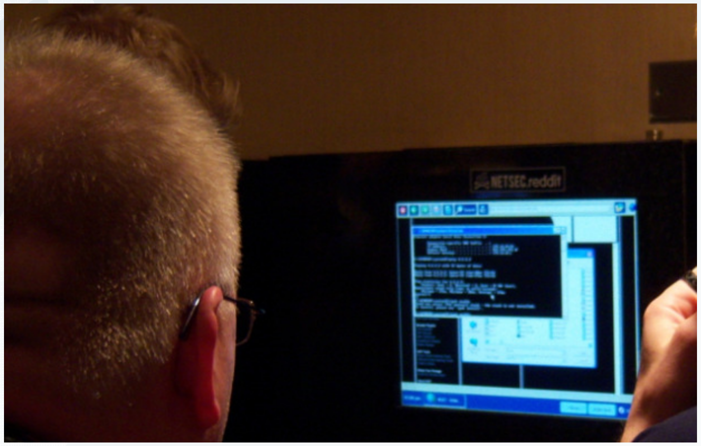
From: http://ikat.ha.cked.net

☑ Always trust content from this publisher.

- **My research was released in the form of a tool.**
  - Technically, its a website you visit from a Kiosk.
  - Interactive Kiosk Attack Tool - http://ikat.ha.cked.net
  - Exploits the three core Kiosk security weaknesses.
  - Designed to pop shell on a Kiosk as fast as possible.
  - Invaluable when auditing the security of a Kiosk.
  - Its also free to download, if you want your own version.
    - “iKAT Portable”



- **iKAT v1.0 launch 2008 – Defcon 16**
  - Kiosk research released at Defcon
  - I showed the world iKAT.
  - Rivera Kiosk hacked seconds after my talk!
  - 23 Las Vegas Strip Kiosks hacked.



  - iKAT popped shell anywhere in Vegas, in seconds.

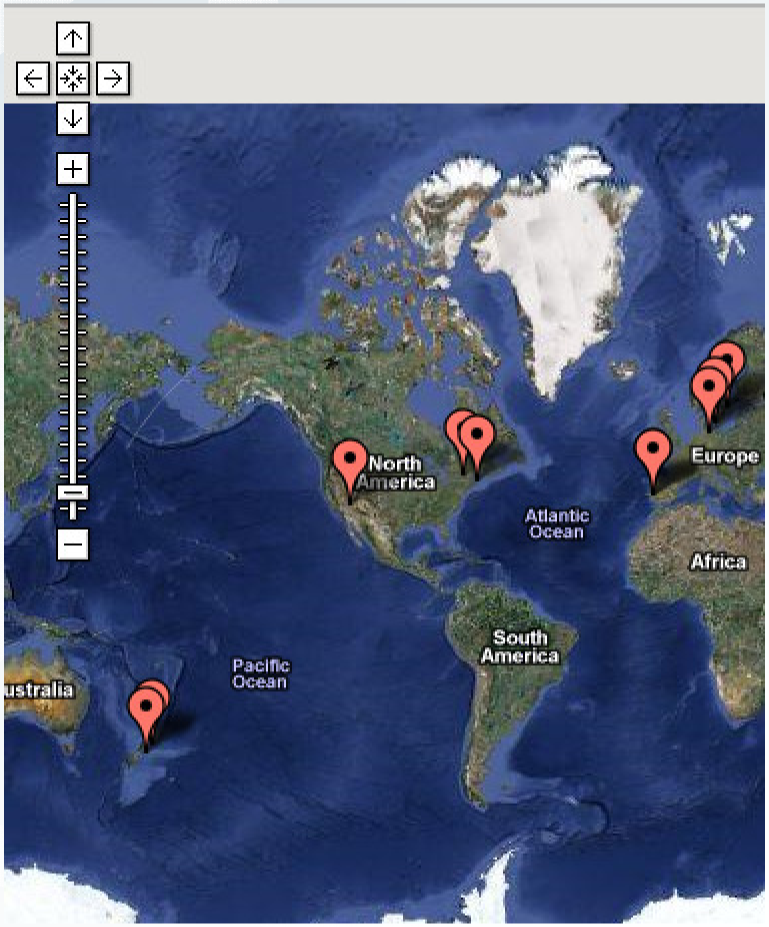
DEFCON 16

  - HTTP logs show iKAT is being used, a lot, everywhere in the world.
  - 4 Windows Kiosk vendors have extensively used iKAT
  - New versions of Kiosk software released, blocking the URL.

- **“Submit your hacked Kiosk”**
  - I wonder who would tell me what Kiosks they hacked with iKAT?
  - Purely voluntarily information.

- **Logs indicate Kiosks hacked at**

  Lots of Hotels, Motels, Train Stations, Libraries, Airports, Café’s, Malls, Universities, high schools, event centers.

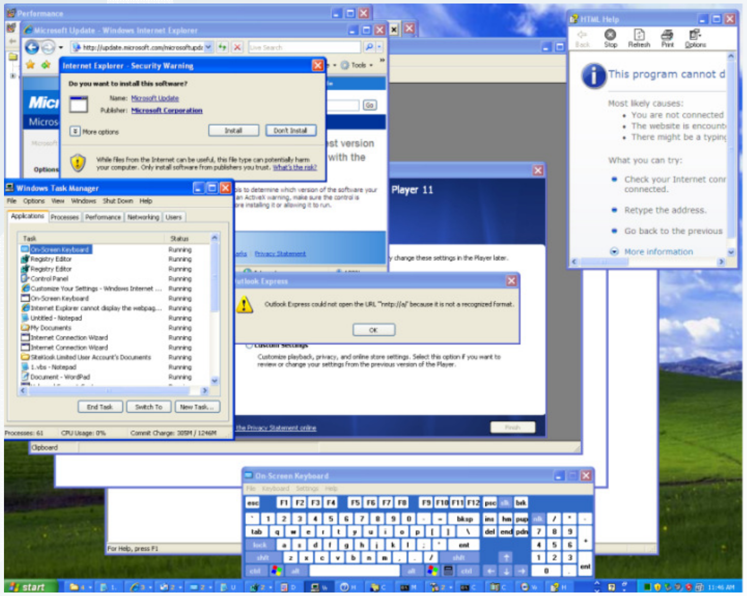


- **“Paul, why the f&!# do you want to hack Kiosks?”**
  - Industries that use Kiosk software.

    Cities
    Media
    Churches
    Vending Machines
    Welfare Services
    Museums
    Chemical & Medicine
    Transportation
    Tourism
    Sports
    Steel Industry
    Insurance
    Health Sector
    Banking/Financial Services
    Automobile
    Government Authorities
    Schools & Universities
    Retailers
    Air/Space Travel
    Energy/Oil
    Real Estate
    Food & Drink
    Consulting
    Electronics
    Accommodation
    Communication
    Military

  - NASA, Army, Navy, Calvary, Air Force, Government, Banks.
  - Kiosks may be connected to a desktop LAN environment.
  - Ideal network entry point.
  - **No one else seems to be hacking Kiosks.**

- **How iKAT Works:**
  - Employs everyday browser/client side technology.
    - ActiveX , Java Applets, ClickOnce .NET
    - JavaScript, VBScript, Flash
    - URI Handlers, File Types


Performance
Microsoft Update - Windows Internet Explorer
http://update.microsoft.com/microsoftupdt
Live Search
Tools
Internet Explorer - Security Warning
Install
Don't Install
More options
Windows Task Manager
File Options View Windows Shut Down Help
Applications Processes Performance Networking Users
End Task
Switch To
New Task...
Player 11
Outlook Express
OK
HTML Help
Back Stop Refresh Print Options
On Screen Keyboard
File Keyboard Settings Help
start

Do you want to install this software?

Name: Microsoft Update

Publisher: Microsoft Corporation

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Task | Status
On-Screen Keyboard | Running
Registry Editor | Running
Registry Editor | Running
Control Panel | Running
Customize Your Settings - Windows Internet ... | Running
On-Screen Keyboard | Running
Internet Explorer cannot display the webpag... | Running
Untitled - Notepad | Running
My Documents | Running
Internet Connection Wizard | Running
Internet Connection Wizard | Running
SiteKiosk Limited User Account's Documents | Running
1.vbs - Notepad | Running
Document - WordPad | Running

Processes: 61 CPU Usage: 0% Commit Charge: 305M / 1246M

Outlook Express could not open the URL "nntp://a/" because it is not a recognized format.

Customize playback, privacy, and online store settings. Select this option if you want to review or change your settings from the previous version of the Player.

This program cannot d

Most likely causes:
- You are not connected
- The website is encount
- There might be a typing

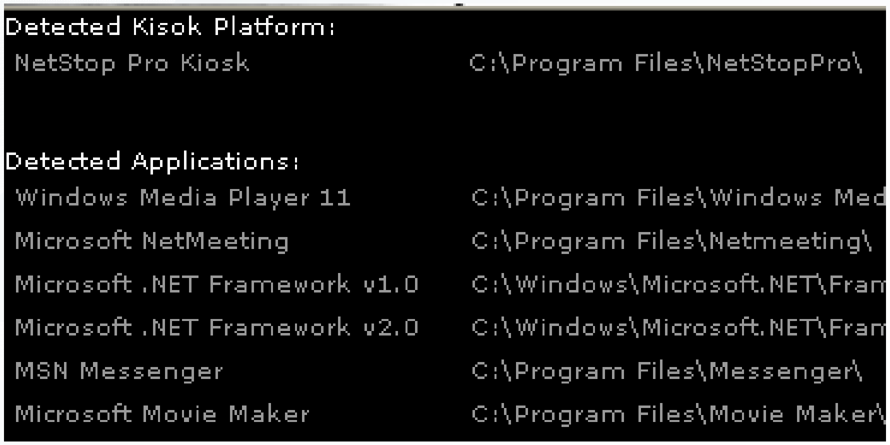
What you can try:
- Check your Internet conn connected.
- Retype the address.
- Go back to the previous

More information

For Help, press F1

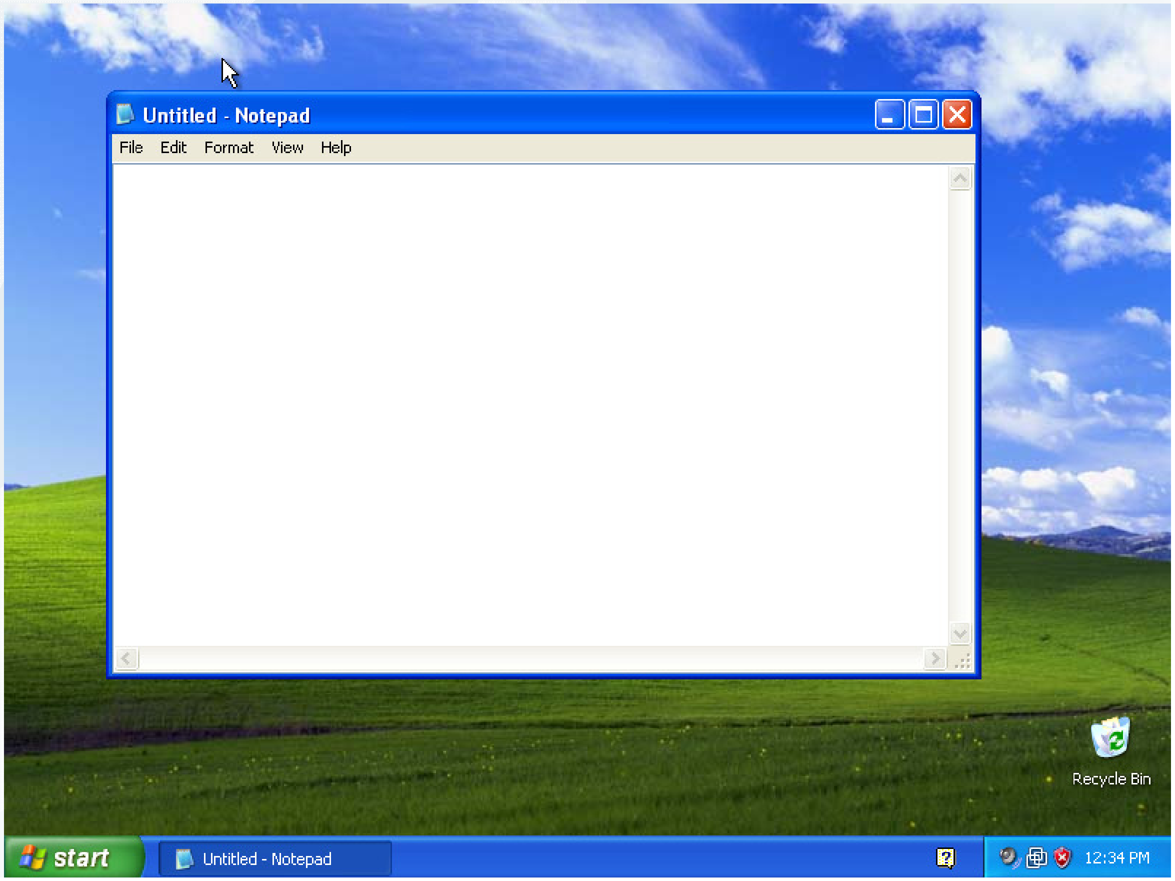
- **iKAT Tries To Make ‘Stuff Happen’**
  - Interact with the Kiosk!
  - Spawns processes!!
  - Working within the boundaries of the Internet Security Zone.
  - Provides an ‘escape path’ from a graphically jailed environment.
  - Reliably produces a shell.

- **Java, ActiveX, ClickOnce, WPF**
  - Capable of spawning local processes.
    - “Spawn Cmd.exe”
  - Only ActiveX requires administrative authority.
  - Most Kiosks will have either a Java runtime, or a .NET runtime installed.
  - Client side runtimes can be detected
  - If the runtime is installed, you win.



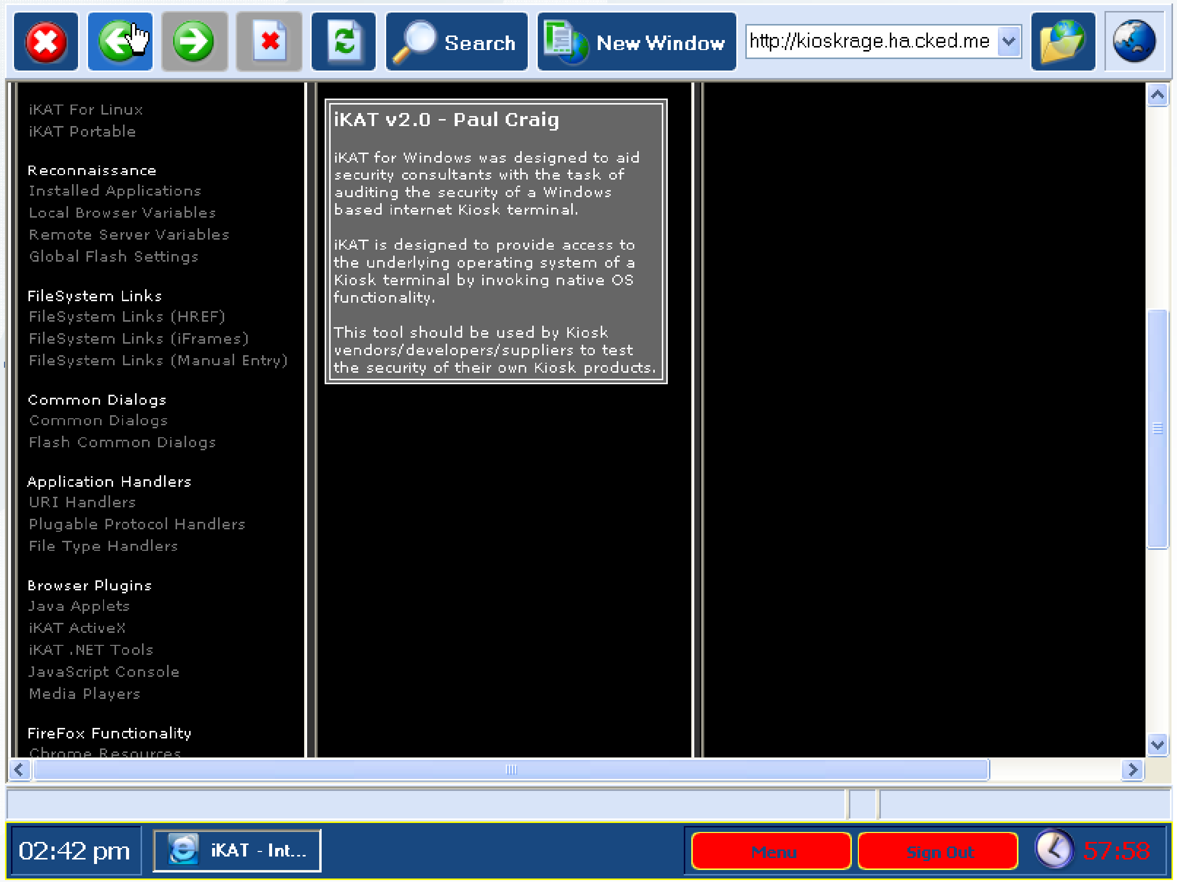
```
Detected Kisok Platform:
 NetStop Pro Kiosk                C:\Program Files\NetStopPro\


Detected Applications:
 Windows Media Player 11          C:\Program Files\Windows Med
 Microsoft NetMeeting             C:\Program Files\Netmeeting\
 Microsoft .NET Framework v1.0    C:\Windows\Microsoft.NET\Fram
 Microsoft .NET Framework v2.0    C:\Windows\Microsoft.NET\Fram
 MSN Messenger                    C:\Program Files\Messenger\
 Microsoft Movie Maker            C:\Program Files\Movie Maker\
```

- **I have discovered the full potential of notepad.**
  - Common dialogs run applications.
  - File Open/File Save = Explorer
  - File View control is Explorer
  - Notepad is a web browser!
    - Thanks to WebDAV
    - Download/Upload files
  - Remote URI's are supported.
    - http://, ftp://



- **Using file type handlers**
  - Kiosks may let you download certain file types.
  - iKAT ‘offers’ the Kiosk over 100 different files. “Automatic Execution”

- **Web enabled playlists**
  - iKAT.ASX (Playlist file)
  - WMP as a a web browser
  - In a lower security zone!
  - Allows cmd.exe to spawn



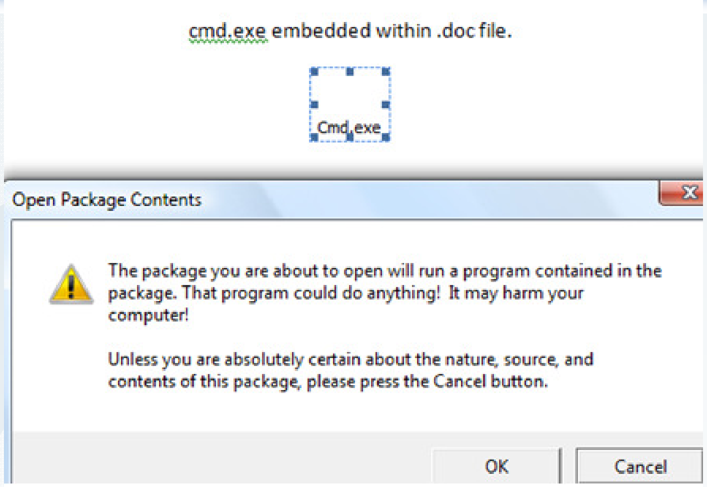
iKAT v2.0 - Paul Craig

iKAT for Windows was designed to aid security consultants with the task of auditing the security of a Windows based internet Kiosk terminal.

iKAT is designed to provide access to the underlying operating system of a Kiosk terminal by invoking native OS functionality.

This tool should be used by Kiosk vendors/developers/suppliers to test the security of their own Kiosk products.

- **Word documents – iKAT.docx**
  - Kiosk has Word installed? Word viewer?
  - Binary objects (cmd.exe) embedded within.
  - Click, Click, shell.

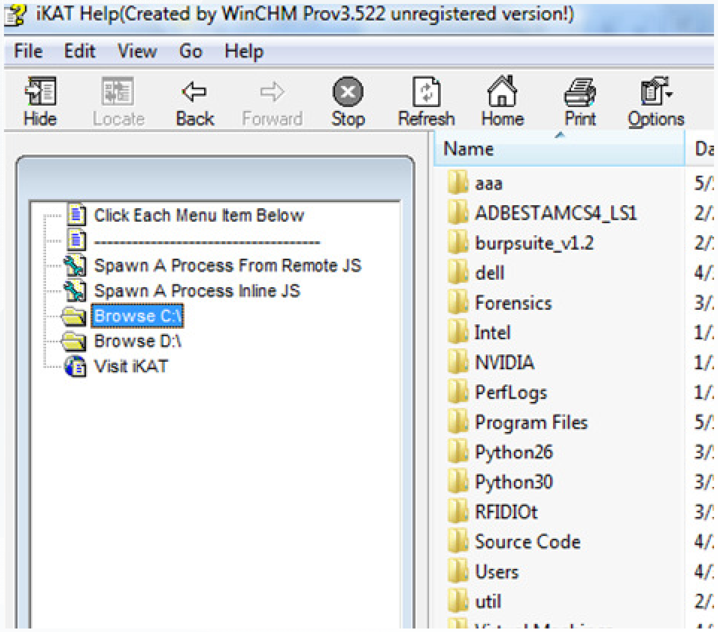


cmd.exe embedded within .doc file.

The package you are about to open will run a program contained in the package. That program could do anything! It may harm your computer!

Unless you are absolutely certain about the nature, source, and contents of this package, please press the Cancel button.

- **Help files – iKATHelp.chm**
  - Perhaps you can download help files?
    - iKAT help will spawn processes.
    - Browse the file system
    - Very helpful.



iKAT Help(Created by WinCHM Prov3.522 unregistered version!)

Click Each Menu Item Below

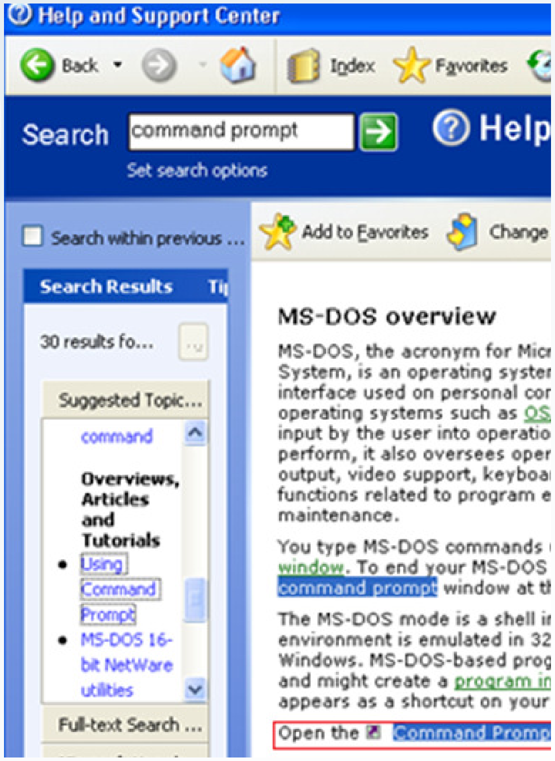
Spawn A Process From Remote JS
Spawn A Process Inline JS
Browse C:\
Browse D:\
Visit iKAT

aaa
ADBESTAMCS4_LS1
burpsuite_v1.2
dell
Forensics
Intel
NVIDIA
PerfLogs
Program Files
Python26
Python30
RFIDIOt
Source Code
Users
util

- **iKAT supports many more file type**
  - Over 100 different file types!

Using Protocol Handlers (URI Handlers)

- We can invoke URI handlers by clicking external handler links.
- mailto:// will spawn your default mail client.
  - Which may contain a common dialog.
- hcp:// will spawn the Windows help.
  - Search for ”Command Prompt”
  - “Click here to launch command prompt”
- mms:// will spawn Microsoft Media Player.
- Applescript:// will spawn the OSX AppleScript tool.
- iKAT automates URI handler invocation.



MS-DOS overview

MS-DOS, the acronym for Micr
System, is an operating syster
interface used on personal cor
operating systems such as OS
input by the user into operatio
perform, it also oversees oper
output, video support, keyboa
functions related to program e
maintenance.

You type MS-DOS commands
window. To end your MS-DOS
command prompt window at th

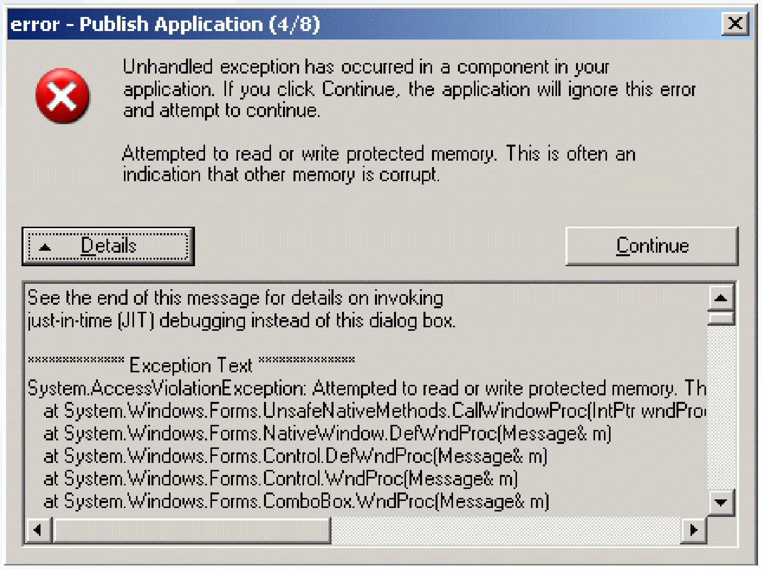
The MS-DOS mode is a shell ir
environment is emulated in 32
Windows. MS-DOS-based prog
and might create a program in
appears as a shortcut on your

Open the Command Promp

Unhandled Exceptions

- The fastest way to escape a Kiosk jail, is to just crash it!
- “Emo Kiosking”

- Create an unhandled exception in the browser, or any of its plug-ins.
- Who here has ever crashed a browser?
  - Flash, ActiveX
  - Java, JavaScript
  - PDF files
  - HTML Rendering
  - Malformed Images



Unhandled exception has occurred in a component in your application. If you click Continue, the application will ignore this error and attempt to continue.

Attempted to read or write protected memory. This is often an indication that other memory is corrupt.

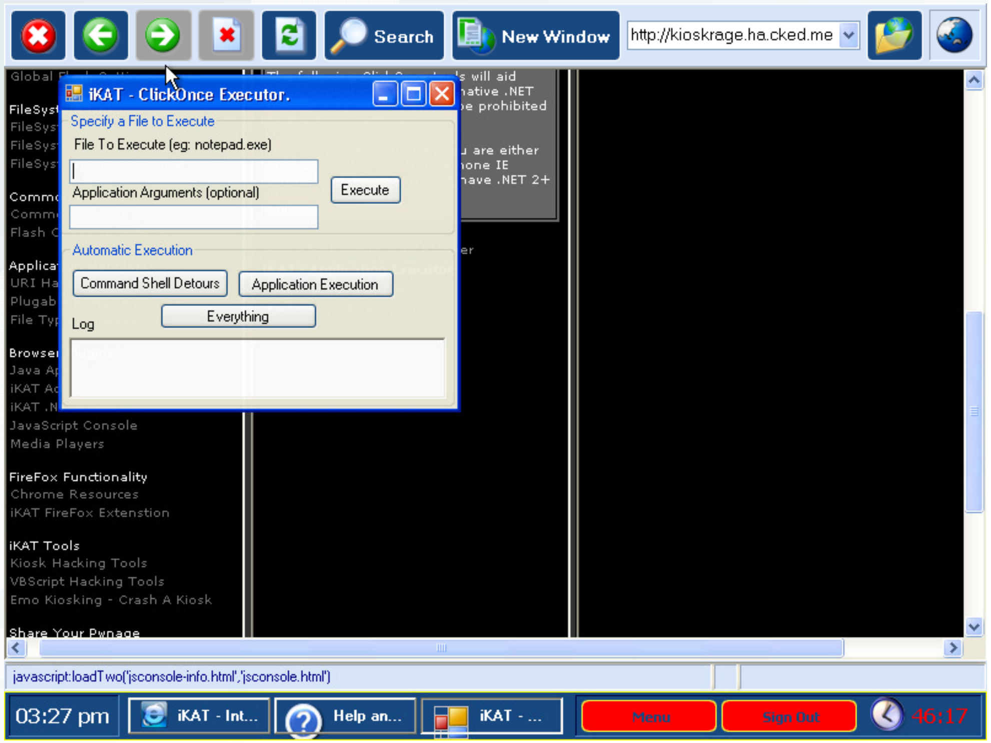
```
See the end of this message for details on invoking
just-in-time (JIT) debugging instead of this dialog box.

*************** Exception Text ***************
System.AccessViolationException: Attempted to read or write protected memory. Th
   at System.Windows.Forms.UnsafeNativeMethods.CallWindowProc(IntPtr wndPro
   at System.Windows.Forms.NativeWindow.DefWndProc(Message& m)
   at System.Windows.Forms.Control.DefWndProc(Message& m)
   at System.Windows.Forms.Control.WndProc(Message& m)
   at System.Windows.Forms.ComboBox.WndProc(Message& m)
```

- Crash the Kiosk, Kiosk freaks out, Windows desktop.
- Only some Kiosks monitor unhandled exceptions, many do not.

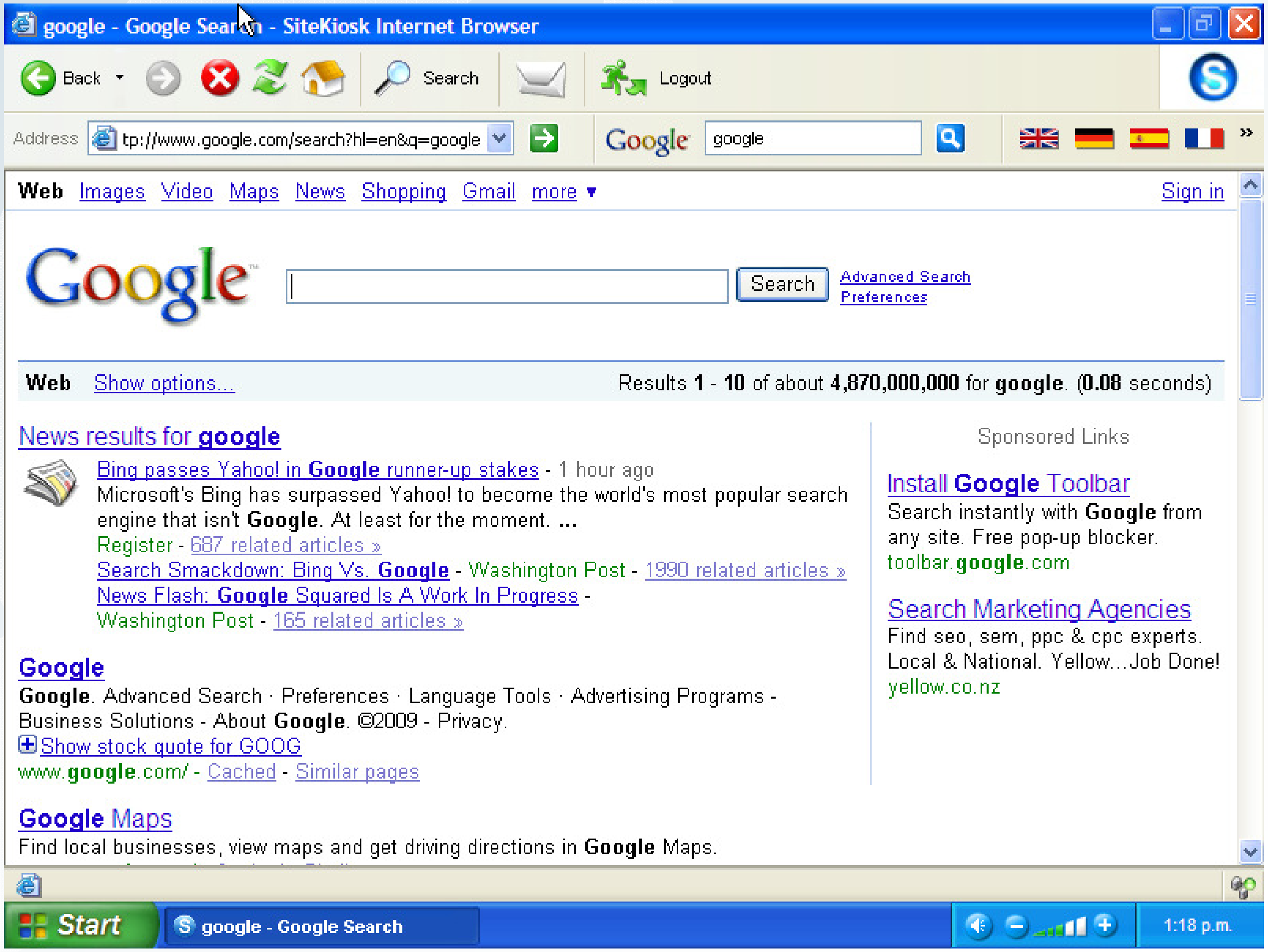
- ## Which Shell To Pop?
  - Kiosks try to block access to the console/command prompt.
  - Native OS permissions on cmd.exe
  - Hook calls to CreateProcess/AllocConsole
  - Group policy/Registry Settings.

  - iKAT tries 17 methods to get shell.
  - Custom none-console shells
  - Modified Windows console.

cmd.exe	command.com	win.com cmd.exe	win.com command.com
Loadfix.com start.exe	sc create testsvc binpath= "cmd /K start" type= own type= interact	loadfix.com cmd.exe	loadfix.com command.com
start loadfix.com cmd.exe	start loadfix.com command.com	start loadfix.com cmd.exe	%COMSPEC%



- **"You cant hack my Kiosk, its a touch screen!"**
  - How do I navigate to http://ikat.ha.cked.net
  - Without a keyboard?
  - Select a letter
  - Drag to an input field
  - Google
- **Agile fingers required!**
  - Touch screen = hack-able


google - Google Search - SiteKiosk Internet Browser
Back
Search
Logout
Address
tp://www.google.com/search?hl=en&q=google
Google
google
Web Images Video Maps News Shopping Gmail more ▾
Sign in
Google
Search
Advanced Search
Preferences
Start
google - Google Search
1:18 p.m.

Web Show options...

Results **1** - **10** of about **4,870,000,000** for **google**. (**0.08** seconds)

News results for **google**

Bing passes Yahoo! in **Google** runner-up stakes - 1 hour ago
Microsoft's Bing has surpassed Yahoo! to become the world's most popular search engine that isn't **Google**. At least for the moment. **...**
Register - 687 related articles »
Search Smackdown: Bing Vs. **Google** - Washington Post - 1990 related articles »
News Flash: **Google** Squared Is A Work In Progress - Washington Post - 165 related articles »

Google
Google. Advanced Search · Preferences · Language Tools · Advertising Programs - Business Solutions - About **Google**. ©2009 - Privacy.
Show stock quote for GOOG
www.**google**.com/ - Cached - Similar pages

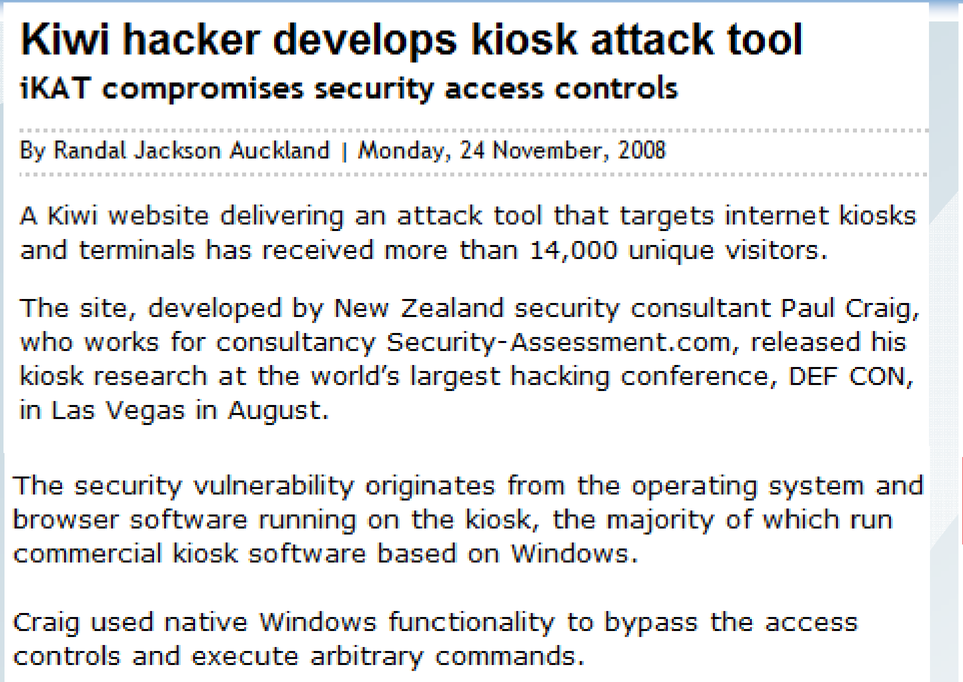
Google Maps
Find local businesses, view maps and get driving directions in **Google** Maps.

Sponsored Links

Install **Google** Toolbar
Search instantly with **Google** from any site. Free pop-up blocker.
toolbar.**google**.com

Search Marketing Agencies
Find seo, sem, ppc & cpc experts. Local & National. Yellow...Job Done!
yellow.co.nz

After the iKAT v1.0 Release



Kiwi hacker develops kiosk attack tool

iKAT compromises security access controls

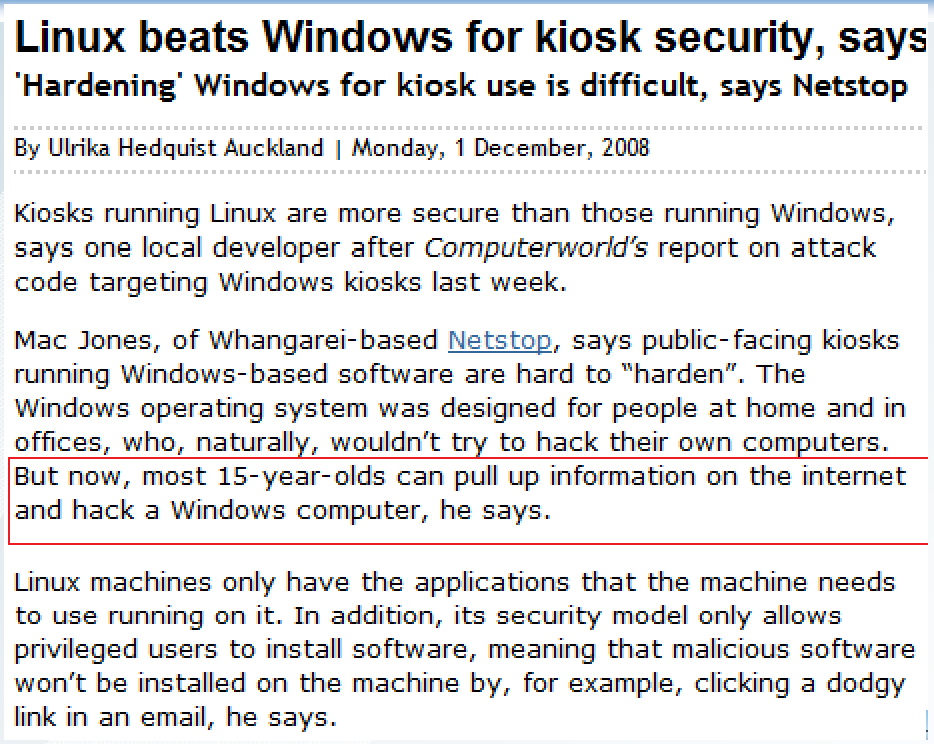
By Randal Jackson Auckland | Monday, 24 November, 2008

A Kiwi website delivering an attack tool that targets internet kiosks and terminals has received more than 14,000 unique visitors.

The site, developed by New Zealand security consultant Paul Craig, who works for consultancy Security-Assessment.com, released his kiosk research at the world's largest hacking conference, DEF CON, in Las Vegas in August.

The security vulnerability originates from the operating system and browser software running on the kiosk, the majority of which run commercial kiosk software based on Windows.

Craig used native Windows functionality to bypass the access controls and execute arbitrary commands.



Linux beats Windows for kiosk security, says

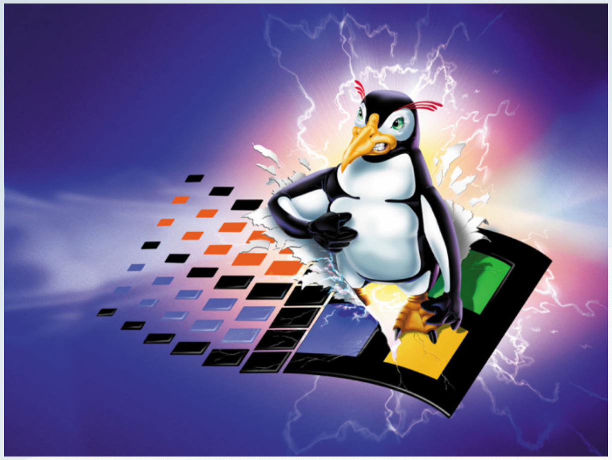
'Hardening' Windows for kiosk use is difficult, says Netstop

By Ulrika Hedquist Auckland | Monday, 1 December, 2008

Kiosks running Linux are more secure than those running Windows, says one local developer after *Computerworld's* report on attack code targeting Windows kiosks last week.

Mac Jones, of Whangarei-based Netstop, says public-facing kiosks running Windows-based software are hard to "harden". The Windows operating system was designed for people at home and in offices, who, naturally, wouldn't try to hack their own computers. But now, most 15-year-olds can pull up information on the internet and hack a Windows computer, he says.

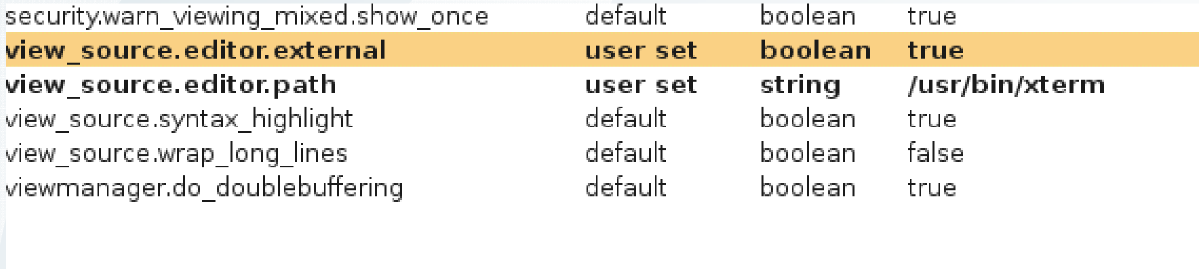
Linux machines only have the applications that the machine needs to use running on it. In addition, its security model only allows privileged users to install software, meaning that malicious software won't be installed on the machine by, for example, clicking a dodgy link in an email, he says.



- **Oh yeah mate?**
  - "Windows was designed for people at home"
  - Most 15-year-olds can hack Windows.
  - All OS's are insecure!
  - Physical access = You Win.

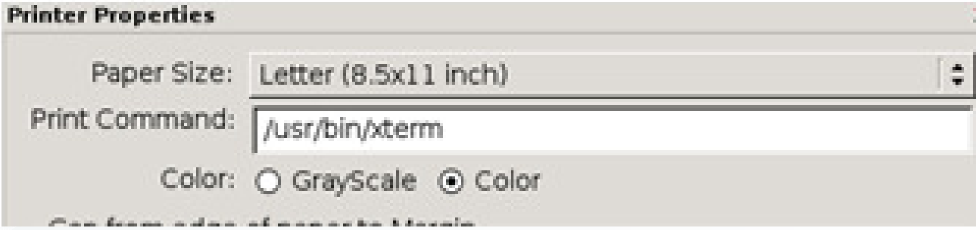
- **Hacking Linux Kiosks.**
  - Linux Kiosks are based on Mozilla/FireFox.
  - Linux browsers have **less** functionality than Windows.
  - ClickOnce, ActiveX, VBScript don’t exist.
  - It took me over a week to break SiteKiosk 7
  - “Linux *should* take me months.”
    - I tried to hack 8 different Linux Kiosks.
    - All 8 Kiosks allowed command execution!
    - 2 root privilege escalation vulnerabilities discovered!
- **I was expecting more..**
  - Kiosks were often built on default unhardened Linux installations.
  - Wtf I thought Linux guys were hardcore.

- **Hacking Linux Kiosk’s**
  - Objective: Spawn /usr/bin/xterm
- **Accessing about:config**
  - Reconfigure Mozilla/Firefox to spawn xterm!
  - Define an external **view_source.editor.external.path**
  - “View Source” -> Shell



security.warn_viewing_mixed.show_once	default	boolean	true
view_source.editor.external	**user set**	**boolean**	**true**
view_source.editor.path	**user set**	**string**	**/usr/bin/xterm**
view_source.syntax_highlight	default	boolean	true
view_source.wrap_long_lines	default	boolean	false
viewmanager.do_doublebuffering	default	boolean	true

  - Define external handler for a file type .pdf -> /usr/bin/xterm
  - Define protocol handler for mailto:// -> /usr/bin/xterm
  - Disable silent printing.



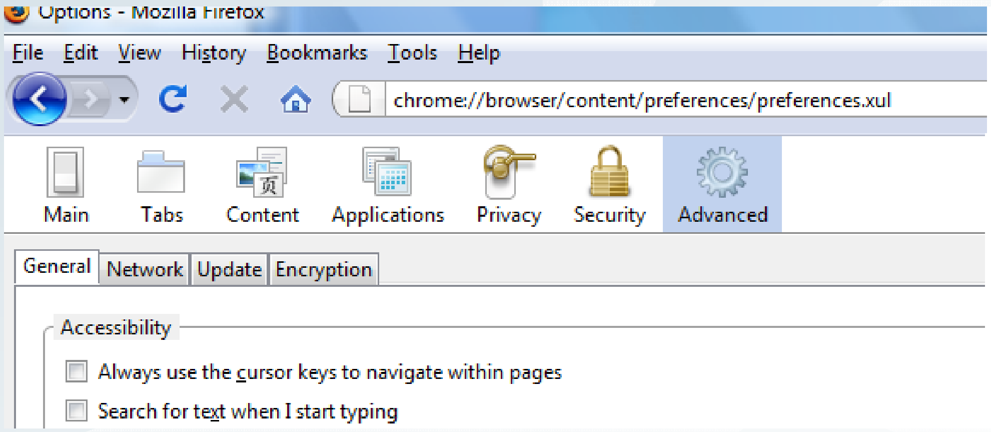
Printer Properties

Paper Size: Letter (8.5x11 inch)

Print Command: /usr/bin/xterm

Color: ○ GrayScale ● Color

- **Only one Kiosk allowed direct access to about:config ☹**
  - about:config is an alias to chrome://global/content/config.xul
  - Blacklist approach fails again.
    - chrome://global/content/config.xul
    - chrome://browser/content/preferences/preferences.xul
  - **Works on almost every Linux Kiosk tested!**

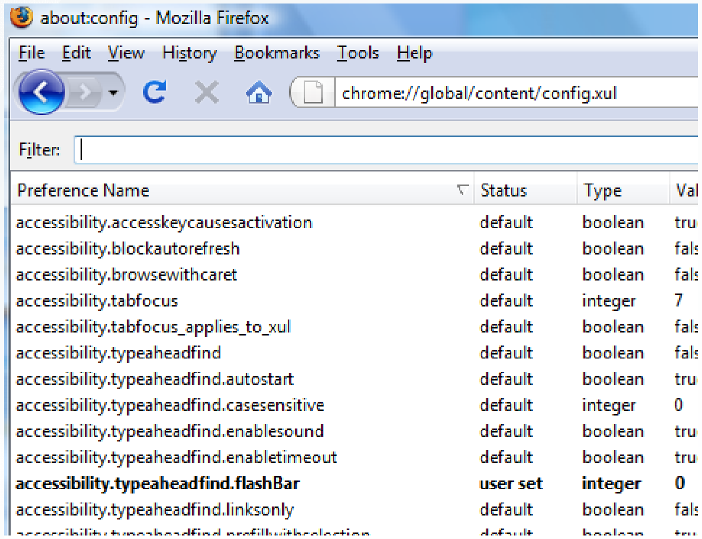


chrome://browser/content/preferences/preferences.xul

Accessibility

□ Always use the cursor keys to navigate within pages

□ Search for text when I start typing


about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help

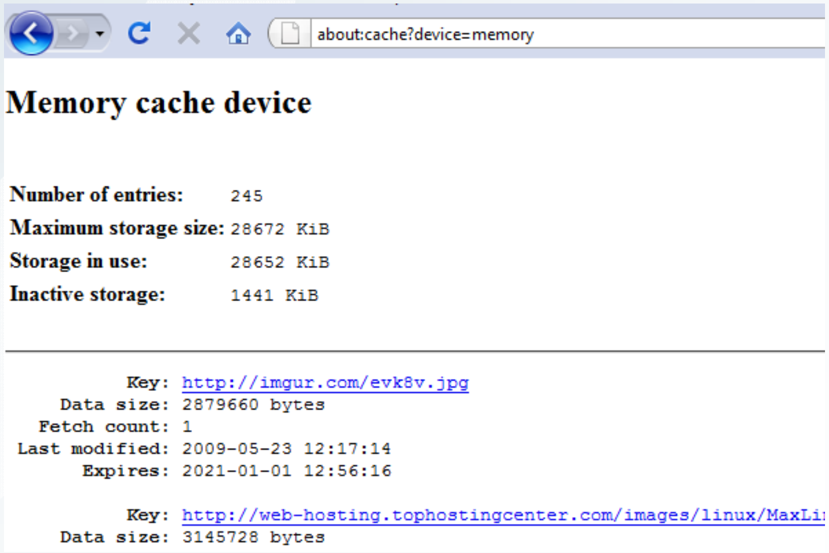
chrome://global/content/config.xul

Filter:

Preference Name	Status	Type	Val
accessibility.accesskeycausesactivation	default	boolean	tru
accessibility.blockautorefresh	default	boolean	fals
accessibility.browsewithcaret	default	boolean	fals
accessibility.tabfocus	default	integer	7
accessibility.tabfocus_applies_to_xul	default	boolean	fals
accessibility.typeaheadfind	default	boolean	fals
accessibility.typeaheadfind.autostart	default	boolean	tru
accessibility.typeaheadfind.casesensitive	default	integer	0
accessibility.typeaheadfind.enablesound	default	boolean	tru
accessibility.typeaheadfind.enabletimeout	default	boolean	tru
accessibility.typeaheadfind.flashBar	**user set**	**integer**	**0**
accessibility.typeaheadfind.linksonly	default	boolean	fals
accessibility.typeaheadfind.prefillwithselection	default	boolean	tru

- **about:cache**
  - Read Memory, Disk, Offline cache information
  - See previous requests made by other Kiosk users.
  - Detailed information regarding the browser activity.

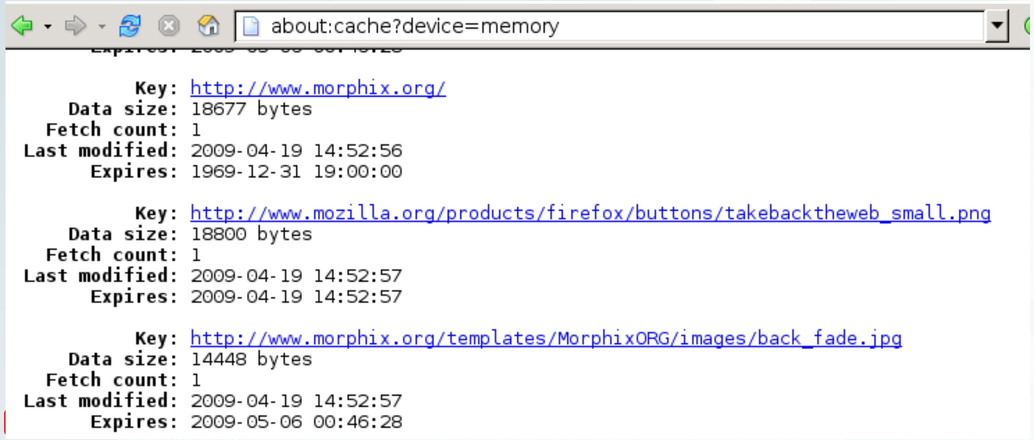
  - about:cache?device=disk
  - about:cache?device=memory
  - about:cache?device=offline



Memory cache device

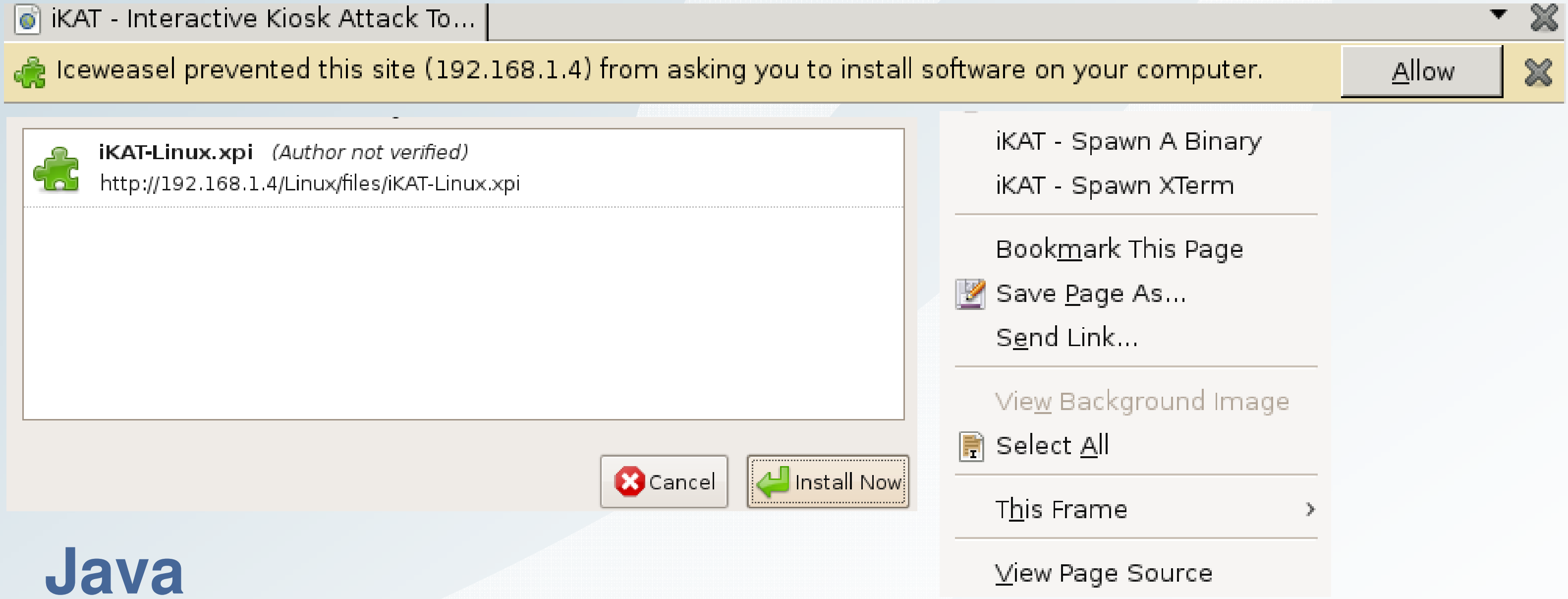
Number of entries:	245
Maximum storage size:	28672 KiB
Storage in use:	28652 KiB
Inactive storage:	1441 KiB

```
          Key: http://imgur.com/evk8v.jpg
    Data size: 2879660 bytes
  Fetch count: 1
Last modified: 2009-05-23 12:17:14
      Expires: 2021-01-01 12:56:16

          Key: http://web-hosting.tophostingcenter.com/images/linux/MaxLi
    Data size: 3145728 bytes
```



```
          Key: http://www.morphix.org/
    Data size: 18677 bytes
  Fetch count: 1
Last modified: 2009-04-19 14:52:56
      Expires: 1969-12-31 19:00:00

          Key: http://www.mozilla.org/products/firefox/buttons/takebacktheweb_small.png
    Data size: 18800 bytes
  Fetch count: 1
Last modified: 2009-04-19 14:52:57
      Expires: 2009-04-19 14:52:57

          Key: http://www.morphix.org/templates/MorphixORG/images/back_fade.jpg
    Data size: 14448 bytes
  Fetch count: 1
Last modified: 2009-04-19 14:52:57
      Expires: 2009-05-06 00:46:28
```

- ## iKAT Firefox Extension
  - Some Linux Kiosks allow you to install your own FireFox Extensions!
    - iKAT FireFox Extension for Windows & Linux
    - FireFox XUL using Process.init to spawn /usr/bin/xterm!



iKAT - Interactive Kiosk Attack To...

Iceweasel prevented this site (192.168.1.4) from asking you to install software on your computer.

iKAT-Linux.xpi *(Author not verified)*
http://192.168.1.4/Linux/files/iKAT-Linux.xpi

- ## Java
  - Signed Java applets can also spawn /usr/bin/xterm

- **Hang on, Is this 0day?**
  - Accessing chrome:// is not 0day
  - Firefox is acting COMPLETELY as expected.
  - Internet Explorer was designed to run .NET Applications
  - .NET tools are running in the correct security zone.
  - Java is capable of spawning processes.
  - Everything is functioning as it was designed.
  - These are features of the platform and the environment.
- **Kiosks are fundamentally insecure**
  - Built on operating systems which trust local users.
  - Authenticated local users should not be trusted.

- **Photo Kiosks**
  - It’s a Kiosk, fuck yeah, why not.
  - Most run Windows.
  - Its shouting *‘Hey Paul Hack Me’*
  - No internet connection.
  - Input vectors:
    - Memory card
    - CDRom
    - USB
  - May hold customers photos!

- **Introducing iKAT Photo**
  - Designed to aid exploitation of Photo Printing Kiosk’s!
  - Extract it to a USB Stick/Memory Card
  - Contains:
    - Autorun.inf
    - iKATPhoto.exe
    - All the iKAT Kiosk hacking tools.
    - Heaps of malformed images.
    - 100% touch screen centric.

  - Automatic exploitation through Autorun.inf
  - Manual exploitation using Common Dialogs.
  - Unhandled exception through malformed images.

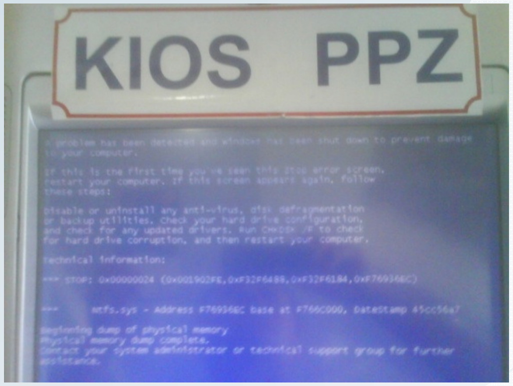
- **Conclusion:**
  - Kiosks can be hacked, you saw me do it in heaps today!

  - Do not use Kiosks for sensitive, private information.
  - Do not keep Kiosks on shared network infrastructure.
  - Minimize your risk, because Kiosks are not secure.

  - If you run a Kiosk, take security seriously.
  - Your Kiosk is hack able, I promise you.
  - Use iKAT yourself and witness the magic.

  - iKAT portable available: Download and host your own iKAT!

- **Questions ?**
  - Email me: Paul@ha.cked.net
  - iKAT: http://ikat.ha.cked.net



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Disable or uninstall any anti-virus, disk defragmentation
or backup utilities. Check your hard drive configuration,
and check for any updated drivers. Run CHKDSK /F to check
for hard drive corruption, and then restart your computer.

Technical information:

*** STOP: 0x00000024 (0x001902FE,0xF32F6488,0xF32F6184,0xF76936EC)


***      ntfs.sys - Address F76936EC base at F766C000, DateStamp 45cc56a7

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

```
An exception 0D has occurred at 0028:FF015E73 in VxD ks(05) +
00001E13.  This was called from 0028:C000358F in VxD VMM(01) +
0000258F.  It may be possible to continue normally.

*  Press any key to attempt to continue.
*  Press CTRL+ALT+DEL to restart your computer.  You will
   lose any unsaved information in all applications.

                    Press any key to continue
```