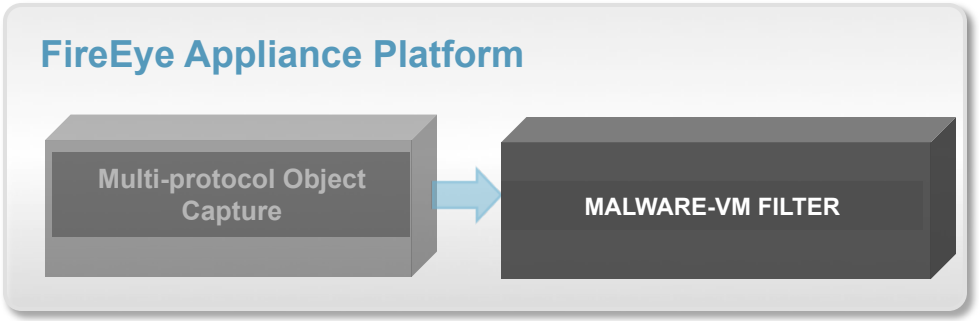
Malware Detection using Advanced Behavior Analysis

Josh McCarthy, Sr. Solutions Architect

Multi-Protocol, Real-Time VX Engine



Phase 1 – Web MPS
- Aggressive Capture
- Web Object Filter

Phase 1 – Email MPS
- Email Attachments
- URL Submission

Phase 1 – MAS appliance
- User submissions
- Batch mode processing

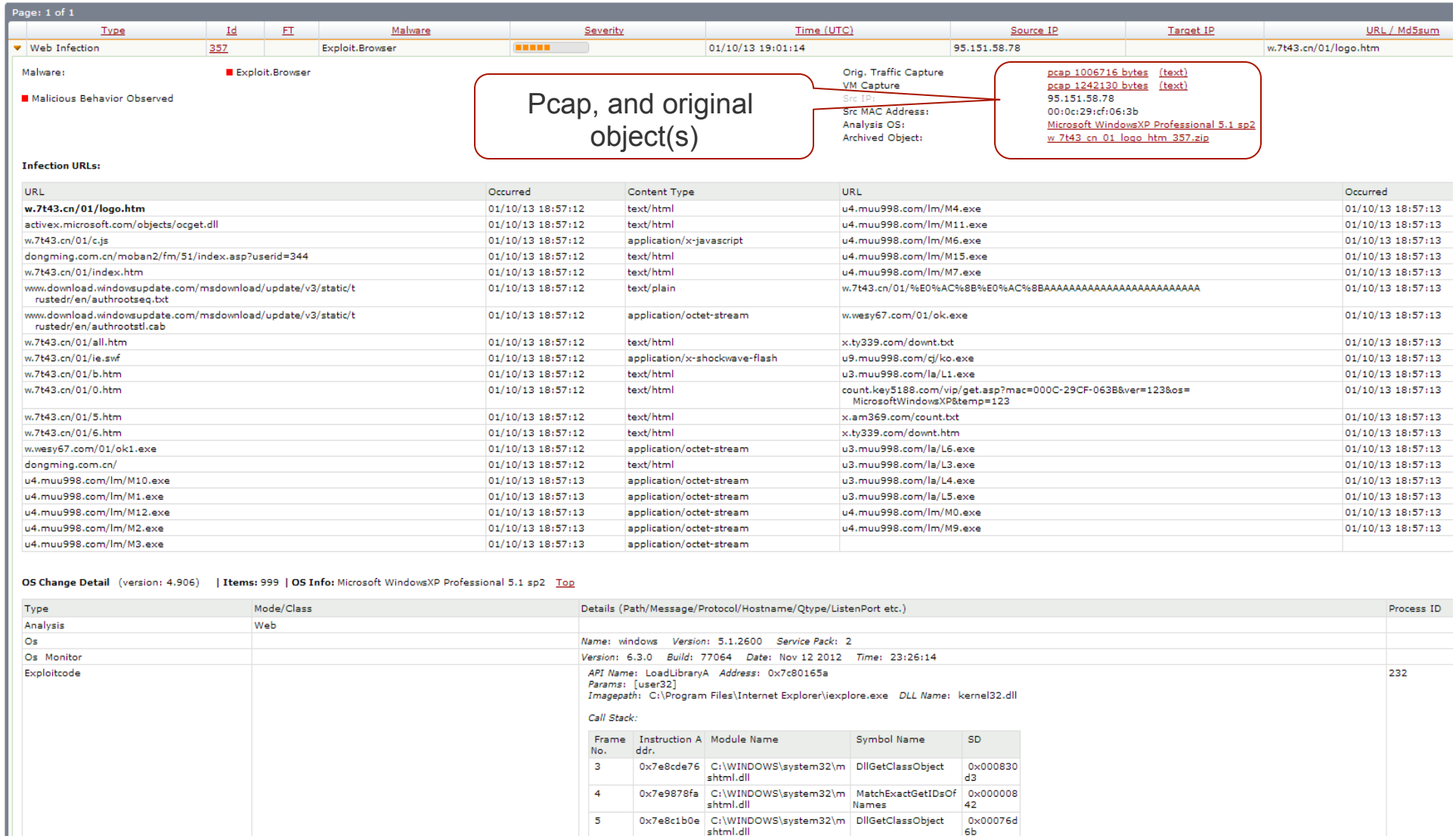
Map To Target OS&Apps

Virtual Execution Environments
Phase 2

Dynamic, real-time analysis
- Presence Of Malware
- Malware Binary
- Attack Profile
- Originating URL
- Subsequent URLs
- Obfuscation Techniques
- Host Modification Rpt
- Malware Identification
- C&C Profile
- C&C PCAP
- C&C Block List
- C&C Encryption Profile
- Management Reports
- Beaconing Volume
- Call Back Volume
- Infected Hosts
- Malware Type Reports

FireEye

Sample Web Exploit



Page: 1 of 1

Type	Id	FT	Malware	Severity	Time (UTC)	Source IP	Target IP	URL / Md5sum
Web Infection	357		Exploit.Browser		01/10/13 19:01:14	95.151.58.78		w.7t43.cn/01/logo.htm

Malware: ■ Exploit.Browser

■ Malicious Behavior Observed

Pcap, and original object(s)

Orig. Traffic Capture: pcap 1006716 bytes (text)
VM Capture: pcap 1242130 bytes (text)
Src IP: 95.151.58.78
Src MAC Address: 00:0c:29:cf:06:3b
Analysis OS: Microsoft WindowsXP Professional 5.1 sp2
Archived Object: w_7t43_cn_01_logo_htm_357.zip

Infection URLs:

URL	Occurred	Content Type	URL	Occurred
w.7t43.cn/01/logo.htm	01/10/13 18:57:12	text/html	u4.muu998.com/lm/M4.exe	01/10/13 18:57:13
activex.microsoft.com/objects/ocget.dll	01/10/13 18:57:12	text/html	u4.muu998.com/lm/M11.exe	01/10/13 18:57:13
w.7t43.cn/01/c.js	01/10/13 18:57:12	application/x-javascript	u4.muu998.com/lm/M6.exe	01/10/13 18:57:13
dongming.com.cn/moban2/fm/51/index.asp?userid=344	01/10/13 18:57:12	text/html	u4.muu998.com/lm/M15.exe	01/10/13 18:57:13
w.7t43.cn/01/index.htm	01/10/13 18:57:12	text/html	u4.muu998.com/lm/M7.exe	01/10/13 18:57:13
www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt	01/10/13 18:57:12	text/plain	w.7t43.cn/01/%E0%AC%8B%E0%AC%8BAAAAAAAAAAAAAAAAAAAAAAAA	01/10/13 18:57:13
www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab	01/10/13 18:57:12	application/octet-stream	w.wesy67.com/01/ok.exe	01/10/13 18:57:13
w.7t43.cn/01/all.htm	01/10/13 18:57:12	text/html	x.ty339.com/downt.txt	01/10/13 18:57:13
w.7t43.cn/01/ie.swf	01/10/13 18:57:12	application/x-shockwave-flash	u9.muu998.com/cj/ko.exe	01/10/13 18:57:13
w.7t43.cn/01/b.htm	01/10/13 18:57:12	text/html	u3.muu998.com/la/L1.exe	01/10/13 18:57:13
w.7t43.cn/01/0.htm	01/10/13 18:57:12	text/html	count.key5188.com/vip/get.asp?mac=000C-29CF-063B&ver=123&os=MicrosoftWindowsXP&temp=123	01/10/13 18:57:13
w.7t43.cn/01/5.htm	01/10/13 18:57:12	text/html	x.am369.com/count.txt	01/10/13 18:57:13
w.7t43.cn/01/6.htm	01/10/13 18:57:12	text/html	x.ty339.com/downt.htm	01/10/13 18:57:13
w.wesy67.com/01/ok1.exe	01/10/13 18:57:12	application/octet-stream	u3.muu998.com/la/L6.exe	01/10/13 18:57:13
dongming.com.cn/	01/10/13 18:57:12	text/html	u3.muu998.com/la/L3.exe	01/10/13 18:57:13
u4.muu998.com/lm/M10.exe	01/10/13 18:57:13	application/octet-stream	u3.muu998.com/la/L4.exe	01/10/13 18:57:13
u4.muu998.com/lm/M1.exe	01/10/13 18:57:13	application/octet-stream	u3.muu998.com/la/L5.exe	01/10/13 18:57:13
u4.muu998.com/lm/M12.exe	01/10/13 18:57:13	application/octet-stream	u4.muu998.com/lm/M0.exe	01/10/13 18:57:13
u4.muu998.com/lm/M2.exe	01/10/13 18:57:13	application/octet-stream	u4.muu998.com/lm/M9.exe	01/10/13 18:57:13
u4.muu998.com/lm/M3.exe	01/10/13 18:57:13	application/octet-stream		

OS Change Detail (version: 4.906) | **Items:** 999 | **OS Info:** Microsoft WindowsXP Professional 5.1 sp2 Top

Type	Mode/Class	Details (Path/Message/Protocol/Hostname/Qtype/ListenPort etc.)	Process ID
Analysis	Web		
Os		*Name*: windows *Version*: 5.1.2600 *Service Pack*: 2	
Os Monitor		*Version*: 6.3.0 *Build*: 77064 *Date*: Nov 12 2012 *Time*: 23:26:14	
Exploitcode		*API Name*: LoadLibraryA *Address*: 0x7c80165a *Params*: [user32] *Imagepath*: C:\Program Files\Internet Explorer\iexplore.exe *DLL Name*: kernel32.dll *Call Stack:*	232

Frame No.	Instruction Addr.	Module Name	Symbol Name	SD
3	0x7e8cde76	C:\WINDOWS\system32\mshtml.dll	DllGetClassObject	0x000830d3
4	0x7e9878fa	C:\WINDOWS\system32\mshtml.dll	MatchExactGetIDsOfNames	0x0000842
5	0x7e8c1b0e	C:\WINDOWS\system32\mshtml.dll	DllGetClassObject	0x00076d6b

DLL Entry Points

File	Close	C:\WINDOWS\system\DVL MD5: d41d8cd98f00b204e9800998ecf8427e SHA1: da39a3ee5e6b4b0d3255bfef95601890afd80709
Regkey	Setval	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Rsskplm" = rundll32.exe C:\WINDOWS\system32\ngnvkf97.dll,Start
Malicious Alert	Misc Anomaly	*Message*: Startup services added *Detail*: Malware adding itself to windows startup areas
File	Created	C:\WINDOWS\system32\ngnvkf97.dllmmc.pkm
File	Close	C:\WINDOWS\system32\ngnvkf97.dllmmc.pkm MD5: 8d9c307cb7f3c4a32822a51922d1ceaa SHA1: b51a60734da64be0e618bacbea2865a8a7dcd669
Folder	Open	C:\Documents and Settings\Administrator\Cookies
File	Open	C:\Documents and Settings\Administrator\Cookies\index.dat
Mutex		*Imagepath*: C:\WINDOWS\system32\rundll32.exe
Regkey	Setval	\REGISTRY\USER\S-1-5-21-527237240-1580818891-725345543-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\"ProxyEnable" = 0x00000000
Regkey	Setval	\REGISTRY\USER\S-1-5-21-527237240-1580818891-725345543-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\"SavedLegacySettings" = 46 00 00 00 e6 03 00 00 01 00 00 00 0d 00 00 00 31 30 2e 30 2e 30 2e 32 3a 38 30 38 30 00 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
Driver	Loaded	*Registrypath*: \Registry\Machine\System\CurrentControlSet\Services\ngnvkf97 *Driverimage*: \??\C:\WINDOWS\system32\drivers\ngnvkf97.sys *Method*: NtLoadDriver *Imagepath*: C:\WINDOWS\system32\services.exe
Malicious Alert	Misc Anomaly	*Message*: Malware is loading a driver
Regkey	Deleteval	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"Rsskplm"
Malicious Alert	Misc Anomaly	*Message*: Startup services deleted *Detail*: Malware deleting entries in windows startup areas

Entry point passed to driver by malware in user mode

Kernel mode driver

File	Created	C:\WINDOWS\system32\cobox.dll
Malicious Alert	Misc Anomaly	*Message*: System services modified *Detail*: New exe/dll/sys file created under WINDOWS or SYSTEM32 directories
Process	Started	C:\WINDOWS\system32\rundll32.exe *Packed*: no *GUI*: no *Parentname*: C:\malware.exe *Command Line*: Rundll32 C:\WINDOWS\system32\cobox.dll Exucute
Mutex		\BaseNamedObjects\SHIMLIB_LOG_MUTEX

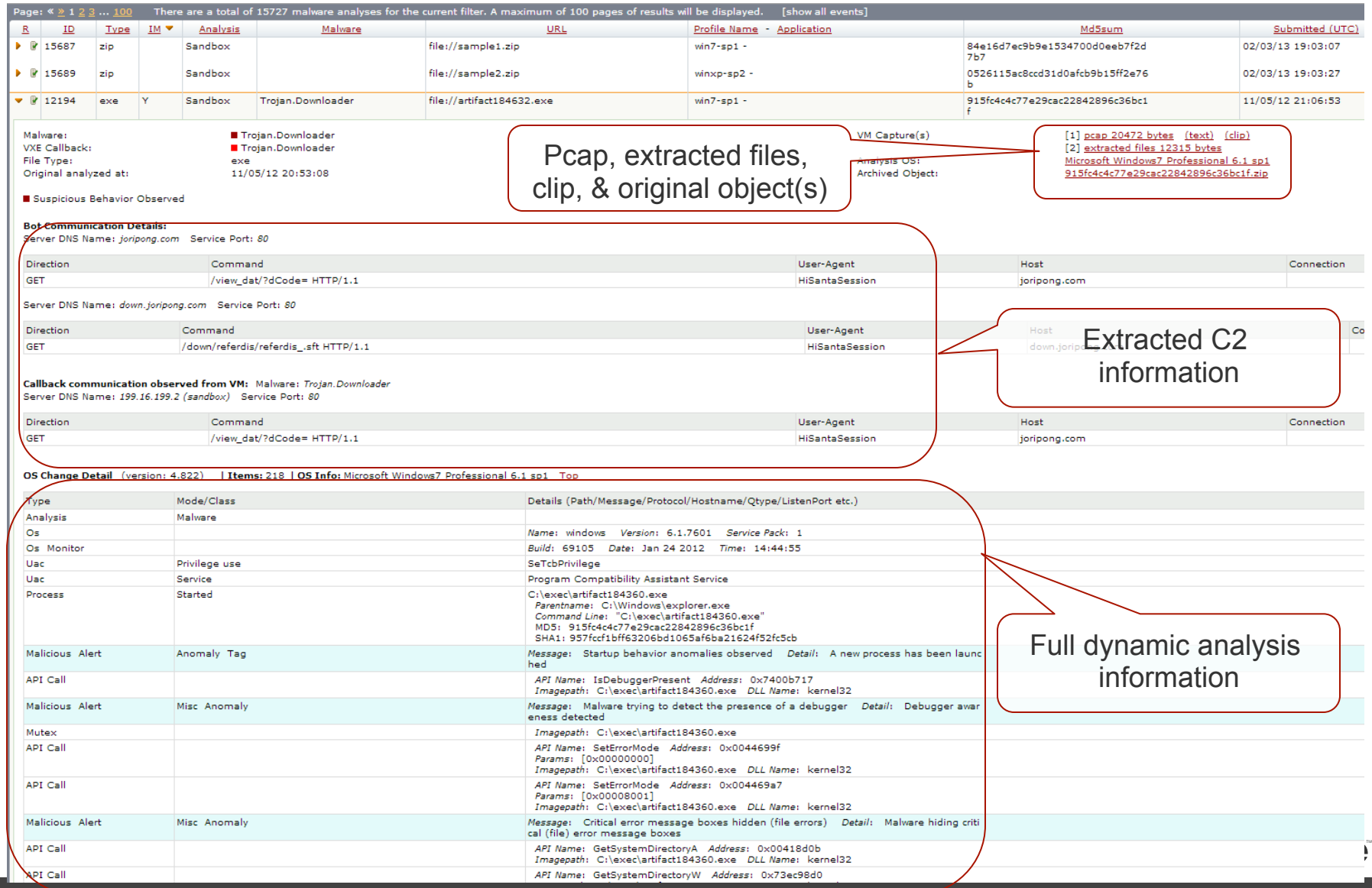
Recent PDF Zero-Day Sleep Example

OS Change Detail (version: 4.975) | **Items:** 1020 | **OS Info:** Microsoft WindowsXP Professional 5.1 sp2 Top

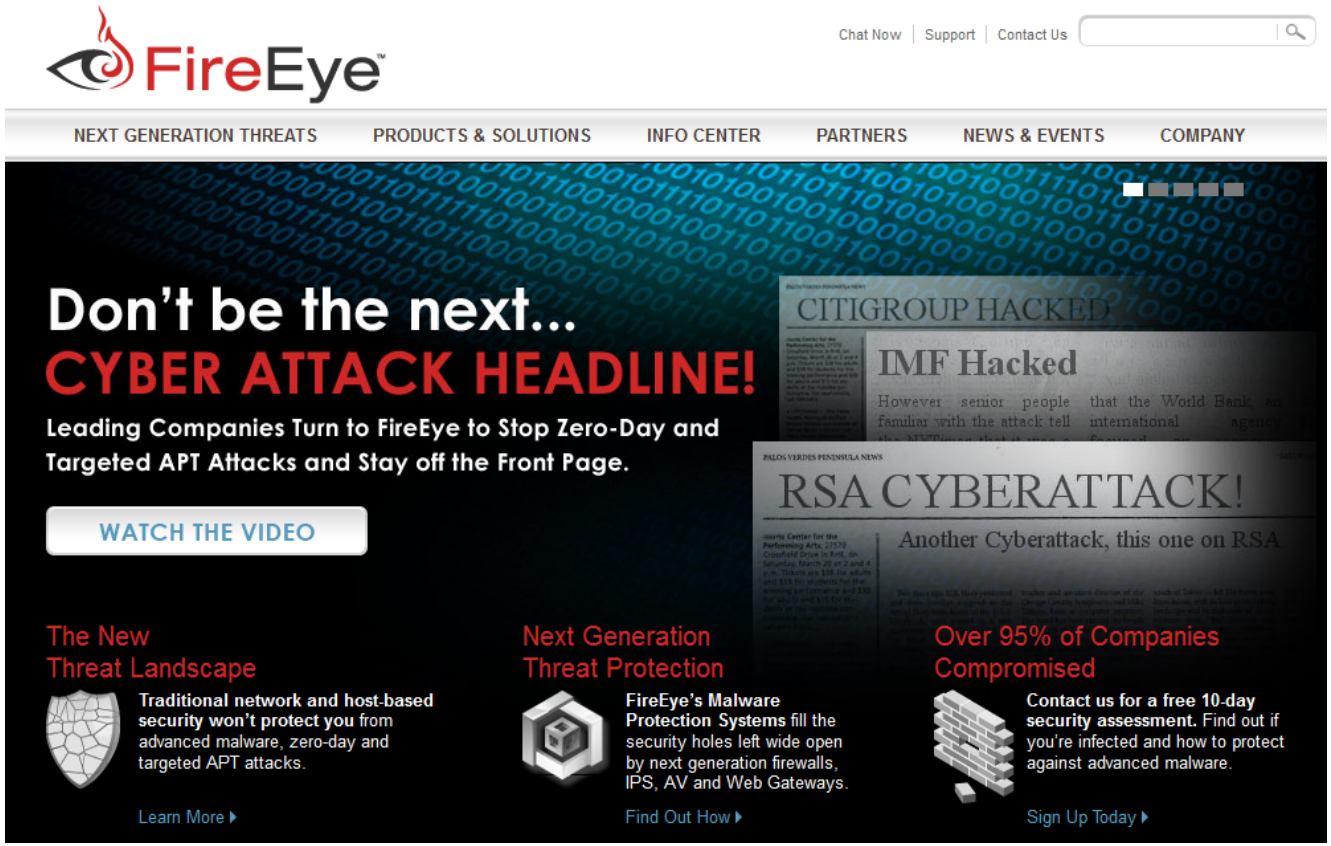
Type	Mode/Class	Details (Path/Message/Protocol/Hostname/Qtype/ListenPort etc.)	Process ID	Parent ID	File Size
Analysis	Malware				
Os		*Name*: windows *Version*: 5.1.2600 *Service Pack*: 2			
Os Monitor		[redacted]			
Process	Started	C:\WINDOWS\system32\rundll.exe *Parentname*: C:\WINDOWS\system32\cmd.exe *Command Line*: "c:\windows\system32\rundll.exe" "c:\[redacted].dll" MD5: [redacted] SHA1: [redacted]	400	644	720896
Malicious Alert	Anomaly Tag	*Message*: Startup behavior anomalies observed *Detail*: A new process has been launched			
API Call		*API Name*: SystemTimeToFileTime *Address*: 0x7c833ece *Params*: [0x12f0a4, 0x12eef8] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		
API Call		*API Name*: SystemTimeToFileTime *Address*: 0x0045f9ff *Params*: [0x12f094, 0x12f08c] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		
API Call		*API Name*: SystemTimeToFileTime *Address*: 0x7c833ece *Params*: [0x12f9d8, 0x12f82c] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		
API Call		*API Name*: SystemTimeToFileTime *Address*: 0x0045f9ff *Params*: [0x12f9c8, 0x12f9c0] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		
API Call		*API Name*: SystemTimeToFileTime *Address*: 0x7c833ece *Params*: [0x12f8f4, 0x12f748] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		
API Call		*API Name*: SystemTimeToFileTime *Address*: 0x0045f9ff *Params*: [0x12f8e4, 0x12f8dc] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		
3 Repeated items skipped					
API Call		*API Name*: SetErrorMode *Address*: 0x7c8219fb *Params*: [32769] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		
API Call		*API Name*: SetErrorMode *Address*: 0x7c821ce6 *Params*: [1] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		
DLL Exports		*DLL Name*: c:\97777F~1.DLL *Exports*: [Call32W, Call32W@16, CallW, CallW@16, ClearPropVariantArray, ClearVariantArray, DllCanUnloadNow, DllGetClassObject, DllMain, DllMain@12, DllRegisterServer, DllUnregisterServer, GetProxyDllInfo, InitPropVariantFromBooleanVector, InitPropVariantFromBuffer, InitPropVariantFromCLSID, InitPropVariantFromDoubleVector, InitPropVariantFromFileTime, InitPropVariantFromFileTimeVector, InitPropVariantFromGUIDAsString, InitPropVariantFromInt16Vector, InitPropVariantFromInt32Vector, InitPropVariantFromInt64Vector, InitPropVariantFromPropVariantVectorElem, InitPropVariantFromResource, InitPropVariantFromStrRet, InitPropVariantFromStringAsVector, InitPropVariantFromStringVector, InitPropVariantFromUInt16Vector, InitPropVariantFromUInt32Vector, InitPropVariantFromUInt64Vector]			
DLL Loaded		*Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Path*: C:\[redacted].dll MD5: [redacted] SHA1: [redacted]	400		
API Call		*API Name*: WaitForMultipleObjectsEx *Address*: 0x77df9b26 *Params*: [2, 0xe7ff6c, 0, 300000, 1] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		
Regkey	Added	\REGISTRY\USER\S-1-5-21-1409082233-688789844-725345543-1003\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	400		
API Call		*API Name*: Sleep *Address*: 0x666c3689 *Params*: [15000] *Imagepath*: C:\WINDOWS\system32\rundll.exe *DLL Name*: kernel32.dll	400		

Tracking sleep call

MAS Object and Info Availability



FireEye Security Assessment



http://www.fireeye.com/stopapts

FireEye

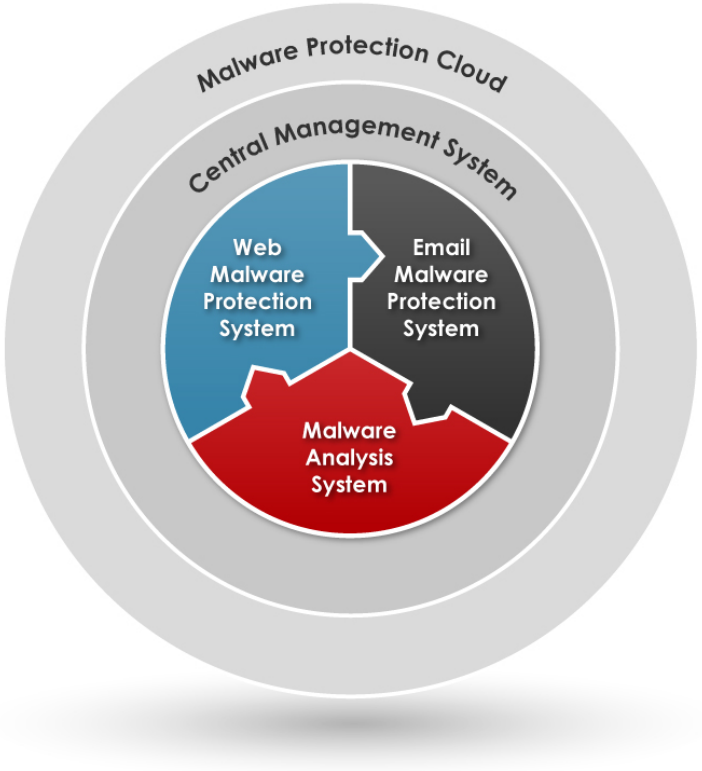
How to Detect Advanced Malware

- Implement automated behavior analysis of inbound network traffic using virtual analysis techniques
  - Analyze multiple version of Adobe files and Microsoft Office files
  - Java exploits
  - DLL injects
  - Heap spray attacks
- Implement automated mechanisms to discover Call-back Channels via behavioral analysis
- Implement automated dynamic behavior analysis mechanism to evaluate email attachments and URLs to identify and protect against targeted spear phishing attacks

FireEye

FireEye Advanced Malware Protection

Complete Protection Against Advanced Malware



FireEye