



PROTECTPOINT
Network Security



ProtectPoint Channel Weekly Review

August 25, 2008



PROTECTPOINT
Network Security

Press Release

FOR IMMEDIATE RELEASE

ProtectPoint Security, Inc. achieves SAS 70 Type II Certification For Second Consecutive Year

Fort Lauderdale, FL (August 20, 2008) – ProtectPoint Security, Inc., a leading managed security services provider (MSSP), today announced it has obtained a Statement on Auditing Standards No. 70 (SAS 70) Type II Service Auditors' Report for the second consecutive year. This extensive audit was conducted by SAS 70 Solutions, Inc., one of the largest and first-ever national firms to specialize in SAS 70 audit services. This internationally recognized auditing standard validates that a service organization has completed an in-depth audit of their control activities, which include controls over information technology processes

“The completion of our second consecutive SAS 70 Type II Audit again confirms that ProtectPoint control objectives, control processes and procedures have passed rigorous, third-party testing,” states ProtectPoint CEO, Steve Harris. “In today’s ever changing environment, organizations must have confidence that their trusted security service provider is supplying the highest levels of 24/7/365 security monitoring, management, response and controls to protect their valuable business assets. We are extremely pleased to confirm our valued clients trust in ProtectPoint by continuing to obtain this stringent audit.”

Many companies, especially financial services organizations that are highly regulated, require credible proof that a managed security services provider has processes and controls in place to provide a consistent, stable and secure environment to safely monitor and manage customer data.



How long it takes until an Exploit appears in the Wild (Hacking Gmail)

By Jamie Gausemel, ProtectPoint SOC Analyst

In this edition of “How long it takes until an Exploit appears in the Wild” we will talk about a Gmail vulnerability.

Several weeks ago at Defcon, the world’s largest annual hacker convention, Mike Perry, a reverse engineer from San Francisco, presented a tool that will automatically steal IDs of non-encrypted sessions which can then be used to gain access to Gmail accounts.

When logging into Gmail the website will send the user a cookie, which is nothing more than a text file, containing the users session ID to the browser. With this cookie file the website will automatically know the user is authenticated without ever asking them for their login credentials for up to two weeks unless they manually hit the sign out button. Once the user signs out, the cookie is then cleared.

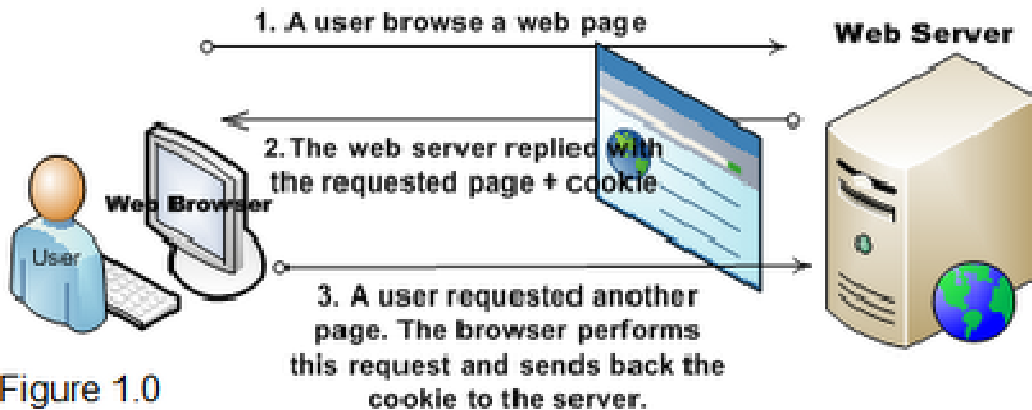
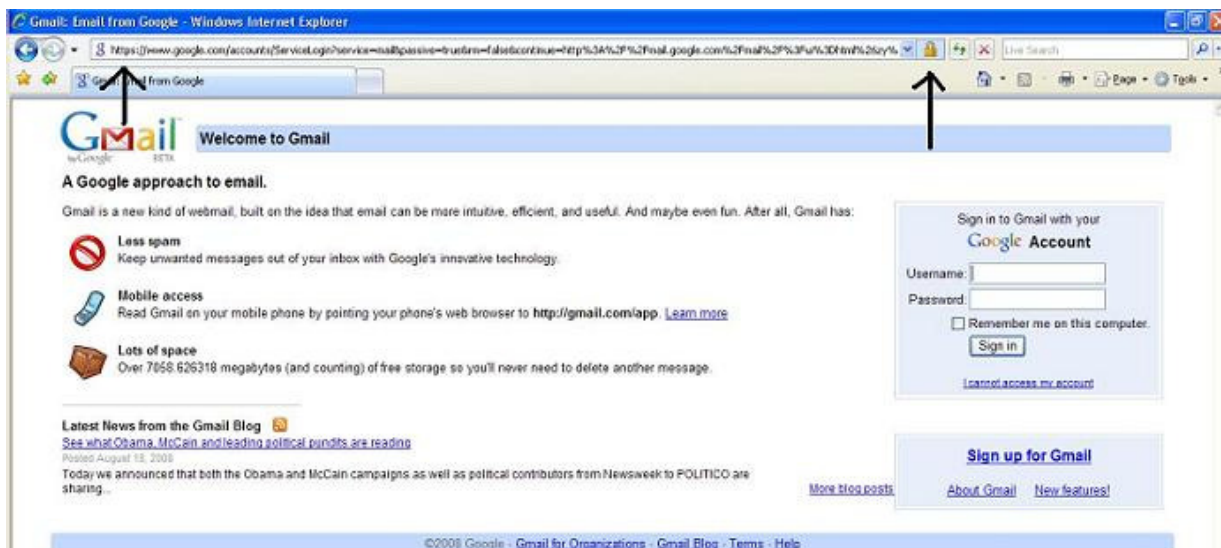
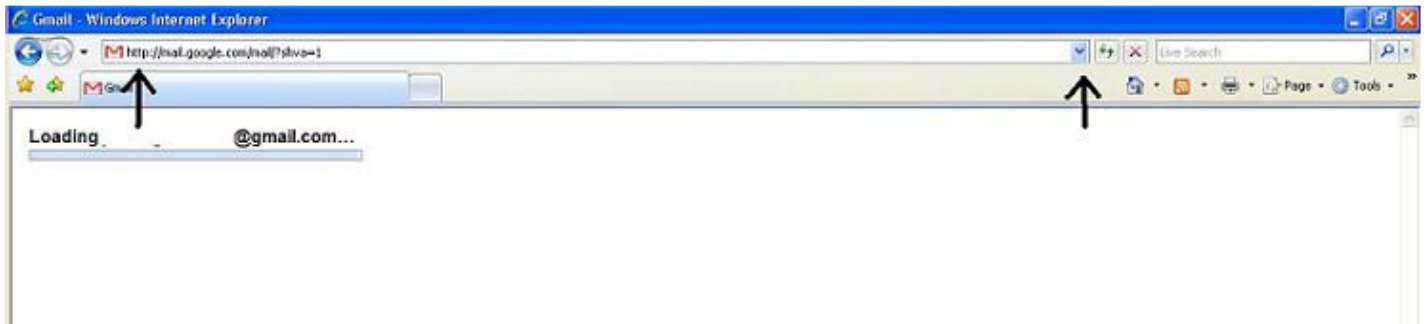


Figure 1.0

Over a secure SSL connection using a cookie as authentication would not be a problem, however Gmail does not use a secure http connection entirely unless you explicitly tell it to. The only time Gmail uses a SSL connection is when you initially log in however it then reverts back to an unencrypted connection.



(Gmail forces an encrypted connection to login)

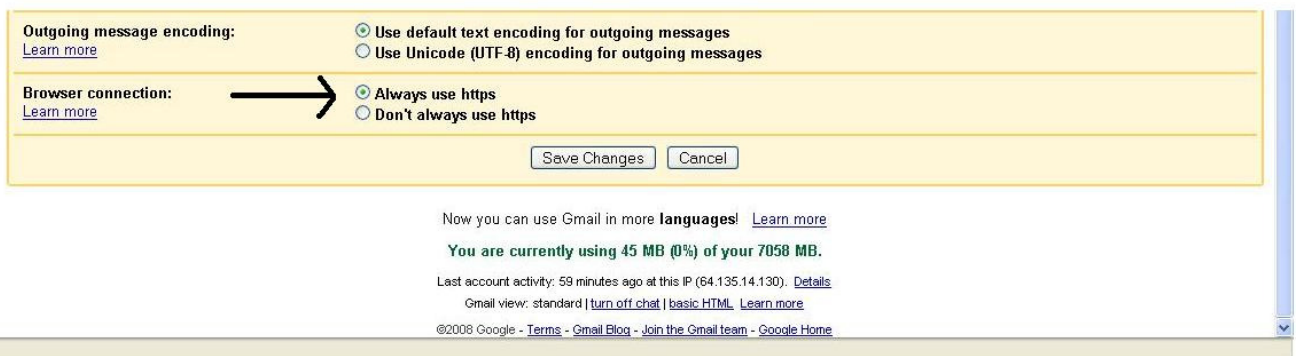


(Gmail then reverts to an unencrypted session)

The problem that is created with this cookie is that every time a user accesses anything on Gmail, such as an image, the user's browser will send that cookie to the website over the unencrypted connection. With this knowledge an attacker sniffing traffic on the network can insert an image served from <http://mail.google.com> which will force your browser to send the cookie file, and they can then intercept the user's session ID. Now that the attacker has the user's cookie they can simply go to Gmail and they will be automatically authenticated. Users checking their web mail from public wireless hotspots are more likely to be attacked than users using secured wired networks.

Perry stated that he informed Google of this situation over a year ago, and although they made an option available to always use SSL he is unhappy with the lack of information notifying or explaining to users this new feature. He explains the implications of not informing users, "This gives people who routinely log in to Gmail beginning with an <https://> session a false sense of security, because they think they're secure but they're really not."

Users who login to Gmail from different locations and would like to benefit from this option only when logging in from unsecured networks can force Gmail to use a secure connection by manually typing <https://mail.google.com> before logging in. This will use a secure connection over the entire session and not only during the authentication phase. Users who would like for Gmail to use a secure connection all of the time irregardless of where they are logging in from should go to their Gmail settings and select "Always use https" at the bottom of the page.



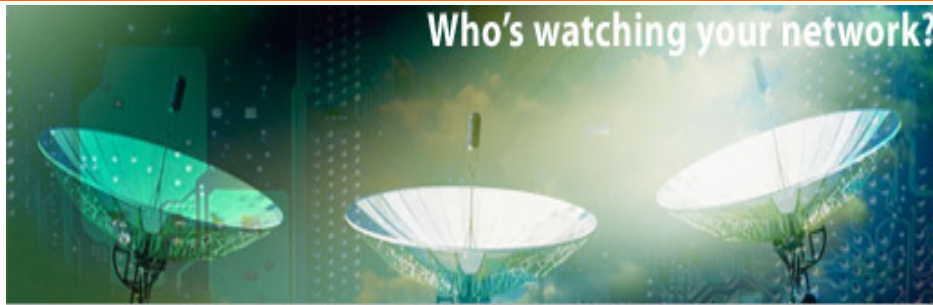
(Always use https setting)

REFERENCES:

<http://www.hungry-hackers.com/2008/08/gmail-account-hacking-tool.html>

http://en.wikipedia.org/wiki/DEF_CON

<http://blog.iantivirus.com/2008/03/cookies-threat-to-your-privacy.html>



[News you can Use](#)

Microsoft Adds ActiveX Fix For Monster Patch Release

Microsoft issued a late set of fixes for the ActiveX control but didn't provide a security rating due to the fact that the update addresses a third party control.

<http://newsletter.varbusiness.com/cgi-bin4/DM/y/eBLF30HoTNf0Elw0GZsZ0EN>

When It Comes to VoIP, Beware Of The Weak Spots

VoIP Security vendor VoIPshield Systems tests for vulnerabilities in Cisco's Call Manager 5.0.

<http://newsletter.varbusiness.com/cgi-bin4/DM/y/eBLF30HoTNf0Elw0GZsl0Ef>

U.K. justice agency lost 45,000 personal records in last fiscal year

In an annual report; the U.K. Ministry of Justice said the personal data of about 45,000 people were exposed in a series of security breaches - some of which weren't disclosed publicly until now.

<http://cwflyris.computerworld.com/t/3471223/8111479/133534/2/>

Opinion: VMware and SSL settings: How to stay safe

Using Secure Socket Layers with virtualization can be a complicated affair. Edward Haletky explains what to look out for.

<http://cwflyris.computerworld.com/t/3471223/8111479/133536/2/>

Microsoft patches, updates Mac Office

The latest release fixes multiple flaws in Excel, Word and Entourage

<http://cwflyris.computerworld.com/t/3471398/8111480/133543/2/>

Internet fraud: lots of complaints, few repercussions

Two groups have released research showing that, despite tens of thousands of complaints by consumers, states rarely bring Internet-related fraud cases to court.

<http://cwflyris.computerworld.com/t/3471550/8111481/133553/2/>

Torvalds: Fed up with 'security circus'

The industry needs a middle ground between vulnerability secrecy and hype, says the creator of the Linux kernel.

<http://cwflyris.computerworld.com/t/3471550/8111481/133555/2/>

Frankly Speaking: Declare war on unsecured Wi-Fi

Find unauthorized Wi-Fi access points on your network and secure them ASAP, warns Frank Hayes.

<http://cwflyris.computerworld.com/t/3471550/8111481/133558/2/>

Sensitive data on 100,000 students exposed by Princeton Review

<http://cwflyris.computerworld.com/t/3479980/341067/133865/2/>

Mac, Windows clipboards poisoned by URL attacks

<http://cwflyris.computerworld.com/t/3479980/341067/133863/2/>

Online encyclopedia lists internal network security threats

<http://cwflyris.computerworld.com/t/3487838/341067/134161/2/>

10 quick fixes for the worst security nightmares

Try these simple solutions for some of the most common security vulnerabilities.

<http://cwflyris.computerworld.com/t/3471550/8111481/133559/2/>

Microsoft Adds ActiveX Fix For Monster Patch Release

Microsoft issued a late set of fixes for the ActiveX control but didn't provide a security rating due to the fact that the update addresses a third party control.

<http://newsletter.varbusiness.com/cgi-bin4/DM/y/eBLH40HoTNf0Elw0GZsZ0EQ>

Cyberwarfare Escalates Between Georgia, Russia

Further fanning the flames of conflict between Georgia and Russia, hackers from both nations continue to launch attacks on the news and governmental Websites in each others countries.

<http://newsletter.crn.com/cgi-bin4/DM/y/eBLIF0HoTNf0EIQ0GZdO0Ef>

Olympic Phishing: 11 Scams To Watch

The phishers and spammers are at it again. And what better vehicle to distribute malware than a highly trafficked, international sporting event like the 2008 Beijing Summer Olympic Games? From the convincing to the inane, here are a few scams to watch for in the next few weeks. Let the games begin.

<http://newsletter.crn.com/cgi-bin4/DM/y/eBLIF0HoTNf0EIQ0GZdN0Ee>

Security gag order against MIT students gets another day in court

A federal judge in Boston will consider whether a restraining order barring three MIT students from talking about security holes they found should be extended or allowed to expire.

<http://cwflyris.computerworld.com/t/3479767/8111479/133845/2/>

WebEx ActiveX Control Buffer Overflow

Upgrading and determining your current version are not straightforward.

<http://ct2.eneews.pcmag.com/rd/cts?d=42-1756-584-956-234345-499002-0-0-0-1-9-269>

Changes to PCI standard not expected to up ante on protecting payment card data

<http://cwflyris.computerworld.com/t/3487838/341067/134156/2/>

Opera patches 7 bugs but keeps one secret

Opera Software patched seven vulnerabilities in its flagship browser but omitted information on one of the fixes, hinting that other software remains at risk from a cross-site scripting vulnerability.

<http://cwflyris.computerworld.com/t/3489214/8111483/134179/2/>

Nokia admits security flaws in Series 40 OS

Nokia confirmed Thursday its widely used Series 40 operating system has security vulnerabilities that could allow activation of stealth applications

<http://cwflyris.computerworld.com/t/3494381/8111480/134436/2/>

SSDs are hot, but come with security risks

Solid-state drives offer more data security than traditional hard drives, but experts caution that they may be prone to hacks and data erasing issues.

<http://cwflyris.computerworld.com/t/3500532/8111479/134678/2/>

Microsoft admits posting flawed update

Microsoft has re-released one of its Aug. 11 security updates, saying it posted an incomplete version to its own download center last week. <http://cwflyris.computerworld.com/t/3500532/8111479/134679/2/>

Brazilian charged in botnet scheme will be extradited to U.S.

A Brazilian man has been charged for trying to broker a deal to rent out a botnet in order to send spam, U.S. authorities said Thursday.

<http://cwflyris.computerworld.com/t/3500532/8111479/134683/2/>



PROTECT POINT
Network Security

Weekly Virus Update

By Christopher Martincavage, ProtectPoint Virus Administrator

The Symantec Threat Index for the week is **Level 1: Normal**.

W32.Rispif.A is a worm that spreads by copying itself to removable and fixed drives from C through Z.

Trojan.Bankpatch.C!inf is a detection for files infected with [Trojan.Bankpatch.C](#).

Bloodhound.Exploit.201 is a heuristic detection for files attempting to exploit the Microsoft PowerPoint List Value Parsing Remote Code Execution Vulnerability ([BID 30579](#)).

W32.Rispif.A

Risk Level 2: Low

Definition: W32.Rispif.A is a worm that spreads by copying itself to removable and fixed drives from C through Z.

Target of Infection: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000

Details:

Once executed, the worm creates some of the following files:

- C:\lo.tmp
- %SYSTEM%\wuauclt.exe
- %SYSTEM%\dllcache\wuauclt.exe
- %SYSTEM%\wsotdet.dll
- %SYSTEM%\wssndet.dll

It spreads across fixed and removable drives from C-Z by creating some of the following files:

- C:\AUTORUN.INF
- C:\RIS.PIF (copy of the worm)
- C:\RVS.PIF (copy of the worm)

The worm creates the following registry entry, so that it runs every time Windows starts:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\explorer\run  
"explorer" = "%System%\wuauclt.exe"
```

It creates the following mutex so only one instance of the worm is running on the compromised computer:

```
CNNLAST
```

It then changes the system date by setting the year back to 2004.

The worm temporarily overwrites the following file to run a kernel mode component:

```
%System%\drivers\beep.sys
```

The kernel mode component is detected as [Hacktool.Rootkit](#) and it uses rootkit functionalities to restore KeServiceDescriptorTable to the original values and disable security software's.

It runs the Windows CACLS.EXE tool to change permissions for the following files and enables the use of WinPCAP libraries to any user on the compromised computer:

- c:\windows\system32\packet.dll
- c:\windows\system32\pthreadVNC.dll
- c:\windows\system32\drivers\npf.sys
- c:\windows\system32\drivers\npptools.dll
- c:\windows\system32\drivers\acpidisk.sys
- c:\windows\system32\drivers\wanpacket

The worm may perform ARP injection or may download a component to do so.

It modifies the following registry entries to disable security programs and tools:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360rpt.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360safe.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360safebox.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\360tray.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ANTIARP.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Ast.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AutoRunKiller.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AvMonitor.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AVP.COM\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\AVP.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\CCenter.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Frameworkservice.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GFUpd.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GuardField.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IceSword.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Iparmor.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KASARP.EXE\debugger = "%System%\dllcache\wuauclt.exe"

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KAVPFW.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kavstart.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kmailmon.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KRegEx.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KVMonxp.KXP\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KVSrvXP.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KWSC.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kwatch.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Mmsk.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msconfig.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Navapsvc.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\nod32krn.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Nod32kui.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RAV.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RavStub.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Regedit.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rfwmain.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rfwProxy.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rfwsrv.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rfwstub.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Runiep.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\safeboxTray.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SREngLdr.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VPC32.EXE\debugger = "%System%\dllcache\wuauclt.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VPTRAY.EXE\debugger = "%System%\dllcache\wuauclt.exe"

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WOPTILITIES.EXE\debugger = "%System%\dllcache\wuauclt.exe"

It tries to end the following processes which may be security-related:

- 360rpt.exe
- 360Safe.exe
- 360tray.exe
- AntiArp.exe
- Avp.exe
- CCenter.exe
- FrameworkService.exe
- GFUpd.exe
- GuardField.exe
- Iparmor.exe
- KASARP.exe
- KAVPFW.EXE
- kavstart.exe
- kmailmon.exe
- KRegEx.exe
- kvsrvxp.exe
- kvsrvxp.kxp
- KVWSC.EXE
- KvXP.kxp
- kwatch.exe
- nod32krn.exe
- nod32kui.exe
- Rav.exe
- RAVMON.exe
- RavStub.exe
- Ravxp.exe
- rfwmain.exe
- rfwProxy.exe
- rfwsrv.exe
- rfwstub.exe
- Runiep.exe
- scan32.exe
- TBMon.exe
- UpdaterUI.exe
- VPC32.exe
- VPTRAY.exe
- VsTskMgr.exe

It tries to delete the following services related to security products:

- KPfwSvc
- KWhatchsvc
- McAfee Framework
- McShield
- Norton Antivirus Server
- Symantec Antivirus
- Symantec Antivirus Definition Watcher
- Symantec Antivirus Drivers Services

It modifies the following registry entry:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL = "2"

It deletes the following registry subkeys to prevent the compromised computer restarting in Safe Mode:

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SafeBoot\Network\{4D36E967-E325-11CE-BFC1-08002BE10318}
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-BFC1-08002BE10318}
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\{4D36E967-E325-11CE-BFC1-08002BE10318}

Users may then experience any of the following messages while trying to restart the computer in Safe Mode:

- blue-screen
- network problems
- error: "STOP: 0x0000007B"

It runs a hidden Internet Explorer windows to download and install the following malicious files:

- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/[REMOVED]
- [http://]m.d5x8.com/dd/10.[REMOVED]

The files are downloaded and saved as the following files:

- C:\Documents and Settings\All Users\1.pif
- C:\Documents and Settings\All Users\2.pif
- C:\Documents and Settings\All Users\3.pif
- C:\Documents and Settings\All Users\4.pif
- C:\Documents and Settings\All Users\5.pif
- C:\Documents and Settings\All Users\6.pif
- C:\Documents and Settings\All Users\7.pif
- C:\Documents and Settings\All Users\8.pif
- C:\Documents and Settings\All Users\9.pif
- C:\Documents and Settings\All Users\10.pif
- C:\Documents and Settings\All Users\ms.pif

Removal:

- Disable System Restore (Windows Me/XP).
- Update the virus definitions.
- Run a full system scan.
- Delete any values added to the registry.

Trojan.Bankpatch.Clinf**Risk Level 1: Very Low**

Definition: Trojan.Bankpatch.Clinf is a detection for files infected with [Trojan.Bankpatch.C](#).

Target of Infection: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000

Details:

Trojan.Bankpatch.Clinf is a detection for the following system files infected with

[Trojan.Bankpatch.C](#):

%System%\kernel32.dll

%System%\powrprof.dll

%System%\wininet.dll

%System%\dllcache\kernel32.dll

%System%\dllcache\powrprof.dll

%System%\dllcache\wininet.dll

Removal:

1. Disable System Restore (Windows Me/XP).
2. Update the virus definitions.
3. Run a full system scan.

Bloodhound.Exploit.201**Risk Level 1: Very Low**

Definition: Bloodhound.Exploit.201 is a heuristic detection for files attempting to exploit the Microsoft PowerPoint List Value Parsing Remote Code Execution Vulnerability ([BID 30579](#)).

CVE References: [CVE-2008-1455](#)

Target of Infection: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000

Details:

Applies to: Microsoft Office.

Removal:

1. Disable System Restore (Windows Me/XP).
2. Update the virus definitions.
3. Run a full system scan.



Weekly IDS Signature Update

By Jamie Gausemel, ProtectPoint SOC Analyst

Common Signatures observed for the week of August 25th, 2008

Signature: POLICY poll.gotomypc.com access (SID/Security Identifier: 1429)

- This event is generated when network traffic indicates GoToMyPC is being used.

How does this exploit work?

- Though not an exploit, GoToMyPC may be used to bypass security measures designed to restrict the flow of corporate information to destinations external to the corporation. This may be a violation of corporate policy.

Possibility of “False Positives” or “False Negatives”

- This is a specific signature for a custom application protocol and so has little chance for false positives.
- False negatives are also unlikely.

Preventive Measures or Corrective Actions

- Ensure adherence to best security practices and strict adherence to corporate policy.

Signature: POLICY PCAnywhere server response (SID/Security Identifier: 566)

4. This event is generated when network traffic indicates PCAnywhere is being used.

How does this exploit work?

4. Though not an exploit, PCAnywhere may be used to bypass security measures designed to restrict the flow of corporate information to destinations external to the corporation. This may be a violation of corporate policy.

Possibility of “False Positives” or “False Negatives”

5. This is a specific signature for a custom application protocol and so has little chance for false positives.
6. False negatives are also unlikely.

Preventive Measures or Corrective Actions

- Ensure adherence to best security practices and strict adherence to corporate policy.
-