

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

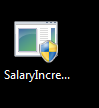
**Tools Used:**

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

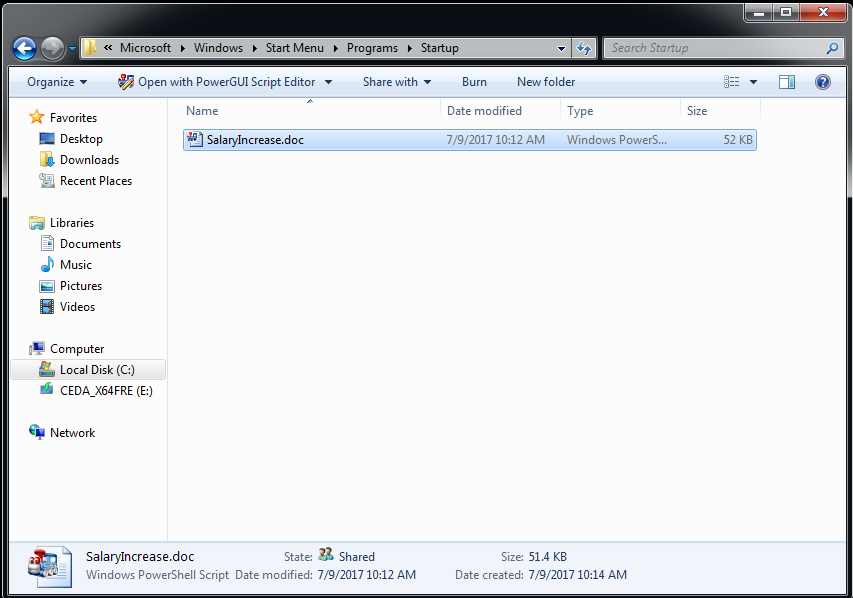
The C2 server here is hosted on **000webhost.com**. The script itself is quasi-stealthy. I didn’t have enough resources to test all the functionalities it offers on VM on Windows 10, so some might not be working properly.

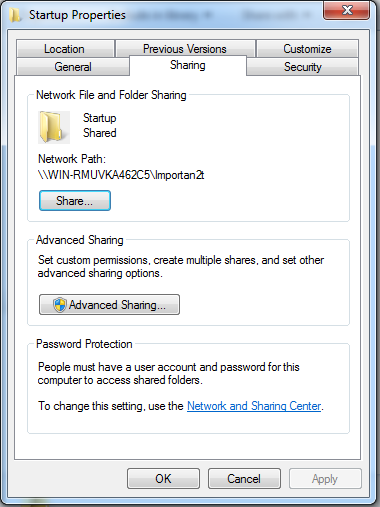
**Basic Flow:**

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



1. 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.



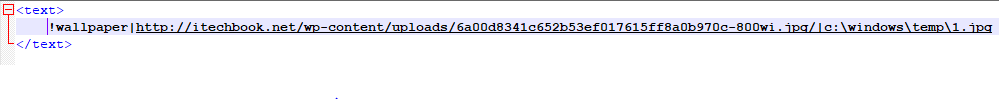


1. Script’s name is SalaryIncrease and it’s been **disguised as a doc file** to attract users to click on it.
2. Now, since the script has been copied into the Startup folder, this will execute the next time any user starts this system
3. It **communicates with the server** using special commands. Like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

A screenshot of a social media post

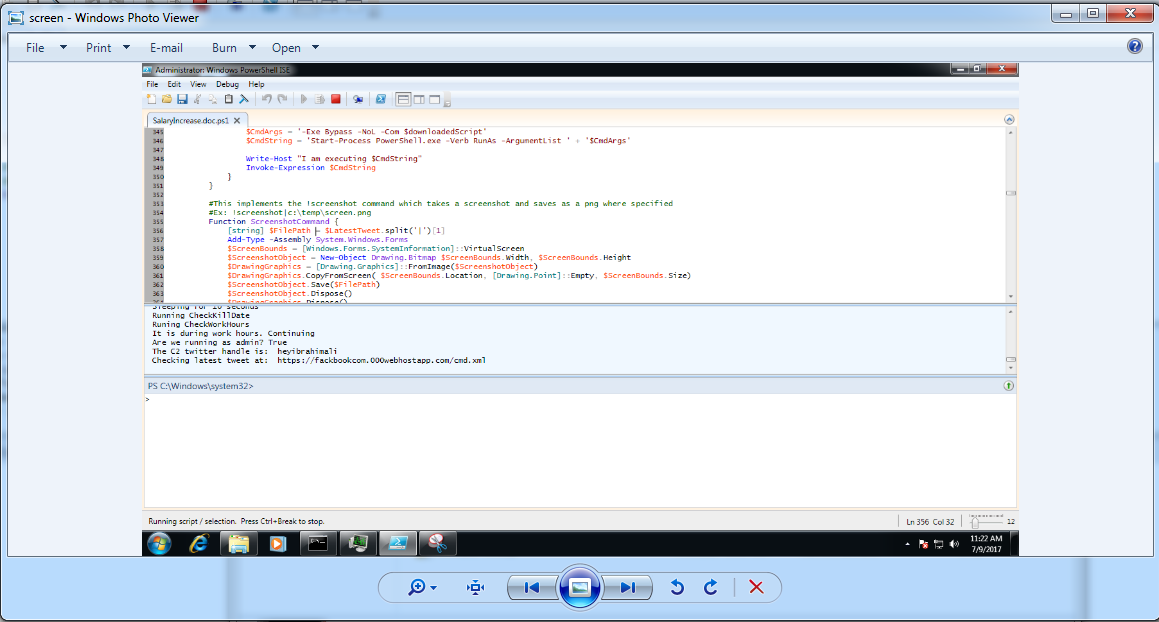
Description generated with very high confidence

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

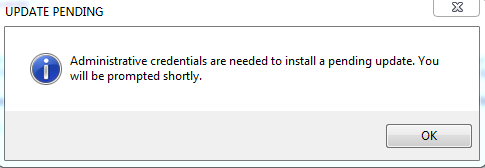


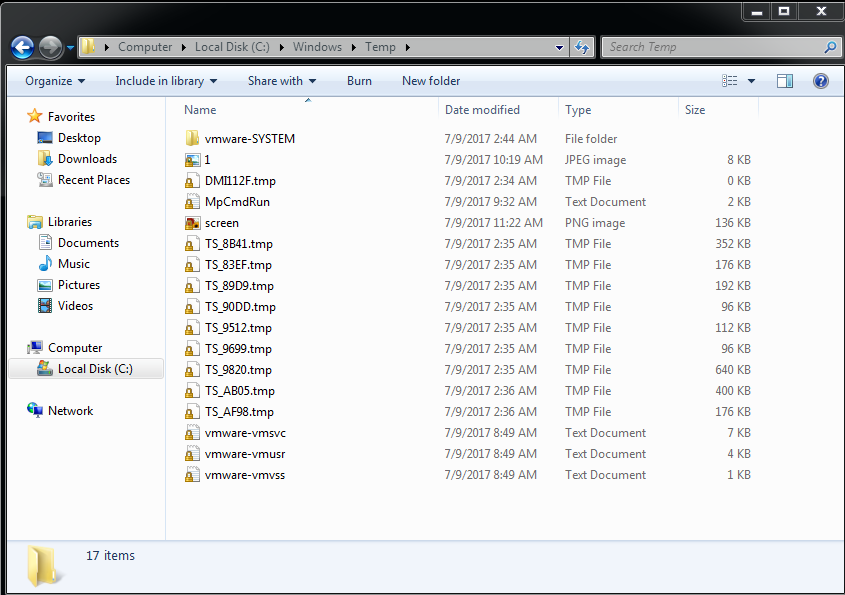
**List of commands that are working:**

* Screenshot



* sleep
* popup



* wallpaper****
* speak
* thunderstruck