Q and A

```
Q1 - attacker use many C2 server , but use persistence Tactic for just one server , what is the IP of this server?
A:192.92.250.65 (wo12.py)
```

```
Q3 - attacker creates Backdoor User, what is the username and password :
answer format : username&password
A:blackcat&JapanNight123
```

```
Q4 - How many minutes require before forcing an immediate reboot （after you run the executable)
A:10
```

```
Q5 - what is the Key used in AES-encrypted file (service_probes.aes)
A:62bee40fb0bfdb424117610ecc4480e8
```

```
Q6 - How many minutes require before launching the ransomware, clearing the logs （after you run the executable)
A:1
```

```
Q7 - what is the name of file which contain ransomware note
A:RECOVER-wragz12-FILES.txt
```

```
Q8 - attacker use many C2 server , but using 2 constant ports , what is the ports?
answer format : Port1&Port2
A:443&8443
```

```
Q9 - what is the Sha-1 of the Advanced_IP_scanner.exe
A: 86233a285363c2a6863bf642deab7e20f062b8eb
```