October 12, 2012

Malware

New Multiplatform Backdoor Jacksbot Discovered

Posted on October 12th, 2012 by Lysa Myers 

Update – October 15, 2012

Upon further analysis, it's been determined that this trojan is the Java RAT (aka jRAT) created by the hacker/programmer redpois0n.

A new Java backdoor trojan called Java/Jacksbot.A has been discovered that has partial multiplatform support. It is fully functional on Windows, and partially functional on OS X and Linux. This trojan is currently considered low risk as it is not known to have infected users, and it does not run without root permissions. Jacksbot has the usual backdoor functionality, including the following capabilities:

- gathering system information
- taking screenshots
- performing denial of service attacks
- deleting files
- stealing passwords (including specifically Minecraft passwords)
- visiting remote URLs, likely to perform Clickfraud

```
  localObject21 = System.getenv("APPDATA");
  if (localObject21 != null)
    localObject16 = new File((String)localObject21, ".minecraft");
  else
    localObject16 = new File((String)localObject10, ".minecraft");
}
else if (((String)localObject5).contains("mac"))
{
```

This code is looking for Minecraft passwords.

It appears likely that this trojan is intended to be dropped by another component that has not yet been identified. The present component will exit with an error message if the Java archive is not run with root permissions. There is also no functionality to trick the user into running the file. We will post additional information about the threat as more is discovered.

Intego VirusBarrier users with up-to-date virus definitions are protected from this threat, which is detected as Java/Jacksbot.A.