Flashback Trojan for Macs

Nathan Paulson

April 18, 2012

OS X Historically

1. Considerably less problems with malware than Windows.
   1. Unix based.
   2. Less market share.
2. Selling point for Apple : "with virtually no effort on your part, OS X defends against viruses and other malicious applications, or malware"
3. Users likely are less careful about security issues.

Beginning of the End

1. Sami Koivu reports a vulnerability with Java around December and Oracle patches it for Windows users by February.
2. Apple doesn't allow Oracle to patch Java for Macs
3. Apple doesn't release patch until the first week of April.

Flashback Trojan hits

1. More than a four month window to exploit the Java vulnerability.

Flashback Trojan hits

1. More than a four month window to exploit the Java vulnerability.
2. By the time the patch is released by Apple, 600,000 OS X users are infected.

Flashback Trojan hits

1. More than a four month window to exploit the Java vulnerability.
2. By the time the patch is released by Apple, 600,000 OS X users are infected.
3. First large scale infection in OS X history.

About the Trojan

1. Infects users that visit malicious/infected websites with Java enabled.
2. Botnet is created with infected users.
    1. Different purpose than most Trojans/Botnets : Click Fraud

Things to be afraid of:

```
/Library/Little Snitch
/Applications/Xcode.app/Contents/MacOS/Xcode
/Applications/VirusBarrier X6.app
/Applications/iAntiVirus/iAntiVirus.app
/Applications/avast!.app
/Applications/ClamXav.app
/Applications/HTTPScoop.app
/Applications/Packet Peeper.app
```

Catching On

1. Botnet is controlled entirely through different Command and Control servers.
2. Security firm Dr. Web monitors these servers and lets Apple know what's happening.
3. Counts unique IDs with sinkholing

Apple's Response

1. Apple finally releases the necessary Java update
2. Apple works with ISPs to shut down C&C servers
3. Multiple security firms release programs to test for and remove the Flashback Trojan.
4. Numbers have already dropped below 250,000 and a final security update was just released by Apple.

Apple's Responsibility

1. Apple's delayed patch is not unusual
2. Flashback's success means future attacks are more likely
3. Growing market share means more responsibility

References

http://waxy.org/2012/04/flashback_trojan_creators_scared_of_xcode_users_but_not_norton_antivir

http://www.telegraph.co.uk/technology/apple/9201908/Apple-Flashback-virus-outbreak-tackled.html

http://www.macworld.com/article/1166254/what_you_need_to_know_about_the_flashback_trojan.htmll

http://en.citizendium.org/wiki/Sinkhole_(Computer_network)

http://www.macworld.com/article/1140704/java_vulnerability.html