SNEAK ATTACKS USED BY TODAYS MOST DEVIOUS HACKERS

*Based on an article by **Roger A Grimes** in InfoWorld, ComputerWorld, and NetworkWorld*

Robert W. (Bob) Hodges - BBA, CISSP, GCIH, GSEC Gold, GSLC Gold
President ISSA-Yorktown Chapter
Systems Security Administrator Colonial Williamsburg Foundation

January 14, 2014

SNEAK ATTACKS USED BY TODAYS MOST DEVIOUS HACKERS

*Based on an article by **Roger A Grimes** in InfoWorld, ComputerWorld, and NetworkWorld*

Robert W. (Bob) Hodges - BBA, CISSP, GCIH, GSEC Gold, GSLC Gold
President ISSA-Yorktown Chapter
Systems Security Administrator Colonial Williamsburg Foundation

January 14, 2014

Think of all the times you -- or your users -- have gone to the local coffee shop, airport, or public gathering place and connected to the "free wireless" network. Hackers at Starbucks who call their fake WAP "Starbucks Wireless Network" or at the Atlanta airport call it "Atlanta Airport Free Wireless" have all sorts of people connecting to their computer in minutes.

Stealth attack No. 1: Fake wireless access points

http://hakshop.myshopify.com/products/wifi-pineapple

Stealth attack No. 1: Fake wireless access points

- **The WiFi Pineapple Mark V** is the latest generation wireless network auditing tool from **Hak5**. With its custom, purpose built hardware and software, the WiFi Pineapple enable users to quickly and easily deploy advanced attacks using our intuitive web interface.
- From a man-in-the-middle hot-spot honeypot to an out-of-band pentest pivot box, the WiFi Pineapple is unmatched in performance, value and versatility.

Stealth attack No. 1: Fake wireless access points

- ***Lesson:*** *You can't trust public wireless access points. Always protect confidential information sent over a wireless network. Consider using a VPN connection, which protects all your communications, and don't recycle passwords between public and private sites.*

Stealth attack No. 1: Fake wireless access points

Stealth attack No. 2: Cookie theft

- Browser cookies are a wonderful invention that preserves "state" when a user navigates a website.
- When a hacker steals our cookies, and by virtue of doing so, becomes us -- an increasingly frequent occurrence these days.
- They become authenticated to our websites as if they were us and had supplied a valid log-on name and password.

Stealth attack No. 2: Cookie theft

- **Firesheep**
  - Countered by using HTTPS, a virtual private network (VPN) connection, or using wireless security
- **Beast**
  - You really aren't fully protected unless you disable all other HTTPS protocols prior to TLS 1.1 and 1.2.
  - HTTPS websites should be using the latest crypto, including TLS Version 1.2.

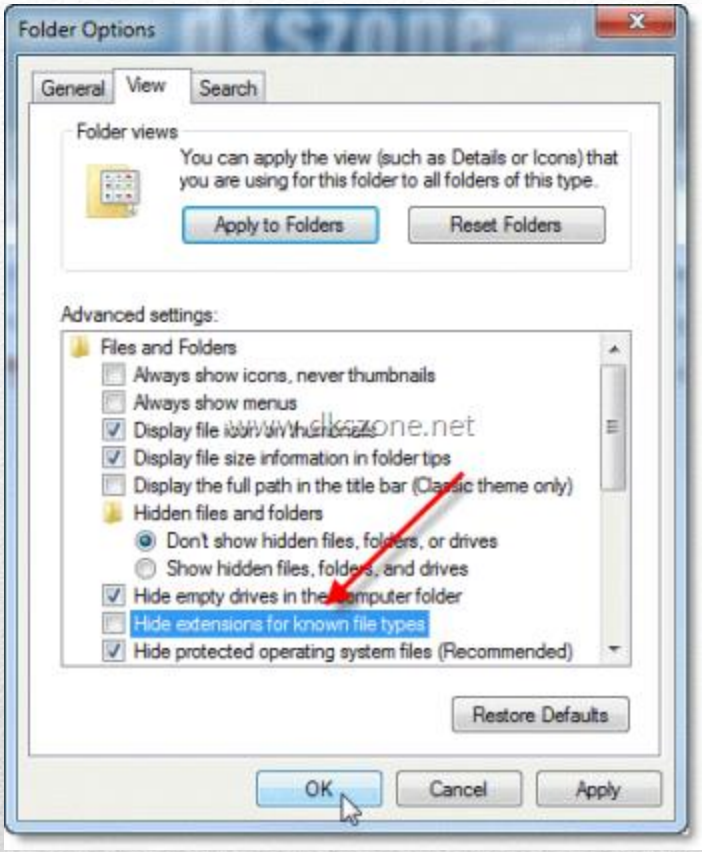
Stealth attack No. 2: Cookie theft

- ***Lessons:*** *Even encrypted cookies can be stolen. Connect to websites that utilize secure development techniques and the latest crypto. Your HTTPS websites should be using the latest crypto, including TLS Version 1.2.*

Stealth attack No. 2: Cookie theft

Stealth attack No. 3: File name tricks

- **Double extensions**
  - KatyPerryNudePics.Zip.exe
  - Windows sees by default as KatyPerryNudePics.Zip
- **.COM v. .EXE**
  - CMD.exe = Command shell in windows
  - Copy CALC.exe to CMD.COM
  - Run CMD in start/run and it brings up a calculator.



Stealth attack No. 3: File name tricks

- Unicode character (U+202E), called the Right to Left Override
- It could make an .EXE look like an .AVI extension

Stealth attack No. 3: File name tricks

- ***Lesson:*** *Whenever possible, make sure you know the real, complete name of any file before executing it.*

Stealth attack No. 4: Location, location, location

- **“Relative versus Absolute“ file paths.**
- Malware could create a malicious file called calc.exe and hide it in the current directory or your home folder; when you try to execute calc.exe, it would run the bogus copy instead.

Stealth attack No. 4: Location, location, location

- ***Lesson:*** *Use operating systems that enforce absolute directory and folder paths, and look for files in default system areas first.*

- C:\Windows\System32\Drivers\Etc**HOSTS**

1. The client checks to see if the name queried is its own.
2. The client then searches a local Hosts file, a list of IP address and names stored on the local computer.
3. Domain Name System (DNS) servers are queried.
4. If the name is still not resolved, NetBIOS name resolution sequence is used as a backup. This order can be changed by configuring the NetBIOS node type of the client.

Stealth attack No. 5: Hosts file redirect

- ***Lesson:*** *If you can't figure out why you're being maliciously redirected, check out your Hosts file.*

Stealth attack No. 5: Hosts file redirect

Stealth attack No. 6: Waterhole attacks

- **Poison the Waterhole Example:**

A Web page visitor counter containing a simple URL that loaded a small logo along with the applet. The author's open source contract said that anyone could use and modify the applet as needed, as long as the URL was left intact in original form without modification. Harmless enough. Then one day the URL pointing to the logo graphic ended up pointing to a JavaScript redirection link instead, which prompted visiting users to install malware. Tens of thousands of users were instantly infected on their next visit.

Stealth attack No. 6: Waterhole attacks

- ***Lesson:*** *Make sure your employees realize that popular "watering holes" are common hacker targets.*

Stealth attack No. 7: Bait and switch

- Victims are told they are downloading or running one thing, and temporarily they are, but it is then switched out with a malicious item.

Stealth attack No. 7: Bait and switch

- **Examples:**
- Free Scan of your PC!
- Poisoned search results
- **FakeAlert.D** often takes the form of an unsuspecting pop-up that tries to warn you of a serious issue: malware has been detected!
- **Typosquatting:**
  - goole.com
  - g00gle.com

Stealth attack No. 7: Bait and switch

- ***Lesson:*** *Beware of any link to any content not under your direct control because it can be switched out on a moment's notice without your consent.*

- *When a hacker modifies your system in a stealthy way, it isn't your system anymore -- it belongs to the hackers.*

Roger A. Grimes

C 16. Mental break time. This is your last regular (non-final) test of the year. You deserve an easy question. What is 1 + 1?

a. Not this one
b. Still not this one
c. 2
d. You've gone too far, go back to C.