

Late-Breaking Computer Attack Vectors



PaulDotCom Enterprises, LLC

November 2008

Larry Pesce

PaulDotCom Enterprises, LLC

larry@pauldotcom.com

Introduction

- Grey Hat + Larry = haxorthematrix
- PaulDotCom Security Weekly
- Penetration Testing, Security Consulting, Device Testing
- WRT54G Hacking book & others...



PaulDotCom Security Weekly
<http://www.pauldotcom.com>

Outline

- PDF Javascript and E-mail attachments, oh my!
- Need Credentials? Just ask!
- Metasploit 3.2
- Information gathering with Metadata
- WPA/TKIP Cracking
- FAIL Of The Month (FOTM)

“...hacking is the action of outsmarting the others and as such it may take any form”

- pdp, gnucitizen.org

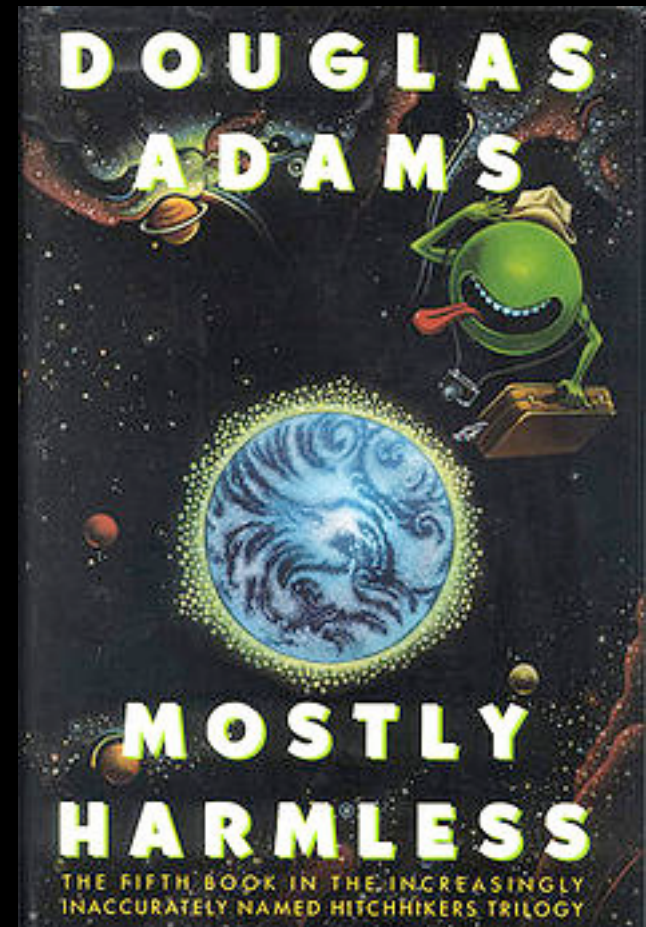
Exploit via PDF

- Who lets PDF documents in?
 - Download from web
 - E-mail
 - Compare this to other document types



So long, and thanks for all the fish.

- Most think PDF is “mostly harmless”
 - No macros
 - Not executable
 - ...but can execute javascript!



Filter!

- Consider adjusting e-mail attachment filters
 - ...but needed for operations
 - sanitized repository, mimedefang?
- Download via browser
 - GPO policies
 - Of course, UPDATE CLIENTS!



Metasploit 3.2



- Updated License to BSD
- Unbelievable new features
- Attackers will use it, and so should you!
- Get it. Use it. Love it.

New features!



- Web application testing
- Token manipulation support
- Improved AV evasion techniques
- Improved post exploitation techniques

But wait, there is more!

- METASM
- browser_autopwn
- Reflexive DLL injection
- scraper.rb



METASPLOIT

Now how much would you pay?



- Significant updates to the licensing model
- BSD based
- Open for use in commercial products
- Opens the door for additional improvements, modules and exploits.

Information gathering with Metadata

- Let's gather some usernames from Office documents
 - .doc, .ppt and .xls
- Several tools available
 - Maltego
 - Metagoofil
 - How about wget and EXIFtool?



EXIFtool, not just for JPEGs anymore!

- Office document Metadata storage based on the FlashPix standard
- Output in a nice, readable, HTML report
- Unknown (by me) compatibility with Office 2007 documents
 - Not everyone upgrades right away
- Give it a go on a directory of documents

```
exiftool -r -h -a -u -g1 * >output.html
```

Mining the goods

- Re-run EXIFtool with limited output

```
exiftool -r -a -Author -LastSavedBy * >users.txt
```

- Add some Unix text processing-fu

```
strings users.txt | cut -d":" -f2 | grep -v "\=" | grep -v \  
"image files read" | tr '[:space:]' '\n' | sort | uniq \  
>cleanusers.txt
```

- Take the final list and manually remove “odd names”
- Even more text processing could incorporate more names



Preventing exposure

- On the internet already?
- Clean up what you can and create a sanitized “store”
- Segregation of publishing duties
- Regular audits!



Basic Auditing



- Look at your own website(s)
- Repeat at regular intervals and compare differences
- How about a shell script?
 - Uses metagoofil, wget and EXIFtool
 - Analyzes Office documents and JPEGs
 - E-mails results

<http://www.pauldotcom.com/getmeta.sh>

WPA/TKIP Cracking

- Cracking client communication with WPA/TKIP combination.
 - ~12 - 15 minutes, does not reveal keys
- Released by Erik Tews at PacSec (mid-November)
- Specific combinations affected
 - WPA or WPA2 with TKIP and QoS
 - PSK and Dot1X implementations

How it works

- Capture TKIP packet (ARP)
- Drop last payload byte
 - breaks ICV and MIC.
 - fix ICV and send
- AP drops all but one with good ICV and bad MIC triggers countermeasures
 - this reveals correct ICV for that one byte
- Wait 60 seconds, try next previous byte
- Josh Wright's fabulous webcast slides and audio



<https://www.sans.org/webcasts/show.php?webcastid=92188>

Defensive measures

- Don't use wireless!
- Disable wireless QoS
- Migrate to AES-CCMP instead of TKIP
- Can and string?



FAIL Of The Month (FOTM)

- Hi! Your distant relative is in trouble in Nigeria and needs \$100...
- \$100, OK. Shame on me.
- Retirement, new mortgage and car loan. \$400,000! Shame on you.
- User education? You can lead a horse...



/* End */

- Web: <http://pauldotcom.com/>
- Wiki: <http://pauldotcom.com/wiki/> - Show notes for each episode
- Forum: <http://forum.pauldotcom.com>
- Email: larry@pauldotcom.com



PaulDotCom Enterprises, LLC

