

Late Breaking  
Computer Attack Vectors  
March 25, 2009



---

PaulDotCom Enterprises, LLC



---

PaulDotCom Enterprises, LLC

## Synopsis

This lively session will discuss recent and anticipated computer and network attack vectors, highlighting the current trends in information security and hacking. For each attack vector, we will look at practical, real-world solutions for stemming the tide and keeping your network a safer place.

This webcast is hosted by Mick Douglas.

The webcast is being recorded and a link to that recording will be available to all who have registered.

## Vendor Involvement

We are fortunate today to have this webcast sponsored by Thawte.

There is a live opportunity for Q&A from the audience.

# About me

Mick Douglas

PaulDotCom Enterprises, LLC

[mick@pauldotcom.com](mailto:mick@pauldotcom.com)

---

- Curiosity + evil thoughts + good deeds = Mick
- Sr. Systems Engineer for InfoSec at OCLC
- Member of PaulDotCom crew
- Mentor instructor for SANS 504 & 507



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



# Introduction

---

- PDC: It's a website – but so much more!!
- PaulDotCom Security Weekly Podcast
- Penetration Testing, Security Consulting, Device Testing
- Forum, IRC, Hack Naked TV, Wiki, Mailing List

# Outline

---

- Rogue DHCP server malware
- PDFs that strike without warning
- DLP 101
- Welcome back L0phtCrack – I missed ya!
- PaulDotCom's Top 5 Defensive Recommendations for March

# Rogue DHCP server malware

---

- Flush.M - DHCP hijacker you'll love to hate!
  - Redirects DHCP & DNS traffic for entire networks
- Why should I care?
  - Anyone not use DHCP?
  - You use DNS for everything.
  - Level of sophistication is high... so should your concern.

# Don't get "Flushed" down

---

- Steps to take:
  - Watch for rogue DHCP servers
  - Check for DNS traffic going directly to DNS servers that aren't under your control
  - Keep up to date Anti-Virus protections



# PDF exploit – user interaction *\*not\** needed

---

- JBIG2Decode bug

- Triggers anytime meta data is accessed
- Grants SYSTEM level access



- Why should I care?

- Google Desktop
- Windows indexing service
- Windows desktop search (not a total loss – but still bad!)

# PDF exploit – what to do

---

- Know thy files
- Anti-Virus
- Train end-users and admins
- Uninstall IFilter features

# DLP 101

---

- Data Leakage/Loss Prevention/Protection
- Strict access controls on data
  - Once the horse has left the barn...
  - Audit access for important data
- You do have a data inventory, right?
- What's your policy? When was it last updated? Does it include new tech?

# DLP 101 Continued

---

- Attacks have been shifting to this as an end game
- Know the “ins” and “outs” for data
  - Where does it flow?
  - How?
  - Who?
- Your managers should love you for this!

# LC6 – The return of L0phtCrack

---

- Welcome back you old scoundrel!
- Are you safe from password crackers?
  - Do your passwords age?
  - Are they long & complex enough?
  - Do you try cracking your own passwords?

# PaulDotCom's Top 5 Defensive Recommendations

---

1. Defense in depth on hosts is needed too! A/V is only the start. Remember you need malware detectors & host based firewalls!
2. Watch your logs, act on anomalies.
3. Look for rogue systems on your network.
4. Conduct regular “radar” vulnerability assessments. Act on findings!
5. Keep up with user awareness training, make it fun for them and you too!

# Thanks!

---

Thank you to our vendor sponsor, Thawte. Without their involvement we would not be able to bring you great content like this.

Hope you had fun!

Fire away with your questions!

`/* End */`

---

- Presentations: <http://pauldotcom.com/presentations.html>
- Forum: <http://forum.pauldotcom.com/viewforum.php?id=17>
  - Special category just for this webcast series!
- Email: [mick@pauldotcom.com](mailto:mick@pauldotcom.com)