

Late-Breaking Computer Attack Vectors



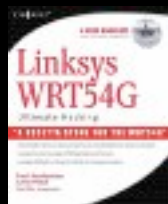
PaulDotCom Enterprises, LLC

January 2009
Larry Pesce
PaulDotCom Enterprises, LLC
larry@pauldotcom.com

Wednesday, March 11, 2009

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>



PaulDotCom Security Weekly

<http://pauldotcom.com>

January 2009

Wednesday, March 11, 2009

Outline

- SSL Certificate collisions
- Cisco cross platform attack code
- Multiple Attack Vectors
- Password abuses
- FAIL Of The Month (FOTM)

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

- pdp, gnucitizen.org

SSL MD5 Collisions

- Research released at 25C3
 - Illustrates method for MD5 collisions with SSL
 - Only CAs using MD5 affected
 - Need to predict serial number



Show me the money!

- Expensive attack?
 - Took lots tries to get the serial number guessed properly
 - 200 PS3s for computation
- A small investment for large returns?
 - Under \$1000 for guesses
 - How about renting a botnet?



The end result...

- Ability to create a rogue CA
 - Can sign certs in a vacuum.
 - End up as valid in the browser
 - How many CAs are listed in your browser?
 - How many do you need?
- Now signing with more valid methods is possible!



Cisco IOS Attacks

- Released by FX of Phenoelit at 25C3
 - Exploit for multiple hardware platforms
 - Exploit for multiple IOS versions
 - Now combine the two!
- Only on 1500 and 2700 series currently
- PPC platform

Needle in a Haystack

- Previously only one at a time
 - ~100,000 IOS versions ~15,000 supported
 - Each exploit coded individually
- A wrong guess forced a router reload
 - I wonder who will notice that?
- Chances of guessing correctly ~1 in 100,000



One to rule them all

- Use something that is relatively static
- ROMMON!
 - Significantly fewer versions
 - Not (easily) upgradable
 - Supports all of the features needed
 - Exploit now can run regardless of IOS version and



Gandalf's army?

- Exploit interaction?
 - Requires some level of connectivity
 - Practice defense in depth
 - filter traffic on the device
 - filter up stream and down stream as well!



Attacks with Multiple Vectors

- Traditional is one to one
 - One attack, one exploit
- Downadup/Conficker uses multiple methods to spread.
- The attackers are getting smart!



Downadup/Conficker

- What makes this so special?
- Uses 4 different attack vectors
 - Exploits local network for MS08-067
 - Propagates to open shares on local network
 - Probes local network for weak admin passwords
 - Infects USB drives with Autorun



Fighting on Multiple Fronts

- Updated AV Signatures
- Apply Windows patches
 - prevents connection to windows update!
- Close open shares, require authentication
- Enforce good password policies
- Disable Autorun
- Disable USB thumb drive support
- These are reasons Defense in Depth makes sense!



Wednesday, March 11, 2009

Only as good as sigs, blocks connection to AV vendors and windows update. Password complexity and frequent change

consider SCCM, SMS or gpo for patches and auto run

Password Abuses

- Continual, ongoing problem!
 - Windows domains
 - Websites
 - Consumer devices
- Not just the bad ones we set ourselves, what about defaults and “hidden” ones
- A tie in to our FOTM



Good policies?

- How about...
 - Complexity rules
 - Account lockout
 - Passphrase
 - Two factor
 - Token, Proximity, Biometric
 - Testing!



Testing with THC-Hydra

- Available from <http://freeworld.thc.org/thc-hydra/>
- Password wordlist attacks on multiple services
 - plain text and encrypted services
- Password lists
 - not included, but limited free ones exist
 - John the Ripper: <http://www.openwall.com/mirrors/>
- Custom wordlists (user and password)
 - Custom password lists: <http://www.pauldotcom.com/wiki/index.php/Episode129>
 - Custom user lists: <http://pauldotcom.com/2008/12/creating-custom-userlists-from.html>



HTTPS Example

- Form analysis
 - View source, find post method and fields

```
Authorized access only!</p>
<form method="post" action="/login_post.yaws" name="f" target="_
<table cellpadding="5">
<tr>
<td valign="top">
<p class="black_bread">Login Status:</p></td>
<td nowrap><em class="black_bread"><font color="red">not logged
<tr>
<td>
<p class="black_bread">Username:</p></td>
<td><input name="user" type="text" size="20"></td></tr>
<tr>
<td>
<p class="black_bread">Password:</p></td>
<td><input name="password" type="password" size="20"></td></tr>
<tr>
```

- Find text to indicate login failure

Login Status: *not logged in
bad password or user*

Off we go!

- Test it!

- Single user and password

```
./hydra -s 443 -l <user> -p <password> -t 36 -m /login_post.php?  
user=^USER^&password=^PASS^&login=Login:password or user -V  
example.com https-post-form
```

- Password and user list

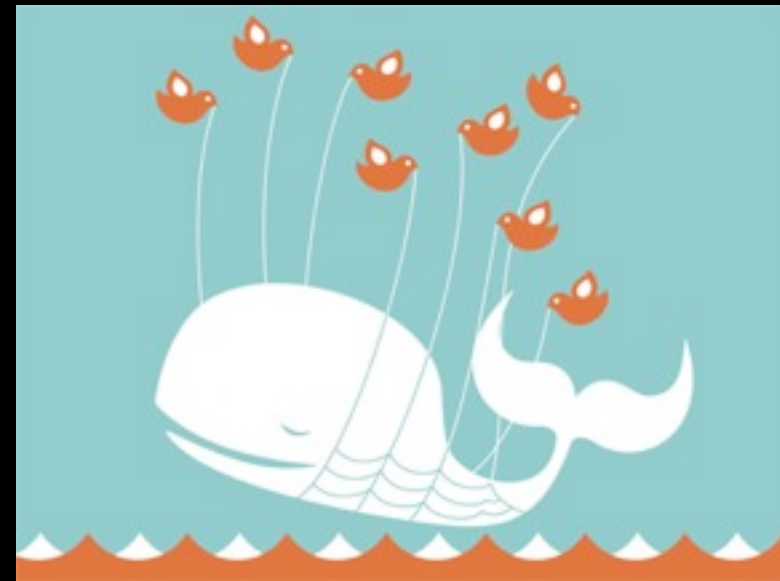
```
./hydra -s 443 -L <user list> -P <password list> -e -t 36 -m /  
login_post.php?user=^USER^&password=^PASS^&login=Login:password  
or user -V example.com https-post-form
```

-s port
-l single user
-p single password
-t # of threads
-m website path - login_post.php?<variable>=^USER^ for username ...etc
&login=Login:<text on failure page>
-V verbose
https=post-form = method

-L
-P
-e Try user as password

FAIL Of The Month (FOTM)

- Twitter Passwords!
 - Can you say “Fail Whale”?
- Allowed for weak passwords
- No account lockout
 - Brute force possible!
- Administrative interface exposed publicly!
- Wrote tool, 12 hour run, found happiness



/* 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



<http://pauldotcom.com>

January 2009

Wednesday, March 11, 2009