# Symantec's pcAnywhere Hacked

Ryan Mahin

CS466: Computer Security

February 22, 2012

# Introduction

pcAnywhere is a program by Symantec that allows the user of the program to connect to a personal computer anywhere so long as they are both connected to the internet.

# Hacked

Last month Symantec issued a warning to stop using their product until a patch is released.

# Six Years Ago

- Source code of product was exposed in 2006 hack

# Six Years Ago

- Source code of product was exposed in 2006 hack
- Could potentially allow remote code execution and other MITM attacks.

# Six Years Ago

- Source code of product was exposed in 2006 hack
- Could potentially allow remote code execution and other MITM attacks.
- "Honestly, the toughest part of incident response is being able to tell what the bad guy took" -Six-Year-Old Breach Comes Back To Haunt Symantec

# Six Years Ago

- Source code of product was exposed in 2006 hack
- Could potentially allow remote code execution and other MITM attacks.
- "Honestly, the toughest part of incident response is being able to tell what the bad guy took" -Six-Year-Old Breach Comes Back To Haunt Symantec
- Nothing was done because all investigation of the produced inconclusive results at the time.

# Extortion

- Hacker, YamaTough (affiliated with Anonymous), attempts to extort Symantec


Figure: Twitter profile

# Extortion

- Hacker, YamaTough (affiliated with Anonymous), attempts to extort Symantec


Figure: Twitter profile

- Exchange emails for about a month.

# Example

2012/1/25 yamatough yamatough@terra.com.ve
If we dont hear from you in 30m we make an official announcement and put your code on sale at auction terms. We have many people who are willing to get your code Dont fuck with us
Sam Thomas sam.thomas.sym@gmail.com 25 January 2012, 23:49:38
We are not trying to trick you. You said you had the PC Anywhere code and we were just being cautious. What would you have us do? We really don't want our code out there. How do you want to proceed.

# Result

**Symantec's pcAnywhere Leaked Source Code**

| | |
|---|---|
| Type: | Other > Other |
| Files: | 1 |
| Size: | 1.27 GiB (1368783787 Bytes) |
| Tag(s): | antisec anonymous leak source |
| Quality: | +32 / -0 (+32) |
| Uploaded: | 2012-02-07 05:40:04 GMT |
| By: | stun |
| Seeders: | 208 |
| Leechers: | 4 |
| Comments | 25 |


Figure: The Pirate Bay

# First attack

- Two weeks later, a DOS python script is created.

# First attack

- Two weeks later, a DOS python script is created.

```
!/usr/bin/python

'''
Exploit Title:  PCAnywhere Nuke
Date: 2/16/12
Author: Johnathan Norman  spoofy <at> exploitscience.org  or @spoofyroot
Version:  PCAnyWhere  (12.5.0 build 463) and below
Tested on: Windows
Description: The following code will crash the awhost32 service. It'll be respawned
so if you want to be a real  pain you'll need to loop this.. my initial impressions
are that controlling execution will be a pain.
'''
```

Figure: Only 40 lines

# Symantec Takes Action

- Identified two serious problems:

# Symantec Takes Action

- Identified two serious problems:
  - Improper validating/filtering with Symantec host services on a specific port.

# Symantec Takes Action

- Identified two serious problems:
  - Improper validating/filtering with Symantec host services on a specific port.
  - Files uploaded during installation were writable by all users.

# Symantec Takes Action

- Identified two serious problems:
  - Improper validating/filtering with Symantec host services on a specific port.
  - Files uploaded during installation were writable by all users.
- Issued numerous security patches.

# Symantec Takes Action

- Identified two serious problems:
  - Improper validating/filtering with Symantec host services on a specific port.
  - Files uploaded during installation were writable by all users.
- Issued numerous security patches.
- "Symantec is not aware of any customers impacted by this issue, or of any attempts to exploit it in the wild." Symantec Security Advisory

# Not a whole lot they can do...

- Source code of current products is almost identical to the 2006 products.

# Not a whole lot they can do...

- Source code of current products is almost identical to the 2006 products.
- Hackers now know pretty much all the inner workings of pcAnywhere, along with Symantec's Live Update system.

# Not a whole lot they can do...

- Source code of current products is almost identical to the 2006 products.
- Hackers now know pretty much all the inner workings of pcAnywhere, along with Symantec's Live Update system.
- "The only hope for Symantec and pcAnywhere is that these days users typically do not run their home or office computers with the ports required for this product open to the Internet" Remote Attack Code Surfaces

# Sources

http://www.darkreading.com/advanced-threats/167901091/security/news/232500587/six-year-old-breach-comes-back-to-haunt-symantec.html?itc=edit_in_body_cross

http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232600404/hackers-post-symantec-source-code-after-failed-extortion-attempt.html

http://pastebin.com/2x8qZrWA https://thepiratebay.se/torrent/7014253

http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012&suid=20120124_00 http://www.informationweek.com/news/security/vulnerabilities/232601182?cid=InformationWeek-Twitter#comments http://pastebin.com/VXkWDM6A

http://twitter.com/#!/yamatough