What Do Phishing, Defense Contractors, and Metasploit Have in Common?

August, 2009

Patrick Cain

Research Fellow
APWG
pcain@antiphishing.org

President
The Cooper-Cain Group, Inc.
pcain@coopercain.com

- Absolutely nothing….

  …But a story NOW…

Not “Defense Contractors” – DEFCON!

DEFCON

BETA

- **Community**
  Hackers Unite
- **About**
  Who We Are, What We Do
- **Resources**
  Hacker Brain Food
- **The Hard Drive**
  DEFCON Preserved
- **Blogs**
  Musings of DT & Community

DEFCON 17 Post-con News

The DEFCON 17 Receipt of Admission is now posted! Be sure to share your photos from the con to pics.defcon.org, and keep your eyes peeled for contest results, presentations, press, and other post-con material coming soon!

DEFCON Qik Feed

You can go to the DEFCON Qik Feed or our Qik group and check out what we and group members filmed live during DEFCON 17!

DEFCON 17 took place July 30 - August 2nd, 2009 at the Riviera Hotel & Casino in Las Vegas! DEFCON 18 will happen July 29th - August 1, 2010!

Upload all of your DEFCON 17 Photos to pics.defcon.org

Help to preserve and share those DEFCON 17 memories on pics.defcon.org! If you have a DEFCON Forums account, you already have a pics account, just use the same login information. While you're at it, submit your galleries to defconpics.org as well!

Hacker Gatherings

DC405 Meeting - 8/21/09 - 7p@OKCCoCo
(Posted By: m00dimus)

Anyone interested in a DC979?
(Posted By: maker)

Show up to the next DEFCON event this month!

Agenda

- Introduction
- Some eCrime Trends
- “I went to Defcon and all I got…
- Metasploit

- So I guess the answer to “how are…. related?”
  - Pat’s gonna talk about them all.

Anti-Phishing Working Group

- Launched in 2003
- 3000+ members
  - 1700+ companies and agencies (worldwide)
  - e-Commerce, financial, telecomm, ISP's, solution vendors, law enforcement, academics, national CERTs, etc.
- Focus: Eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types

Definitions

- Lure – The item used to convince you to respond. E.g., email, SMS, phone call
- Collection site – Where you go to provide your credentials
- eCrime – a violation of regulations that involve a computer

The eCrime landscape

- To us, eCrime is a three headed dog

1. Computer integrity crimes; (computer as target)
   - DoS attacks, intrusion
2. Computer-assisted crimes
   - Phraud, cyber-bullying, AFF/419
3. Computer content crime
   - Porn, copyright, DCMA, libel

(Due to our data sharing, the APWG is trying to craft an eCrime taxonomy.)

Some of my Favourite Lures

- An email warning of phishing and asking you to confirm your bank details
- “Chase and McDonald’s FREE Fry Offer!”
- “We’ve accidentally deleted our credit card database. Please re-enter your card data…”
- A malware that scans for 300 bank names through your browser history file; then captures the screen images when you go to them and sends them off via IRC

New Lure Enhancements

- Now, the lure is used to drop all types of crime-ware onto a computer
  - Keystroke loggers, virii, etc
  - Very sophisticated crime-ware
- Hit many banks with one click!
- A victim that 'clicks' on a picture may get a keystroke.
- Infections are designed to not be removed ☹

New Types of Lures

- Email/SMS lure with “call this phone number”
  - Phone tree recorded directly from bank
  - Compromised Asterisk (VoIP PBX) that relays to odd countries
- Cold-call to home phone number
- Targeted with info from corporate filings
  - Protecting personal info is becoming more important

2009 Trends

- Phishing isn't only Banks !!!!
  - Big stores' debit cards
  - Internet Registrars
  - Corporate VPN accounts, Uni websites
  - (Online gambling, porn sites, on-line games)
- Muling grew up
- *Very* targeted lures
- Criminals think they get one shot at you:
  - Install everything you can!

Recent Trends

- Most of the eCrime lures are not 0-day
  - Physical ID theft is still easier than on-line
- Criminals know where the best bang is
  - Steal uni mail accounts -> send spam
  - Steal corp accounts -> influence stock price
- Criminals are banding together
  - Know any purely bad ASNs? ☺
- Younger people trust their computers too much

Odd Trends

- A *large* number of cold calls via phone
- SMS Text message lures are growing quickly
- From the good economy: resume grabbers
  - "Send me your resume with ALL details…"
- Social network sites are getting into the game
- Phishing lures give you 'presents', too ☺
    - Malware, keyloggers, etc
- Most viruses are not new

How do we interpret the trends?

- Everyone can now google. ☹
  - Very easy to find data on you/me/us
  - Social engineering is no longer hard
  - ‘mistakes’ happen regularly
- Technology is making it easier to hide
  - Find an asterisk server →
    - sell auto warranties, make calls, process ACH
  - Lots of fraud comes from ‘odd’ IP addresses
    - Tor, Amazon EC2, etc

More disturbing news

- The media sees blood, err, a story!
  - Every bump is a media event
- We tell users that a virus/infection is bad
  - Scan WSJ, NYT, Herald for the poor sucker stories
- When a user visit some web pages, they get the little “you’re infected” message. “Click here to save your machine!”
  - The download is a virus + keystroke logger.
  - Welcome to **scareware.**
- Phishers use our countermeasures against us

User ‘Guidance’

- You could tell users not to click on anything!
  - They won’t listen
  - There are people who *have* to click
    - Protection schemes only kind of help…
- The new challenge is trying to figure out how to make users aware enough to make their own clicking decisions.

Social Engineering at its finest…

From: Admin [mailto:admin@southsouthwestern.edu]
Sent: Friday, January 27, 2009 5:38 PM
To: Wheeler, Kay
Subject: Rape on Campus
Attachments: **Suspect_picture.jpeg**

←**W32/Brepibot.gen**
(Keystroke Logger +Bot backdoor)

Hello,
During the early morning of January 25 2009, a campus student was the victim of a horrific sexual assault within college grounds. Eyewitnesses report a tall black man in grey pants running away from the scene. Campus CCTV has caught this man on camera and are looking for ways to identify him. If anyone recognises the attached picture could they inform administraion immediatly
Regards,
Robert Atkins
Campus Administration

Better news

- The amount of crime is causing hesitant people to share data to stop the bad stuff
  - Data correlation works wonders!
  - It looks like most fraud crime comes from a small set of people
  - One can watch DNS to detect problems
  - Use a common format to speed up processing
- Many countries are now paying attention
  - Regulatory arbitrage is receding

The APWG Global Phishing Survey

- APWG members generate a state of phishing and malicious domains report semi-annually
- Report available @ www.apwg.org

Highlights

1. Phishers continue to target specific Top-Level Domains (TLDs) and specific domain registrars
    1. Phishers are increasingly using sub-domains
2. The amount of Internet names and numbers used for phishing has remained fairly steady over the past two years.
    1. IP Addresses as collectors decreased
    2. No IDNs used
3. Anti-phishing programs implemented by domain name registries can have a remarkable effect on the up-times (durations) of phishing attacks.

Basic Statistics

	2H2008	1H2008	2H007
Phishing domain names	30,454	26,678	28,818
IP-based phish (unique IPs)	2,809	3,389	5,217
TLDs phished in	170	155	145
Attacks	>56,969	>47,342	
IDN domains	10	52	10

Rank	TLD	TLD Location	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008
1	ve	Venezuela	1,504	82,500	**182.3**
2	th	Thailand	88	39,880	**22.1**
3	bz	Belize	55	43,377	**12.7**
4	su	Soviet Union	76	85,119	**8.9**
5	ro	Romania	188	310,114	**6.1**
6	cl	Chile	116	232,897	**5.0**
7	kr	Korea	413	983,626	**4.2**
8	vn	Vietnam	37	92,992	**4.0**
9	ru	Russia	676	1,860,179	**3.6**
10	tw	Taiwan	144	406,669	**3.5**
11	fr	France	430	1,289,559	**3.3**
12	my	Malaysia	25	80,786	**3.1**
13	mx	Mexico	80	277,652	**2.9**
14	be	Belgium	240	859,474	**2.8**
14	gr	Greece	71	250,000	**2.8**
14	ir	Iran	29	102,800	**2.8**

What's next?

- The criminals are getting more technical in their forgeries
  - Creative fast flux domains
  - attempts to compromise DNS so they get a 'real' URL
- Can we make stolen credentials close to worthless?
  - "Let 'em get phished" – Marie Antoinette

Thank You

I went to Defcon…

An Intro

- DEFCON is one of the oldest continuous running hacker conventions around, and also one of the largest. About 6000 attendees
- It was invaded about 5 years ago by the IT crowd
- Many cops/feds come to meet the hackers – and go home disappointed

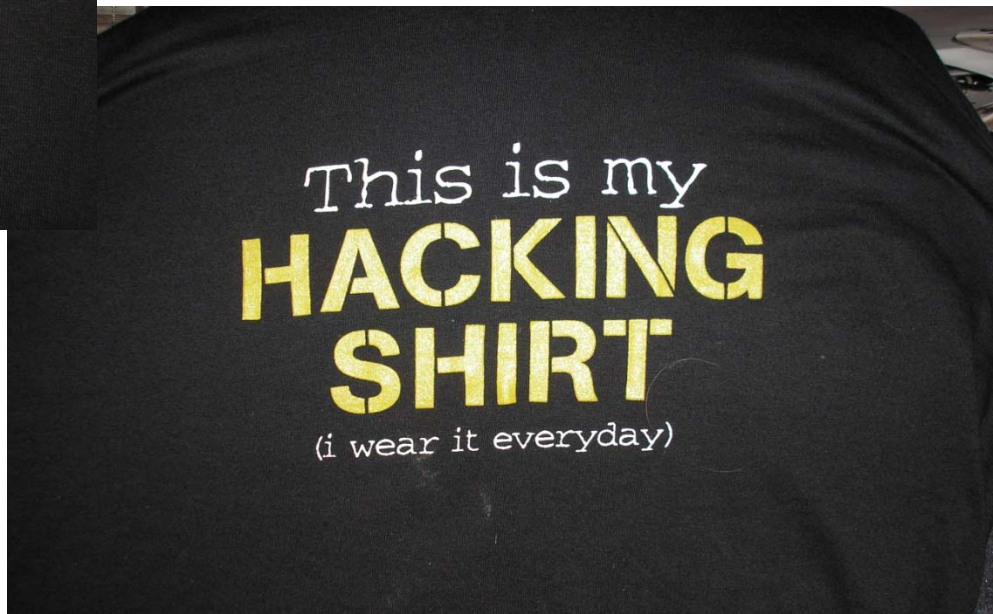
“the network”

- 50ish APs
  - Many rogue
- 3493 dhcp leases
- 69229 streams on defcon tv
  - 40,860 from outside hotel
- **Avg per hr**: 306 Dos, 226 mitm, 120 policy (rogues, etc)
- 20 mb line; 39 APs -> 50 vlans,
- 46 conf rooms -> 35 vlans
- defconnetworking.org

Schwag


TOOOL
The Open Organisation Of Lockpickers


DEFCON
HUMAN


This is my
HACKING
SHIRT
(i wear it everyday)

Why Do I Go?

- Listen to find out what everyone thinks is sexy
  - What's everyone talking about
  - What do the loonies think is fun?
- See if I'm missing any good tools
  - mandiant -> memoryze (grab stuff out of memory on the fly)
- Talk to some people I would not be seen dead with in public
- Make fun of people

Interesting Points

- Metasploit was everywhere!
  - It's gonna, if not already, show up in your net
- Lots of talks from pen testing companies
  - I guess that makes them elite ;)
- Super sekrit (aka, "we can't tell you because we figured it out") talks from people looking for company funding
- A number of talks on SSL hacks
  - bowser X.509 certificate processing errors

More Stuff

- Normal Silly stuff
- NIST brought an optical network and showed how to ‘hack’ it
- “Forensics on a Picked Lock”
  - Lockpickingforensics.com
- “How to recover (your) porn from a broken RAID array”

Metaploit

- The Metasploit Framework is a development platform for creating security tools and exploits
- Comes with libraries, tools, scripts, etc.
  - You can concentrate on the payload
- Used by good and evil pen testers

Evoution

- Nmap
  - Discover listening ports/services
  - Discover holes in firewalls ☺
- Nessus
  - Discover vulnerable services
- Metasploit
  - Generate your own exploit code

Metasploit Track at DEFCON 17

- Breaking the "Unbreakable" Oracle with Metasploit
- Using Guided Missiles in Drive-Bys: Automatic browser fingerprinting and exploitation with Metasploit
- WMAP: Metasploit goes Web
- MetaPhish
- MSF Telephony
- Metasploit Evolved, Meterpreter Advances, Hacking the Next Internet
- MSF Wifi
- App Assessment the Metasploit Way
- Macsploitation with Metasploit
- Metasploit Autopsy: Recontructing the Crime Scene

Thank You

Pat Cain
pcain@antiphishing.org
pcain@coopercain.com
patrick.cain.1@bc.edu