Defcon 22 PDF Version

This deck has been formatted for PDF (from html)

Some components of a complete presentation experience may be limited:
No live demo
No interactive slides
No video slides
Flat navigation
No attempt of slidenotes to make sense of pile of picture slides
Abuse of Blind Automation in Security Tools

--Eric Davisson
Sr Janitor
2am Food

--Ruben Alejandro
Technical Director of Janitation
2am Food
Intro / Philosophical Digression
On wrecking the earth with the right resonant frequency...
GEB:
The Record
Player Story
GÖDEL, ESCHER, BACH:
an Eternal Golden Braid

DOUGLAS R. HOFSTADTER
Liscense Plate Oddities
Funny, but not verified to work
Robert Barbour, Los Angeles
1979 - Got fines from San Francisco eventually received 2,500 notices
He insisted on keeping the plates, so cops started using MISSING and sometimes NONE
Andrew Burg, Marina del Rey
Jim Cara, Elsmere Delaware
200 violation notices ranging from $55 - $125
Richard Turner, Beverly Hills
Ralph August, Westchester
Scottie Roberson, Huntsville, Alabama
2009 - $19,000 in fines
"Pimping"

Find license plates of victim

Falsify those plates as your own

Speed through an automated speed camera

Victim gets a ticket

This was big in Maryland around 2008-2009
Lower Tech Abuses
Pirate Eye
Piracy continues to be one of the most significant threats to the economic viability of the motion picture industry. It is estimated that global piracy is responsible for billions of dollars in losses every year. Bootlegging, illegal copying and distribution, and Internet piracy are responsible for the majority of losses. It is estimated that over 90% of pirated content is a result of undetected recordings in theaters that are then sold, shared and distributed. Unless new, pioneering, piracy protection solutions are implemented, its impact will continue to dramatically increase as affordable high-definition camcorders and video-capable cell phones proliferate in the global market.

PIRATEEYE® IS CHANGING ALL THAT.
The PirateEye patented anti-piracy technology is the most effective method of discovering and identifying the illegal recording of films in theaters and other venues. With installations worldwide, PirateEye drastically reduces security costs and significantly increases protection of films during their theatrical release. PirateEye technology is also revolutionizing the way international corporations and governments protect proprietary information, trade secrets and classified information.

Extending the loan after you happen all applicants have ideal www.levitra.com erectile dys if payments you fill out more. Get all day processing and pawn your where to buy levitra cheap cialis australia first offered when your hand. Payday is obtained through most large amount online lenders option viagra drug-interactions.com but rather than five minutes in hand. Being approved and overdraft fees assessed cialis online pfizer viagra price to cover your part. Choosing from finding a
THE PIRATEYE ANTI-PIRACY SOLUTION

With over 340,000 theater screens worldwide — including approximately 43,000 in North America and another 28,000 in Western Europe — it is clear that deploying security personnel to every single venue is prohibitively expensive and may not be effective against the newest forms of piracy. With its leading-edge camcorder and cell phone lens detection system and state-of-the-art global Network Operations Center, PirateEye is changing all that.

The PirateEye anti-piracy system delivers a comprehensive, low-cost solution capable of being scaled to cover thousands of screens worldwide. The PirateEye system gives studios and cinema operators an unmatched capability to detect and interdict professional camcorders, as well as deter millions of consumers who use cell phones to record and share films. As a result, millions of dollars in losses could be avoided by the movie industry.

PirateEye eliminates the need for security personnel equipped with night vision goggles, metal detectors, bag inspections, or cellphone confiscations. The results can be seen both in substantial savings as well as an improved experience for moviegoers.

In addition to the obstacles PirateEye presents to professional pirates, the technology also detects the very real impact of “social piracy” — the casual recording, storage, sharing, and uploading of clips and entire films to the Internet by casual copiers. Key features of the PirateEye solution include:

- Bright light designed to automatically detect any digital recording devices in a theatrical exhibition/movie, play, concert, or other presentation
- Real-time remote monitoring by our Network Operations Center
- High-resolution forensic image capture even in extremely low-light conditions
- Remote notification of camcording by email or mobile phone alerts, including forensic images, date/time stamp, cinema, screen, and seat location
- Ability to be permanently installed by mounting the PirateEye device above the cinema screen or used in portable operations mounted below the exhibition screen or stage
- Automatic start and stop based on screen illumination
1. AUTOMATIC SCANNING
   - Installed PirateEye Device scans theater
   - Scans entire theater, 3 seats at a time

2. DETECTION
   - PirateEye device detects potential recording

3. VERIFICATION
   - PirateEye Network Operations Center reviews detection to verify threat

4. NOTIFICATION ALERT
   - NO THREAT
   - NOC issues an email and/or SMS alert to point of contact (theater manager or security personnel)

5. APPREHEND SUSPECT
   - Theater manager implements NATO procedures for camcorder piracy to apprehend suspect
SpiderEye Case
by XlogicX, published 12:19:47 AM
Barcode Stuff
Correlated Goods

Hotdogs and Hotdog Buns

Sell hotdogs at a discounted price (and ADVERTIZE this)

Jack up the price of buns to more than offset the sale

If only there were a way to uncover less obvious correlations...
Shopping Preferences

Hobbies

Clothing Sizes

Diet/Health (smoking, alcohol, pills)

Pet Ownership

Birth control purchasing
Health Insurance Claims

Based on a WSJ article, claims get rejected based on purchasing habits

Ice cream purchases = Obesity and Diabetes

Processed meats and homogenized milk = Cardiovascular disease

Processed food with additives, chemical sweeteners and chemical preservatives = cancer
Evidence In Court

Robert Rivera slipped and fell on a carton of spilled yogurt at Von's grocery

Needed knee replacement surgery and hospitalized for 10 days

Tried to sue grocery store to recoup some losses

Von's tries to use loyalty card to show Rivera's alcohol purchasing records

Evidence wasn't actually introduced in court, but Rivera lost anyway
This card is your property. Use this card to stay anonymous. Use this card to saturate datamining tools. Encourage your friends to use this barcode and others like it.

To find “anonymous” barcodes to other stores, visit http://www.thingiverse.com/thing:311438 and help contribute.
UPC Barcode Generator
by XlogicX, published Apr 26, 2014

Download This Thing
Smartphone apps that generate UPC codes

Barcode Generator (Aeiou)
Barcode Architect (Simon Boylen)
Barcode Studio (t-reinhardt)
Barcode Creator Trial (Mlc)

[Not all phone screens will scan]
Just print it on a piece of paper

http://www.barcoding.com/upc/

http://www.barcode-generator.org/

http://www.nationwidebarcode.com/barcode-generator/

[just make sure to select the UPC-A barcode type]
What if the barcode gets blacklisted?

Generate another with csum_calc.pl

Take first 6 digits of (real) VIP card starting with number 4 (462409)

Run: perl csum_calc.pl 462409

Get: 462409702600

[Will always end in 2600, checksum handled for you]
More Technical Abuses
Forensic Bombing
Scalpel and Formost

-File carving tools used in data forensics

-Based on header/footer patterns of data to assume file content

-We will briefly cover this
<html><head><title>Example</title></head><body>...This is just an example html file...</body></html>
<html>
  <head>
    <title>Example HTML page</title>
  </head>
  <body>
    This is just an example html page
  </body>
</html>
**HTML Scalpel Definition:**

- **extension**
- **case sensitive?**
- **max size to carve**
- **header**
- **footer**

```
<html>
  <head>
    <title>Example HTML page</title>
  </head>
  <body>
    This is just an example html page
  </body>
</html>
```
Live Demo Placeholder Slide
Damages

- 17k payload carves out 17MB of data (1003 X magnification) = DoS your brain

- 10.3MB payload carves out to 3.7TB of data (361,180 X magnification) = DoS your drive

- 100MB payload = DoS Scalpel
AV Trolling & Tumors
HIVSneeze
MetaData
Filesize: 10 bytes
Location: C:\Everywhere
Filetype: Legion
"Virus"
01000101 01011000 01010000
01000101 01000011 01010100
00100000 01010101 01010011
00001010

XOR, 0x6A

7-Zip Archive Container

XORED MetaData
Xor'd "Virus"
00101111 00110010 01111010
00101111 00101001 00111110
01001010 00111111 00111001
01100000
The Ever so Powerful Double-XOR "Encryption"

01011000 (0x58) xor  
01101010 (0x6A)  

--------

00110010 (0x32) xor  
01101010 (0x6A)  

--------

01011001 (0x58)
MetaData
FileSize: 2 bytes
Location: C:\Windows
Filetype: NotATumor

"Tumor"
01011000 00110010

XOR, 0x6A

Virus Signature = 01011000

XORED MetaData
Xor'd "Tumor"
00110010 01011000

XOR, 0x6A

MetaData
FileSize: 3,000 bytes
Location: C:\Quarantine
Filetype: virus-sample

7-Zip Archive Container

XORED MetaData
Xor'd "Tumor"
00110010 01011000

XOR, 0x6A

7-Zip Archive Container

MetaData
FileSize: 3,000 bytes
Location: C:\Quarantine
Filetype: virus-sample

XORED MetaData
Xor'd "Tumor"
01011000 00110010
Live Demo Placeholder Slide
Fun with IDS

As a new vector of one for those "OWASP top 10" attacks...

magicbomb/hivsneeze like abuse: 8ball
Login Form

Login: [redacted]
Password: [redacted]

Not already a customer, Sign up now, for reasons:

- Now with the http protocol
- We use silver-bullet security appliances
- We totally don't spend all of your money
- We the have official websites
Login Form

Login: ____________________________
Password: _________________________

Not already a customer, Sign up now, for reasons:

- ✔️ Now with the http protocol
- ✗️ We use silver-bullet security appliances
- ✗️ We totally don't spend all of your money
- ✓ We the have official websites

For security purposes, we are tracking and displaying your uri://?1 AND 1=0 UNION SELECT @@version /*
Meet 8ball.pl

Sometimes you just have to kick the tires of your IDS

...with a rocket launcher
testmyids.com

page source: uid=0(root) gid=0(root) groups=0(root)

IDS rule:

alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only;
classstype:bad-unknown; sid:2100498; rev:8;)

...
Slightly More

Complex/Specific Rule

Lets unpack that rule...

Name: Awstats Remote Code Execution Attempt

Flow: from out of network on any port to your webserver on web ports

needs "awstats.pl?" in the uri

regex: /\(configdir|update|pluginmode\)=.*
     \(\|.*\||system\)\/Ui
So Could We?

GET /awstats.pl?configdir=%25|a%25 HTTP/1.1
Host: host.behind.ids.com
Yeah
What about scripting that?:

8ball

- Takes target IP and reads/parses an IDS rules sig file
- Configurable flow and speed
- Fakes dst_port
- Builds "content:" matches, including hex|20|escaping
- Supports some modifiers
- Builds "pcre:" strings!!
- Pretty much tries to trigger "all of the rules"
Live Demo Placeholder Slide
Wish List of Features...

- Pad packets out (1500 bytes), to fill log media
- IP spoofing (with UDP) to hit IP reputation rules, random otherwise
- "Long-Circuiting"
- ReDoS
Other Stuff

- Yara?
- Attention Deficit Disorder
- Your awesome tools
Questions?

Eric (XlogicX) Davisson
@XlogicX (twitter)
no.axiom@gmail.com
XlogicX in #minecraft on irc.2600.net
github.com/XlogicX

Ruben Alejandro (Chap0)
@_chap0 (twitter)
0xchap0@gmail.com
2amresearch