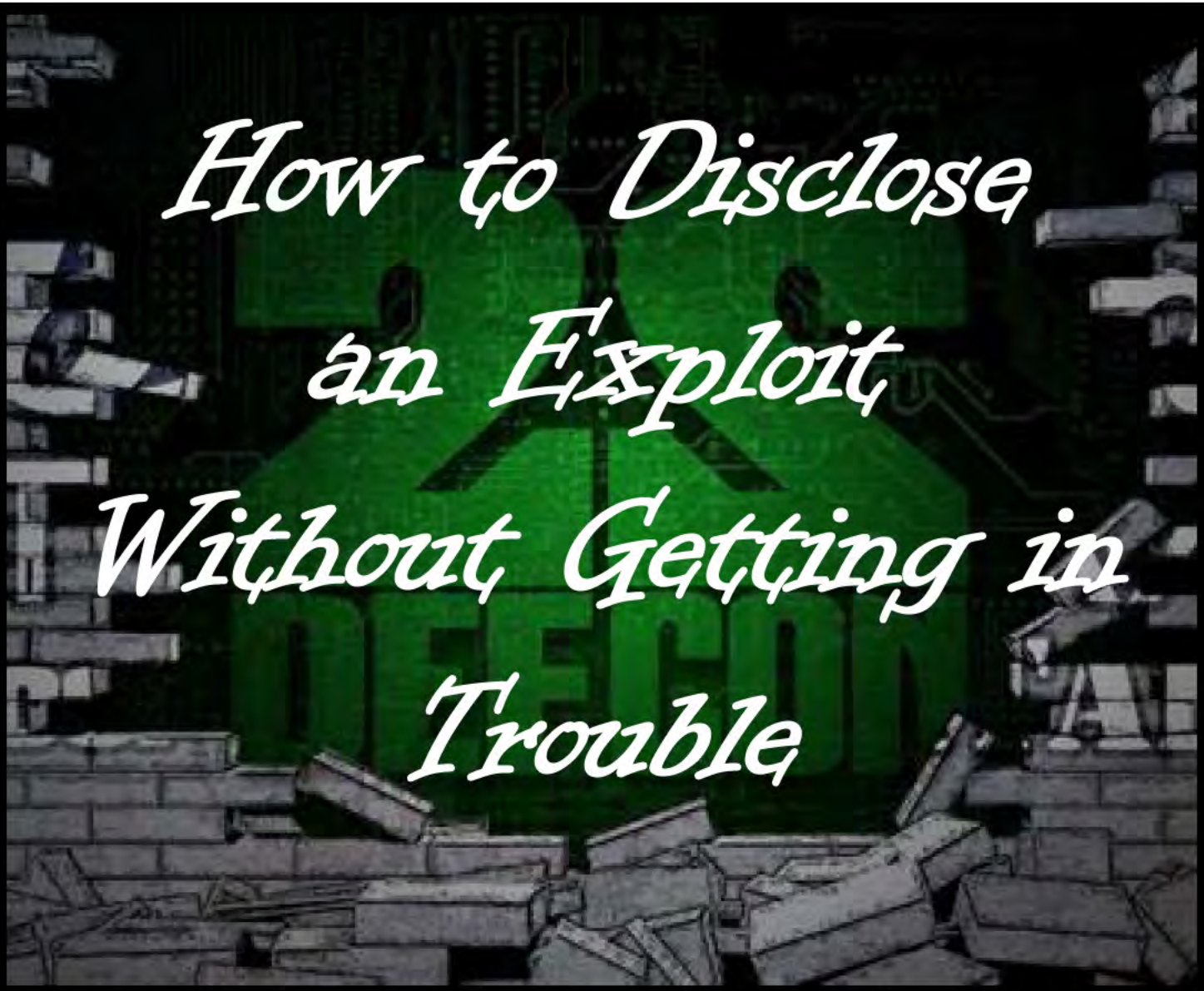


Jim Denaro
jim@cipherlaw.com
PGP: 0xD840D7A5

Tod Beardsley
todb@metasploit.com
PGP: 0xF577904A


DEFCON
PART II
This presentation is for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem. Please ask your attorney if disclosing exploits is right for you.
@cipherlaw
@todb

About Us

Jim Denaro / CipherLaw

jim@cipherlaw.com
PGP: 0xD840D7A5
RedPhone/TextSecure
SilentCircle: CipherLaw
@CipherLaw

Tod Beardsley / Rapid7

todb@metasploit.com
PGP: 0xF577904A / 0xADB9F193
@todb

Overview

- Risk
  - From research activities
  - From disclosure
- Risk mitigation strategies
- Disclosure options

Your Goal: Be a Harder Target

Potentially Risky Research

along a spectrum

- You found out how to see other people's utility bills by changing the http query string
- You discovered your neighbor's WiFi is using the default password
- You broke the DRM protecting media
- You wrote a better RAT

Risks In Disclosure

Get your research buried by a court
Get sued by an angry vendor
Get arrested by a government
Accidentally disclose 0-day!

Rewards of Disclosure!

@cipherlaw

@todb

Specifics: CFAA

Computer Fraud and Abuse Act

access “without authorization”
or “exceeds authorized access”

Specifics: CFAA

Computer Fraud and Abuse Act

- Are you connected to the internet?
- Are you accessing a remote system?
- Do you have permission to access it?
- Did you obtain information?

Recent CFAA Cases

Criminal prosecution (technical acts)

- Andre Nestor (exploited video poker bug [CFAA charge dropped])
- David Nosal (had others use active accts to login [no CFAA violation, 9th Cir.])
- Aaron Swartz (spoofed MAC address etc to obtain journals)
- Andrew Auernheimer (scripting http queries to public API)
- Jeremy Hammond (Stratfor email leak)

Civil prosecution

- Available on the same grounds to private parties

Aggravating Factors

- Nestor: Made > $500,000 from the games
- Nosal: Downloaded a large volume of "highly confidential and proprietary" data
- Aaron Swartz: Entered the premises to connect equipment
- Andrew Auernheimer: Trolling, 110,000 email addresses
- Jeremy Hammond: Intentional disclosure of sensitive documents

CFAA Risk Mitigation

In Research

Stick to Proof of Concept

@cipherlaw

@todb

CFAA Risk Mitigation

In Disclosing

Be Professional

"We're supposed to be…professionals!" – Mr. Pink

@cipherlaw

@todb

CFAA Risk Mitigation

In Disclosing

Never ask for ask for anything of value

money
recognition
employment
etc.

CFAA Risk Mitigation

Do not direct technique information to someone you *suspect* or *should know* is likely to use it illegally.

CFAA Risk Mitigation

Be careful in providing “support”.

“If I were your lawyer, I’d advise you not to answer that tweet.”

CFAA Risk Mitigation

Do not provide technique information *directly to any individuals* and limiting distribution to websites only.

Do not promote the disclosure on *forums known to support or promote illegal activity*.

On a website, *disable comments* to avoid possibility of users discussing illegal use on your site.

Use secure communications and do not maintain logs.

Disclosure Options

Identity: Acknowledged
You did everything “right”

Responsible Disclosure
Initial disclosure of the vulnerability.
Offer specifics under hold harmless agreement.

Disclosure Options

Identity: Anonymous

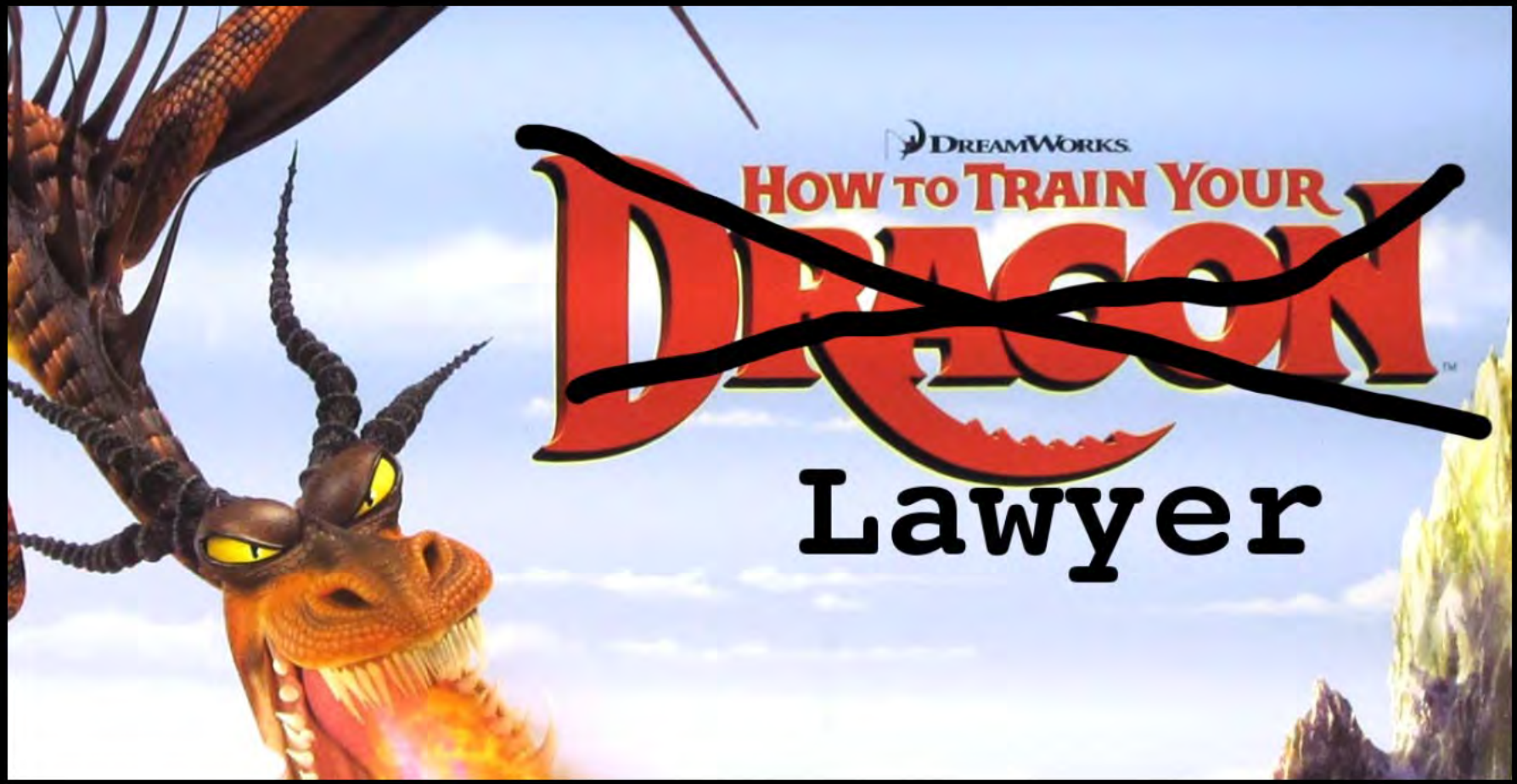
Maybe you didn't do everything "right"

Open-Source Responsible Disclosure Framework

Developed with 

Key Elements:

- Scope published online
- Researcher stays in scope
  - Avoids PII, disruption, etc
- Company agrees not to sue / support prosecution
- Researcher discloses responsibly
  - keeps confidential for initial term
  - to allow for patch



@cipherlaw

@todb

Obfuscating Meta-Data

Authorship Analysis in Cybercrime Investigation

http://www.personal.psu.edu/faculty/h/u/huz2/Zan/papers/authorship.isi03.pdf

@cipherlaw

@todb

Know your Adversary

A litigious multinational corporation?
An organization with disclosure experience?
A free, open source software project?
...an important one?
Do any governments have an interest?

@cipherlaw

@todb

Reasonable Precautions

@cipherlaw

@todb

Secure Comms Are Really Hard

@cipherlaw

@todb

Case Study: R7-2014-10

Yokogawa BKBCopyD.exe Unauthenticated File System Access

Vendor: Yokogawa

Details: Due to a lack of authentication on the CENTUM 3000 HIS, commands such as PMODE, RETR, and STOR are available to unauthenticated users. This, in turn, allows for arbitrary file reading and writing with the privilege of the CENTUM user.

URL: http://blog.metasploit.com (Soon!)

Disclosure Timeline: R7-2014-10

Day 1: Attorney-Client relationship established between Cipherlaw and Rapid7

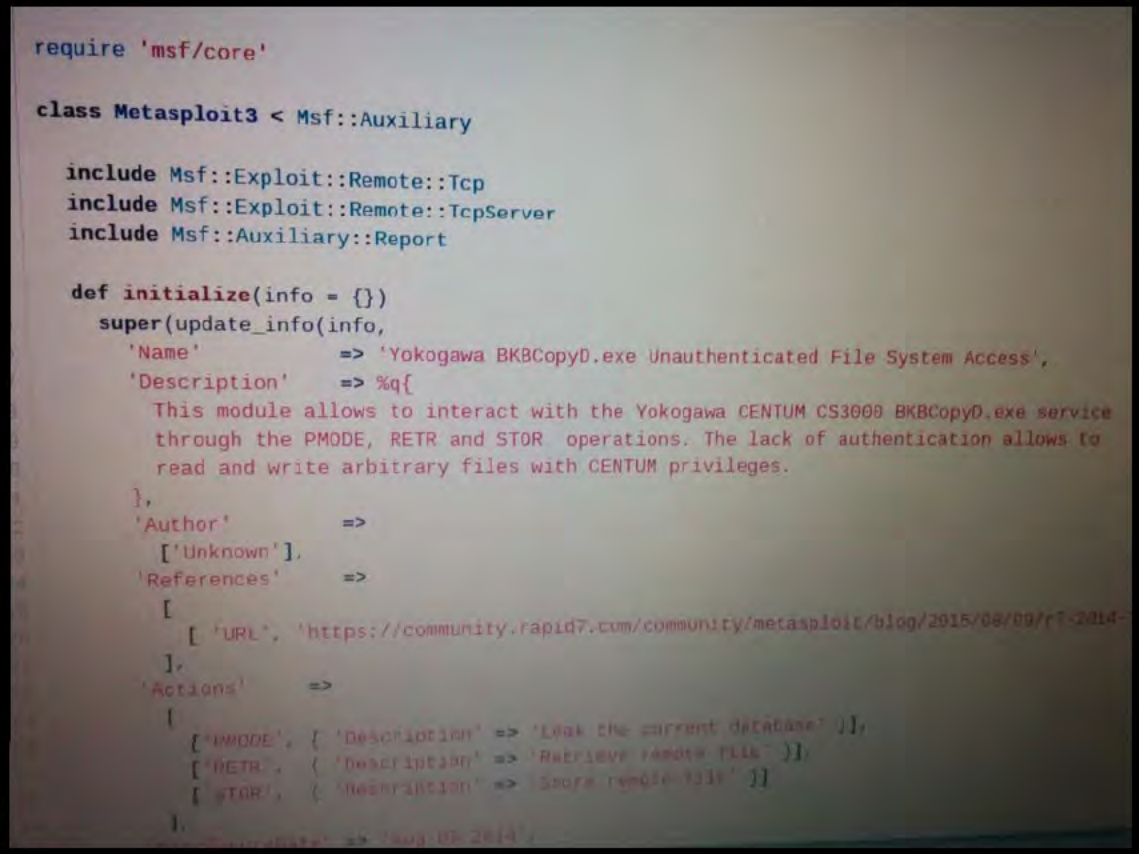
April 14, 2014: Vulnerability details disclosed to attorney

May 1, 2014: Details disclosed to vendor

June 25, 2014: Details disclosed to CERT

Today: Details published

Obligatory Source Code



```
require 'msf/core'

class Metasploit3 < Msf::Auxiliary

  include Msf::Exploit::Remote::Tcp
  include Msf::Exploit::Remote::TcpServer
  include Msf::Auxiliary::Report

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'Yokogawa BKBCopyD.exe Unauthenticated File System Access',
      'Description'    => %q{
        This module allows to interact with the Yokogawa CENTUM CS3000 BKBCopyD.exe service
        through the PMODE, RETR and STOR  operations. The lack of authentication allows to
        read and write arbitrary files with CENTUM privileges.
      },
      'Author'         =>
        ['Unknown'],
      'References'     =>
        [
          [ 'URL', 'https://community.rapid7.com/community/metasploit/blog/2015/08/09/r7-2014-
        ],
      'Actions'        =>
        [
          ['PMODE', { 'Description' => 'Leak the current database' }],
          ['RETR', { 'Description' => 'Retrieve remote file' }],
          [ 'STOR', { 'Description' => 'Store remote file' }]
        ],
      'DisclosureDate' => 'Aug 09 2014',
```

Disclosure doc to CERT/CC

Yokogawa Centum CS3000 R3.08.50 Vulnerability

Subject: Yokogawa Centum CS3000 R3.08.50 Vulnerability
From: James Denaro <jdenaro@cipherlawgroup.com>
Date: 6/25/2014 11:35 AM
To: cert@cert.org

CERT:

I represent a security researcher who has identified an exploitable security vulnerability in the Yokogawa Centum CS3000 R3.08.50. A PDF detailing the vulnerability is attached here.

On 5/1/2014, we informed Yokogawa of the fact of a vulnerability using all of the email addresses below:

security-alert@yokogawa.com
secure@yokogawa.com
security@yokogawa.com
support@yokogawa.com
info@yokogawa.com

While we did not provide technical details of the vulnerability at that time, we invited Yokogawa to contact us to discuss the vulnerability. We have not been contacted by Yokogawa.

We intend to publicly disclose this vulnerability in 30 days.

Please contact me if you would like to discuss or have any questions about the vulnerability.

Regards,
Jim Denaro

James Denaro | CipherLaw
jdenaro@cipherlawgroup.com
https://www.cipherlawgroup.com
202-596-7303 (office)
202-494-3982 (mobile)
PGP: 0xD840D7A5 [https://www.cipherlawgroup.com/cipherlawkey.txt]
RedPhone/TextSecure | SilentCircle: CipherLaw

Attachments:

Centum CS3000 R3.08.50 (public).pdf 129 KB

Yokogawa Centum CS3000 R3.08.50

The Yokogawa Centum CS3000[1] includes a "BKBCopyD.exe" service which, when started by running the "FCS / Test Function", listens by default on TCP/20111. An attacker can abuse several operations provided by the service to leak the CENTUM project database location, read arbitrary files, and write arbitrary files. Reading and writing to the file system will happen with the privileges of the CENTUM user.

A working Metasploit module has been developed for Yokogawa Centum CS3000 R3.08.50 running on Windows XP.

The "BKBCopyD.exe" service provides several operations, which can be abused without further authentication by anyone with network access to the service. The operations are described as follows:

PMODE: this command allows getting the value for environment variables. It includes the MR_DBPATH variable with the project path in the file system or network resource.

```
[*] Connected to 192.168.172.131:20111
PMODE MR_DBPATH
210 PMODE C:\YCS3000\ENG\BKPROJECT\MYPJT\TestMaster\WS0103\database command successful
QUIT
221 Goodbye.
```

RETR: this command allows reading arbitrary files from the remote file system with the privileges of the CENTUM user. To read arbitrary files, an attacker only needs to know the inner workings of the RETR command. The service doesn't provide any authentication or authorization mechanism.

STOR: this command allows storing arbitrary files in the remote file system with the privileges of the CENTUM user. To write arbitrary files, an attacker just needs to know the inner workings of the STOR command. The service doesn't provide any authentication or authorization mechanism.

[1] http://www.yokogawa.com/dcs/products/cs3000/overview/dcs-3k-0101en.htm

@cipherlaw

@todb

Questions?

Shoot!