

The Bugs I've Found,  
The Bugs I have Yet To Find

Mike Ryan

**ICE9**  
CONSULTING

It was the 90's...



**ICE9**  
**CONSULTING**

The Bugs I've Found,  
The Bugs I Have Yet To Find



**IGS**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find



Salamèche



Carapuce



Bulbizarre

**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

# POKÉMON

Gotta catch 'em all!



**ICES**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find



**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

*“You can play Game Boy games  
on the computer”*







**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

VGB-Windows 4.9

File Hardware Video Audio Help



**IG29**  
CONSULTING

The Bugs I've Found,  
The Bugs I Have Yet To Find

```

ROM0:2016 AF      xor  a      :1  1
ROM0:2017 DA C7 CF  ld  (CFC7),a  :5  4
ROM0:201A EA EE C8  ld  (C0EE),a  :9  4
ROM0:201D EA CA CF  ld  (CFC9),a  :13 4
ROM0:2020 3D      dec  a      :14 1
ROM0:2021 C3 B1 23  jp  23B1     :18 4
ROM0:2024 F5      push af     :22 4
ROM0:2025 C5      push bc     :26 4
ROM0:2026 D5      push de     :30 4
ROM0:2027 E5      push hl     :34 4
ROM0:2028 F0 B8      ld  a,(FF00+B8) :37 3
ROM0:202A EA 22 D1  ld  (D122),a  :41 4
ROM0:202D F0 AE      ld  a,(FF00+AE) :44 3
ROM0:202F E0 43      ld  (FF00+43),a ;lcd scrol:47 3
ROM0:2031 F0 AF      ld  a,(FF00+AF) :50 3
ROM0:2033 E0 42      ld  (FF00+42),a ;lcd scrol:53 3
ROM0:2035 FA A0 D0  ld  a,(D0A0)   :57 4
ROM0:2038 A7      and  a      :58 1
ROM0:2039 20 04      jr   nz,203F   :60 2/3
    
```



```

af = 0140  z = 0
bc = 0160  n = 1
de = 0000  h = 0
hl = 0088  c = 0
sp = DFF3  DI
pc = 2027  ROM01
    
```

```

RAM1:DFF3:0000
RAM1:DFF1:0000
RAM1:DFEF:20A2
RAM1:DFED:1FC0
RAM1:DFEB:35E4
RAM1:DFE9:4DF1
RAM1:DFE7:3E67
RAM1:DFE5:0170
RAM1:DFE3:35E4
RAM1:DFE1:0107
    
```

```

ROM0:0000 FF00000000000000FF00000000000000
ROM0:0010 FF00000000000000FF00000000000000
ROM0:0020 FF00000000000000FF00000000000000
ROM0:0030 FF00000000000000FF00000000000000
ROM0:0040 C324200000000000FF00000000000000  $
ROM0:0050 C306230000000000C325210000000000  #
    
```



ZD Lite (news-only version)

Founded November 9, 1996

Bringing emulation to you for over 2 years

Last Updated Thursday, April 29, 1999 06:42:42PM EDT

You are # **8343835** in the Domain!

Feel free to [submit](#) news to Zophar's Domain.

Emulators: Arcade

Single Arcade  
Multi Arcade  
M.A.M.E.

Emulators: Calculator

HP Calculator  
TI Calculator

Emulators: Computer

Amiga  
Amstrad CPC  
Apple II  
Atari 8 bit  
Atari ST  
Commodore 64  
COCO 1/2/3  
Macintosh  
MSX

Welcome to Zophar's Domain!

Welcome to Zophar's Domain! We're 2 years old and counting now. We are the #1 site for all your MS-DOS, Windows (3.1, 9x, and NT), and Unix (Linux, FreeBSD, Solaris, etc.) emulation needs. Here you'll find emulators, utilities, front ends and other useful items.

Be sure to check out the [message domains](#) for various discussions, the [poll](#) where you can voice your opinion on a multitude of subjects and the Miscellaneous area which contains many interesting items. If you're new to emulation or just to Zophar's Domain, be sure to check out the [FAQ](#) which should answer all your initial questions.

Remember, ZD is here for your benefit. If you can't find what you need, let us know, and if it exists, we'll make it available here ASAP. Please Note: While there are a few legal ROMs located here, this is **not** a ROM site. We will not send you any ROMS, so don't even ask. Instead, check the [links](#) section for links to all the best ROM sites and other great emulation sites. Macintosh users should check out our Macintosh emulators section for Macintosh emulators & utilities! Now enjoy your visit to ZD & please keep all body parts inside at all times.



Vimm's Lair

**ICE9**  
CONSULTING

The Bugs I've Found,  
The Bugs I Have Yet To Find

# The New Millennium



**ICE9**  
**CONSULTING**

The Bugs I've Found,  
The Bugs I Have Yet To Find

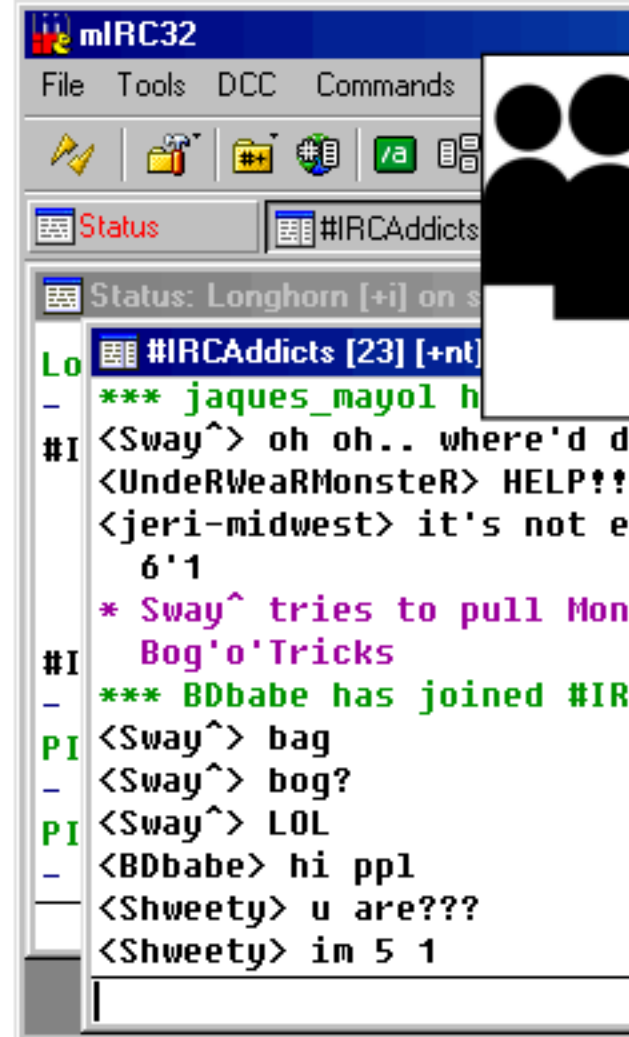
# TERMINALLY ONLINE



**GA**  
**CONSULTING**  
The [unclear] I've Found,  
The Business Have Yet To Find



**IGES**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

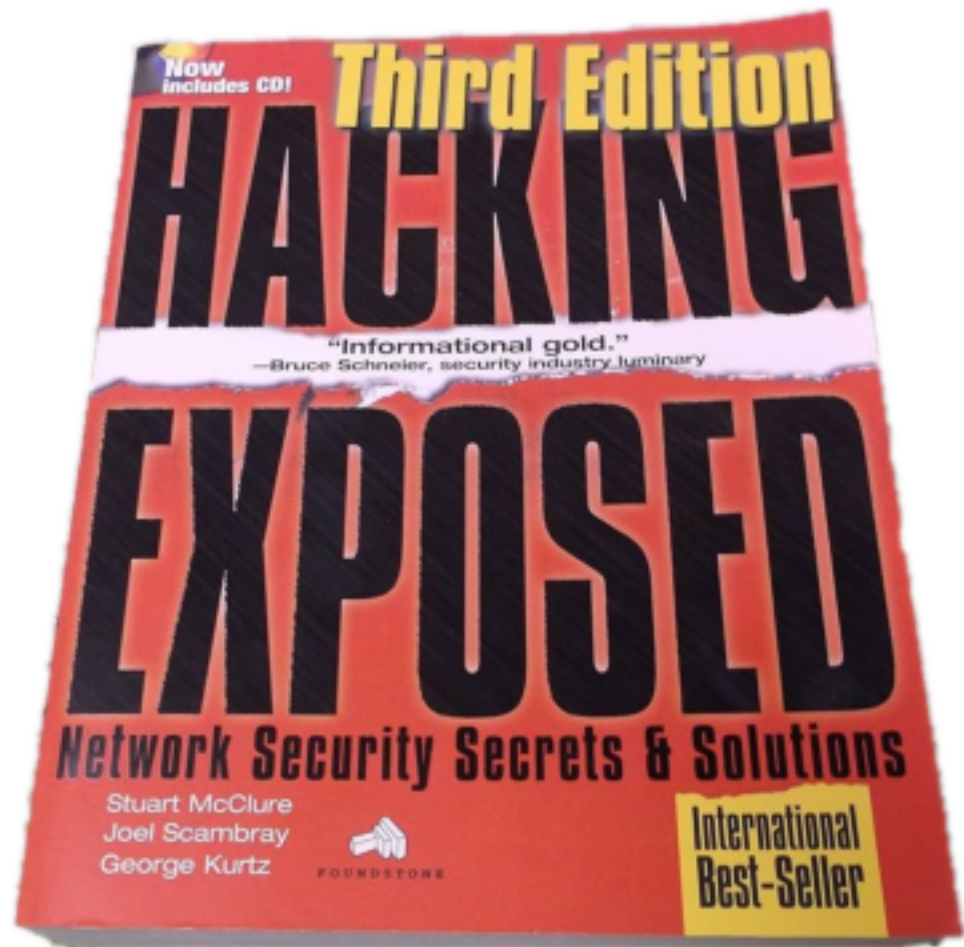


 **myspace**  
a place for friends



**ICES9**  
CONSULTING  
The Bugs I've Found,  
The Bugs I Have Yet To Find





Watch me



**ICES9**  
**CONSULTING**

The Bugs I've Found,  
The Bugs I Have Yet To Find



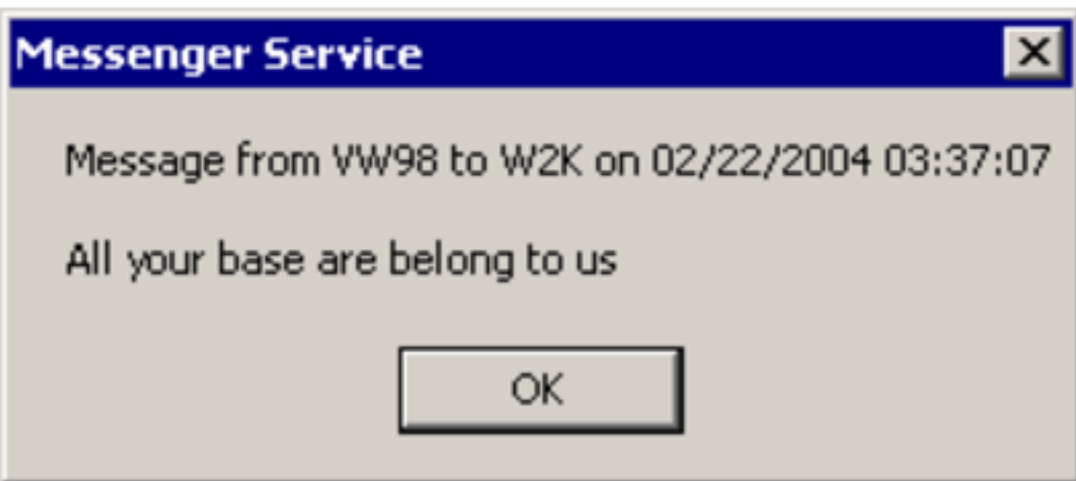
milw0rm.com

packet storm

**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find








**ICES9**  
**CONSULTING**

The Bugs I've Found,  
The Bugs I Have Yet To Find

Consent is not optional





```
00 00 00 00 00 00 00 00 .....  
00 00 00 00 00 2C 39 C2 .....9T  
00 31 00 00 00 00 00 00 A.....1.....  
00 49 20 6A 75 73 74 20 .....I just  
73 61 79 20 4C 4F 56 45 want to say LOUE  
21 21 00 00 00 00 00 00 YOU SAN?!.....  
61 74 65 73 20 77 68 79 .billy gates why  
6D 61 6B 65 20 74 68 69 do you make thi  
6C 65 20 3F 20 53 74 6F s possible ? Sto  
20 6D 6F 6E 65 79 20 61 p making money a  
6F 75 72 20 73 6F 66 74 nd fix your soft  
00 00 00 00 00 00 00 00 ware?!.....
```

Blaster

---

Welcome to <http://www.worm.com> !

Hacked By Chinese!

Code Red

**ICES9**  
CONSULTING

The Bugs I've Found,  
The Bugs I Have Yet To Find

# The 2010's

facebook



reddit

twitter 

**ICE9**  
CONSULTING  
The Bugs I've Found,  
The Bugs I Have Yet To Find



WhatsApp



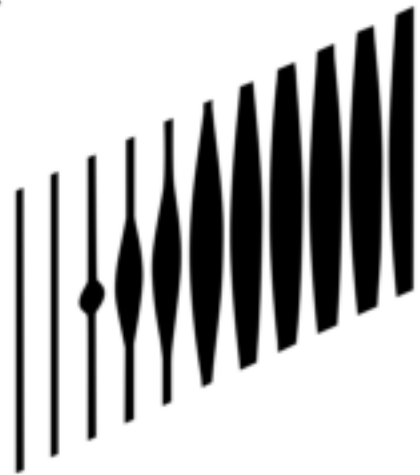
**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find





# The Decade of the Breach

ASHLEY MADISON<sup>®</sup>



**SONY  
PICTURES**

***EQUIFAX***



**TARGET**

**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

You became victim of the PETYA RANSOMWARE!

The haddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

<http://petya37h5tbhvyuki.onion/N19fvE>

<http://petya5koahtsf7sv.onion/N19fvE>

3. Enter your personal decryption code there:

If you already purchased your key, please enter it below.

Key:

Wana Decrypt0r 2.0

your files have been encrypted!

English

### What happened to My Computer?

Your files are encrypted.

Documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### How to Recover My Files?

We guarantee that you can recover all your files safely and easily. But you have to pay for some of your files for free. Try now by clicking <Decrypt>.

To decrypt all your files, you need to pay.

After you submit the payment, after that the price will be doubled.

If you don't pay in 7 days, you won't be able to recover your files forever.

We have many events for users who are so poor that they couldn't pay in 6 months.

How?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Check the current price of Bitcoin and buy some bitcoins. For more information, click <Buy bitcoins>.

Send the exact amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

**ICE9**  
CONSULTING

The Bugs I've Found,  
The Bugs I Have Yet To Find





**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find



**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find



**MPR 2200 MERV 13**  
**16" x 20" x 1"**

**2**  
FILTERS



**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

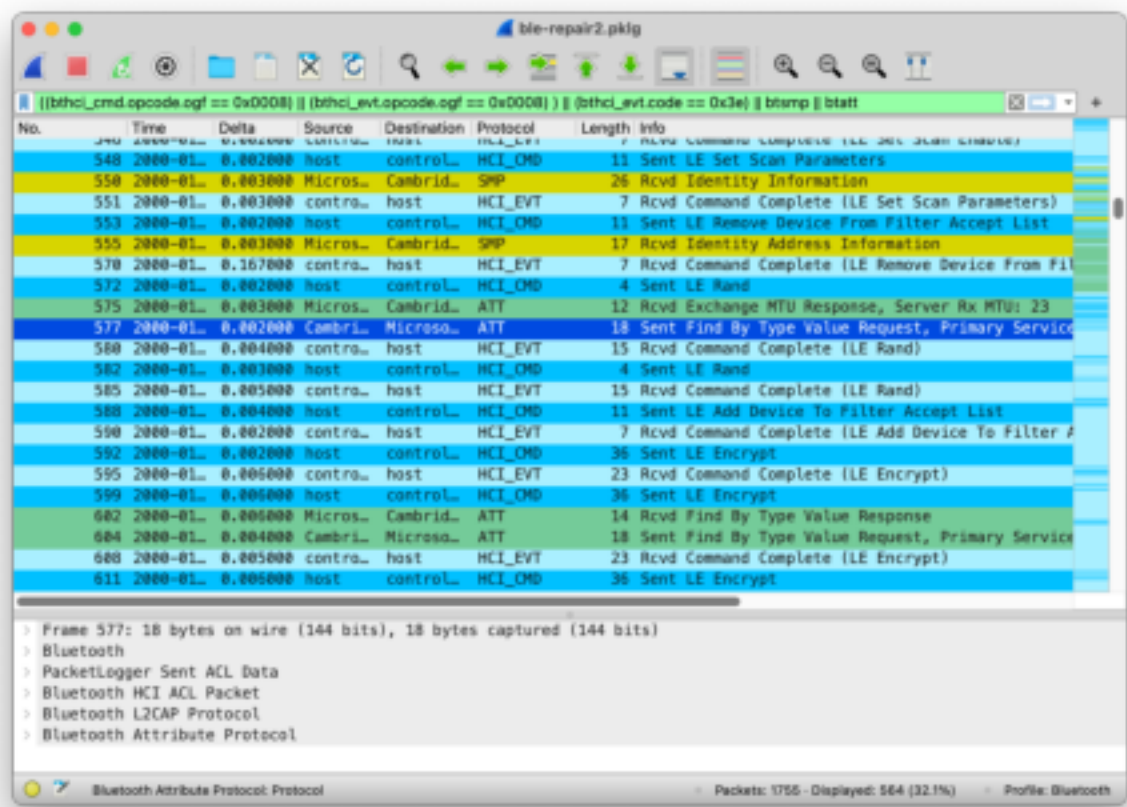


# BOOSTED



**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

# WIRESHARK



A screenshot of the Wireshark network protocol analyzer interface. The main pane displays a list of captured Bluetooth HCI packets. The filter bar at the top shows the active filter: `[[bthci_cmd.opcode == 0x0008] || (bthci_evt.opcode == 0x0008) || (bthci_evt.code == 0x3e) || btstamp >= btstart]`. The packet list table below shows various HCI commands and events, such as 'Sent LE Set Scan Parameters', 'Rcvd Identity Information', and 'Sent LE Encrypt'. The bottom pane shows the details of the selected packet (Frame 577), including the Bluetooth Attribute Protocol structure.

No.	Time	Delta	Source	Destination	Protocol	Length	Info
548	2000-01...	0.002000	host	control	HCI_CMD	11	Sent LE Set Scan Parameters
550	2000-01...	0.003000	Micros...	Cambrid...	SMP	26	Rcvd Identity Information
551	2000-01...	0.003000	contra...	host	HCI_EVT	7	Rcvd Command Complete (LE Set Scan Parameters)
553	2000-01...	0.002000	host	control	HCI_CMD	11	Sent LE Remove Device From Filter Accept List
555	2000-01...	0.003000	Micros...	Cambrid...	SMP	17	Rcvd Identity Address Information
570	2000-01...	0.167000	contra...	host	HCI_EVT	7	Rcvd Command Complete (LE Remove Device From Fil
572	2000-01...	0.002000	host	control	HCI_CMD	4	Sent LE Rand
575	2000-01...	0.003000	Micros...	Cambrid...	ATT	12	Rcvd Exchange MTU Response, Server Rx MTU: 23
577	2000-01...	0.002000	Cambrid...	Micros...	ATT	18	Sent Find By Type Value Request, Primary Service
580	2000-01...	0.004000	contra...	host	HCI_EVT	15	Rcvd Command Complete (LE Rand)
582	2000-01...	0.003000	host	control	HCI_CMD	4	Sent LE Rand
585	2000-01...	0.005000	contra...	host	HCI_EVT	15	Rcvd Command Complete (LE Rand)
588	2000-01...	0.004000	host	control	HCI_CMD	11	Sent LE Add Device To Filter Accept List
590	2000-01...	0.002000	contra...	host	HCI_EVT	7	Rcvd Command Complete (LE Add Device To Filter #
592	2000-01...	0.002000	host	control	HCI_CMD	36	Sent LE Encrypt
595	2000-01...	0.005000	contra...	host	HCI_EVT	23	Rcvd Command Complete (LE Encrypt)
599	2000-01...	0.005000	host	control	HCI_CMD	36	Sent LE Encrypt
602	2000-01...	0.005000	Micros...	Cambrid...	ATT	14	Rcvd Find By Type Value Response
604	2000-01...	0.004000	Cambrid...	Micros...	ATT	18	Sent Find By Type Value Request, Primary Service
600	2000-01...	0.005000	contra...	host	HCI_EVT	23	Rcvd Command Complete (LE Encrypt)
611	2000-01...	0.005000	host	control	HCI_CMD	36	Sent LE Encrypt



# ICES9 CONSULTING

The Bugs I've Found,  
The Bugs I Have Yet To Find



Price: \$\$\$\$

Capabilities: ++



Price: \$

Capabilities: --

**ICE9**  
**CONSULTING**

The Bugs I've Found,  
The Bugs I Have Yet To Find



RC021F2\r

RC02035\r

RC010DE\r

“checksum”

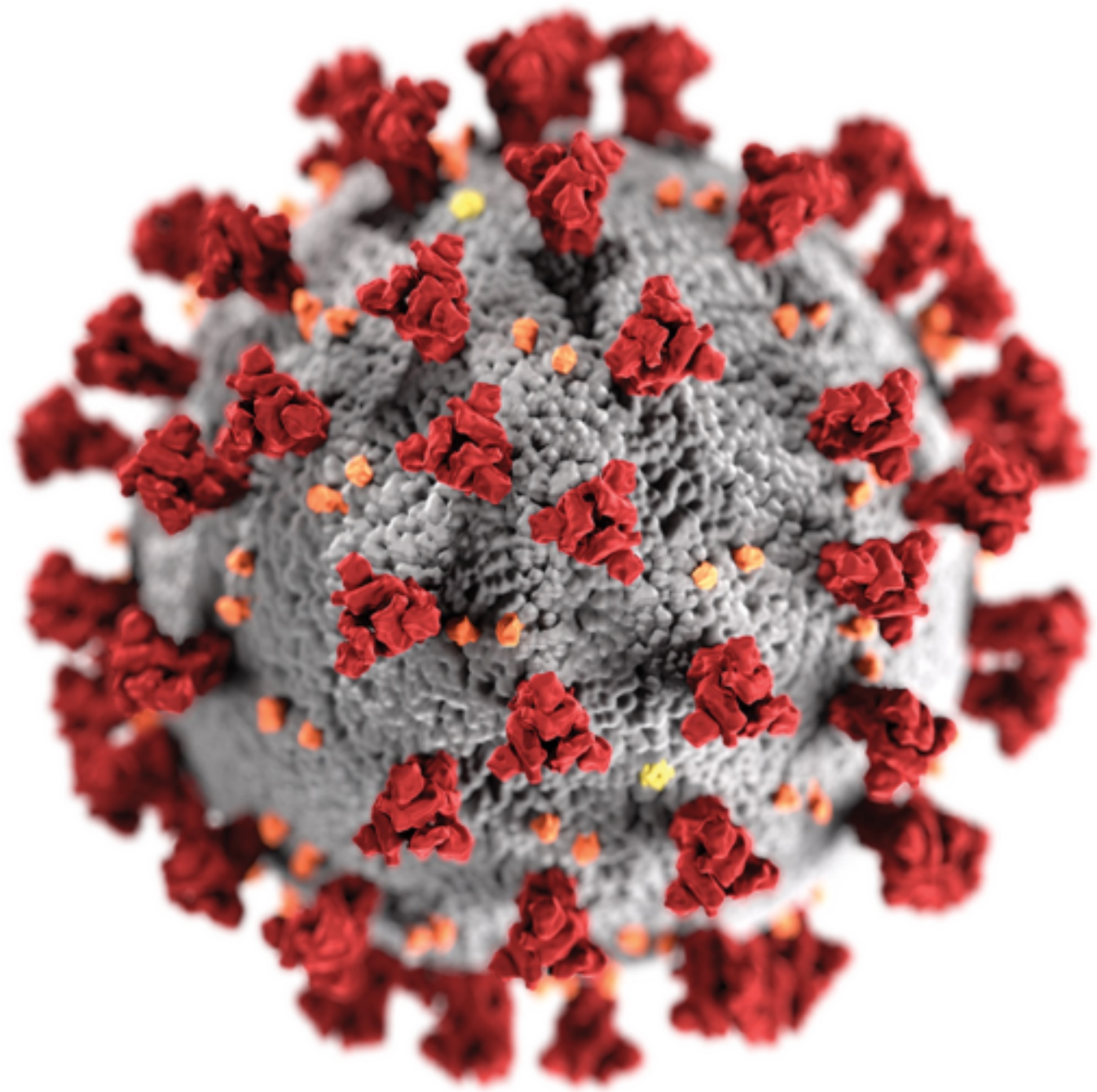
**ICE9**  
**CONSULTING**

The Bugs I've Found,  
The Bugs I Have Yet To Find

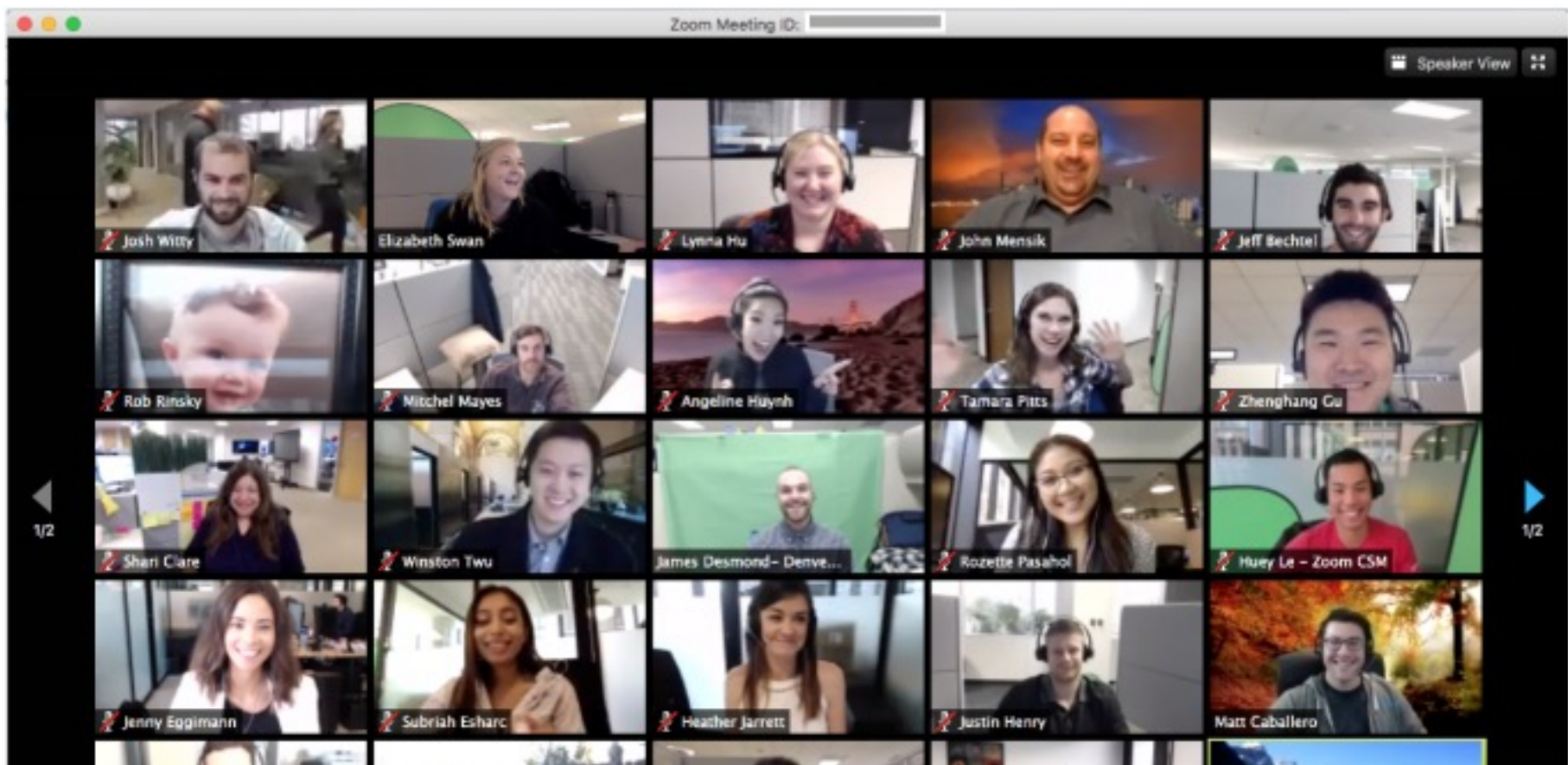
# CVE-2015-2247



# The 20's



**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find





**ICE9**  
**CONSULTING**

The Bugs I've Found,  
The Bugs I Have Yet To Find



**COLONIAL PIPELINE CO.**

**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

# solarwinds



**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

# MINECRAFT

LOG4J







**ICE9**  
**CONSULTING**  
The Bugs I've Found,  
The Bugs I Have Yet To Find

*Seek not bugs but understanding*

Patch your 🍌

Rotate your passwords

You are a target

*mike@ice9.us*