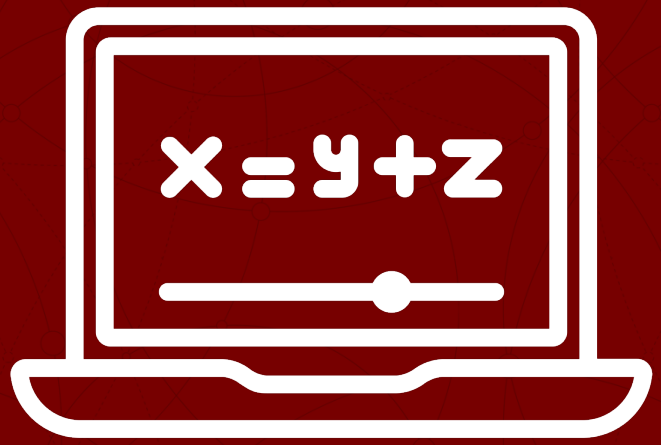
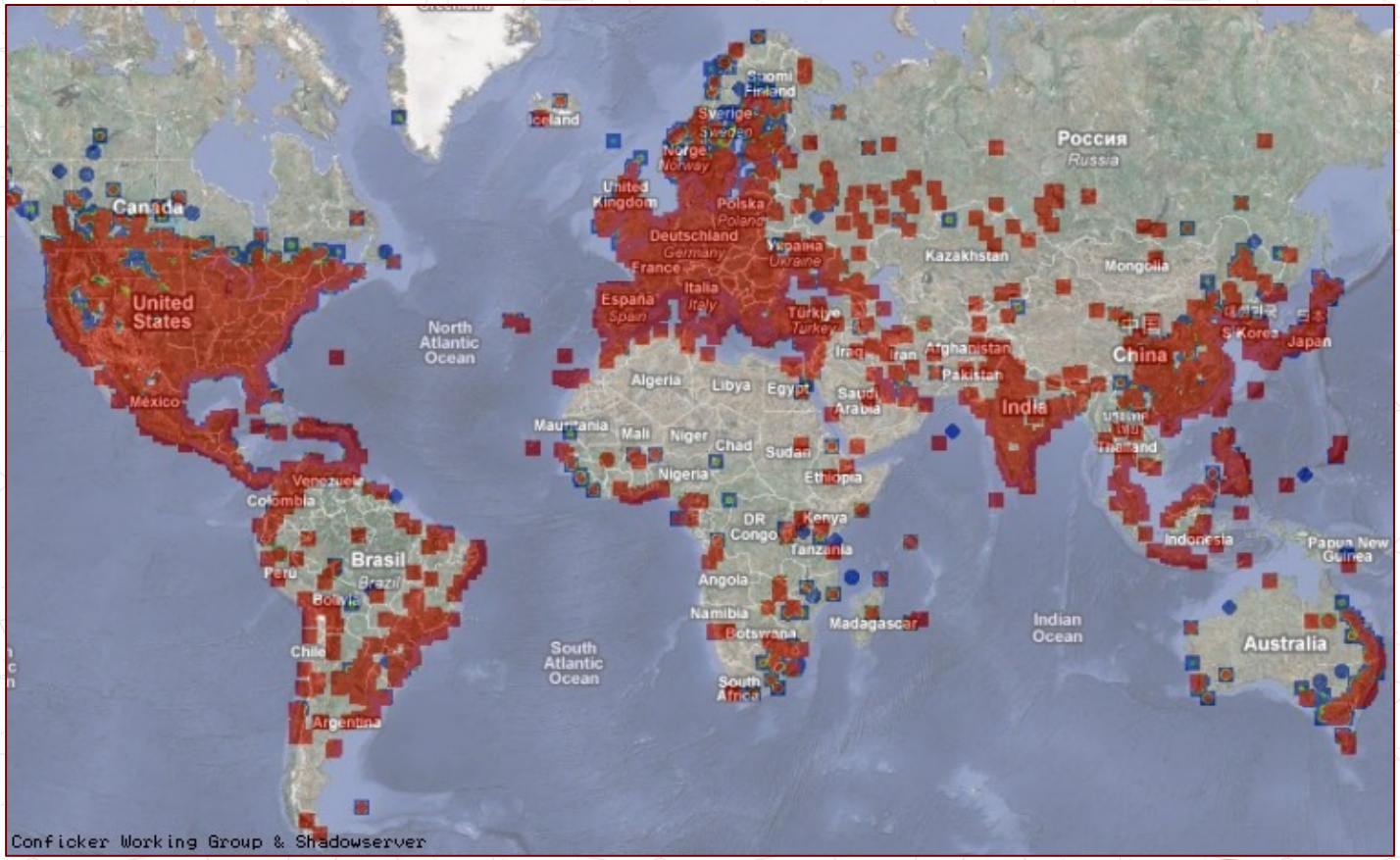



# Constraint Solving

Florida Tech IoT Security & Privacy Lab

# 15 Years Ago, The Internet Almost Died

- In 2008, the Conficker virus spread rapidly.
- It targeted an unprotected vulnerability in Windows.
- It communicated to its handlers with a secret channel.

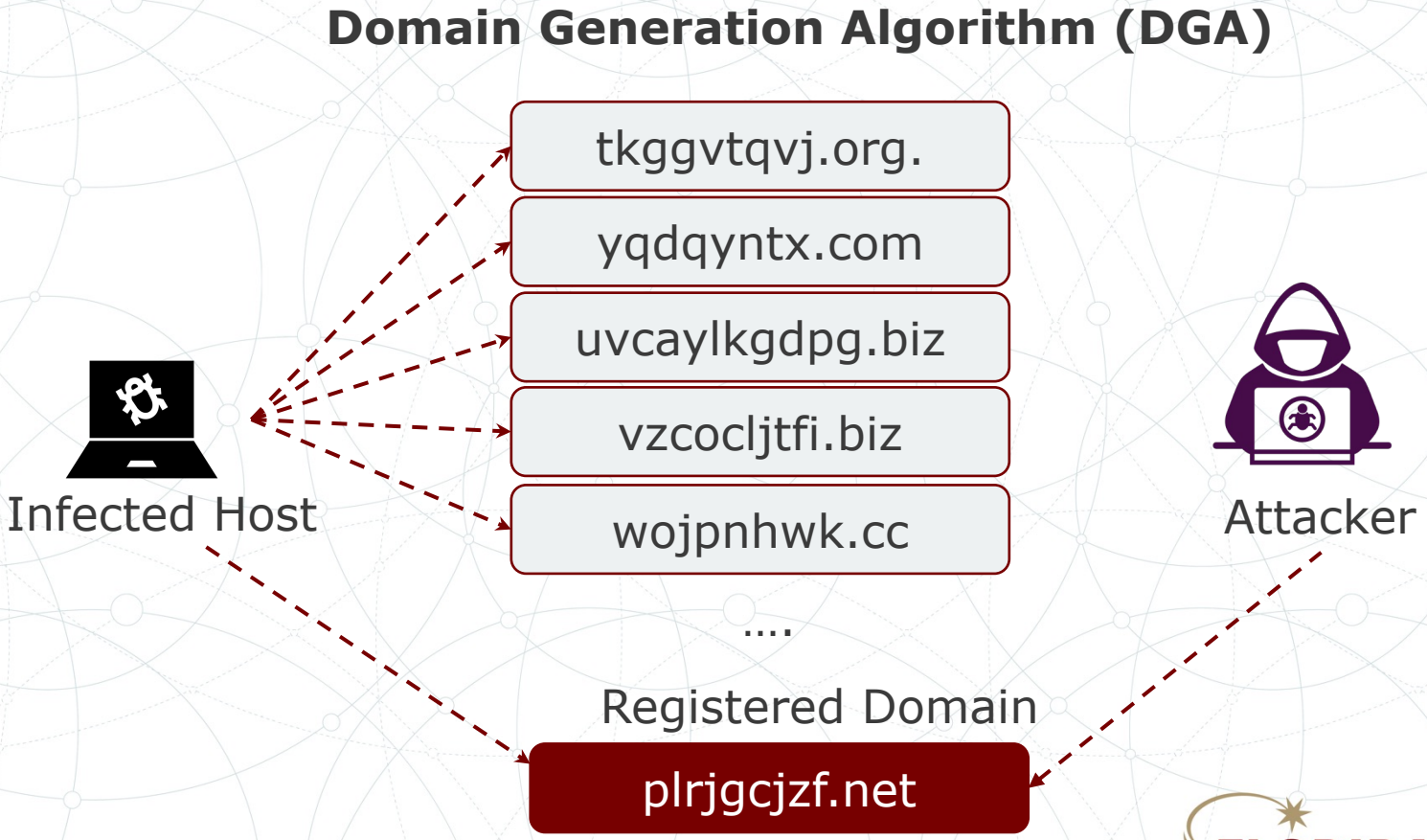



https://archive.f-secure.com/weblog/archives/00001646.html

FLORIDA TECH

# Confickers Communication Channel

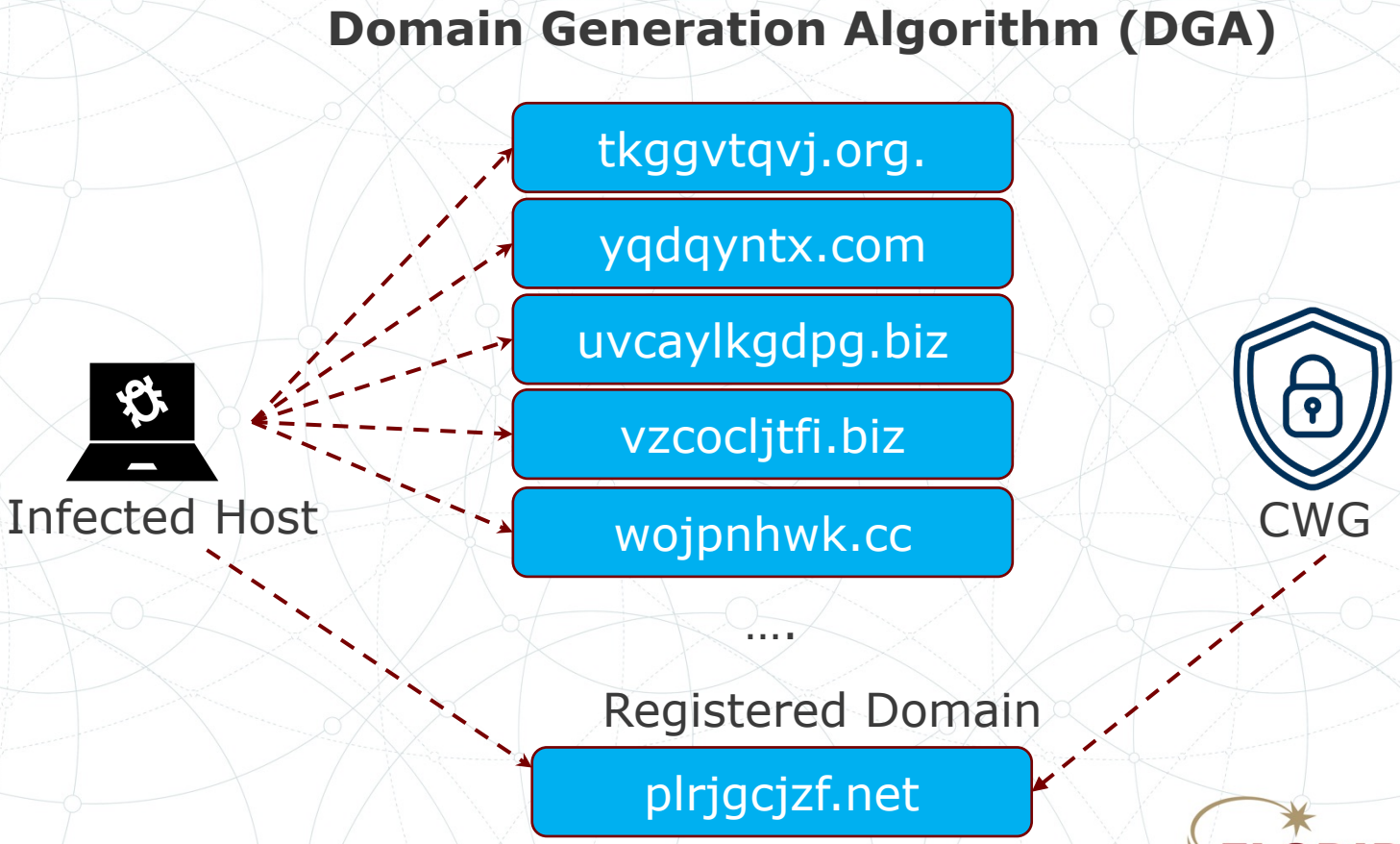
- Conficker used a DGA to create daily list of 500 domain names
- Attackers only registered a few of the actual domain names
- These registered domains served as rendezvous points for the attacker




FLORIDA TECH

# Predicting Communication Channel

- The Conficker Working Group (CWG) used constraint solving to determine the next domain names for the communication channels
- They registered the domain names before the attackers could and took command of conficker, saving the Internet.




FLORIDA TECH

# Constraint Solving Problems

what does that even mean?

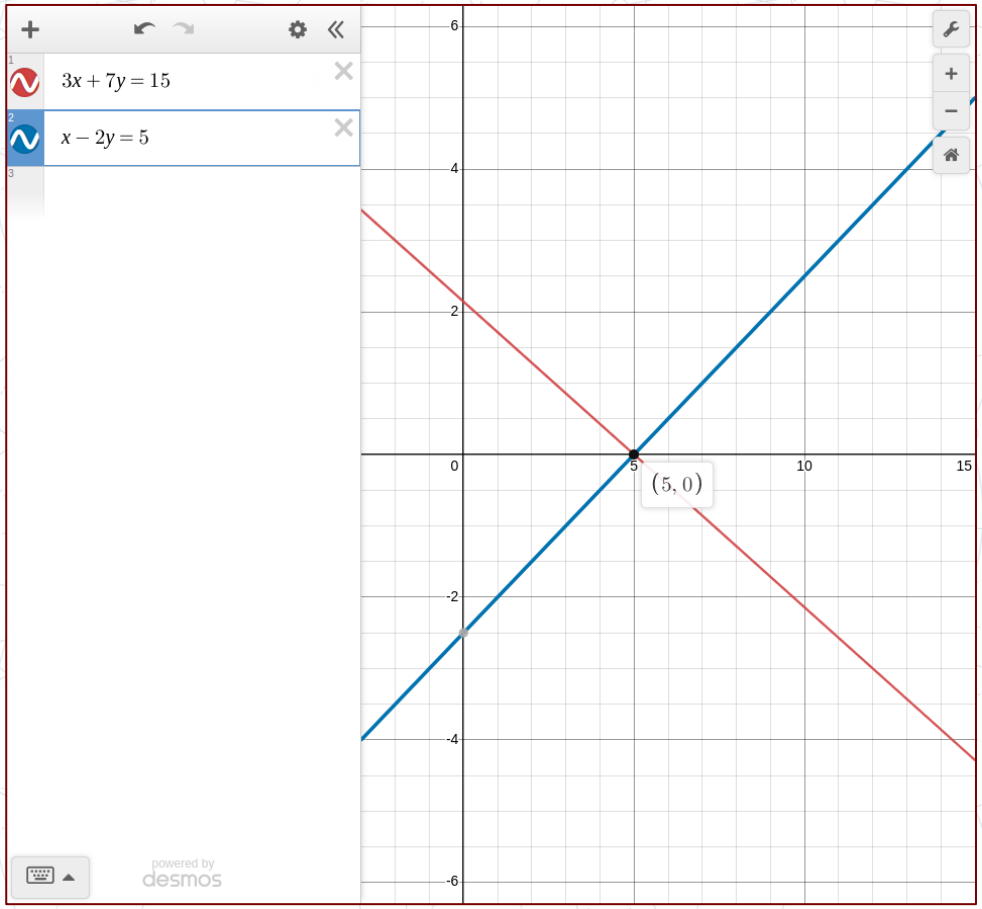
FLORIDA TECH

# How fast can you solve this?

$$3x + 7y = 15$$
$$x - 2y = 5$$

FLORIDA TECH

# Systems of Equations




Given the following equations:

$3x + 7y = 15$

$x - 2y = 5$

**Find appropriate values for x and y.**

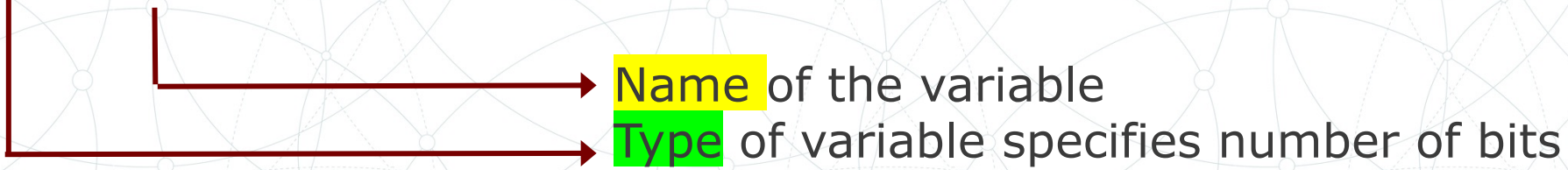
# Using Z3 in Python

FLORIDA TECH

$$3x + 7y = 15$$
$$x - 2y = 5$$

# Define Variables

```
x = Real('x')
y = Real('y')
```




FLORIDA TECH

$$3x + 7y = 15$$
$$x - 2y = 5$$

# Initialize Solver

```
x = Real('x')
y = Real('y')


s = Solver()
```

Create the variables and solver objects to find the solution

FLORIDA TECH

$$3x + 7y = 15$$
$$x - 2y = 5$$

# Add Constraints

```
x = Real('x')
y = Real('y')

s = Solver()

s.add(3 * x + 7 * y == 15)
s.add(x - 2 * y == 5)
```

Define the rules (constraints) for each variable

FLORIDA TECH

$$3x + 7y = 15$$
$$x - 2y = 5$$

# Determine Solution

```
x = Real('x')
y = Real('y')

s = Solver()

s.add(3 * x + 7 * y == 15)
s.add(x - 2 * y == 5)

s.check()

print("x:", s.model()[x])
print("y:", s.model()[y])
```

- s.check() will return either "sat" or "unsat"
- Print the value of each variable stored in the solver's "model"

FLORIDA TECH

$$3x + 7y = 15$$
$$x - 2y = 5$$

# Constraint Solving Steps

```
x = Real('x')
y = Real('y')

s = Solver()

s.add(3 * x + 7 * y == 15)
s.add(x - 2 * y == 5)

s.check()

print("x:", s.model()[x])
print("y:", s.model()[y])
```

Initialize variables

Initialize solver object

Add constraints

Determine Solution

FLORIDA TECH

# But what if the problem was harder?

$$3x + 7y = 15$$
$$x - 2y = 5$$
$$(x-5)^2/3 + y = 0$$
$$x-5 = y^3$$
$$y = (1/x) - (1/5)$$

FLORIDA TECH

# Computers Solve Hard Problems Fast

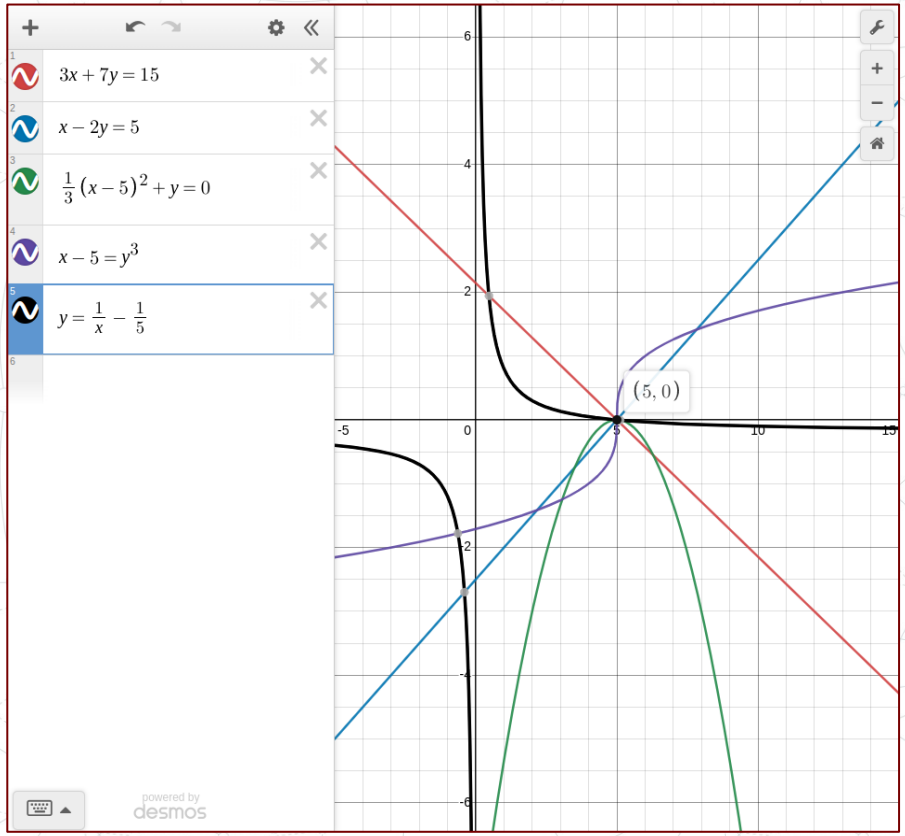
```
x = Real('x')
y = Real('y')

s = Solver()

s.add(3 * x + 7 * y == 15)
s.add(x - 2 * y == 5)
s.add(((x - 5) ** 2)/3 + y == 0)
s.add(x - 5 == y ** 3)
s.add(y == 1 / x - 1 / 5)

s.check()

print("x:", s.model()[x])
print("y:", s.model()[y])
```




FLORIDA TECH

# Beating Rumpelstiltskin

Win the game and escape the forest!

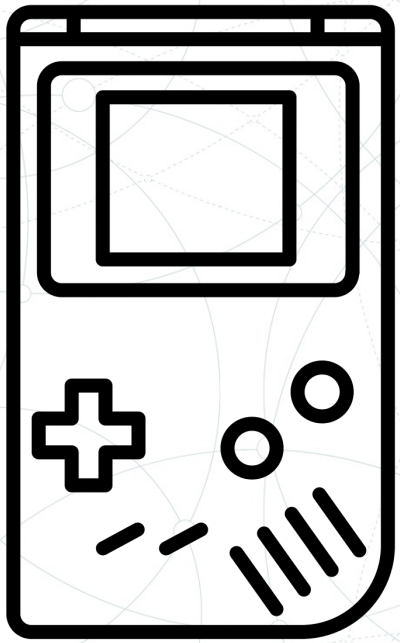
FLORIDA TECH

# Solve the Riddle

Use what you've learned to guess Rumpelstiltskin's favorite number!

Connect to WiFi Access Point

Go to http://10.3.141.1 to get started



Initialize variables
Initialize solver object
Add constraints
Determine Solution

FLORIDA TECH

FLORIDA TECH

# Thank you.