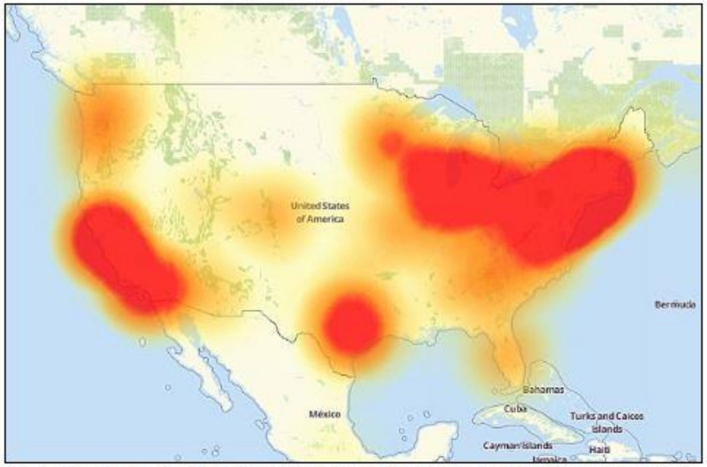
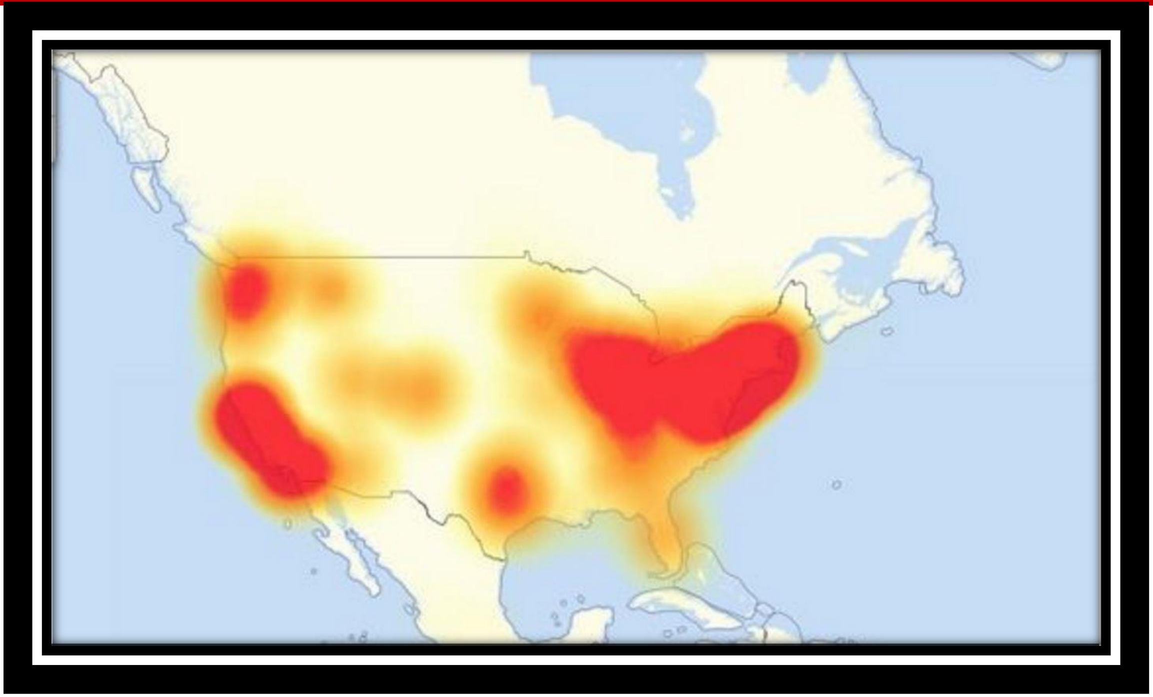
Mirai Botnet



Internet users across the globe were hit throughout the day as 'several' massive cyber attacks hit a DNS service provider. This image shows problems reported with Level 3, a business service provider.

October 21, 2016 Screenshot from:
http://downdetector.com/

Mirai Botnet: How IoT Botnets Performed Massive DDoS Attacks and Negatively Impacted Hundreds of Thousands of Internet Businesses and Millions of Users in October 2016



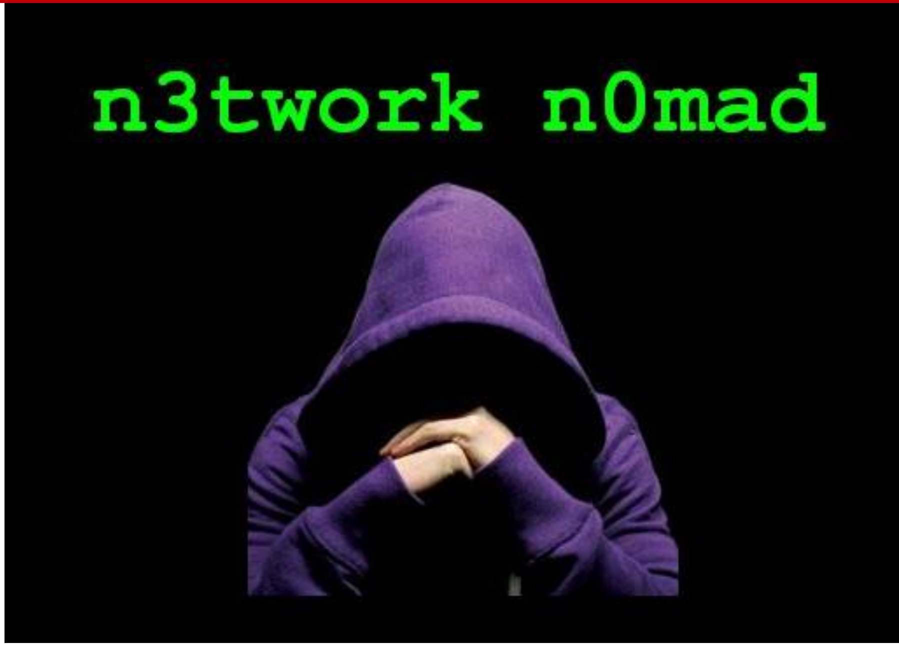
William Favre Slater, III, M.S. MBA, PMP, CISSP, CISA

Sr. Cybersecurity Consultant and Adjunct Professor, IIT School of Applied Technology

ILLINOIS INSTITUTE OF TECHNOLOGY

Agenda

- Introduction
- WHY Is This important?
- Internet of Things – Size and Typical Devices
- What is a Botnet?
- DDoS Attacks
- Little Known Roots of the Mirai Botnet
- Pre-Attack Events
- What Did the Mirai Botnet Do in October 2016?
- How Did Mirai Work?
- Post-Attack Events
- How Can an Organization Protect Against Mirai and other Botnet Attacks?
- Hajime! Some Recent “Good News”
- Conclusion
- Questions
- References
- Bio



ILLINOIS INSTITUTE OF TECHNOLOGY

Introduction

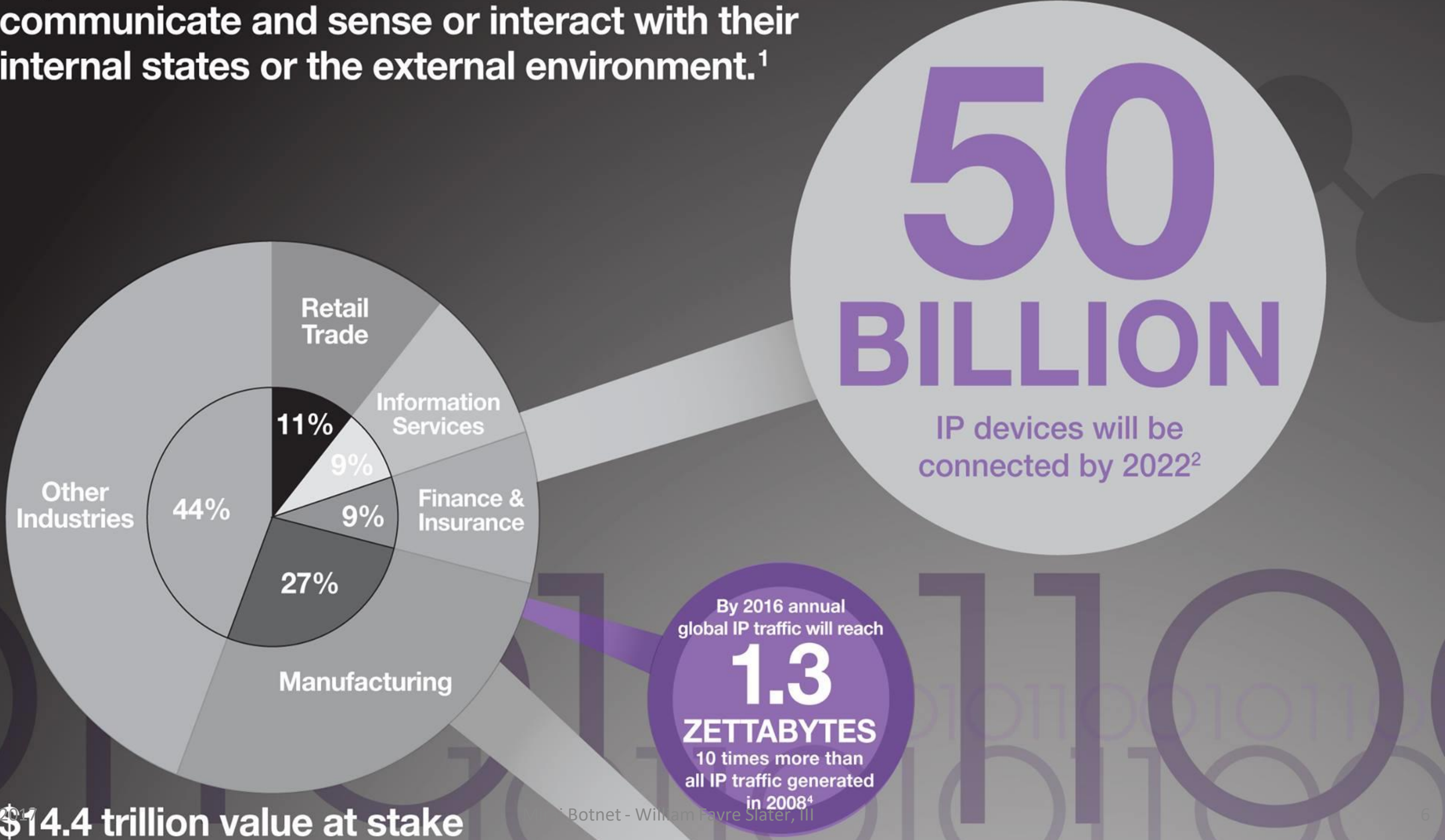
- Mirai is the Japanese word for “The Future”
- The Mirai Botnet Attack of October 2016 used known security weaknesses in tens of millions of Internet of Things (IoT) Devices to launch massive Distributed Denial of Services Attacks against DYN, which is a major DNS Service provider. The result was a notable performance degrades in tens of thousands of businesses who rely heavily on the Internet, and millions of users who used these services. A short time before the attack, the Mirai Botnet code was shared on the Internet as it was placed into Open Source. With the exponential rise of the population of IoT devices, what does the Mirai Botnet attack mean for the future of Internet Security?
- This presentation will examine the implications of the Mirai Botnet code and the explosion of IoT.

WHY Is this Presentation Important?

- The Internet has been business critical since 1997
- The Internet, the World Wide Web, web applications, data, and resources they represent are often considered by many to be *critical infrastructure*
- Outages (any) can cost *money*, *lost customers*, and even *brand damage*
- Everyone who uses the Internet in a business capacity should be aware of the DDoS Threat that the *Mirai Botnet* and similar programs represent
- The *Internet of Things* that plays a major role in this saga, continues to grow exponentially in popularity and in capability

Internet of Things

The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.[1]

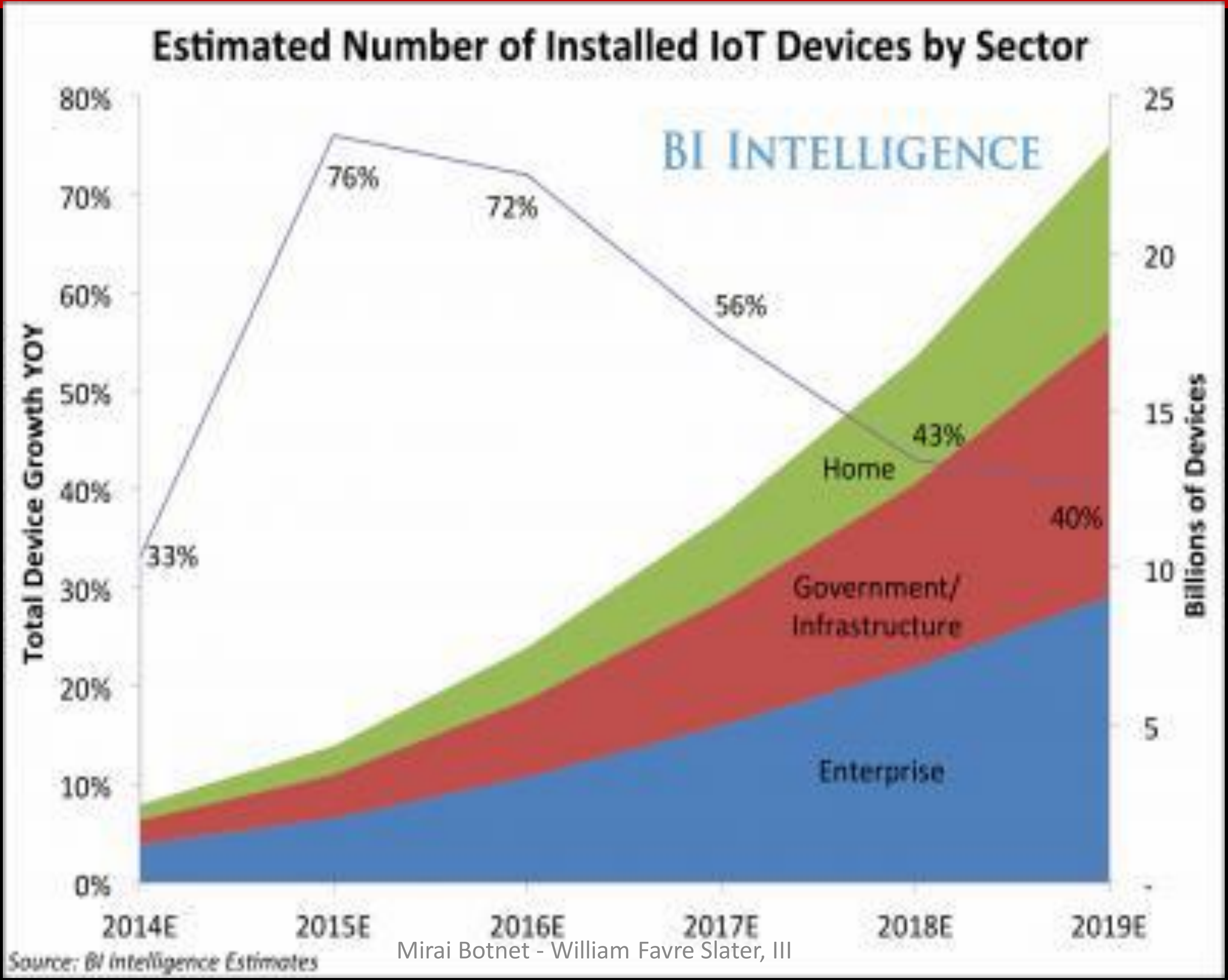


50 BILLION IP devices will be connected by 2022[2]

By 2016 annual global IP traffic will reach **1.3 ZETTABYTES** 10 times more than all IP traffic generated in 2008[4]

$14.4 trillion value at stake

How Big is the "Internet of Things"?

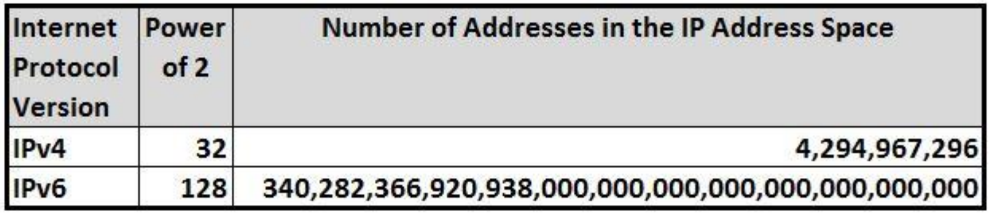


Source: BI Intelligence Estimates

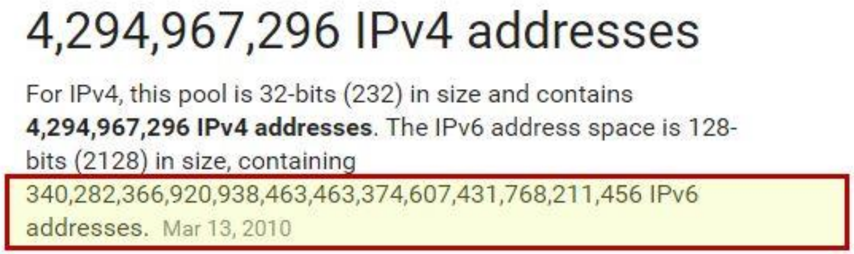
Typical IoT Devices

- CCTV cameras
- DVRs
- Digital TVs
- Home routers
- Printers
- Alexa
- Security systems
- Garage doors
- Industrial systems
- Medical systems
- Home appliances
- Smart Utility Meters
- Cars
- Other stuff

Often "Internet of Things" Devices and Typically Cell Phones are Accessing the Internet Via IPv6



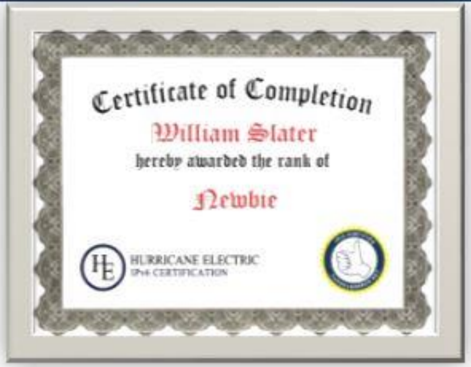
Internet Protocol Version	Power of 2	Number of Addresses in the IP Address Space
IPv4	32	4,294,967,296
IPv6	128	340,282,366,920,938,000,000,000,000,000,000,000,000



4,294,967,296 IPv4 addresses

For IPv4, this pool is 32-bits (232) in size and contains **4,294,967,296 IPv4 addresses**. The IPv6 address space is 128-bits (2128) in size, containing 340,282,366,920,938,463,463,374,607,431,768,211,456 IPv6 addresses. Mar 13, 2010

Learn more about IPv6 and get up to five free IPv6 certifications at http://ipv6.he.net



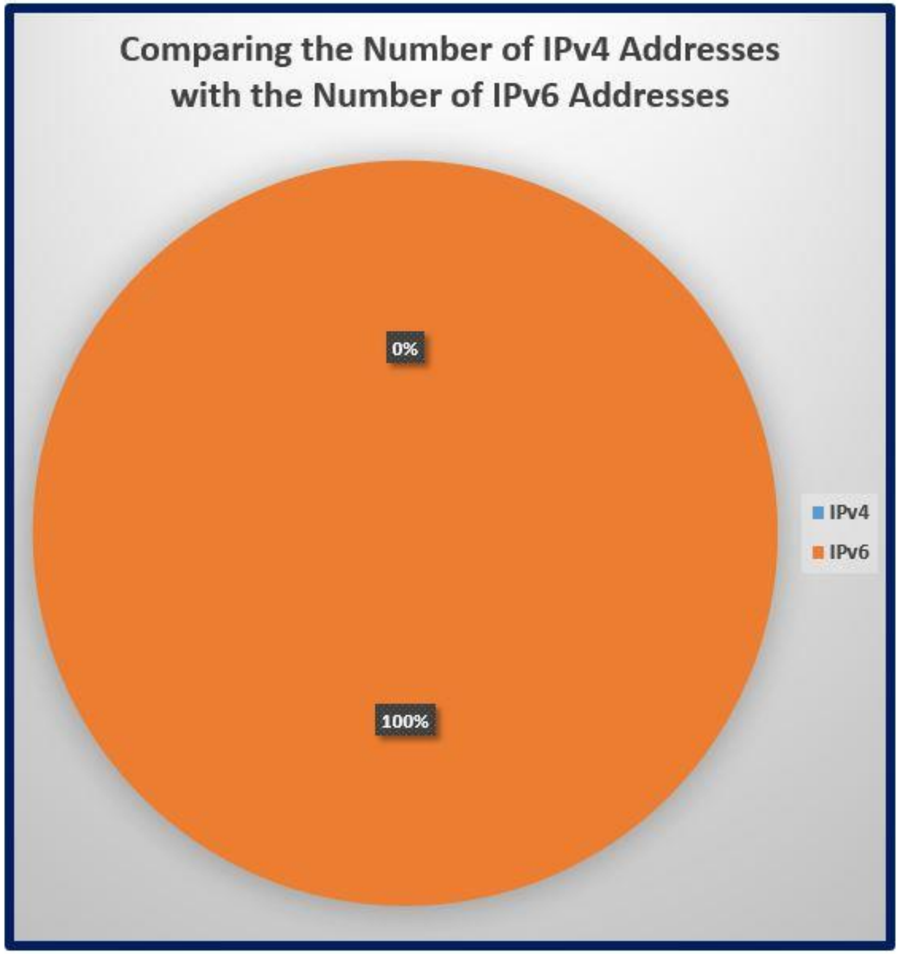
Certificate of Completion

William Slater

hereby awarded the rank of

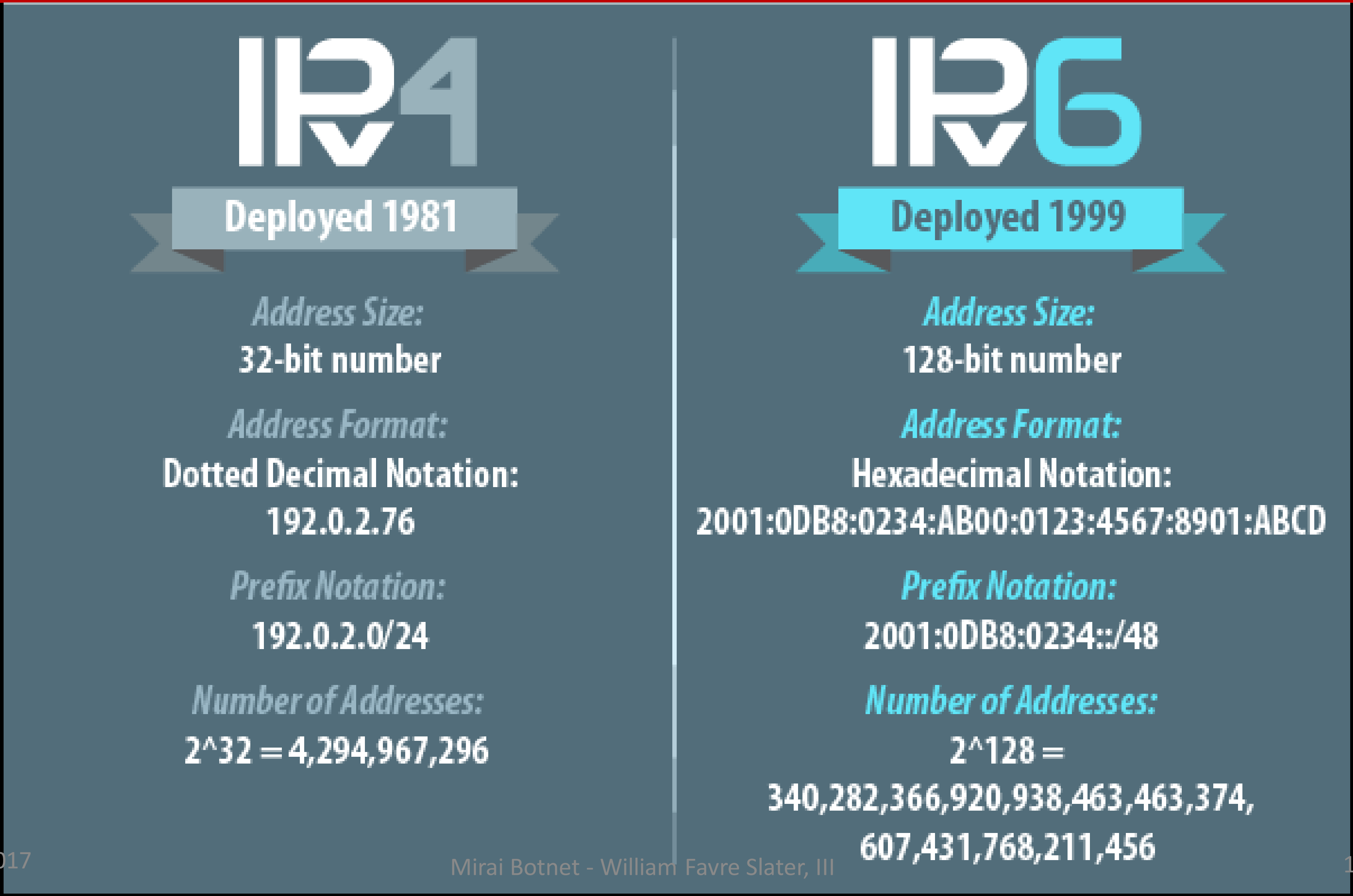
Newbie

HURRICANE ELECTRIC
IPv6 CERTIFICATION



ILLINOIS INSTITUTE OF TECHNOLOGY

Comparing IPv4 and IPv6



IPv4

Deployed 1981

Address Size:
32-bit number

Address Format:
Dotted Decimal Notation:
192.0.2.76

Prefix Notation:
192.0.2.0/24

Number of Addresses:
2^32 = 4,294,967,296

IPv6

Deployed 1999

Address Size:
128-bit number

Address Format:
Hexadecimal Notation:
2001:0DB8:0234:AB00:0123:4567:8901:ABCD

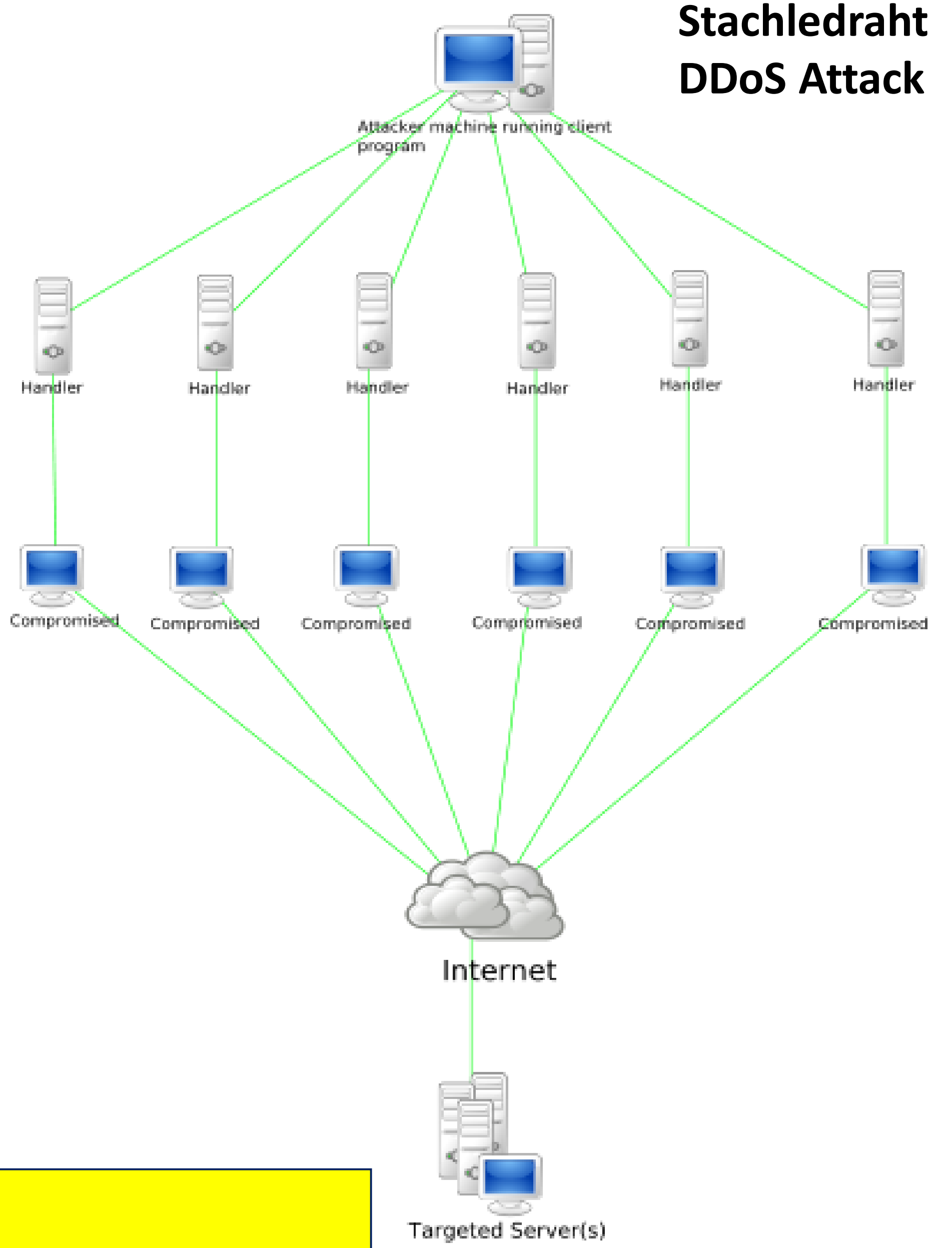
Prefix Notation:
2001:0DB8:0234::/48

Number of Addresses:
2^128 =
340,282,366,920,938,463,463,374,
607,431,768,211,456

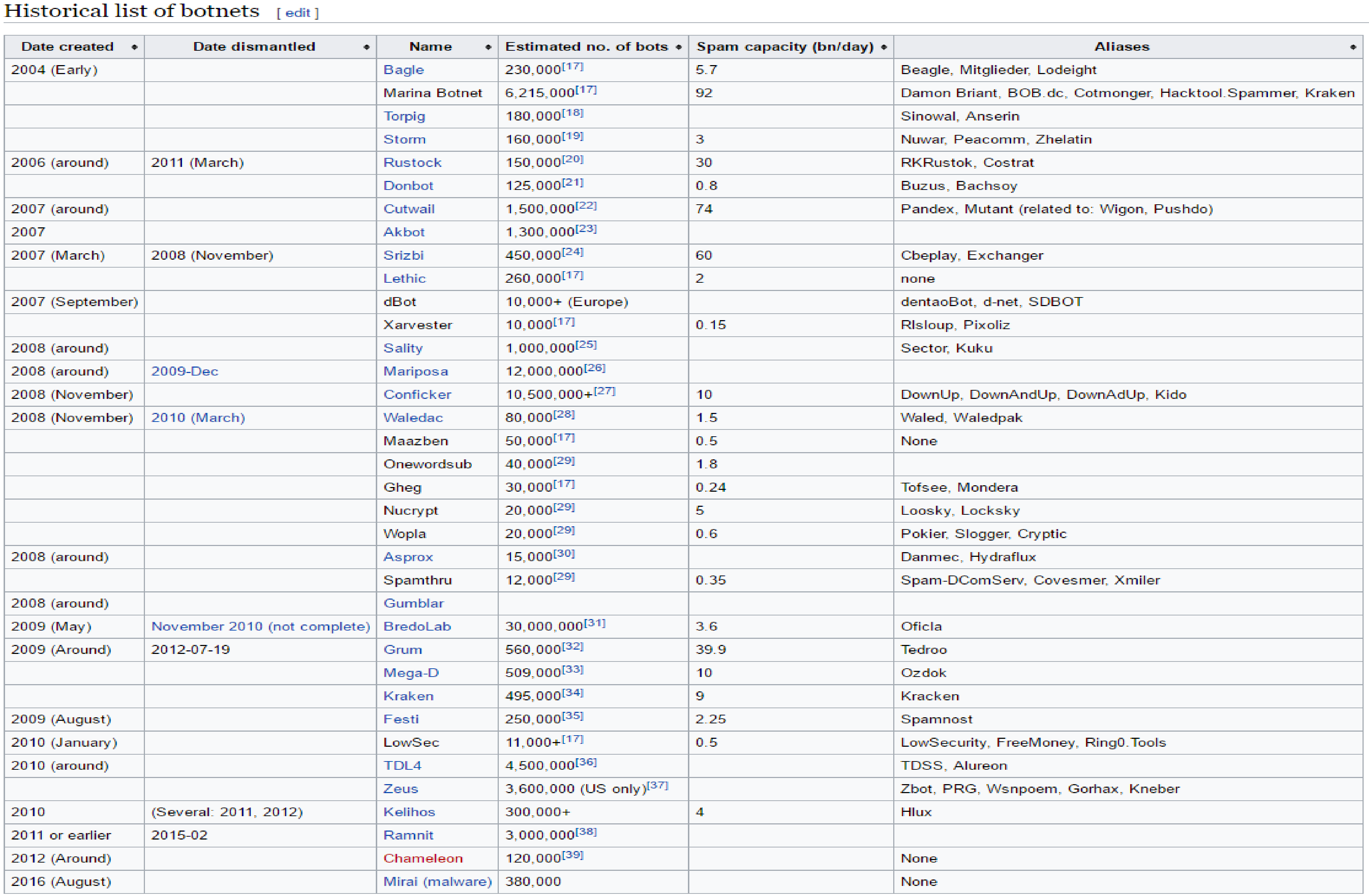
What is a Botnet?

- A ***botnet*** is a number of Internet-connected devices used by a botnet owner to perform various tasks. Botnets can be used to perform Distributed Denial Of Service Attack, steal data, send spam, allow the attacker access to the device and its connection. The owner can control the botnet using command and control (C&C) software. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation.
- ***Botnets have been around since 2004.***
- Attacker machines are usually running the ***Linux operating system***.

Stachledraht DDoS Attack



Sources:
Wikipedia https://en.wikipedia.org/wiki/Botnet
Cheng, G. (2005) . http://www.giac.org/paper/gcih/229/analysis-ddos-tool-stacheldraht-v1666/102150



Historical list of botnets [edit]

Date created	Date dismantled	Name	Estimated no. of bots	Spam capacity (bn/day)	Aliases
2004 (Early)		Bagle	230,000[17]	5.7	Beagle, Mitglieder, Lodeight
		Marina Botnet	6,215,000[17]	92	Damon Briant, BOB.dc, Cotmonger, Hacktool.Spammer, Kraken
		Torpig	180,000[18]		Sinowal, Anserin
		Storm	160,000[19]	3	Nuwar, Peacomm, Zhelatin
2006 (around)	2011 (March)	Rustock	150,000[20]	30	RKRustok, Costrat
		Donbot	125,000[21]	0.8	Buzus, Bachsoy
2007 (around)		Cutwail	1,500,000[22]	74	Pandex, Mutant (related to: Wigon, Pushdo)
2007		Akbot	1,300,000[23]		
2007 (March)	2008 (November)	Srizbi	450,000[24]	60	Cbeplay, Exchanger
		Lethic	260,000[17]	2	none
2007 (September)		dBot	10,000+ (Europe)		dentaoBot, d-net, SDBOT
		Xarvester	10,000[17]	0.15	Rlsloup, Pixoliz
2008 (around)		Sality	1,000,000[25]		Sector, Kuku
2008 (around)	2009-Dec	Mariposa	12,000,000[26]		
2008 (November)		Conficker	10,500,000+[27]	10	DownUp, DownAndUp, DownAdUp, Kido
2008 (November)	2010 (March)	Waledac	80,000[28]	1.5	Waled, Waledpak
		Maazben	50,000[17]	0.5	None
		Onewordsub	40,000[29]	1.8	
		Gheg	30,000[17]	0.24	Tofsee, Mondera
		Nucrypt	20,000[29]	5	Loosky, Locksky
		Wopla	20,000[29]	0.6	Pokier, Slogger, Cryptic
2008 (around)		Asprox	15,000[30]		Danmec, Hydraflux
		Spamthru	12,000[29]	0.35	Spam-DComServ, Covesmer, Xmiler
2008 (around)		Gumblar			
2009 (May)	November 2010 (not complete)	BredoLab	30,000,000[31]	3.6	Oficla
2009 (Around)	2012-07-19	Grum	560,000[32]	39.9	Tedroo
		Mega-D	509,000[33]	10	Ozdok
		Kraken	495,000[34]	9	Kracken
2009 (August)		Festi	250,000[35]	2.25	Spamnost
2010 (January)		LowSec	11,000+[17]	0.5	LowSecurity, FreeMoney, Ring0.Tools
2010 (around)		TDL4	4,500,000[36]		TDSS, Alureon
		Zeus	3,600,000 (US only)[37]		Zbot, PRG, Wsnpoem, Gorhax, Kneber
2010	(Several: 2011, 2012)	Kelihos	300,000+	4	Hlux
2011 or earlier	2015-02	Ramnit	3,000,000[38]		
2012 (Around)		Chameleon	120,000[39]		None
2016 (August)		Mirai (malware)	380,000		None

Sources:
Wikipedia https://en.wikipedia.org/wiki/Botnet

ILLINOIS INSTITUTE
OF TECHNOLOGY

DDoS Attacks

DoS Attack

A Denial of Service (DoS) attack is an attack that can make your website or application unavailable to end users. To achieve this, attackers use a variety of techniques that consume network or other resources, disrupting access for legitimate end users. In its simplest form, a DoS attack against a target is executed by a lone attacker from a single source, as shown in Figure 1.

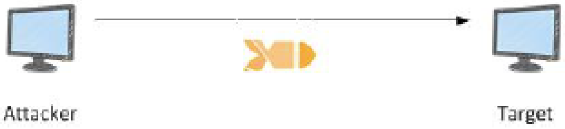


Figure 1: Diagram of a DOS attack

DDoS Attacks

In the case of a Distributed Denial of Service (DDoS) attack, an attacker uses multiple sources—which may be compromised or controlled by a group of collaborators—to orchestrate an attack against a target. As illustrated in Figure 2, in a DDoS attack, each of the collaborators or compromised hosts participates in the attack, generating a flood of packets or requests to overwhelm the intended target.

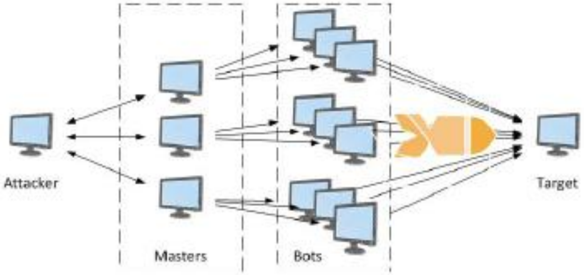


Figure 2: Diagram of a DDOS attack

Source:
AWS Best Practices for DDoS Resiliency
https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

Types of DDoS Attacks

- HTTP Floods
- DNS Query Floods
- SSL Abuse
- TCP SYN Floods
- TCP ACK Floods
- TCP NULL Floods
- Stream Flood
- UDP Flood
- UDP Reflection
- Smurf Attack
- ICMP PING Floods
- GRE IP Floods
- GRE ETH Floods

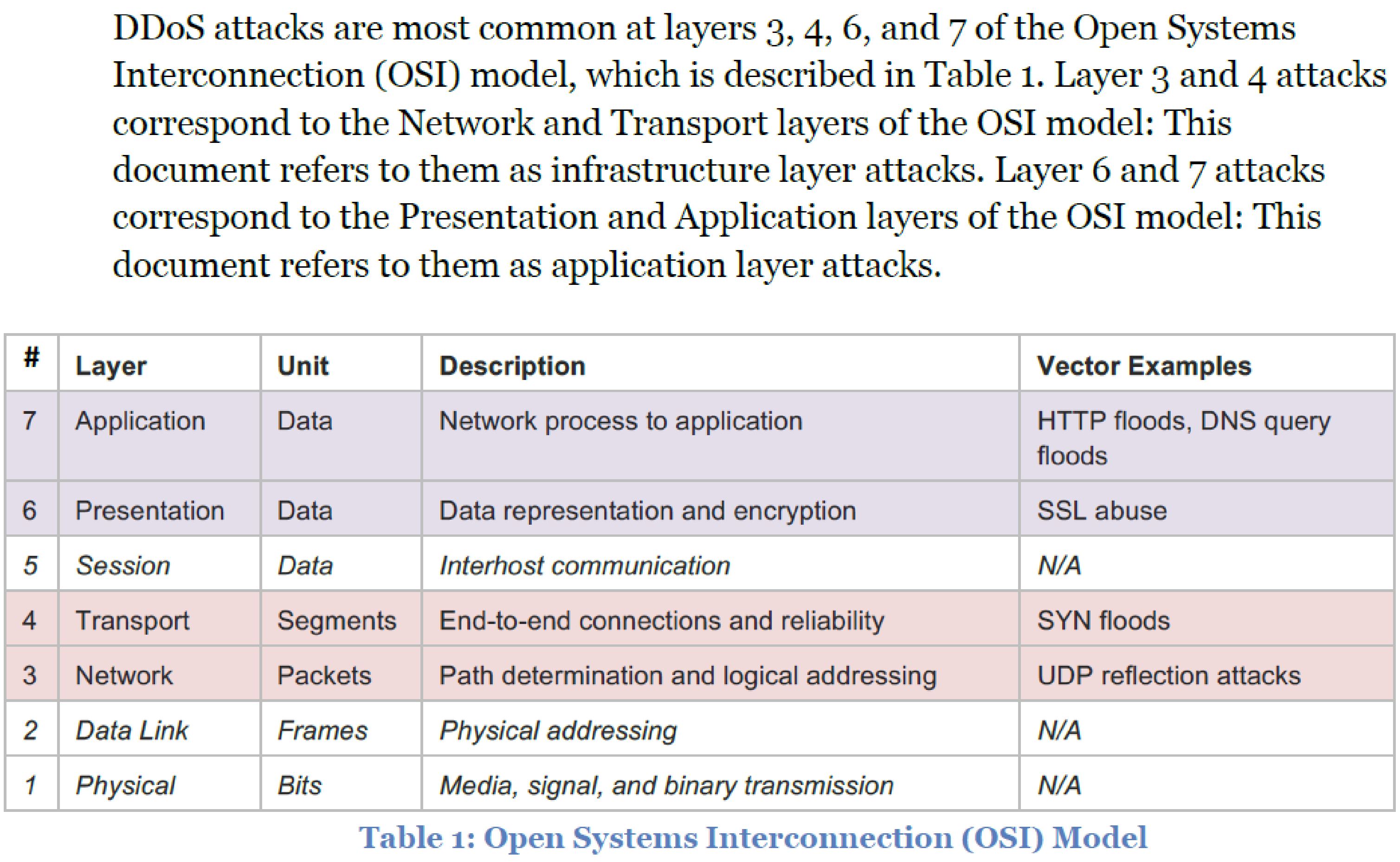
The Mirai Botnet infected and harnessed millions of IoT Devices to attack 17 DYN DNS Provider Data Centers and impair their ability to resolve DNS requests.

Mirai is designed and was implemented to employ SEVERAL of these DDoS attack methods.

Sources:
AWS Best Practices for DDoS Resiliency
https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf
Cheng, G. (2005). http://www.giac.org/paper/gcih/229/analysis-ddos-tool-stacheldraht-v1666/102150
Herzberg, B., Bekerman, D., and Zeifman, I
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

ILLINOIS INSTITUTE OF TECHNOLOGY

Types of DDoS Attacks



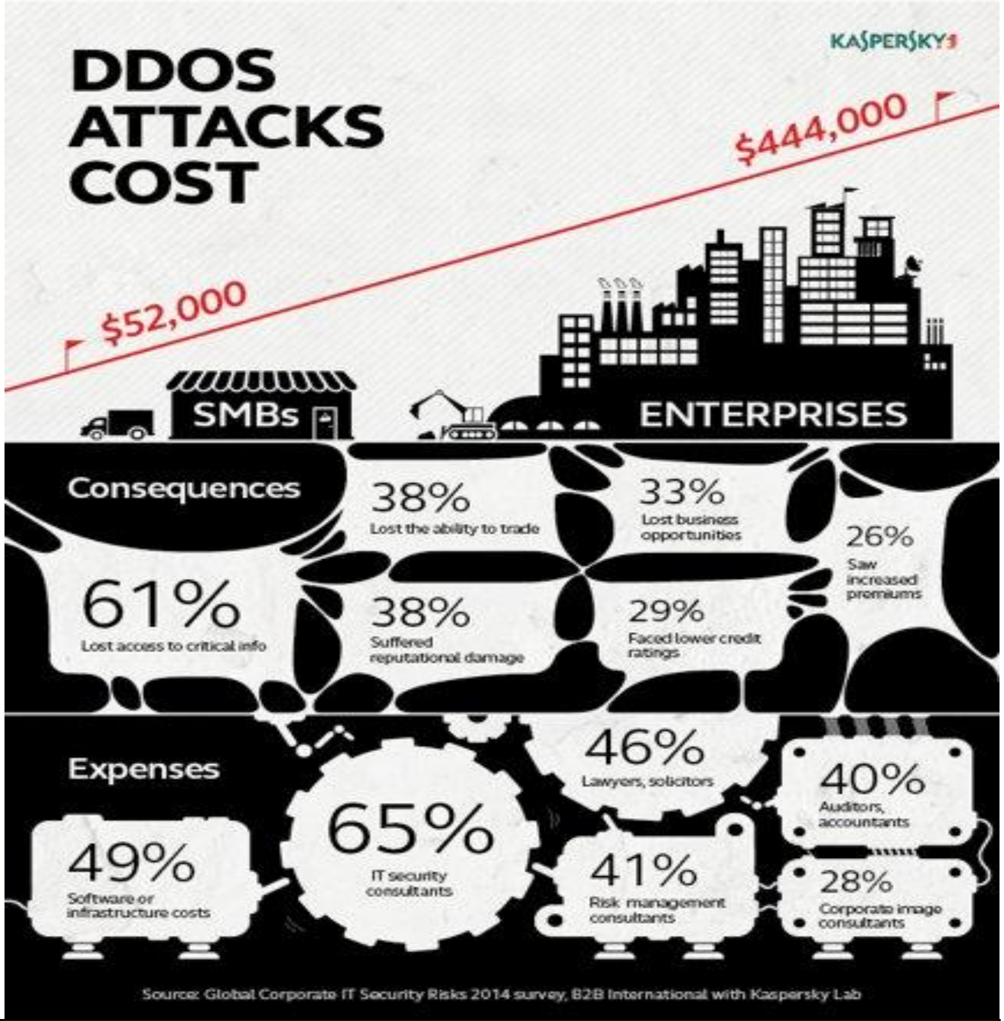
DDoS attacks are most common at layers 3, 4, 6, and 7 of the Open Systems Interconnection (OSI) model, which is described in Table 1. Layer 3 and 4 attacks correspond to the Network and Transport layers of the OSI model: This document refers to them as infrastructure layer attacks. Layer 6 and 7 attacks correspond to the Presentation and Application layers of the OSI model: This document refers to them as application layer attacks.

#	Layer	Unit	Description	Vector Examples
7	Application	Data	Network process to application	HTTP floods, DNS query floods
6	Presentation	Data	Data representation and encryption	SSL abuse
5	*Session*	*Data*	*Interhost communication*	*N/A*
4	Transport	Segments	End-to-end connections and reliability	SYN floods
3	Network	Packets	Path determination and logical addressing	UDP reflection attacks
2	*Data Link*	*Frames*	*Physical addressing*	*N/A*
1	*Physical*	*Bits*	*Media, signal, and binary transmission*	*N/A*

Table 1: Open Systems Interconnection (OSI) Model

Source:
AWS Best Practices for DDoS Resiliency
https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

DDoS Attack Costs
Money, Time and Risk Brand Damage

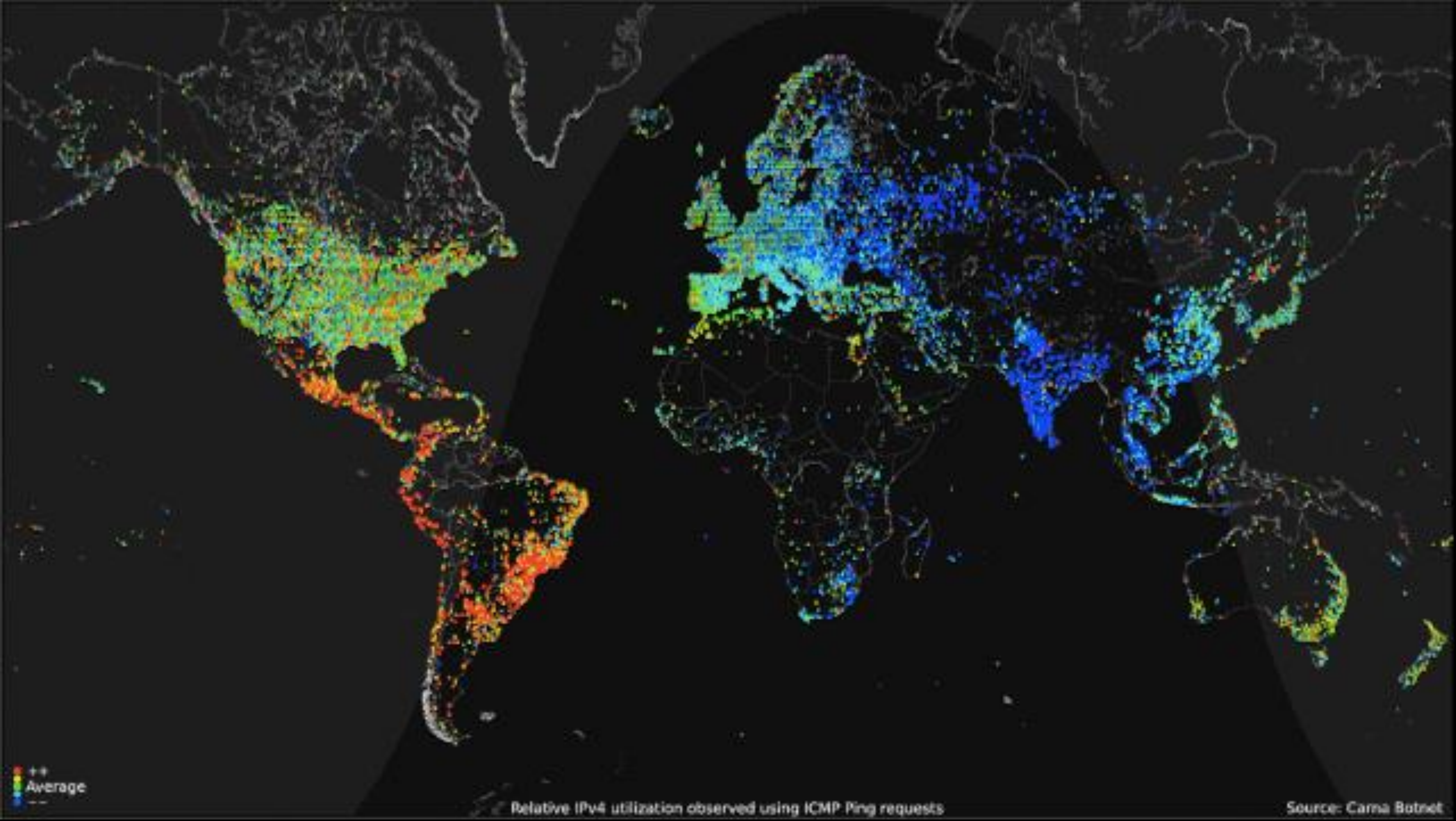


Source: Kaspersky

Little-Known Roots of the Mirai Botnet

- The ***2012 Carna Botnet Census*** exploited over public-facing 420,000 IPv4 devices that had _no passwords or weak passwords_
- Of the 4.3 billion possible IPv4 addresses, Carna Botnet found a total of 1.3 billion addresses in use, including 141 million that were behind a firewall and 729 million that returned reverse domain name system records. The remaining 2.3 billion IPv4 addresses are probably not used. [Wikipedia]
- The website at http://internetcensus2012.github.io/InternetCensus2012/paper.html shows the paper written which describes the methods used and data collected
- The author admitted in his paper that he enjoyed the "feeling of power" being able to simultaneously control over 400,000 devices from a single desktop.
- Over 4 TB of device data and IP addresses were collected
- This data remains a standard for "check up" to ensure that administrators have no public facing insecure devices
- The author, who remains a secret, could face prosecution in every country that has applicable network intrusion laws

ILLINOIS INSTITUTE OF TECHNOLOGY

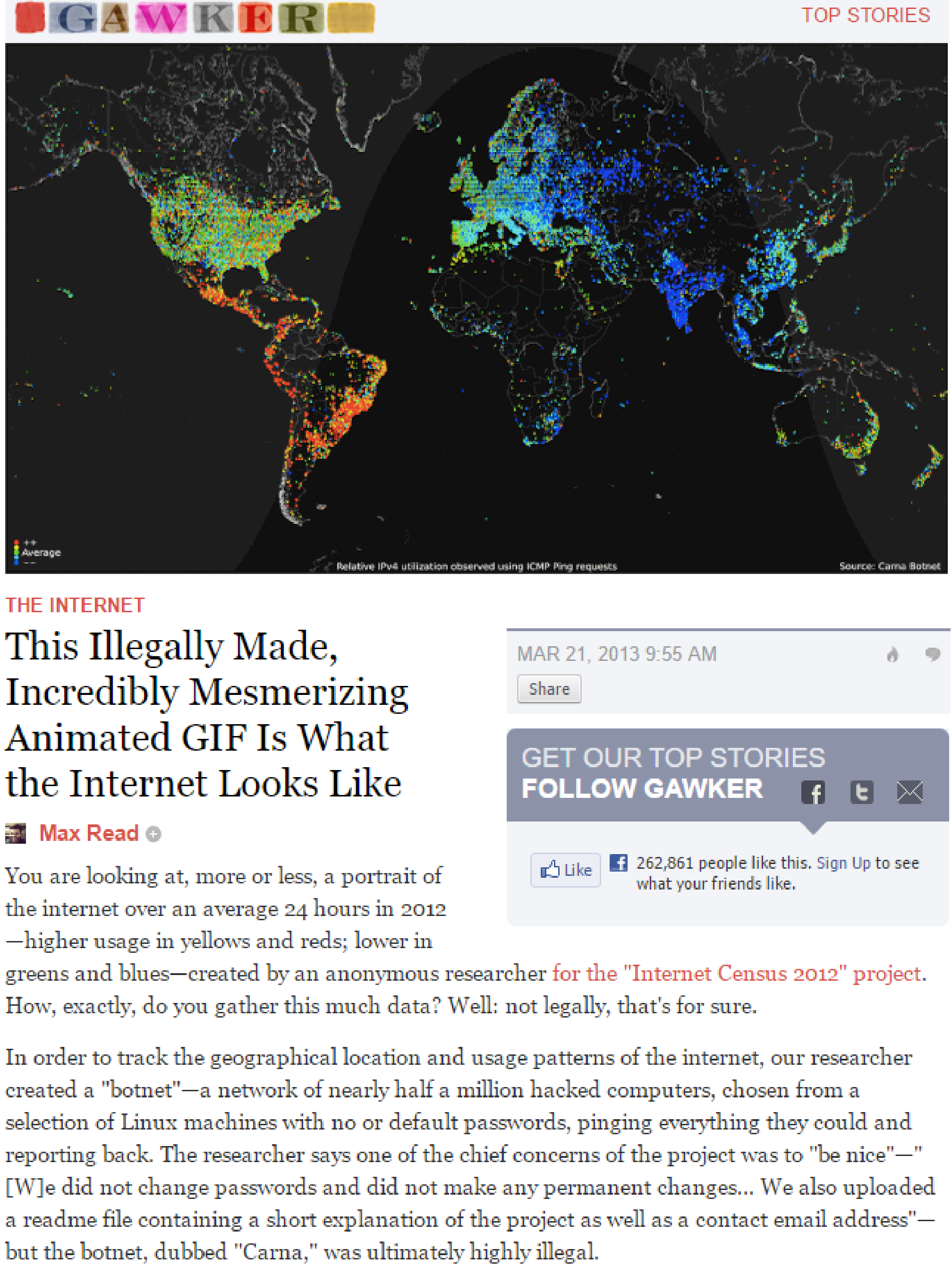


Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet

Source:
Carna Botnet Census of 2012
http://census2012.sourceforge.net/paper.html

Little Known Roots of the Mirai Botnet



THE INTERNET

This Illegally Made, Incredibly Mesmerizing Animated GIF Is What the Internet Looks Like

Max Read

MAR 21, 2013 9:55 AM

Share

GET OUR TOP STORIES
FOLLOW GAWKER

Like 262,861 people like this. Sign Up to see what your friends like.

You are looking at, more or less, a portrait of the internet over an average 24 hours in 2012—higher usage in yellows and reds; lower in greens and blues—created by an anonymous researcher for the "Internet Census 2012" project. How, exactly, do you gather this much data? Well: not legally, that's for sure.

In order to track the geographical location and usage patterns of the internet, our researcher created a "botnet"—a network of nearly half a million hacked computers, chosen from a selection of Linux machines with no or default passwords, pinging everything they could and reporting back. The researcher says one of the chief concerns of the project was to "be nice"—"[W]e did not change passwords and did not make any permanent changes... We also uploaded a readme file containing a short explanation of the project as well as a contact email address"—but the botnet, dubbed "Carna," was ultimately highly illegal.

Source:
https://web.archive.org/web/20130324015330/http://gawker.com:80/5991667/this-illegally-made-incredibly-mesmerizing-animated-gif-is-what-the-internet-looks-like

ILLINOIS INSTITUTE OF TECHNOLOGY

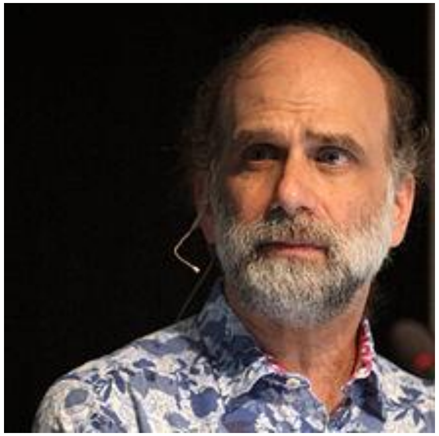
Pre-Attack Events

- August 2016 - Bruce Schneier predicts, based on his research and observations that a DDoS attack or series of attacks would take down the Internet
- September 2016 - Brian Krebs' website and his Provider were hit with DDoS attacks at about 665 Gbs
- October 2016 - Mirai Source Code placed in Open Source

DDoS Attack Prediction in September 2016 by Bruce Schneier

- **Someone Is Learning How to Take Down the Internet - by Bruce Schneier, Excerpt: "What can we do about this? Nothing, really. We don't know where the attacks come from. The data I see suggests China, an assessment shared by the people I spoke with. On the other hand, it's possible to disguise the country of origin for these sorts of attacks. The NSA, which has more surveillance in the Internet backbone than everyone else combined, probably has a better idea, but unless the US decides to make an international incident over this, we won't see any attribution. But this is happening. And people should know."**
  - https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

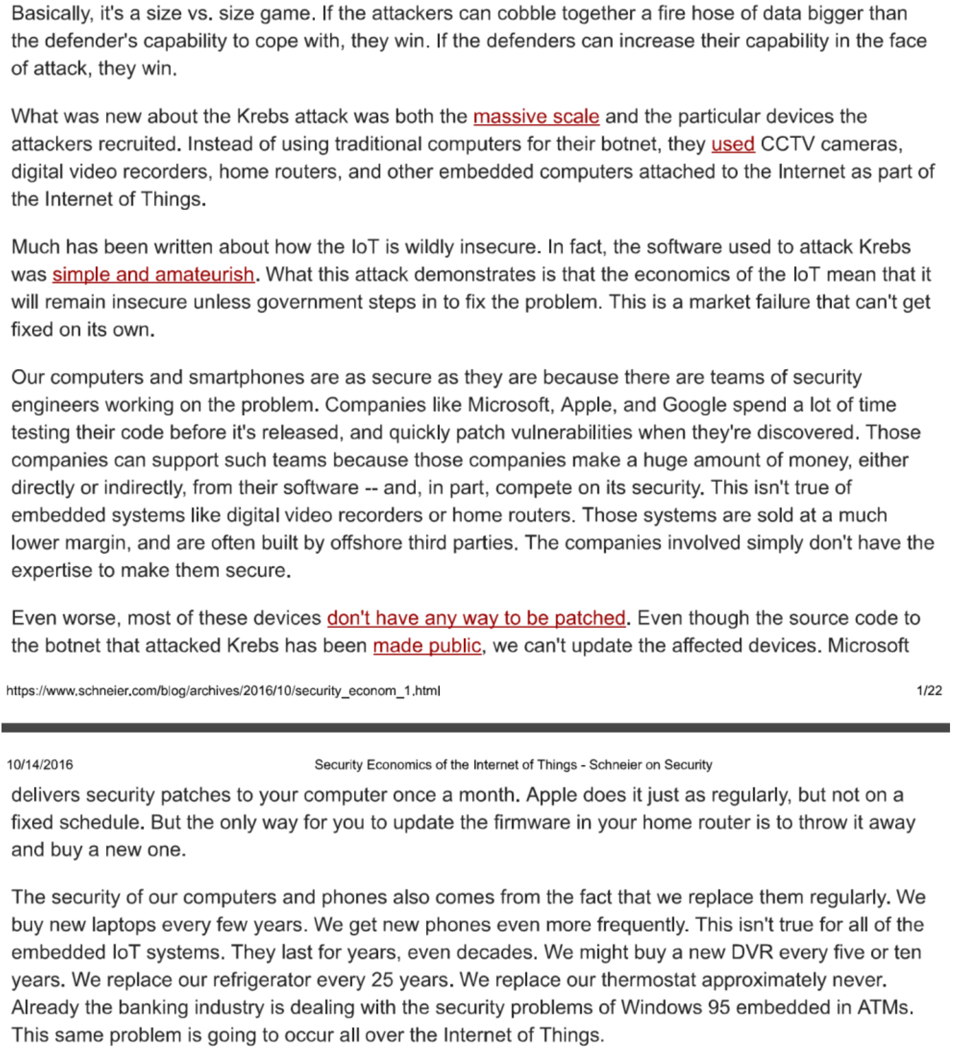
Note: When Dr. Bruce Schneier says something, I believe it. He is one of the greatest Cybersecurity Researchers and Writers in the World.



Bruce Schneier

ILLINOIS INSTITUTE
OF TECHNOLOGY

The Security Economics of Internet of Things (IoT)



Basically, it's a size vs. size game. If the attackers can cobble together a fire hose of data bigger than the defender's capability to cope with, they win. If the defenders can increase their capability in the face of attack, they win.

What was new about the Krebs attack was both the massive scale and the particular devices the attackers recruited. Instead of using traditional computers for their botnet, they used CCTV cameras, digital video recorders, home routers, and other embedded computers attached to the Internet as part of the Internet of Things.

Much has been written about how the IoT is wildly insecure. In fact, the software used to attack Krebs was simple and amateurish. What this attack demonstrates is that the economics of the IoT mean that it will remain insecure unless government steps in to fix the problem. This is a market failure that can't get fixed on its own.

Our computers and smartphones are as secure as they are because there are teams of security engineers working on the problem. Companies like Microsoft, Apple, and Google spend a lot of time testing their code before it's released, and quickly patch vulnerabilities when they're discovered. Those companies can support such teams because those companies make a huge amount of money, either directly or indirectly, from their software -- and, in part, compete on its security. This isn't true of embedded systems like digital video recorders or home routers. Those systems are sold at a much lower margin, and are often built by offshore third parties. The companies involved simply don't have the expertise to make them secure.

Even worse, most of these devices don't have any way to be patched. Even though the source code to the botnet that attacked Krebs has been made public, we can't update the affected devices. Microsoft

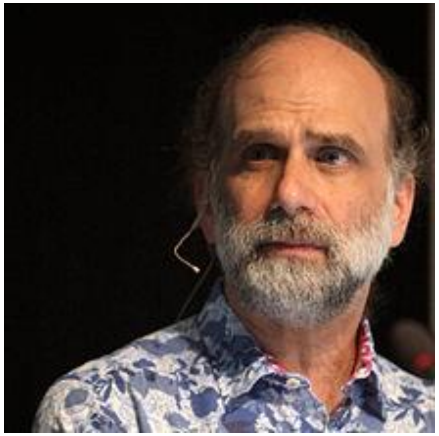
https://www.schneier.com/blog/archives/2016/10/security_econom_1.html 1/22

10/14/2016 Security Economics of the Internet of Things - Schneier on Security

delivers security patches to your computer once a month. Apple does it just as regularly, but not on a fixed schedule. But the only way for you to update the firmware in your home router is to throw it away and buy a new one.

The security of our computers and phones also comes from the fact that we replace them regularly. We buy new laptops every few years. We get new phones even more frequently. This isn't true for all of the embedded IoT systems. They last for years, even decades. We might buy a new DVR every five or ten years. We replace our refrigerator every 25 years. We replace our thermostat approximately never. Already the banking industry is dealing with the security problems of Windows 95 embedded in ATMs. This same problem is going to occur all over the Internet of Things.

Excellent Commentary about IoT, Economics, And Security by Internationally known Security writer and Researcher, Dr. Bruce Schneier



Bruce Schneier

ILLINOIS INSTITUTE OF TECHNOLOGY

Sources: https://www.schneier.com/blog/archives/2016/10/security_econom_1.html

DDoS Attack on Brian Krebs' Website

- KrebsOnSecurity Hit With Record DDoS
  - https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
- DDoS attack takes down Brian Krebs' site - www.krebsonsecurity.com . At 665 Gbps of traffic it was the largest DDoS Attack in Internet History - Attack was so powerful that Akamai threw up its hands
  - http://www.csoonline.com/article/3123785/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html
- Will IoT folks learn from DDoS attack on Krebs' Web site?
  - http://www.csoonline.com/article/3124436/security/will-iot-folks-learn-from-ddos-attack-on-krebs-web-site.html
- Someone, whom he subsequently spent months working to track down, had seized control of hundreds of thousands of internet-connected devices, including home routers, video cameras, DVRs, and printers, to create a botnet, a sort of digital zombie army.
  - https://hub.jhu.edu/magazine/2017/spring/internet-personal-cyberattacks/

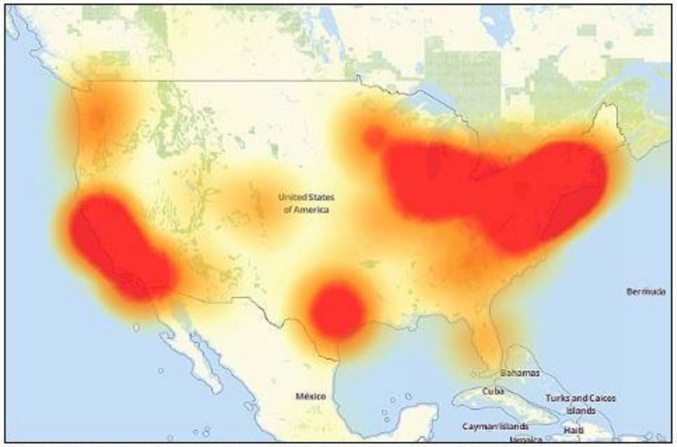
Note: When Brian Krebs, of www.krebsonsecurity.com writes about Cybersecurity, and then gets hit with the Internet's largest DDoS attack ever, it gets everyone's attention, especially Cybersecurity Researchers.

Brian Krebs

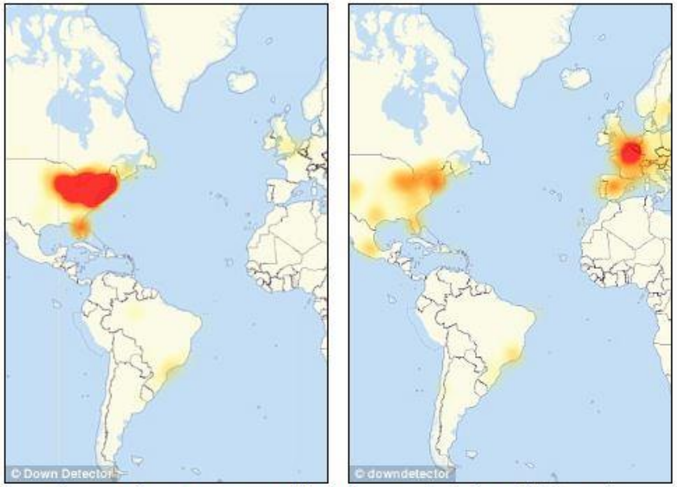
ILLINOIS INSTITUTE OF TECHNOLOGY

WHAT DID THE MIRAI BOTNET DO IN OCTOBER 2016?

DDoS Attacks of October 21, 2016



Internet users across the globe were hit throughout the day as 'several' massive cyber attacks hit a DNS service provider. This image shows problems reported with Level 3, a business service provider.

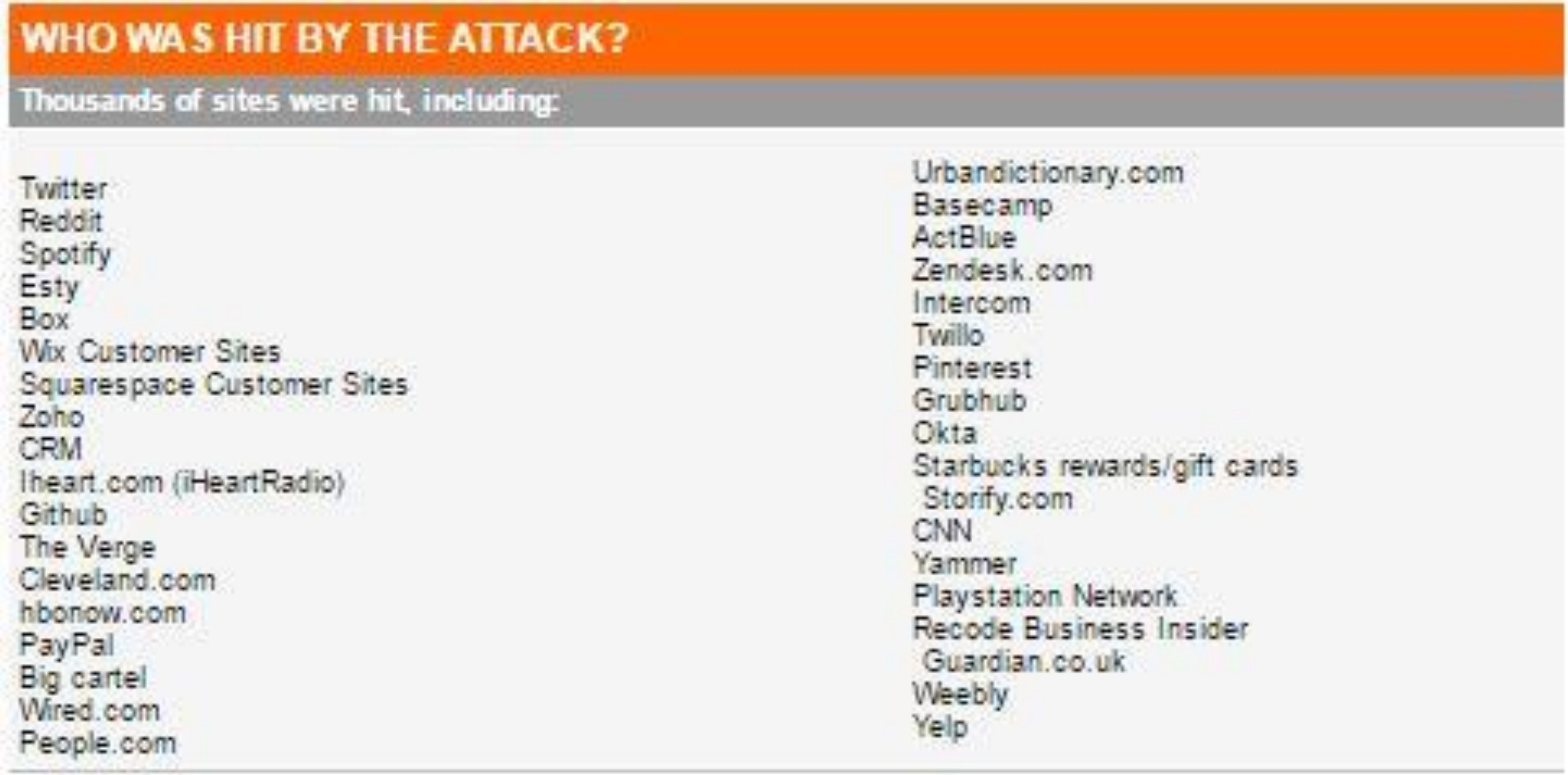


Pictured are maps from Down Detector of the first two attacks, the first of which mostly affected the east coast of the US, while the UK bore the brunt of the second after many services were restored in about two hours

Screenshots from:
http://downdetector.com/
Hint: A GREAT Resource!

The Internet didn't "break" on October 21, 2016, but the attackers who launched the DDoS attacks against Dyn exploited a known DNS Weakness that negatively impacted MANY Internet-related businesses and millions of users.

DDoS Attacks of October 21, 2016 - The Major Internet-Related Businesses Affected



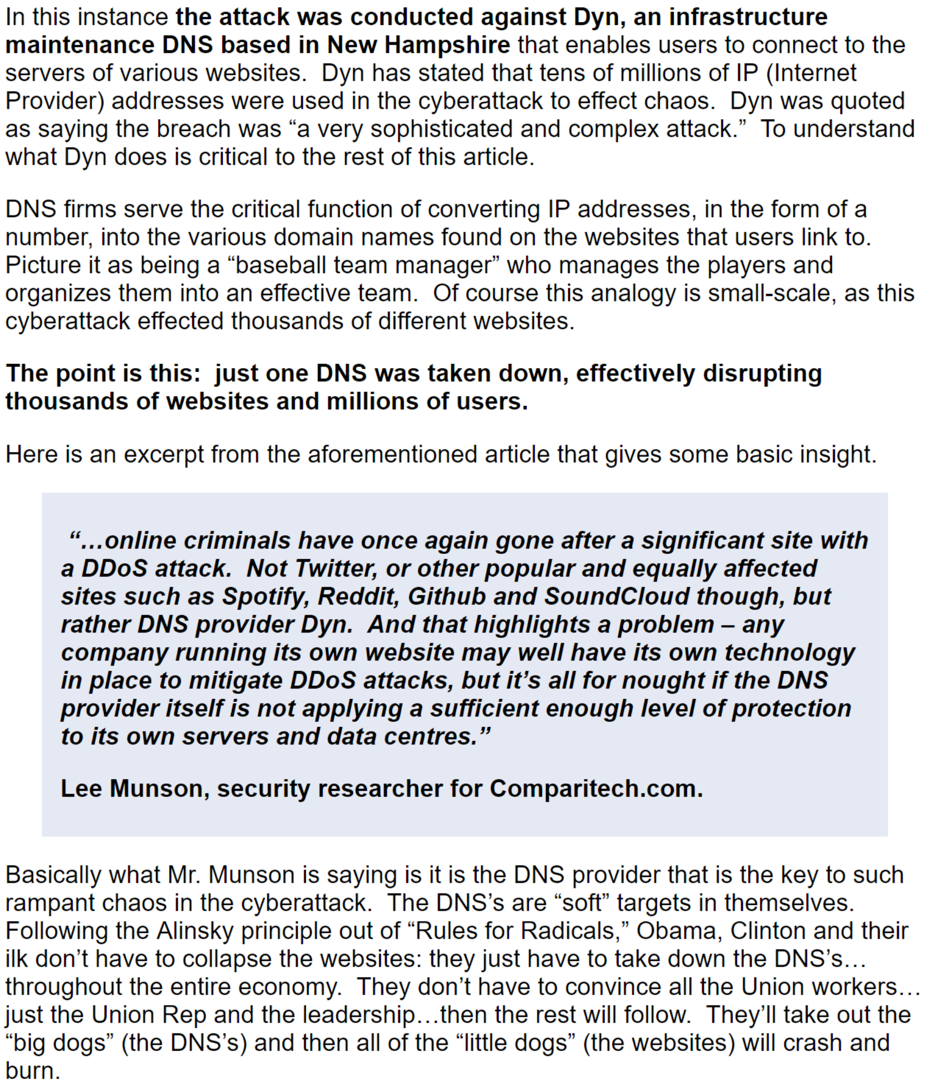
WHO WAS HIT BY THE ATTACK?

Thousands of sites were hit, including:

Twitter
Reddit
Spotify
Esty
Box
Wix Customer Sites
Squarespace Customer Sites
Zoho
CRM
Iheart.com (iHeartRadio)
Github
The Verge
Cleveland.com
hbonow.com
PayPal
Big cartel
Wired.com
People.com

Urbandictionary.com
Basecamp
ActBlue
Zendesk.com
Intercom
Twillo
Pinterest
Grubhub
Okta
Starbucks rewards/gift cards
Storify.com
CNN
Yammer
Playstation Network
Recode Business Insider
Guardian.co.uk
Weebly
Yelp

DDoS Attacks of October 21, 2016



In this instance **the attack was conducted against Dyn, an infrastructure maintenance DNS based in New Hampshire** that enables users to connect to the servers of various websites. Dyn has stated that tens of millions of IP (Internet Provider) addresses were used in the cyberattack to effect chaos. Dyn was quoted as saying the breach was "a very sophisticated and complex attack." To understand what Dyn does is critical to the rest of this article.

DNS firms serve the critical function of converting IP addresses, in the form of a number, into the various domain names found on the websites that users link to. Picture it as being a "baseball team manager" who manages the players and organizes them into an effective team. Of course this analogy is small-scale, as this cyberattack effected thousands of different websites.

The point is this: just one DNS was taken down, effectively disrupting thousands of websites and millions of users.

Here is an excerpt from the aforementioned article that gives some basic insight.

> ***"…online criminals have once again gone after a significant site with a DDoS attack. Not Twitter, or other popular and equally affected sites such as Spotify, Reddit, Github and SoundCloud though, but rather DNS provider Dyn. And that highlights a problem – any company running its own website may well have its own technology in place to mitigate DDoS attacks, but it's all for nought if the DNS provider itself is not applying a sufficient enough level of protection to its own servers and data centres."***
>
> **Lee Munson, security researcher for Comparitech.com.**

Basically what Mr. Munson is saying is it is the DNS provider that is the key to such rampant chaos in the cyberattack. The DNS's are "soft" targets in themselves. Following the Alinsky principle out of "Rules for Radicals," Obama, Clinton and their ilk don't have to collapse the websites: they just have to take down the DNS's… throughout the entire economy. They don't have to convince all the Union workers… just the Union Rep and the leadership…then the rest will follow. They'll take out the "big dogs" (the DNS's) and then all of the "little dogs" (the websites) will crash and burn.

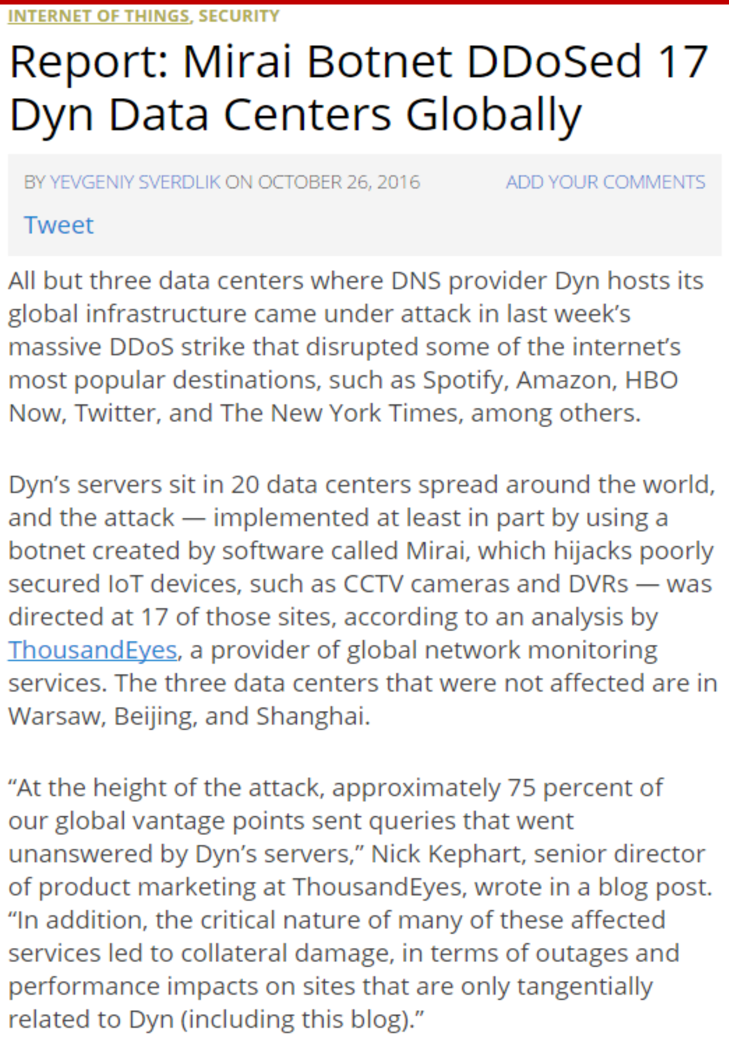
}

The Internet didn't "break" on October 21, 2016, but the attackers who launched the DDoS attacks against Dyn exploited a known DNS Weakness that negatively impacted MANY Internet-related businesses and millions of users.

Note:
Oracle bought DYN in November 2016
Source:
https://www.wired.com/2016/11/oracle-just-bought-dyn-company-brought-internet/

ILLINOIS INSTITUTE OF TECHNOLOGY

DDoS Attacks of October 21, 2016



INTERNET OF THINGS, SECURITY

Report: Mirai Botnet DDoSed 17 Dyn Data Centers Globally

BY YEVGENIY SVERDLIK ON OCTOBER 26, 2016 ADD YOUR COMMENTS

Tweet

All but three data centers where DNS provider Dyn hosts its global infrastructure came under attack in last week's massive DDoS strike that disrupted some of the internet's most popular destinations, such as Spotify, Amazon, HBO Now, Twitter, and The New York Times, among others.

Dyn's servers sit in 20 data centers spread around the world, and the attack — implemented at least in part by using a botnet created by software called Mirai, which hijacks poorly secured IoT devices, such as CCTV cameras and DVRs — was directed at 17 of those sites, according to an analysis by ThousandEyes, a provider of global network monitoring services. The three data centers that were not affected are in Warsaw, Beijing, and Shanghai.

"At the height of the attack, approximately 75 percent of our global vantage points sent queries that went unanswered by Dyn's servers," Nick Kephart, senior director of product marketing at ThousandEyes, wrote in a blog post. "In addition, the critical nature of many of these affected services led to collateral damage, in terms of outages and performance impacts on sites that are only tangentially related to Dyn (including this blog)."

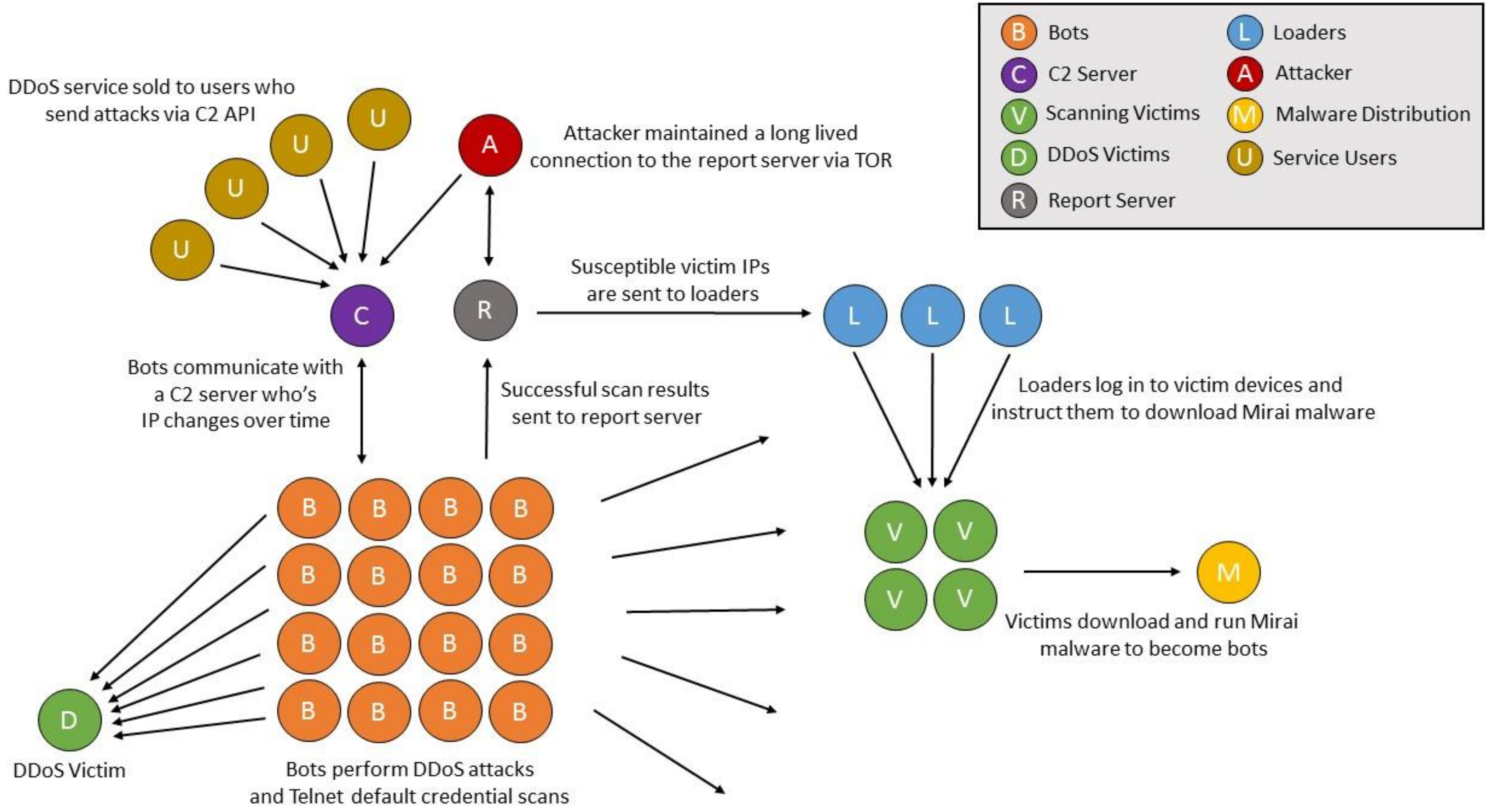
}

The Internet didn't "break" on October 21, 2016, but the attackers who launched the DDoS attacks against Dyn exploited a known DNS Weakness that negatively impacted MANY Internet-related businesses and millions of users.

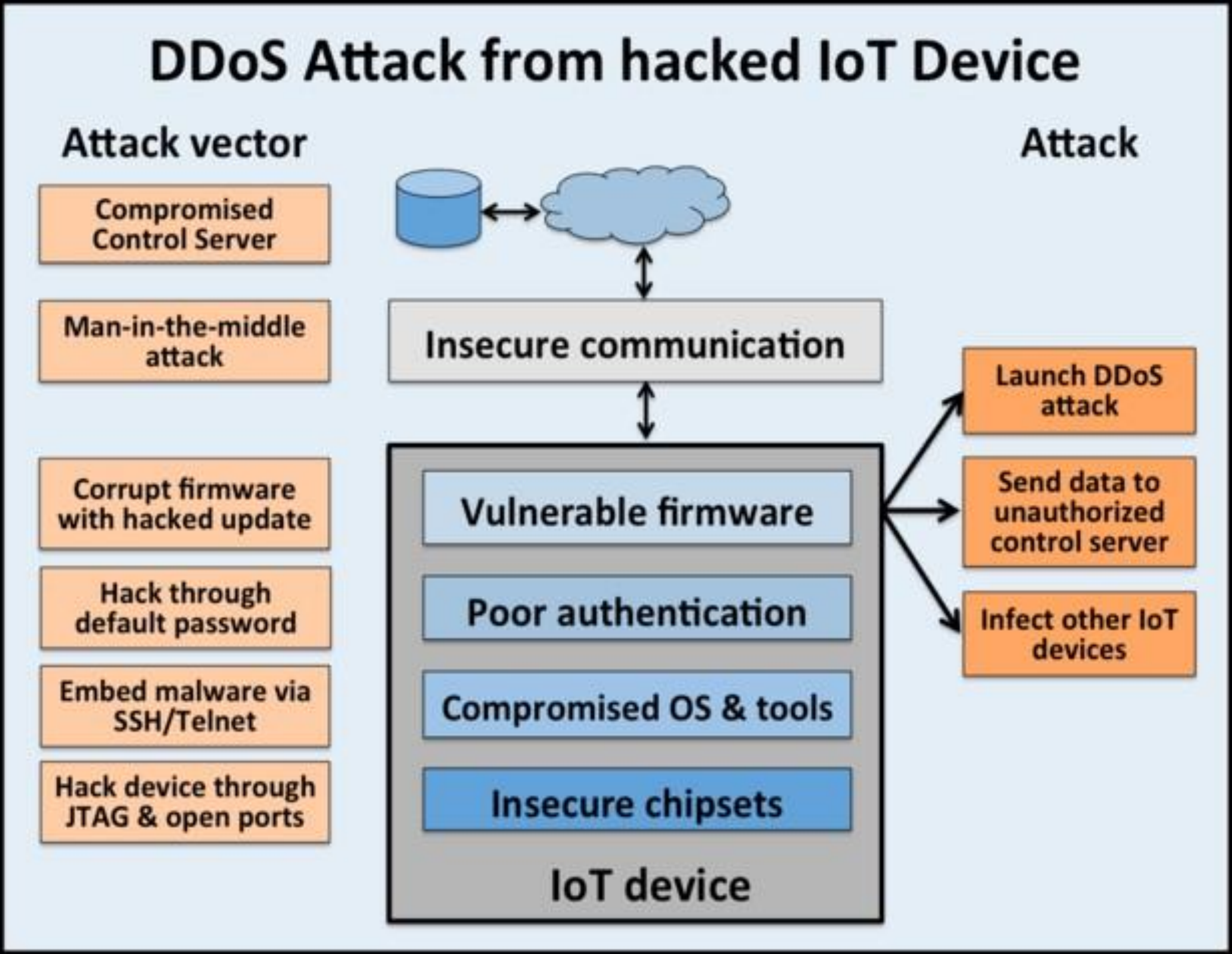
Note:
Oracle bought DYN in November 2016
Source: https://www.wired.com/2016/11/oracle-just-bought-dyn-company-brought-internet/

ILLINOIS INSTITUTE OF TECHNOLOGY

How Did Mirai Work?
DDoS Attacks of October 21, 2016


B Bots
C C2 Server
V Scanning Victims
D DDoS Victims
R Report Server
L Loaders
A Attacker
M Malware Distribution
U Service Users
DDoS service sold to users who send attacks via C2 API
U
U
U
U
A
Attacker maintained a long lived connection to the report server via TOR
C
R
Susceptible victim IPs are sent to loaders
L
L
L
Bots communicate with a C2 server who's IP changes over time
Successful scan results sent to report server
Loaders log in to victim devices and instruct them to download Mirai malware
B
V
M
Victims download and run Mirai malware to become bots
D
DDoS Victim
Bots perform DDoS attacks and Telnet default credential scans

How Did Mirai Work?
DDoS Attacks of October 21, 2016


DDoS Attack from hacked IoT Device
Attack vector
Attack
Compromised Control Server
Man-in-the-middle attack
Corrupt firmware with hacked update
Hack through default password
Embed malware via SSH/Telnet
Hack device through JTAG & open ports
Insecure communication
Vulnerable firmware
Poor authentication
Compromised OS & tools
Insecure chipsets
IoT device
Launch DDoS attack
Send data to unauthorized control server
Infect other IoT devices

Infected IoT Devices:

1) Launch DDoS Attacks
2) Report data to C2 Servers
3) Infect other IoT Devices

How Did Mirai Work?
DDoS Attacks of October 21, 2016

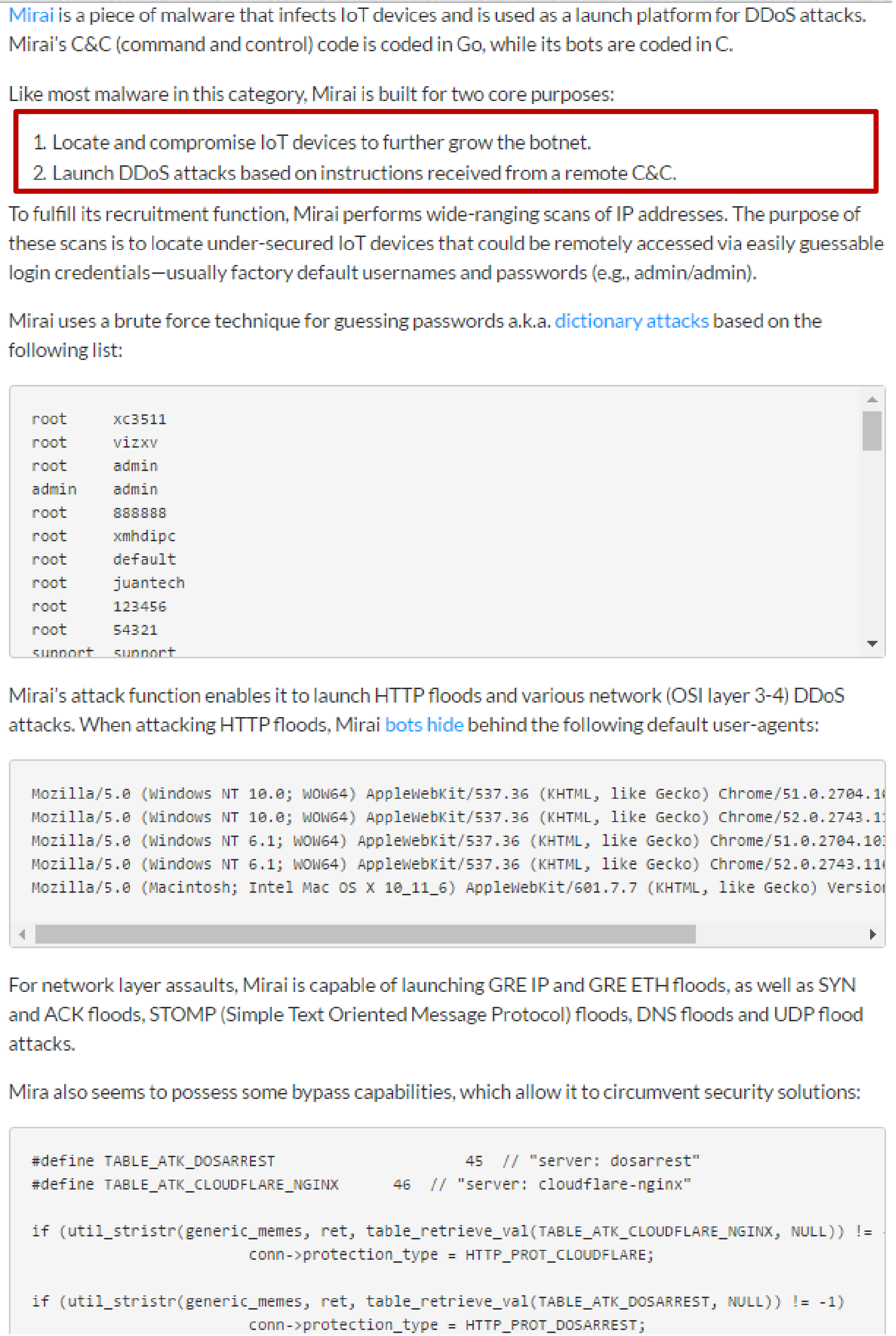
- The Mirai Internet of Things (IoT) botnet has been using STOMP (Simple Text Oriented Messaging Protocol) floods to hit targets, a protocol that isn’t normally associated with distributed denial of service (DDoS) attacks.

- Mirai has been responsible for taking major websites offline for many users by targeting the Dyn DNS service, in addition to hosting firm OVH in attacks that surpassed 1.2 Tbps (terabits per second). Mirai was also in an attack against Brian Krebs’ blog in a 665 Gbps+ (gigabits per second) assault. The botnet uses various attack vectors to power these massive attacks, including STOMP floods.

Source:
http://www.securityweek.com/mirai-used-stomp-floods-recent-ddos-attacks

ILLINOIS INSTITUTE
OF TECHNOLOGY

Mirai's Purposes and Some Source Code Analysis



Mirai is a piece of malware that infects IoT devices and is used as a launch platform for DDoS attacks. Mirai's C&C (command and control) code is coded in Go, while its bots are coded in C.

Like most malware in this category, Mirai is built for two core purposes:

1. Locate and compromise IoT devices to further grow the botnet.
2. Launch DDoS attacks based on instructions received from a remote C&C.

To fulfill its recruitment function, Mirai performs wide-ranging scans of IP addresses. The purpose of these scans is to locate under-secured IoT devices that could be remotely accessed via easily guessable login credentials—usually factory default usernames and passwords (e.g., admin/admin).

Mirai uses a brute force technique for guessing passwords a.k.a. dictionary attacks based on the following list:

```
root     xc3511
root     vizxv
root     admin
admin    admin
root     888888
root     xmhdipc
root     default
root     juantech
root     123456
root     54321
support  support
```

Mirai's attack function enables it to launch HTTP floods and various network (OSI layer 3-4) DDoS attacks. When attacking HTTP floods, Mirai bots hide behind the following default user-agents:

```
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.1
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.1
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.10
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.11
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Versio
```

For network layer assaults, Mirai is capable of launching GRE IP and GRE ETH floods, as well as SYN and ACK floods, STOMP (Simple Text Oriented Message Protocol) floods, DNS floods and UDP flood attacks.

Mira also seems to possess some bypass capabilities, which allow it to circumvent security solutions:

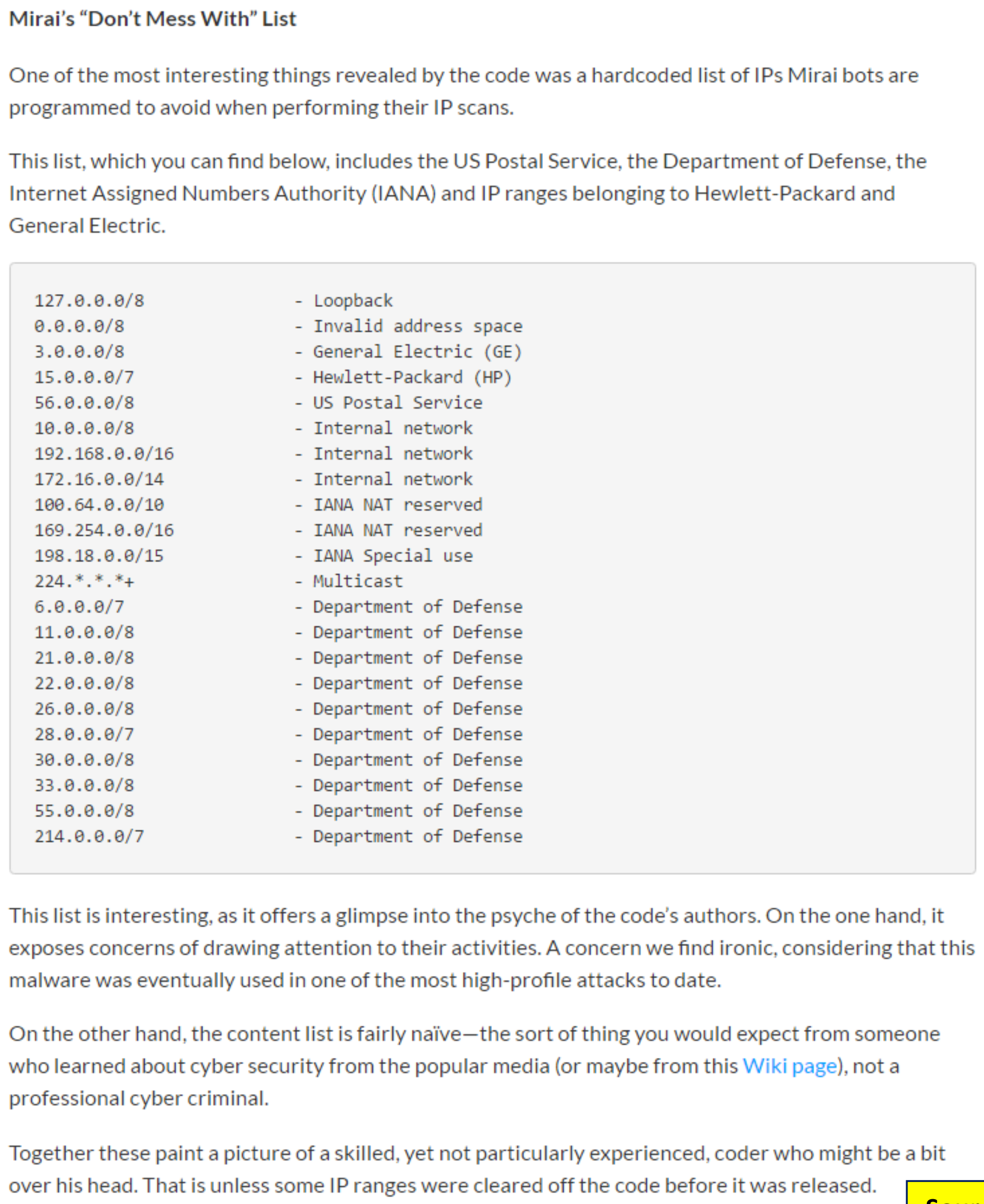
```
#define TABLE_ATK_DOSARREST                     45  // "server: dosarrest"
#define TABLE_ATK_CLOUDFLARE_NGINX      46  // "server: cloudflare-nginx"

if (util_stristr(generic_memes, ret, table_retrieve_val(TABLE_ATK_CLOUDFLARE_NGINX, NULL)) != 
                        conn->protection_type = HTTP_PROT_CLOUDFLARE;

if (util_stristr(generic_memes, ret, table_retrieve_val(TABLE_ATK_DOSARREST, NULL)) != -1)
                        conn->protection_type = HTTP_PROT_DOSARREST;
```

Source:
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Mirai's "Don't Mess With" List and a look at the Coder's Psyche



Mirai's "Don't Mess With" List

One of the most interesting things revealed by the code was a hardcoded list of IPs Mirai bots are programmed to avoid when performing their IP scans.

This list, which you can find below, includes the US Postal Service, the Department of Defense, the Internet Assigned Numbers Authority (IANA) and IP ranges belonging to Hewlett-Packard and General Electric.

```
127.0.0.0/8                - Loopback
0.0.0.0/8                  - Invalid address space
3.0.0.0/8                  - General Electric (GE)
15.0.0.0/7                 - Hewlett-Packard (HP)
56.0.0.0/8                 - US Postal Service
10.0.0.0/8                 - Internal network
192.168.0.0/16             - Internal network
172.16.0.0/14              - Internal network
100.64.0.0/10              - IANA NAT reserved
169.254.0.0/16             - IANA NAT reserved
198.18.0.0/15              - IANA Special use
224.*.*.*+                 - Multicast
6.0.0.0/7                  - Department of Defense
11.0.0.0/8                 - Department of Defense
21.0.0.0/8                 - Department of Defense
22.0.0.0/8                 - Department of Defense
26.0.0.0/8                 - Department of Defense
28.0.0.0/7                 - Department of Defense
30.0.0.0/8                 - Department of Defense
33.0.0.0/8                 - Department of Defense
55.0.0.0/8                 - Department of Defense
214.0.0.0/7                - Department of Defense
```

This list is interesting, as it offers a glimpse into the psyche of the code's authors. On the one hand, it exposes concerns of drawing attention to their activities. A concern we find ironic, considering that this malware was eventually used in one of the most high-profile attacks to date.

On the other hand, the content list is fairly naïve—the sort of thing you would expect from someone who learned about cyber security from the popular media (or maybe from this Wiki page), not a professional cyber criminal.

Together these paint a picture of a skilled, yet not particularly experienced, coder who might be a bit over his head. That is unless some IP ranges were cleared off the code before it was released.

Source:
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Where were the Mirai Botnet Attacks Coming From on October 21, 2016?

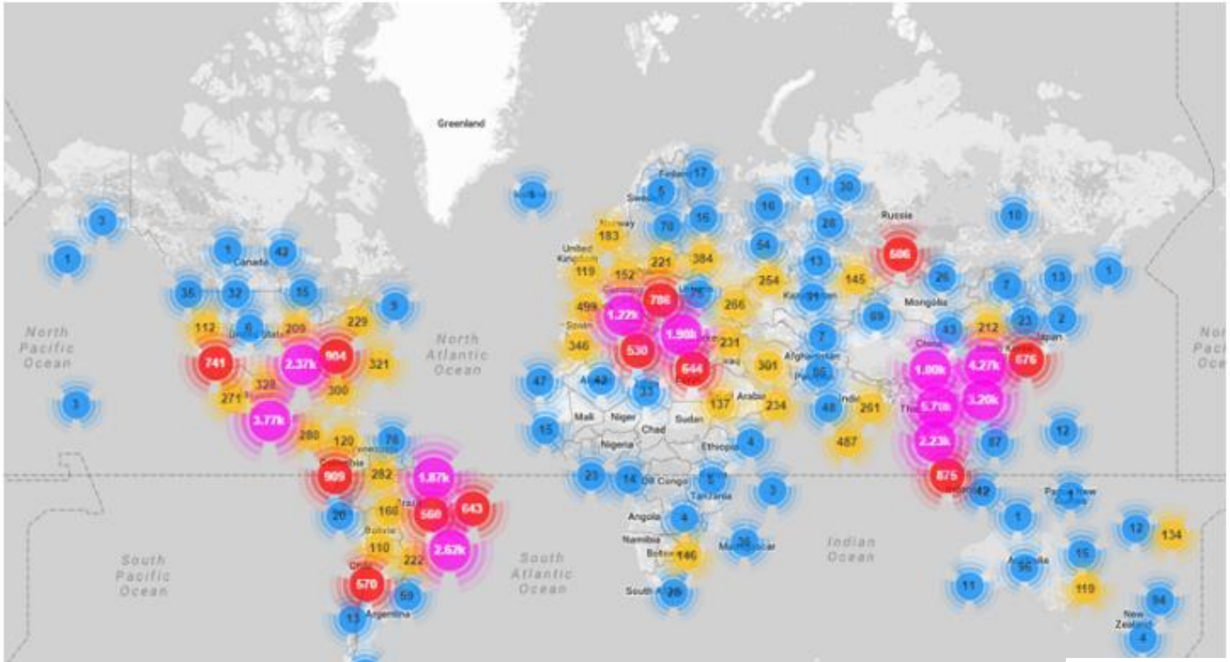
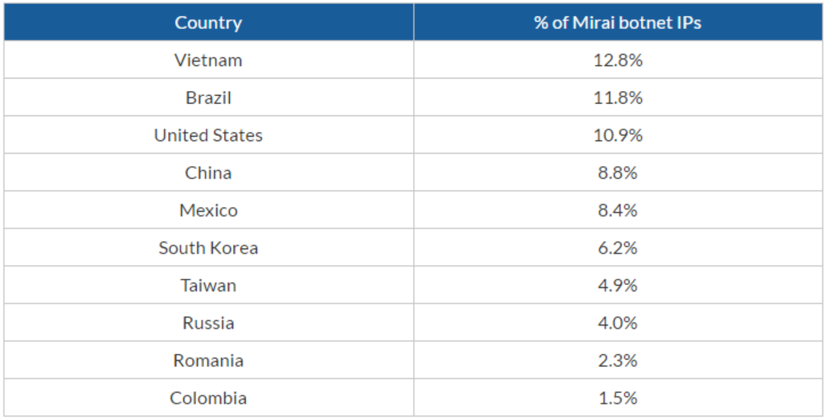


Figure 2: Geo-locations of all Mirai-infected devices uncovered so far



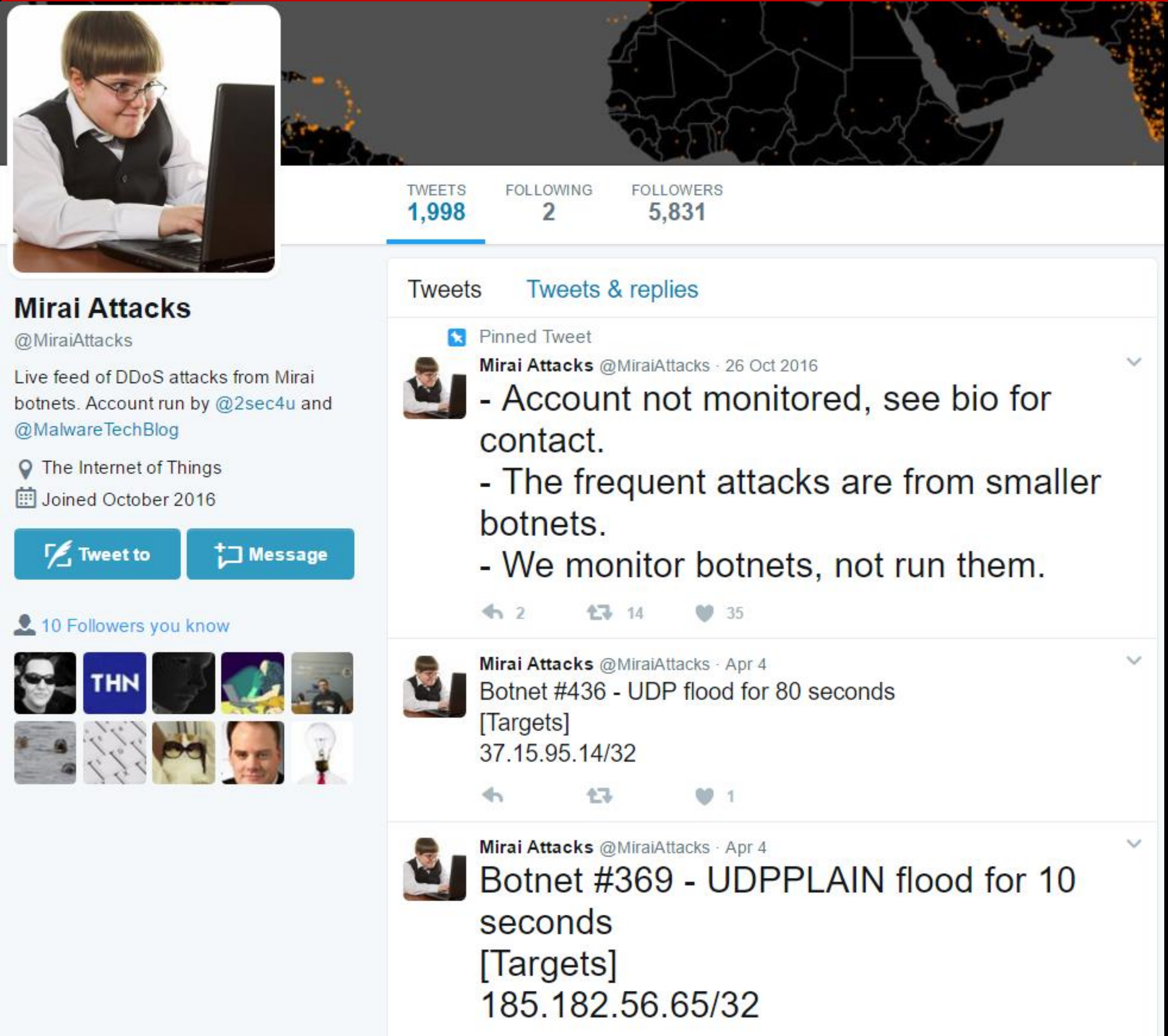
Country	% of Mirai botnet IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

Source:
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Post-Attack Events

- October 2016 - Twitter Account to Monitor Mirai in Real-Time
- November 2016 - Chinese claim Mirai Botnet attack hit Chinese-made IoT Devices, especially CCTVs
- November 2016 - DHS published guideline documents for implementing Secure IoT devices
- Windows Mirai botnet variant identified in 2017
  - **The Windows variant of the infamous Mirai Linux botnet is the offspring of a more experienced bot herder, possibly of Chinese origin, Kaspersky Lab security researchers warn.**
  - Recently detailed by Doctor Web, its main functionality is to **spread the Mirai botnet** to embedded Linux-based devices. The malware also abuses Windows Management Instrumentation (WMI) to execute commands on remote hosts, and targets Microsoft SQL Server and MySQL servers to create admin accounts and abuse their privileges.

Post-Attack Events



Mirai Attacks
@MiraiAttacks

Live feed of DDoS attacks from Mirai botnets. Account run by @2sec4u and @MalwareTechBlog

The Internet of Things
Joined October 2016

Mirai Attacks @MiraiAttacks · 26 Oct 2016
- Account not monitored, see bio for contact.
- The frequent attacks are from smaller botnets.
- We monitor botnets, not run them.

Mirai Attacks @MiraiAttacks · Apr 4
Botnet #436 - UDP flood for 80 seconds
[Targets]
37.15.95.14/32

Mirai Attacks @MiraiAttacks · Apr 4
Botnet #369 - UDPPLAIN flood for 10 seconds
[Targets]
185.182.56.65/32

Follow @miraiattacks on Twitter.com to see Real-time Mirai Attacks.

The Basics:
How to Protect our IoT Devices Against Mirai and Other Botnet Attacks

- ***Change Your Password.*** This is not only good advice for those of us who shop online or who have been notified that the e-commerce site we recently shopped on has been breached, but likewise for IoT devices. In fact, according to this report, these better credentials can be used to provide a bulwark against botnet attacks like Mirai by substituting the hard-coded username and password with ones that are unique to your organization and not, of course, easily guessed.
- ***Turn them off.*** For currently deployed IoT devices, turn them off when not in use. If the Mirai botnet does infect a device, the password must be reset and the system rebooted to get rid of it.
- ***Disable all remote access to them.*** To protect devices from Mirai and other botnets, users should not only shield TCP/23 and TCP/2323 access to those devices, but also to disable all remote (WAN) access to them.
- ***Research Your Purchase.*** Before you even buy a product, research what you are buying and make sure that you know how to update any software associated with the device. Look for devices, systems, and services that make it easy to update the device and inform the end user when updates are available.
- ***Use It or Lose It.*** Once the product is in your office, turn off the functions you're are not using. Enabled functionality usually comes with increased security risks. Again, make sure you review that before you even bring the product into the workplace. If it's already there, don't be shy about calling customer service and walking through the steps needed to shut down any unused functions.

Source:
https://www.pwnieexpress.com/blog/mirai-botnet-part-2

ILLINOIS INSTITUTE OF TECHNOLOGY

How Can an Organization Protect Against Mirai and Other Botnet Attacks?

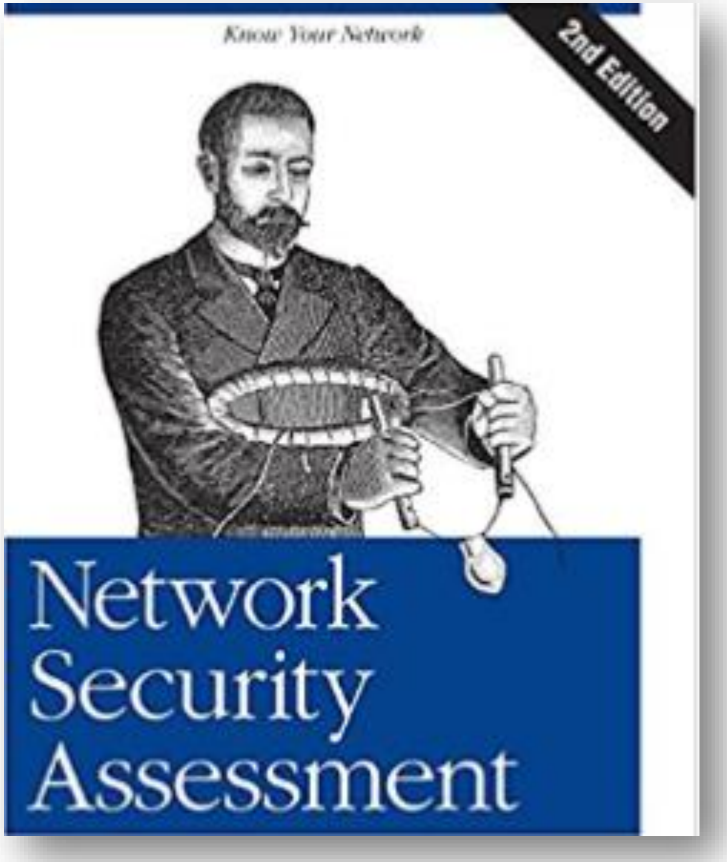
- Take this seriously
- Read up on the DHS Principles on Securing IoT
- Learn about IPv6 – it's a ***BIG Deal*** (http://ipv6.he.net)
- Actively design, engineer, and implement security, from the beginning, not after the fact
- Set or Change the default passwords on IoT
- Have an alternate DNS provider
- Add DDoS attack scenarios into your Incident Management and Response Plans
- Use DDoS scenarios in your Exercises
- Simulate DDoS attacks on your digital infrastructure to stress-test, evaluate, and continually improve your digital infrastructure

ILLINOIS INSTITUTE OF TECHNOLOGY

More Recommendations to Protect Against Mirai and Other Botnet Attacks

- The IoT threat is a serious one but one that can be simply resolved. While it's almost impossible to educate everyone on how to change their user name and passwords on these devices, it is possible for manufacturers to incorporate security features into the design and production of these devices, in particular security telnet communication and its associated ports. Default passwords must be random and users should be advised with simple instructions on how to change them.

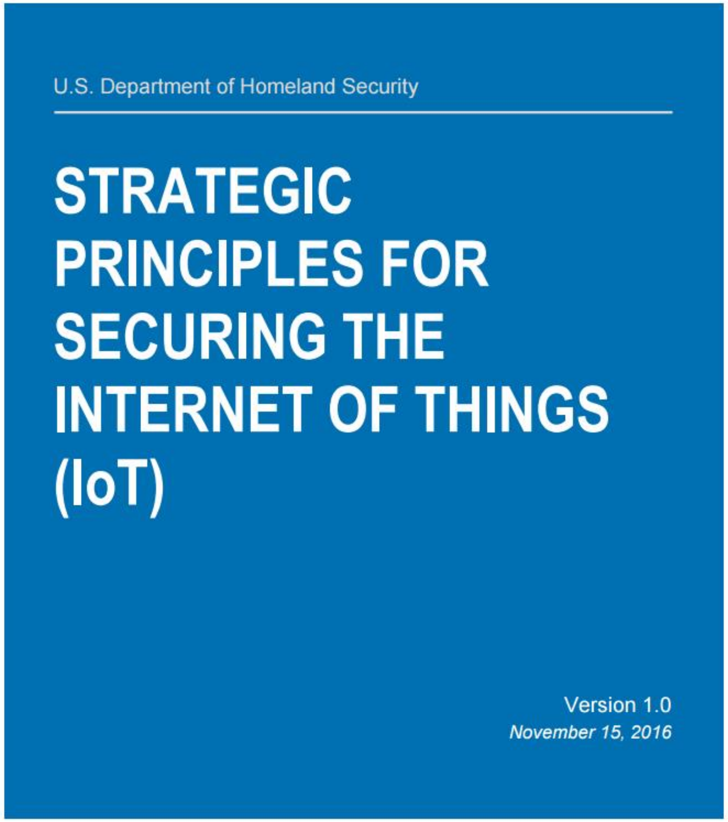
- We also recommend home users take these four steps to better prepare:
  - **Stay current – Update firmware and software regularly**
  - **Authentication – Use unique credentials for each device**
  - **Configuration – Close unnecessary ports and disable unnecessary services**
  - **Segment – Create separate network zones for your IoT systems**



Source:
https://blog.radware.com/security/2017/03/expansion-iot-since-mirai/

ILLINOIS INSTITUTE OF TECHNOLOGY

Read: DHS Strategic Principles for Securing Internet of Things



U.S. Department of Homeland Security

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

Version 1.0
November 15, 2016

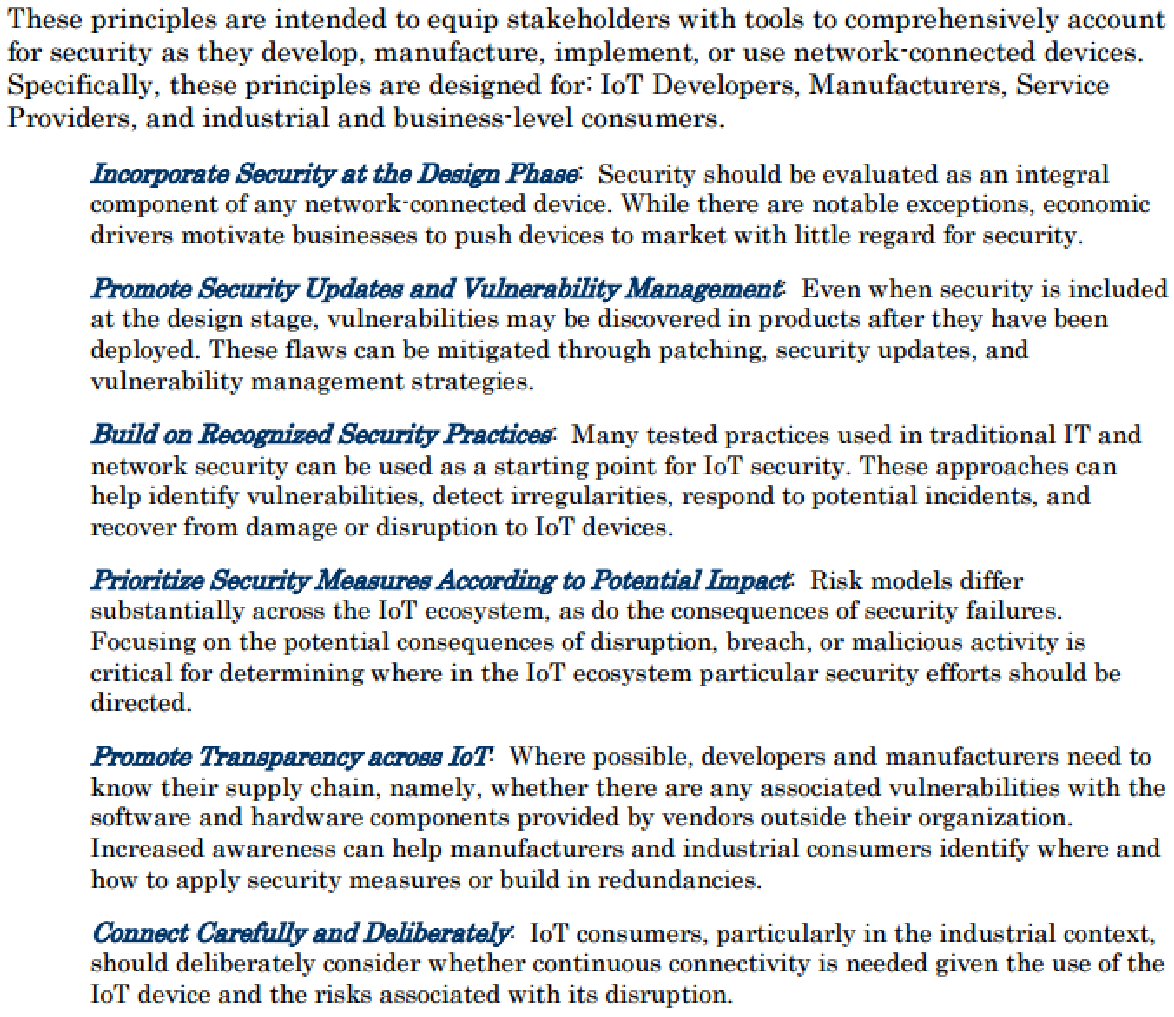
Published about 25 days AFTER the Mirai Botnet attack…

Source:
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

Homeland Security

ILLINOIS INSTITUTE OF TECHNOLOGY

Read: DHS Strategic Principles for Securing Internet of Things



These principles are intended to equip stakeholders with tools to comprehensively account for security as they develop, manufacture, implement, or use network-connected devices. Specifically, these principles are designed for: IoT Developers, Manufacturers, Service Providers, and industrial and business-level consumers.

***Incorporate Security at the Design Phase*:** Security should be evaluated as an integral component of any network-connected device. While there are notable exceptions, economic drivers motivate businesses to push devices to market with little regard for security.

***Promote Security Updates and Vulnerability Management*:** Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates, and vulnerability management strategies.

***Build on Recognized Security Practices*:** Many tested practices used in traditional IT and network security can be used as a starting point for IoT security. These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices.

***Prioritize Security Measures According to Potential Impact*:** Risk models differ substantially across the IoT ecosystem, as do the consequences of security failures. Focusing on the potential consequences of disruption, breach, or malicious activity is critical for determining where in the IoT ecosystem particular security efforts should be directed.

***Promote Transparency across IoT*:** Where possible, developers and manufacturers need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. Increased awareness can help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies.

***Connect Carefully and Deliberately*:** IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption.

Published about 25 days AFTER the Mirai Botnet attack…

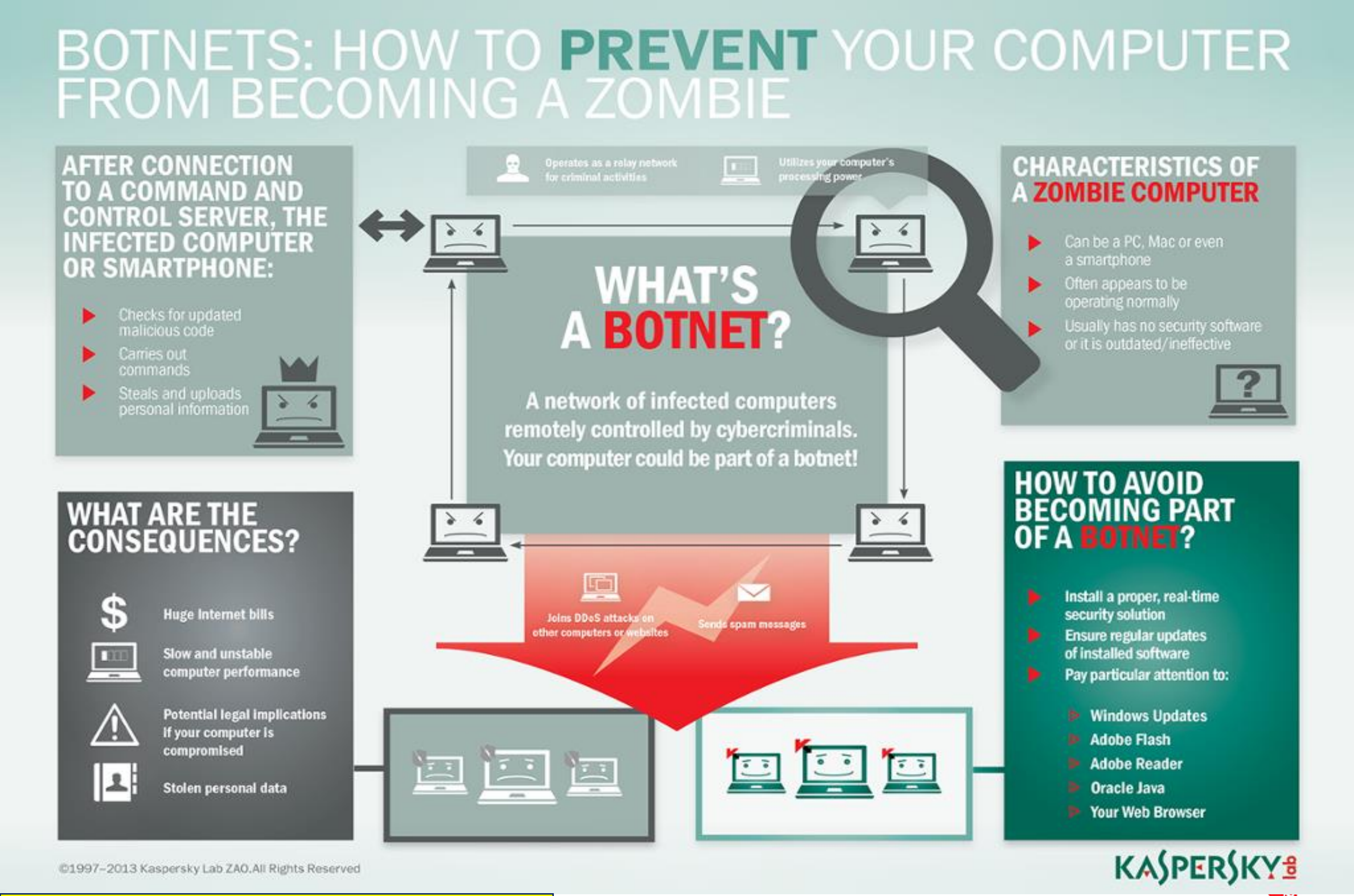
Source: DHS IoT Factsheet
https://www.dhs.gov/sites/default/files/publications/IOT%20fact%20sheet_11162016.pdf

The Mirai Botnet Five Takeaways

1. Not just one attack
2. The attack was sophisticated
3. IoT is to blame
4. This isn't the end
5. The IoT industry needs stricter standards

Source:
http://www.techrepublic.com/article/dyn-ddos-attack-5-takeaways-on-what-we-know-and-why-it-matters/

ILLINOIS INSTITUTE OF TECHNOLOGY



BOTNETS: HOW TO **PREVENT** YOUR COMPUTER FROM BECOMING A ZOMBIE

AFTER CONNECTION TO A COMMAND AND CONTROL SERVER, THE INFECTED COMPUTER OR SMARTPHONE:

- Checks for updated malicious code
- Carries out commands
- Steals and uploads personal information

WHAT'S A BOTNET?

A network of infected computers remotely controlled by cybercriminals. Your computer could be part of a botnet!

Operates as a relay network for criminal activities
Utilizes your computer's processing power
Joins DDoS attacks on other computers or websites
Sends spam messages

CHARACTERISTICS OF A ZOMBIE COMPUTER

- Can be a PC, Mac or even a smartphone
- Often appears to be operating normally
- Usually has no security software or it is outdated/ineffective

WHAT ARE THE CONSEQUENCES?

- $ Huge Internet bills
- Slow and unstable computer performance
- Potential legal implications if your computer is compromised
- Stolen personal data

HOW TO AVOID BECOMING PART OF A BOTNET?

- Install a proper, real-time security solution
- Ensure regular updates of installed software
- Pay particular attention to:
  - Windows Updates
  - Adobe Flash
  - Adobe Reader
  - Oracle Java
  - Your Web Browser

KASPERSKY lab

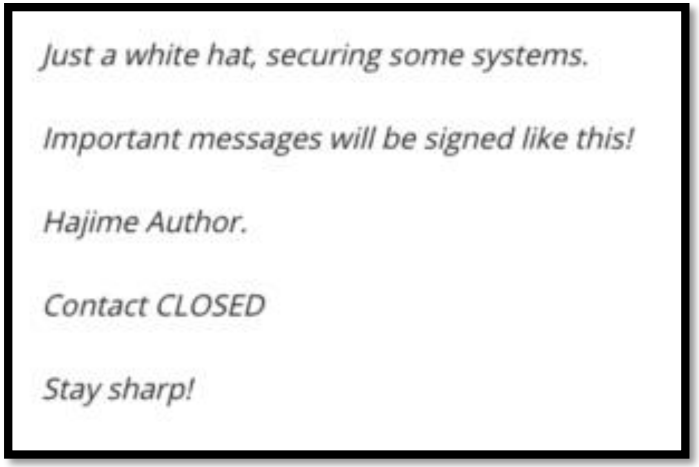
Source: Kaspersky
https://www.pwnieexpress.com/blog/mirai-botnet-part-2

ILLINOIS INSTITUTE OF TECHNOLOGY

HAJIME!
Some Recent “Good News”

A new, more powerful IoT decentralized worm, **Hajime**, is spreading faster and more effectively than **Mirai**.

- Hajime is a Japanese word for “Begin!” or “Beginning”
- First identified and analyzed, and written up in October 2016 by Sam Edwards and Ioannis Profetis of Rapidity Networks Security Research Group
- Later announced April 18, 2017 by Symantec
- Written in C
- Platforms: ARMv5, ARMv7, Intel x86-64, MIPS (little endian)
- Brute force authentication
- Spreads independently via Peer-to-Peer, without using C2
- Infects mostly DVRs and CCTV devices
- Once in control of a target it several blocks ports used by its rival, Mirai
- Only scans about 86% of the IPv4 address space
- Mostly in Asia, Russia, Brazil and Argentina
- Writes benign message “Stay Sharp”
- Thought to be from a “White Hat”, Vigilante Hacker, who prefers English
- Thought to be competing against Mirai
- **Cautionary Note: Like Mirai, still breaking the Law and if Hajime or its variants turn “evil” it could be worse than Mirai.**



Just a white hat, securing some systems.

Important messages will be signed like this!

Hajime Author.

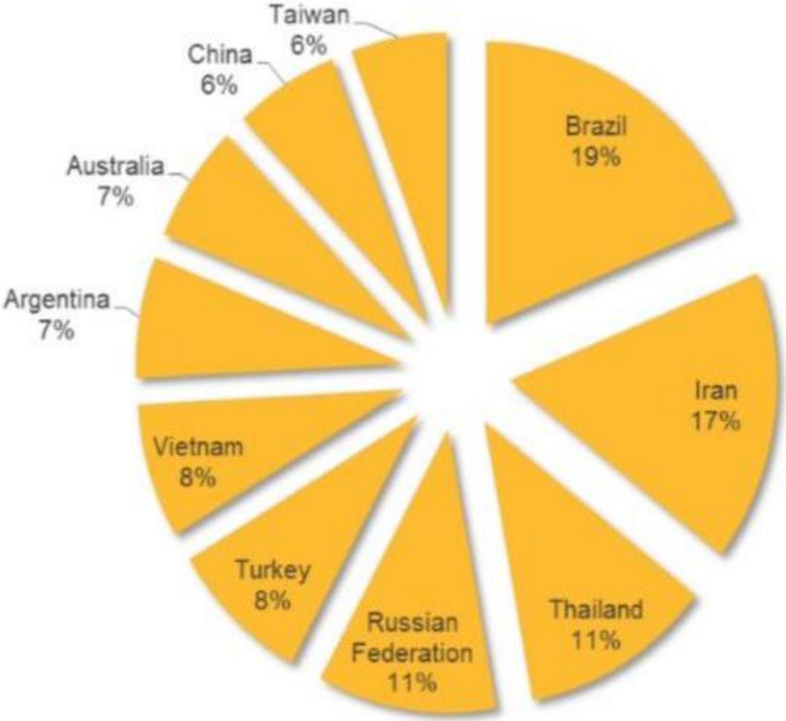
Contact CLOSED

Stay sharp!

Actual Hajime IoT Worm Message

Sources:
http://news.softpedia.com/news/hajime-iot-worm-considerably-more-sophisticated-than-mirai-509423.shtml
http://linkis.com/www.cio.co.nz/articl/2dpeg
https://nakedsecurity.sophos.com/2017/04/20/the-iot-malware-that-plays-cat-and-mouse-with-mirai
https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf ← Technical Analysis Report by Edwards & Profetis

Top 10 Countries with Hajime Infections



Symantec

Top 10 Hajime-infected countries.

Sources:
http://news.softpedia.com/news/hajime-iot-worm-considerably-more-sophisticated-than-mirai-509423.shtml
http://linkis.com/www.cio.co.nz/articl/2dpeg
https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf ← **Technical Report by Edwards & Profetis**

Conclusion

- The Mirai Botnet made history because of its size, power, bandwidth consumption, and impact the Internet-based businesses and people connected to the Internet.
- Because Mirai and Hajime source code have been shared as Open Source on the web, they are being studied and they are evolving.
- The rapid evolution and spread of IoT Devices provides Mirai and Hajime and its variants an ever-expanding target-rich environment
- The more people and organizations pay attention to the Mirai Botnet code and how to survive DDoS attacks, the better off we will be as an Internet-connected Society.
- Remember that presently, Hajime is P2P and power powerful than Mirai
- Remember that ***CIA (Confidentiality, Integrity, and Availability)*** are the simplest principles of Security, and that Mirai and DDoS attacks can and will reduce the ***Availability*** of your digital infrastructure.

ILLINOIS INSTITUTE OF TECHNOLOGY

Questions

References

- Amazon. (2006). AWS Best Practices for DDoS Resiliency. Retrieved on April 3, 2017 from https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf .
- Arghire, I. (2016). Mirai Switches to Tor Domains to Improve Resilience. Published December 19, 2016 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/mirai-switches-tor-domains-improve-resilience .
- Arghire, I. (2016). Mirai Used STOMP Floods in Recent DDoS Attacks. Published November 17, 2016 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/mirai-used-stomp-floods-recent-ddos-attacks .
- Arghire, I. (2016). This Web-based Tool Checks if Your Network Is Exposed to Mirai. Published November 24, 2016 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/web-based-tool-checks-if-your-network-exposed-mirai .
- Arghire, I. (2017). Mirai for Windows Built by Experienced Bot Herder: Kaspersky. Published February 21, 2017 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/mirai-windows-built-experienced-bot-herder-kaspersky .
- Arghire, I. (2017). New Variant of Infamous IoT Botnet Launches Attack Against Network of U.S. College. Published March 29, 2017 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/new-mirai-variant-unleashes-54-hour-ddos-attack .
- Arghire, I. (2017). Windows Trojan Spreads Mirai to Linux Devices. Published February 10, 2017 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/windows-trojan-spreads-mirai-linux-devices .
- Cheng, G. (2015). Analysis on DDOS tool Stacheldraht v1.666. a GIAC paper published by the SANS Institute. Retrieved on April 8, 2017 from http://www.giac.org/paper/gcih/229/analysis-ddos-tool-stacheldraht-v1666/102150 .
- Cimpanu, C. (2017). Hajime IoT Worm Considerably More Sophisticated than Mirai. Published at Softpedia.com on April 18, 2017. Retrieved on April 20, 2017 from http://news.softpedia.com/news/hajime-iot-worm-considerably-more-sophisticated-than-mirai-509423.shtml .
- DHS. (2016) Strategic Principles for Securing the Internet of Things. Published by DHS on November 15, 2016. Retrieved on March 29, 2017 from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
- DHS. (2016) Strategic Principles for Securing the Internet of Things. Published by DHS on November 15, 2016. Retrieved on March 29, 2017 from https://www.dhs.gov/sites/default/files/publications/IOT%20fact%20sheet_11162016.pdf .

ILLINOIS INSTITUTE
OF TECHNOLOGY

References

- Dishon, R. (2017). Bad bots, bad bots, whatcha gonna do. Published at ESET on March 17, 2017. Retrieved on March 30, 2017 from https://www.eset.com/us/about/newsroom/corporate-blog/bad-bots-bad-bots-whatcha-gonna-do/.
- Edwards, S., and Profetis, I. (2016). Hajime: An Analysis of a Decentralized Worm for IoT Devices. Published October 16, 2016 by Rapidity Networks Security Research Group. Retrieved on April 20, 2017 from https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf .
- Finley, K. (2016). Oracle Just Bought Dyn, the Company That Brought Down the Internet. Published at Wired.com on November 21, 2016. Retrieved on April 14, 2017 from https://www.wired.com/2016/11/oracle-just-bought-dyn-company-brought-internet/.
- Gallagher, S. (2016). How one rent-a-botnet army of cameras, DVRs caused Internet chaos. Published at ArsTechnica.com on October 25, 2016. Retrieved on April 12, 2017 from https://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/.
- Forrest, C. (2016). Dyn DDoS attack: 5 takeaways on what we know and why it matters. An article published at TechRepublic on October 24, 2016. Retrieved on October 25, 2017 from http://www.techrepublic.com/article/dyn-ddos-attack-5-takeaways-on-what-we-know-and-why-it-matters/ .
- Henriques. N. (2017). Hacker Who Knocked Million Routers Offline Using MIRAI Arrested at London Airport. Retrieved on February 24, 2017 from https://www.linkedin.com/pulse/hacker-who-knocked-million-routers-offline-using-mirai-nuno-henriques
- Herzberg, B., Bekerman, D., and Zeifman, I. (2016). Breaking Down Mirai: An IoT DDoS Botnet Analysis. Published at Incapsula on October 26, 2016. Retrieved on April 8, 2017 from https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.
- Kan, M. (2017). A vigilante hacker may have built a computer worm to protect the IoT. Published at CIO.com on April 20, 2017. Retrieved on April 20, 2017 from http://linkis.com/www.cio.co.nz/articl/2dpeg .
- Kovacs, E. (2016). German ISP Confirms Malware Attacks Caused Disruptions: Users Around the World Vulnerable to Attacks on Port 7547. Published November 29, 2016 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/german-isp-confirms-malware-attacks-caused-disruptions .
- Kovacs, E. (2016). Hacker Releases Source Code of IoT Malware Mirai. Published October 3, 2016 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/hacker-releases-source-code-iot-malware-mirai .

ILLINOIS INSTITUTE
OF TECHNOLOGY

References

- Kovacs, E. (2016). Over 500,000 IoT Devices Vulnerable to Mirai Botnet. Published October 7, 2016 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet .
- Lipman, P. (2017). The Cybersecurity Industry Is Failing: Time to Get Smart About 'Dumb' Homes. Published at Newsweek.com, on March 23, 2017. Retrieved on April 12, 2017 from http://www.newsweek.com/cybersecurity-industry-failed-threat-572949.
- McLaughlin, J. (2017). The Internet of Bad Things. Published in the Sping 2017 issue of Johns Hopkins Magaine on the Web. Retrieved on March 28, 2017 from https://hub.jhu.edu/magazine/2017/spring/internet-personal-cyberattacks .
- Phys.org. (2016). Disgruntled gamer 'likely' behind October US hacking: expert. Published at Phys.org on November 16, 2016. Retrieved on March 29, 2017 from https://phys.org/news/2016-11-disgruntled-gamer-october-hacking-expert.html .
- Newman, L.H. (2016). The Botnet That Broke the Internet Isn't Going Away. Published at Wired.com on December 9, 2016. Retrieved on April 12, 2017 from https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/.
- Read, M. (2013). This Illegally Made, Incredibly Mesmerizing Animated GIF Is What the Internet Looks Like. Published on GAWKER, Retrieved on April 5, 2017 from http://gawker.com/5991667/this-illegally-made-incredibly-mesmerizing-animated-gif-is-what-the-internet-looks-like.
- Savage, K. (2016) A Post-Mortem on the Mirai Botnet: Part 2: Analyzing the Attack. Published at PwnieExpress.com on December 29, 2016. Retrieved on April 20, 2017 https://www.pwnieexpress.com/blog/mirai-botnet-part-2 .
- Smith, D. (2017). The Expansion of IoT since Mirai. Published at Radware. Retrieved on April 8, 2017 from https://blog.radware.com/security/2017/03/expansion-iot-since-mirai/ .
- Sophos. (2017). The IoT malware that plays cat and mouse with Mirai. Published at NakedSecurity.Sophos.com on April 20, 2017. Retrieved April 20, 2017 from https://nakedsecurity.sophos.com/2017/04/20/the-iot-malware-that-plays-cat-and-mouse-with-mirai .
- Townsend, K. (2016). 100,000 UK Routers Likely Affected by Mirai Variant. Published December 6, 2016 at SecurityWeek. Retrieved on March 29, 2017 from http://www.securityweek.com/100000-uk-routers-likely-affected-mirai-variant .
- Verizon. (2016). Verisign 2016 DDoS Trends Report. Retrieved September 16, 2016, from https://www.verisign.com/assets/report-ddos-trends-Q22016.pdf .
- Wikipedia. (2017). Wikipedia – Carna Botnet. Retrieved April 3, 2017 from https://en.wikipedia.org/wiki/Carna_botnet.
- Woolf, N. (2016). DDoS attack that disrupted internet was largest of its kind in history, experts say. Published October 26, 2016 at TheGuardian.com. Retrieved March 29, 2017 from https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet .

Presenter Bio: William Favre Slater, III

- **Project Manager / Sr. IT Consultant at Slater Technologies, Inc. , and Adjunct Professor at the Illinois Institute of Technology -** Working on projects related to:
  - Security reviews and auditing
  - ISO 27001 Project Implementations
  - Developing Applications for Risk and Compliance
  - Subject Matter Expert in Cybersecurity and IT Service Management for Government Proposals and Contracts related to technical services management and measurement
  - SME for preparing Risk Management and Security Exams at Western Governor's State University in UT
  - Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
  - Providing subject matter expert services to Data Center product vendors and other local businesses.
  - Developing and presenting technical training materials for undergraduate and graduate students at the ***Illinois Institute of Technology*** in the areas of Data Center Operations, Data Center Architecture, Cyber Security Management, and Information Technology hardware and software.
  - Mr. Slater is an internationally published author on Cybersecurity topics related to Cyberwarfare, Social Engineering, and various other topics.
  - Providing Summer Internships to IIT Students via his company, Slater Technologies, Inc.

ILLINOIS INSTITUTE OF TECHNOLOGY

Presenter Bio: William F. Slater, III

- ASIS Member 2012
- 2017 marks the fifth consecutive year Mr. Slater presented at Forensecure at IIT
- Mr. Slater has earned an M.S. in Cybersecurity (2013, Bellevue University, Bellevue, NE), as well as an M.S. in Computer Information Systems (2004, University of Phoenix, Phoenix, AZ), and an MBA (2010, University of Phoenix, Phoenix, AZ). He has also earned 80 professional certifications, including a PMP, CISSP, CISA, SSCP, ISO 27002, and a CDCP.
- Mr. Slater has taught for over 9 years as an Adjunct Professor at the Illinois Institute of Technology and developed and delivered courses on these topics: Data Center Operations, Data Center Architecture, Information Technology hardware and software, Data Warehousing, Java and Object-Oriented Software Development, Cybersecurity Management, and IT in Public Administration. See http://billslater.com/teaching
- Mr. Slater is on a personal Mission to help make the world a better, safer and more productive place, especially when it means helping his students and colleagues become smarter about cybersecurity, Internet of Things, Data Centers, the Internet, and other exciting areas of Information Technology.
- He lives in Chicago's Wicker Park neighborhood with his lovely wife, Joanna Roguska, who is a web developer, musician and belly dancer.
- In his spare time, Mr. Slater teaches Judo and Self Defense at IIT, and he also offers internships to IIT students who want to develop real-world technology skills.
- He can be reached at slater@billslater.com or at 312 – 758 – 0307.

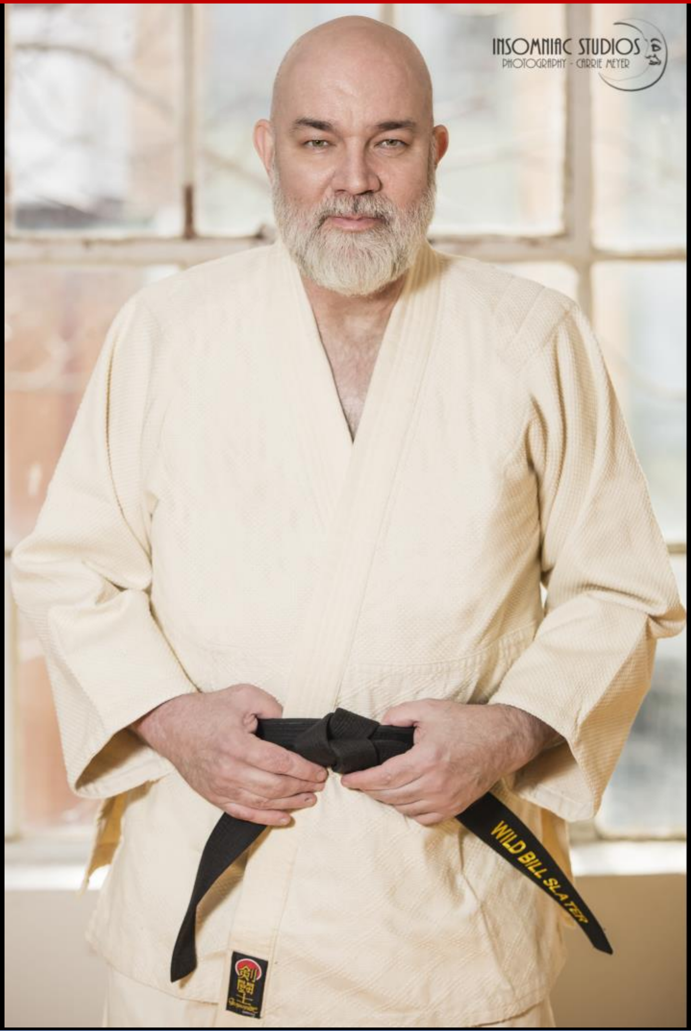
ILLINOIS INSTITUTE OF TECHNOLOGY

William Favre Slater, II

- 312-758-0307
- slater@billslater.com
- williamslater@gmail.com
- http://billslater.com/interview
- 1515 W. Haddon Ave., Unit 309
  Chicago, IL 60642
  United States of America

William Favre Slater, III

Thank You!


INSOMNIAC STUDIOS
PHOTOGRAPHY - CARRIE MEYER
WILD BILL SLATER