ARBOR NETWORKS

The Security Division of NETSCOUT

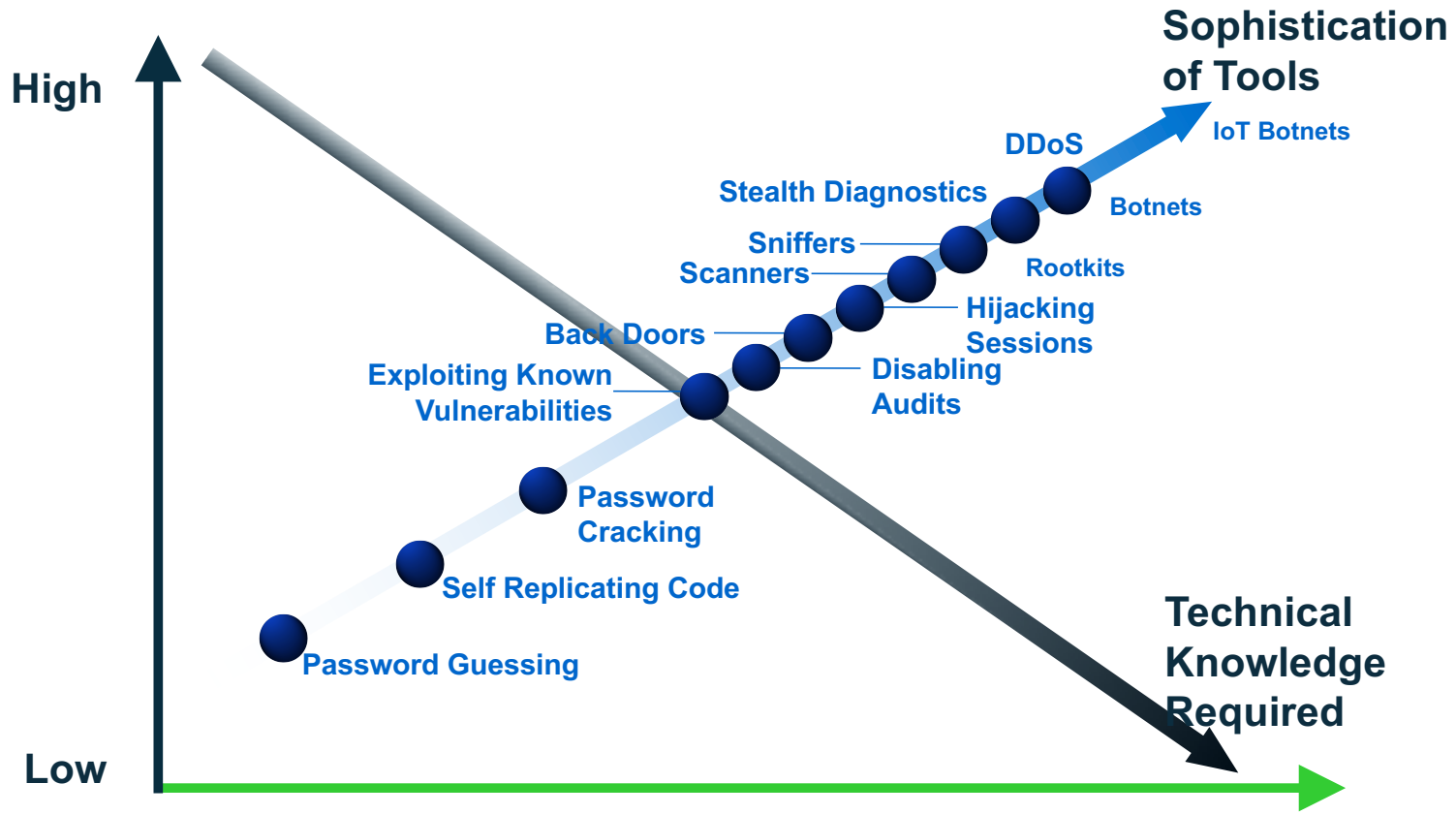
Reaping the Whirlwind

DDoS Defense in the Age of Mirai

Roland Dobbins, *Principal Engineer*
<rdobbins@arbor.net>

Introduction & Context

Evolution of Threats and Exploits



Botnets - The #1 Online Security Threat

Wikipedia on Botnets: **. . . a collection of compromised computers (called zombie computers) [or bots] running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.**

Botnets are the prime enablers of all these activities:

- DDoS
- Extortion
- Advertising click-through fraud
- Fraudulent sales
- Identity theft and financial fraud (phishing, stealing info from PCs, etc.)
- Theft of goods/services
- Espionage/theft of information
- Spam-based stock-market manipulation

ARBOR NETWORKS

DDoS Attacks – A Fact of Life on the Internet

- DDoS attacks are taking place 24/7/365 – they're simply a fact of life on the Internet.
- Any organization, any site, any individual can be affected by DDoS, either as a direct target or via collateral damage.
- Outbound DDoS can be just as devastating to end-customers and SPs as inbound DDoS – botted hosts on broadband access networks, on enterprise networks, and within IDCs affect both the source networks and the targets.
- Situational awareness is key – what's happening in the news? What anniversaries are taking place this year/month/week/today?
- Miscreants attack one another with regularity – collateral damage!

ARBOR® NETWORKS

The Emperor's New Cloud

- We're relying upon 34-year-old protocols designed for use in a laboratory environment and with little/no regard for security as the foundation of our global Internet infrastructure.
- Although there's a large body of work on operational security (opsec) and scalable Internet architectures, it's honored more in the breach than in actual deployments.
- Ongoing, pervasive disconnect between network architects, application architects, operational groups, security teams, management.
- Pollyannaish attitude towards security – 'Why would anyone attack *us*?'
- Lack of accountability – is anyone ever fired as a result of avoidable security incidents?
- Pervasiveness of security theater/security snake-oil.
- Inability/unwillingness to properly assess abstract threat models – a necessary psychological defense mechanism?

ARBOR® NETWORKS

DDoS Background

What is a **D**istributed **D**enial **o**f **S**ervice (DDoS) attack?

- An attempt to **consume** finite **resources**, **exploit weaknesses** in software design or implementation, or **exploit lack** of infrastructure **capacity**
- Targets the **availability** and **utility** of computing and network resources
- Attacks are almost always **distributed** for even more significant effect (i.e., DDoS)
- The **collateral damage** caused by an attack can be as bad, if not worse, than the attack itself
- **DDoS attacks affect availability**! No availability, no applications/services/data/Internet! No revenue!
- DDoS attacks are attacks **against capacity and/or state**!

ARBOR NETWORKS

Three Security Attributes

- The goal of security is to maintain these three attributes.

ARBOR NETWORKS

Three Security Attributes

- The primary goal of DDoS defense is maintaining availability in the face of attack

ARBOR NETWORKS

Almost All Security Spending/Effort is Focused on Confidentiality & Integrity

- Confidentiality and integrity are relatively simple concepts, easy for non-specialists to understand
- In practice, confidentiality and integrity pretty much equate to encryption - again, easy for non-specialists to understand
- The reality is that there's more to them than encryption, but it's easy to proclaim victory - "We have anti-virus, we have disk encryption, we're PCI-compliant, woo-hoo!"
- And yet, hundreds of millions of botted hosts; enterprise networks of all sizes in all verticals completely penetrated, intellectual property stolen, defense secrets leaked, et. al.
- Availability can't be finessed - the Web server/DNS server/VoIP PBX is either up or it's down. No way to obfuscate/overstate/prevaricate with regards to actual, real-world security posture.
- Availability requires operational security (opsec) practitioners who understand TCP/IP and routing/switching; who understand Web servers; who understand DNS servers; who understand security; who understand layer-7.
- These people are rare, and they don't come cheaply. Most organizations don't even understand the required skillsets and experiential scope to look for in order to identify and hire the right folks

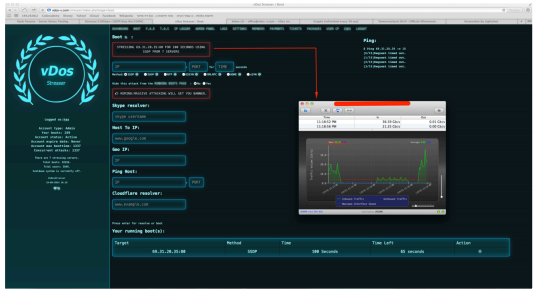
ARBOR NETWORKS

Availability is Hard!

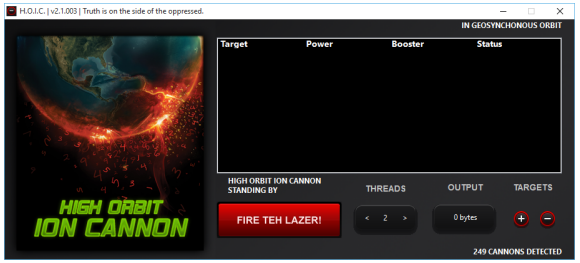
- Maintaining availability in the face of attack requires a combination of skills, architecture, operational agility, analytical capabilities, and mitigation capabilities which most organizations simply do not possess
- In practice, most organizations never take availability into account when designing/speccing/building/deploying/testing online apps/services/properties
- In practice, most organizations never make the logical connection between maintaining availability and business continuity
- In practice, most organizations never stress-test their apps/services stacks in order to determine scalability/resiliency shortcomings and proceed to fix them
- In practice, most organizations do not have plans for DDoS mitigation - or if they have a plan, they never rehearse it!

The weaponization of DDoS

”Weaponize” : *Convert to use as a weapon / simplify use as weapon*



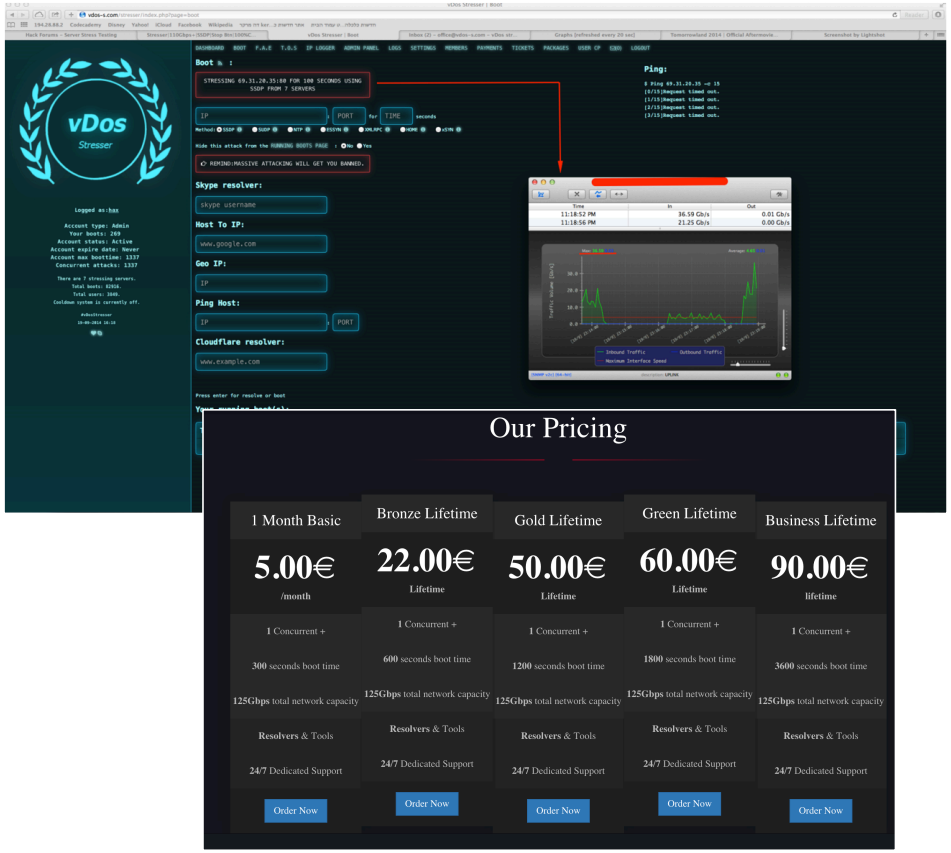
- Increased availability of “Stresser Tools”/”Booters” which perform highly distributed attacks using a combination of non-spoofed and spoofed amplification attacks. Often linked to bot-farms.



- Development of tools for use by voluntarily opt-in attackers:
  - Low Orbit Ion Cannon used to perform non-spoofed UDP/ICMP attacks
  - High Orbit Ion Cannon sends non-spoofed HTTP requests against multiple sites

ARBOR NETWORKS

DDoS tools for the masses



- Anyone which has the capability to click a button can now launch an DDoS attack.
- Cheap and simple to use:
  - VIP accounts!
  - Lifetime subscription!
  - 24x7 customer support!
- Primarily used by gamers attacking each other but recently we have been seeing them used to attack highly visible targets.

ARBOR NETWORKS

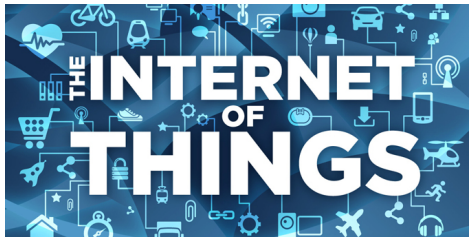
The IoT Situation

INTERNET OF THINGS


```
Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!

. . .

                    .                                   .
                   @88>                                 @88>
      ..     .     :  %8P      .u     .                  %8P
   .888: x888  x888.      .    .d88B :@8c       u          .
  ~ 8888~'888X ?888f   .@88u  =~8888f8888r    us888u.   .@88u
    X888  888X '888>  ''888E    4888>'88~   .@88 ~8888~ ''888E
    X888  888X '888>    888E    4888> '     9888  9888    888E
    X888  888X '888>    888E    4888>       9888  9888    888E
    X888  888X '888>    888E   .d888L .+    9888  9888    888E
   ~*88%~~*88~ '888!    888&   ^~8888*~     9888  9888    888&
     ~     ~    ~       R888~    ~Y~       ~888*~~888~   R888~
                          ~~                  ^Y~   ^Y'    ~~

            - A text-based MUD by Oscar Popodokulus -


No account? Register at www.elrooted.com
Enter user> yop
yop
Enter pass> yop
***

Disconnected by server.
Press any key to exit.
```

ARBOR NETWORKS

The Internet of Things (IoT)



Wikipedia: *The internet of things (IoT) is the network of physical devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data*

But is this something new or just marketing?

- For example, the “Trojan room coffee pot” was connected to the Internet in 1993.

More exact definition: *An IoT device (embedded device) is essentially a computer with a CPU, memory, software and a set of interfaces which are dedicated for specific roles or tasks.*

ARBOR NETWORKS

DEFAULT USERNAMES AND PASSWORDS!!!

https://krebsonsecurity.com/wp-content/uploads/2016/10/IoTbadpass-Sheet1.csv

```
Username/Password,Manufacturer,Link to supporting evidence
,,
admin/123456,ACTi IP Camera,https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko,ANKO Products DVR,http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass,"Axis IP Camera, et. al",http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv,Dahua Camera,http://www.cam-it.org/index.php?topic=5192.0
root/888888,Dahua DVR,http://www.cam-it.org/index.php?topic=5035.0
root/666666,Dahua DVR,http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv,Dahua IP Camera,http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin,Dahua IP Camera,http://www.cam-it.org/index.php?topic=9396.0
666666/666666,Dahua IP Camera,http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox,Dreambox TV receiver,https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx,EV ZLX Two-way Speaker?,?
root/juantech,Guangzhou Juan Optical,https://news.ycombinator.com/item?id=11114012
root/xc3511,H.264 - Chinese DVR,http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518,HiSilicon IP Camera,https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123,HiSilicon IP Camera,https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234,HiSilicon IP Camera,https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd,HiSilicon IP Camera,https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin,IPX-DDK Network Camera,http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system,"IQinVision Cameras, et. al",https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm,Mobotix Network Camera,http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321,"Packet8 VOIP Phone, et. al",http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-
phones/4119+&cd=21&hl=en&ct=clnk&gl=us
root/00000000,Panasonic Printer,https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek,RealTek Routers,
admin/1111111,Samsung IP Camera,https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc,Shenzhen Anran Security Camera,https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin,SMC Routers,http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb,Toshiba Network Camera,http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt,Ubiquiti AirOS Router,http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor,VideoIQ,https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>,Vivotek IP Camera,https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111,"Xerox printers, et. al",https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521,ZTE Router,http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html
```

ARBOR NETWORKS

IOT Security (or lack of it)

IoT security issues:

- IoT devices usually have limited on-board capabilities and often need external configuration and and control.
- Many of these devices stacks are not properly secured:
  - Hard-coded usernames/passwords
  - Unnecessary services enabled by default (Chargen, SSDP, DNS forwarder)
  - Unsecured management interfaces (Web, SNMP, TR-069 et al.)
  - Limited or no software update capabilities
  - Very seldom patched or updated after deployment
- The number of IoT devices in 2020 is estimated to be about 20-30 Billion. However we have more than 6B already online with 5.5M added every day[1]!

ARBOR NETWORKS

1) Gartner research: http://www.gartner.com/newsroom/id/3165317

Millions of vulnerable IoT devices + Weaponization = ?

IoT Botnets!

The history of IoT Botnets

IoT botnets are actually nothing new:

- The first botnet was created back in 1993 when Robey Pointer created an Internet Relay Chat (IRC) bot called “eggbot” which was used to defend IRC channels by launching flooding attacks against unwanted users. The bot was also used to attack other channels attacks using the CTCP and DCC protocols. Multiple instances of the bot could join efforts and work together in “botnets”.
- In 2003, the first (unintentional) DDoS attack against the University of Wisconsin using IoT devices happened due to a hardcoded NTP address in 700.000 Netgear DSL/cable modems. Even after a new software was released, the attack continued for years until the last device was chucked in the bin.
- In 2008, the first recorded DDoS IoT botnet attack was done using a botnet of Linux based CPE broadband routers.
- In 2012, an unknown researcher published a report called the “Internet census of 2012”. The data used in the report was gathered by hacking into an estimated 420,000 CPE devices around the world using default credentials[1]

ARBOR NETWORKS

1) https://en.wikipedia.org/wiki/Carna_botnet

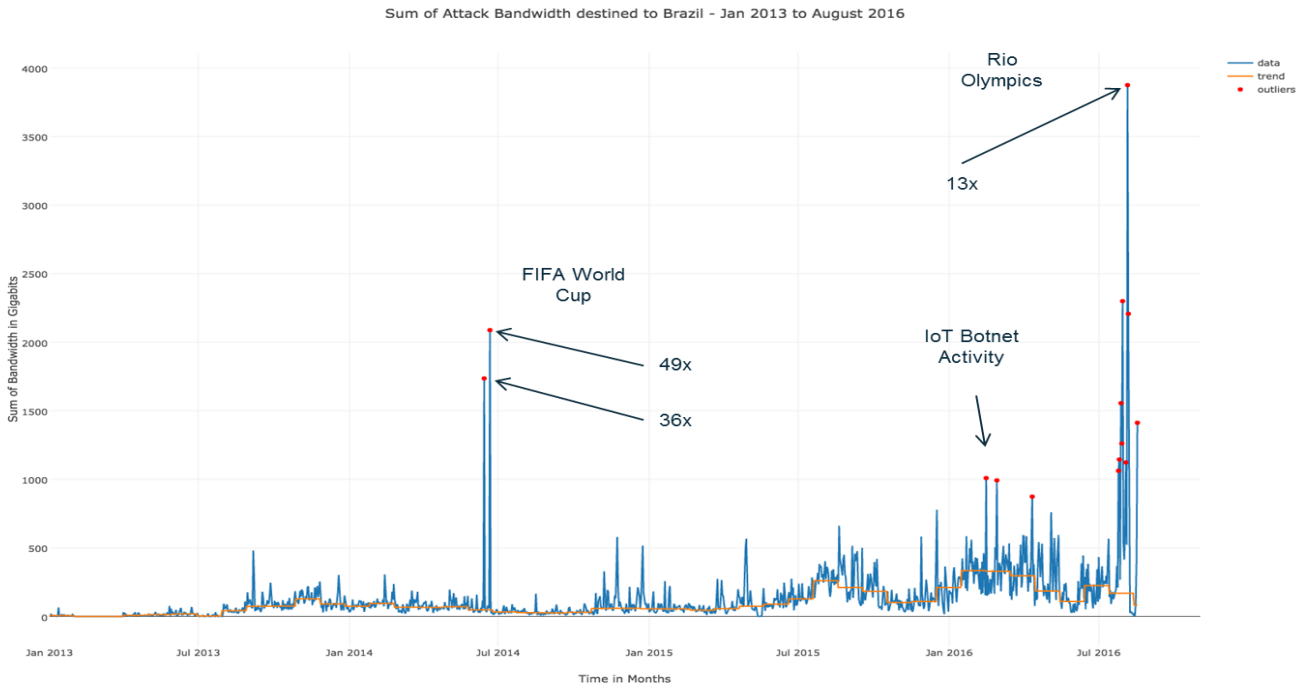
Status of IoT Botnets today

IoT botnets have now been weaponized and are available via booter/stresser services:

- An IoT botnet using Lizardstresser code was used to attack sites in Brazil in 2016 with attack volumes reaching 400gb/sec.
- The same botnet consisting of about 10.000 webcams, was used to launch 540gb/sec sustained attacks against Olympic-affiliated organizations in the summer 2016.
- An IoT botnet based on the Mirai code base was used in the DDoS attacks made in November 2016 against security journalist Brian Krebs, which peaked at 620gb/sec.
- IoT botnets using Mirai code were used in the attacks against authoritative DNS provider Dyn in November 2016.

Source code for both the LizardStresser and Mirai bots has been released into the wild and has spawned multiple new variants.

LizzardStresser Bot Attacks Brazil



- Attacks launched against not only sports-event infrastructure, but also associated sponsors, financial and government institutions.

Dealing with IoT botnets

IoT Botnet Infection vectors – Mirai example

1. A compromised device will create a separate scanning thread to scan for other devices on TCP ports 23,2323,23231,37777 and 7547 (+5555) (TR-069/TR-064 SOAP interface) using random IP's.
2. If a device responds, an attempt will be done to logon using a set of common username/password combinations
3. If successful, the IP address of the vulnerable device is sent to the C&C server
4. The C&C server will log onto the device, download the appropriate malware and compromise the device. The device will now start scanning, go to #1

- As the situation is now, a vulnerable device will get infected within **minutes** of being connected to the Internet.
- Vulnerable devices come primarily from 3 manufactures in China, one of them released a patch in 2014 but only for the English version of their SW.

THE MIRAI BOTNET

Approximately 500,000 devices worldwide

- High concentrations in China, Hong Kong, Macau, Vietnam, Taiwan, South Korea, Thailand, Indonesia, Brazil, and Spain

The same botnet malware used in Krebs, OVH Dyn and Liberia attacks

- Does not imply it was the same adversaries

Multiple possible DDoS attack vectors

At least one variant has been wormified!

IoT Botnet DDoS attack capabilities – Mirai

Flash update Dec. 15th 2016
A new variant of Mirai has been seen in the wild emitting spoofed traffic. Attacks include include SYN-floods, DNS reflection/amplification attacks, and TCP reflection amplification attacks

Attack types:

- UDP flooding
- Valve source engine flooding
- TCP ACK flooding
- TCP "Stomp" attack (ACK flooding on an established TCP connection, designed to bypass DDoS mitigation devices)
- TCP SYN flooding
- GRE Packet flooding
- HTTP request flooding (GET, POST, HEAD)
- DNS pseudo random label-prepending ("DNS Water Torture")

The Mirai malware runs in user space and has until now, not used spoofed IP addresses, prohibiting it from performing spoofed and reflection attacks.

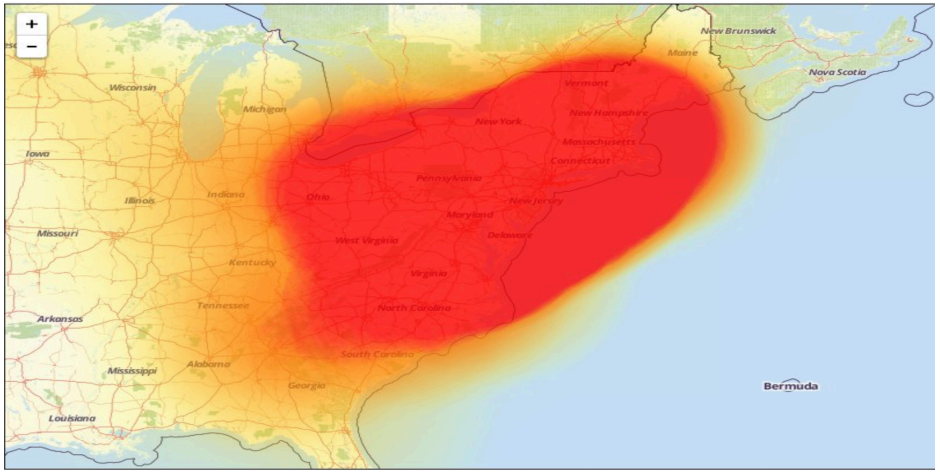
ARBOR NETWORKS

DYN ATTACKS ON OCTOBER 21st

Three Attacks Targeting Dyn's Managed DNS Infrastructure
Dyn Customers include

- Netflix Twitter, Reddit, Github, Spotify, PayPal, Airbnb, NYT, etc.

These attacks resulted in large-scale outages for Dyn Customers, even though the customers were not attacked directly



ARBOR NETWORKS

DYN ATTACK TIMELINE

Attack 1
Start: 11:10 UTC

Duration: 2 hours and 20 minutes

Attack 2
Start: 15:50 UTC

Duration: 1 hour and 10 minutes

Attack 3
Mitigated from the start

Destinations: APAC, South America, Eastern Europe, US-West, US-East
Outages were regional

Understanding & Mitigating the Attacks

Multiple Highly Distributed Attack Vectors
Dyn originally reported ”10s of millions of IP addresses”

Later corrected to an estimate of 100,000

Cascading Effect
DNS service disruption from original attack generates legitimate retry activity

This is what caused Dyn to initially overreport the number of attacking IP’s

Mitigations:

ACLs, S/RTBH, flowspec, IDMS

LIBERIA ATTACKS – BEGINNING OCTOBER 31

SC Magazine US > News > Analysts mixed on reason for Liberia Mirai attack

by Bradley Barth, Senior Reporter

November 04, 2016

Analysts mixed on reason for Liberia Mirai attack

A barrage of Mirai botnet-fueled distributed denial of service (DDoS) attacks reportedly incapacitated Internet operations across the West African coastal nation of Liberia earlier this week, bu industry researchers had mixed views on the rationale behind the attack and damage inflicted.

A large botnet operation dubbed Shadows Kill targeted Liberian IP addresses with a DDoS attack over several days this past week, prompting speculation as to the perpetrators' true motive.

In a Thursday post on the publishing site *Medium*, independent researcher Kevin Beaumont reported a series of "continued short duration attacks" – perpetrated by a Mirai botnet composed of Internet of Things devices such as CCTV cameras – that may have crippled Liberia's Internet infrastructure. Beaumont linked the attacks to the same actor that launched a massive attack against the DNS service Dyn on Oct. 21, knocking out such websites as Amazon, Reddit and Twitter.

ARBOR NETWORKS

~~IoT Botnet~~ DDoS mitigation

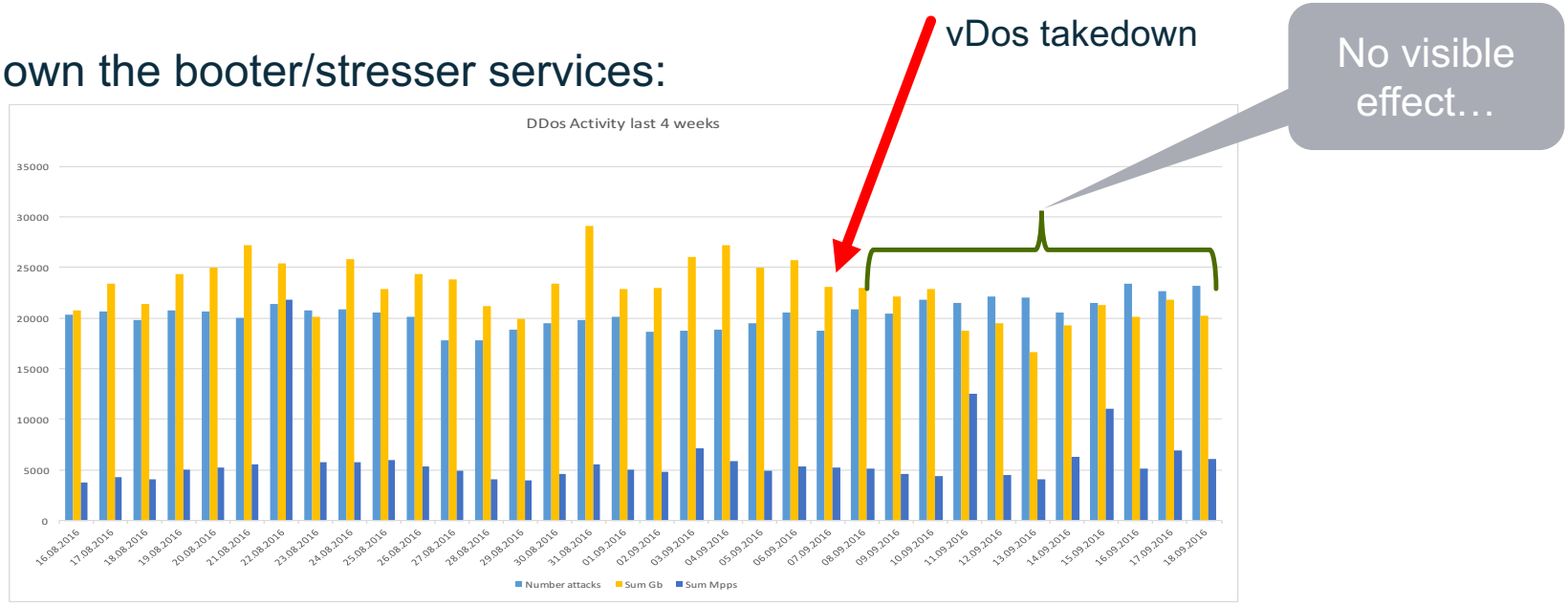
IoT botnets are nothing new and the attacks used are also nothing new. The same DDoS mitigation approaches still apply!

- Implement Best Current Practices (BCP's) for infrastructure, host/application/services and DNS servers. This includes specifying network access polices for common server types.
- Use flow telemetry to detect, classify and traceback DDoS traffic.
- Use S/RTBH, flowspec, intelligent DDoS mitigation solutions (IDMSes) to mitigate attacks.
- Plan and practice dealing with DDoS attacks.

How to Reduce the Threat of IoT Botnets

IoT botnets are popular today because IoT devices are vulnerable and the tools to infect and subvert them for attacks purposes are readily available.

1. Shutdown the booter/stresser services:



How to Reduce the Threat of IoT Botnets (cont.)

2. Stop selling and deploying vulnerable IoT devices:
   - Who is going to enforce this?
   - Who is going to pay for this?
   - Do people care that their webcam is attacking someone else?

3. Patch vulnerable IoT devices:
   - When did you last upgrade your CPE device? Smart TV? Coffee maker? Your smart lightbulbs?
   - The Netgear routers attacking the University of Wisconsin NEVER got patched and the attack died only when the last device was thrown into the bin.

4. If IoT devices cannot be fixed (or trusted), isolate them from the Internet and create barriers!

Example of how to isolate IoT devices – Steinthor's home network! ☺

In 2011, Steinthor connected 3 IP Web Cams to his home network. These devices communicate with a Synology NAS which provides video portal and stores all video recordings.

The network is segmented into 2 areas:

- User VLAN
- Video subnet where an (old) Cisco ASA 5505 controls all communication between the Webcams and the the NAS.

VideoCameras (5 incoming rules)

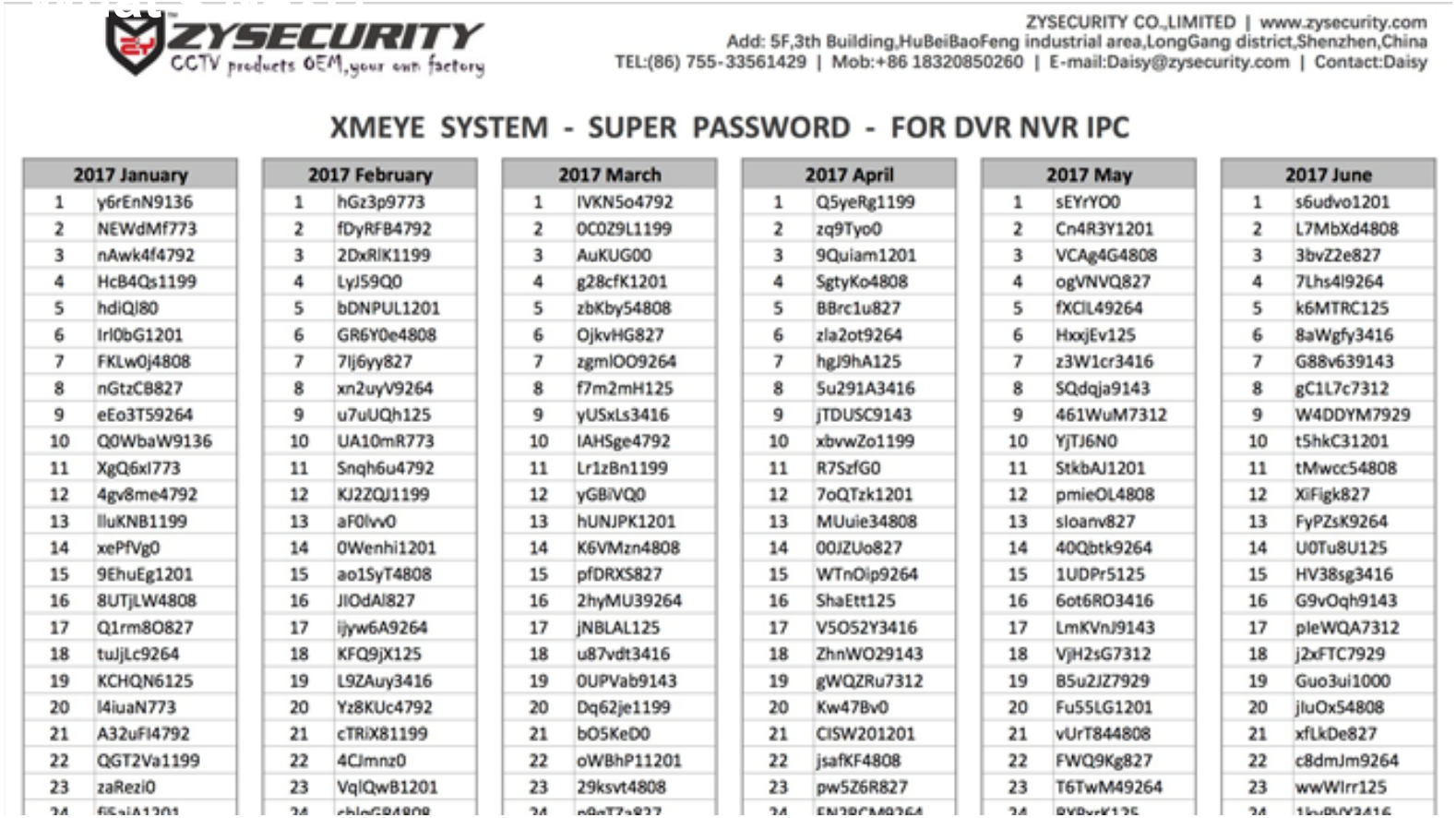
1	☑	any	SynologyNAS	ip	Permit	TOP 10 3975813		
2	☑	any	any	echo-reply	Permit	0		
3	☑	any	any	domain	Permit	0		
4	☑	any	any	ntp	Permit	160		
5		any	any	ip	Deny			Implicit rule

L3 VPN is used to allow remote access to the webcam portal running on the Synology.

1) See also http://robert.penz.name/1341/ready-your-home-network-for-iot/

What's Next?

What's Next?



ZYSECURITY
CCTV products OEM, your own factory

ZYSECURITY CO.,LIMITED | www.zysecurity.com
Add: 5F,3th Building,HuBeiBaoFeng industrial area,LongGang district,Shenzhen,China
TEL:(86) 755-33561429 | Mob:+86 18320850260 | E-mail:Daisy@zysecurity.com | Contact:Daisy

XMEYE SYSTEM - SUPER PASSWORD - FOR DVR NVR IPC

	2017 January		2017 February		2017 March		2017 April		2017 May		2017 June
1	y6rEnN9136	1	hGz3p9773	1	IVKN5o4792	1	Q5yeRg1199	1	sEYrYO0	1	s6udvo1201
2	NEWdMf773	2	fDyRFB4792	2	0C0Z9L1199	2	zq9Tyo0	2	Cn4R3Y1201	2	L7MbXd4808
3	nAwk4f4792	3	2DxRlK1199	3	AuKUG00	3	9Quiam1201	3	VCAg4G4808	3	3bvZ2e827
4	HcB4Qs1199	4	LyJ59Q0	4	g28cfK1201	4	SgtyKo4808	4	ogVNVQ827	4	7Lhs4l9264
5	hdiQl80	5	bDNPUL1201	5	zbKby54808	5	BBrc1u827	5	fXCIL49264	5	k6MTRC125
6	Irl0bG1201	6	GR6Y0e4808	6	OjkvHG827	6	zla2ot9264	6	HxxjEv125	6	8aWgfy3416
7	FKLw0j4808	7	7lj6yy827	7	zgmlOO9264	7	hgJ9hA125	7	z3W1cr3416	7	G88v639143
8	nGtzCB827	8	xn2uyV9264	8	f7m2mH125	8	5u291A3416	8	SQdqja9143	8	gC1L7c7312
9	eEo3T59264	9	u7uUQh125	9	yUSxLs3416	9	jTDUSC9143	9	461WuM7312	9	W4DDYM7929
10	Q0WbaW9136	10	UA10mR773	10	IAHSge4792	10	xbvwZo1199	10	YjTJ6N0	10	t5hkC31201
11	XgQ6xl773	11	Snqh6u4792	11	Lr1zBn1199	11	R7SzfG0	11	StkbAJ1201	11	tMwcc54808
12	4gv8me4792	12	KJ2ZQJ1199	12	yGBiVQ0	12	7oQTzk1201	12	pmieOL4808	12	XiFigk827
13	lluKNB1199	13	aF0lvv0	13	hUNJPK1201	13	MUuie34808	13	sloanv827	13	FyPZsK9264
14	xePfVg0	14	0Wenhi1201	14	K6VMzn4808	14	00JZUo827	14	40Qbtk9264	14	U0Tu8U125
15	9EhuEg1201	15	ao1SyT4808	15	pfDRXS827	15	WTnOip9264	15	1UDPr5125	15	HV38sg3416
16	8UTjLW4808	16	JlOdAl827	16	2hyMU39264	16	ShaEtt125	16	6ot6RO3416	16	G9vOqh9143
17	Q1rm8O827	17	ijyw6A9264	17	jNBLAL125	17	V5O52Y3416	17	LmKVnJ9143	17	pleWQA7312
18	tuJjLc9264	18	KFQ9jX125	18	u87vdt3416	18	ZhnWO29143	18	VjH2sG7312	18	j2xFTC7929
19	KCHQN6125	19	L9ZAuy3416	19	0UPVab9143	19	gWQZRu7312	19	B5u2JZ7929	19	Guo3ui1000
20	l4iuaN773	20	Yz8KUc4792	20	Dq62je1199	20	Kw47Bv0	20	Fu55LG1201	20	jluOx54808
21	A32uFl4792	21	cTRiX81199	21	bO5KeD0	21	CISW201201	21	vUrT844808	21	xfLkDe827
22	QGT2Va1199	22	4CJmnz0	22	oWBhP11201	22	jsafKF4808	22	FWQ9Kg827	22	c8dmJm9264
23	zaRezi0	23	VqlQwB1201	23	29ksvt4808	23	pw5Z6R827	23	T6TwM49264	23	wwWlrr125

What's Next?

Many, many more categories of consumer-grade 'IoT' devices – light-bulbs, thermostats, 'smart meters', et. al.

Large carrier-class and enterprise routers have been compromised before, used for ICMP-flooding DDoS attacks, route hijacking for DDoS and for spam (cisco/cisco creds, even for Juniper routers)

Multi-stage scanning/compromise of IoT devices *behind* NATs/firewalls!

Now we have NETCONF, and various SDN APIs . . .

. . . and the ability to run arbitrary code on the routers themselves.

Network infrastructure BCPs are more important than ever!

All routers are 'IoT' embedded devices – including big ones! So are smartphones!

ARBOR NETWORKS

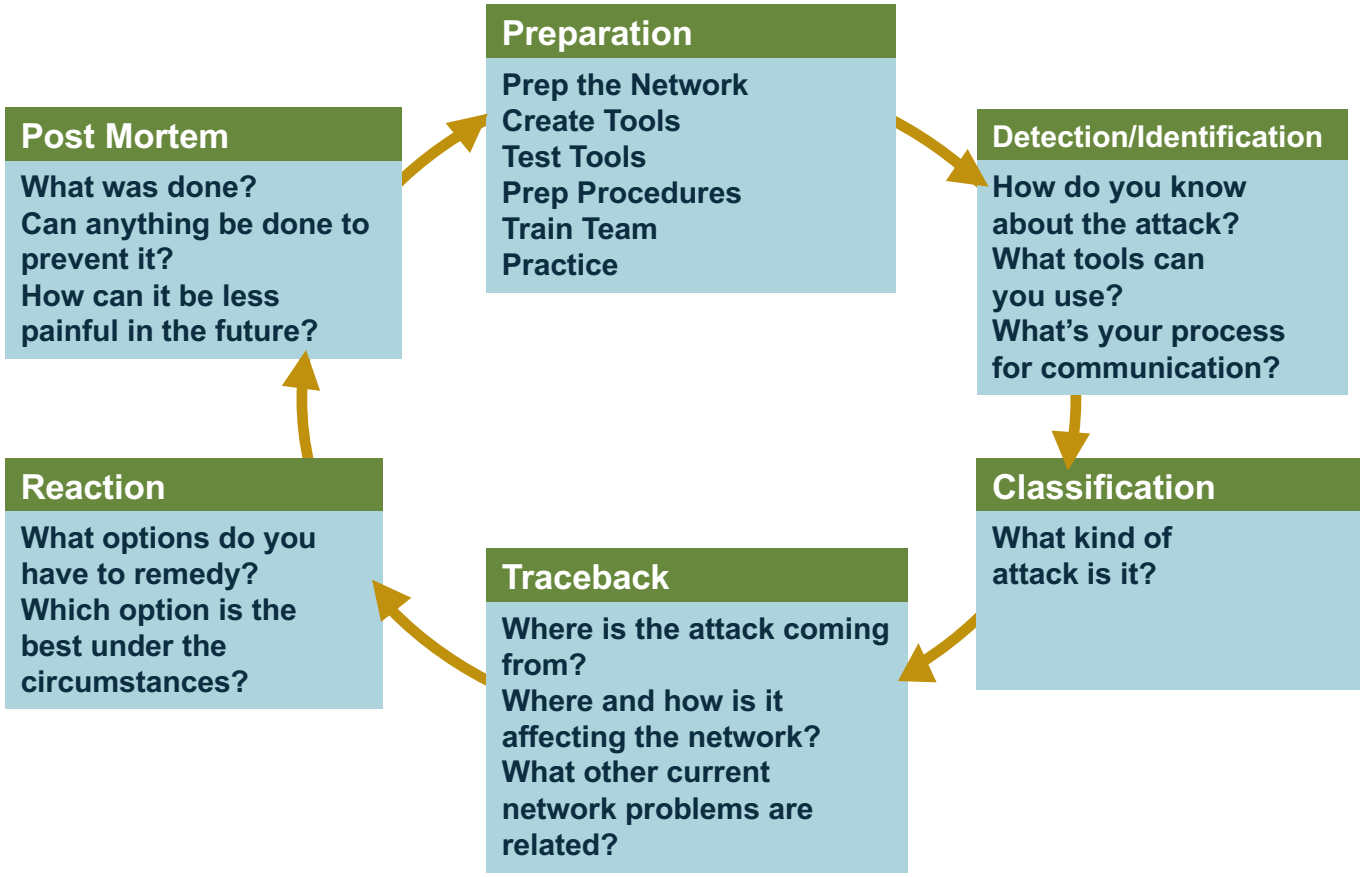
What Can We Do?

Network/Application Availability: Protect the Infrastructure

- Security is the heart of internetworking's future; we have moved from an Internet of implicit trust to an Internet of pervasive distrust
- No packet can be trusted; all packets must earn that trust through a network device's ability to inspect and enforce policy
- Protecting the infrastructure is the most fundamental security requirement
- Infrastructure protection should be included in all high availability designs
- A secure infrastructure forms the foundation for continuous service delivery

ARBOR NETWORKS

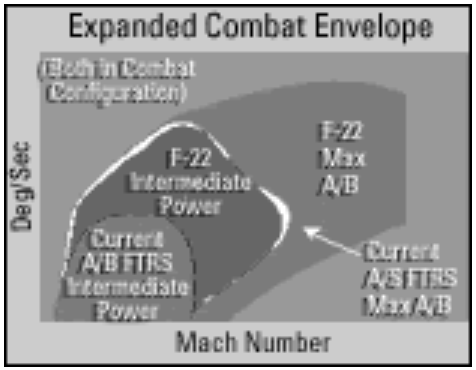
Six Phases of Incident Response

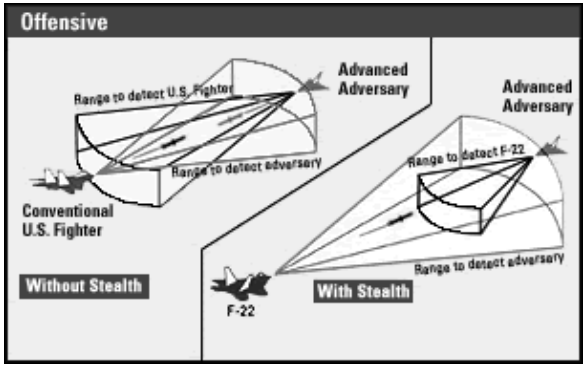


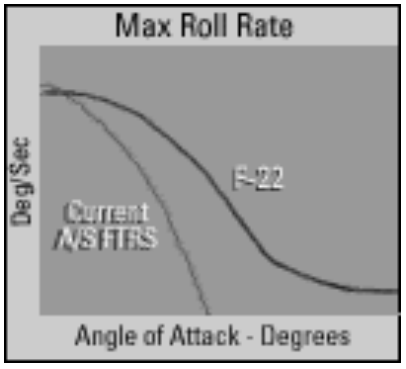
ARE YOU PUSHING THE ENVELOPE?

Know Your Equipment and Infrastructure!

- Know the performance envelope of all your equipment (routers, switches, servers, etc.). You need to know what your equipment is really capable of doing!
- Know the capabilities of your network. If possible, test it. Surprises are not amusing during a security incident
- pps vs. bps vs. qps vs. cps vs. tps - and, how enabling features impacts them





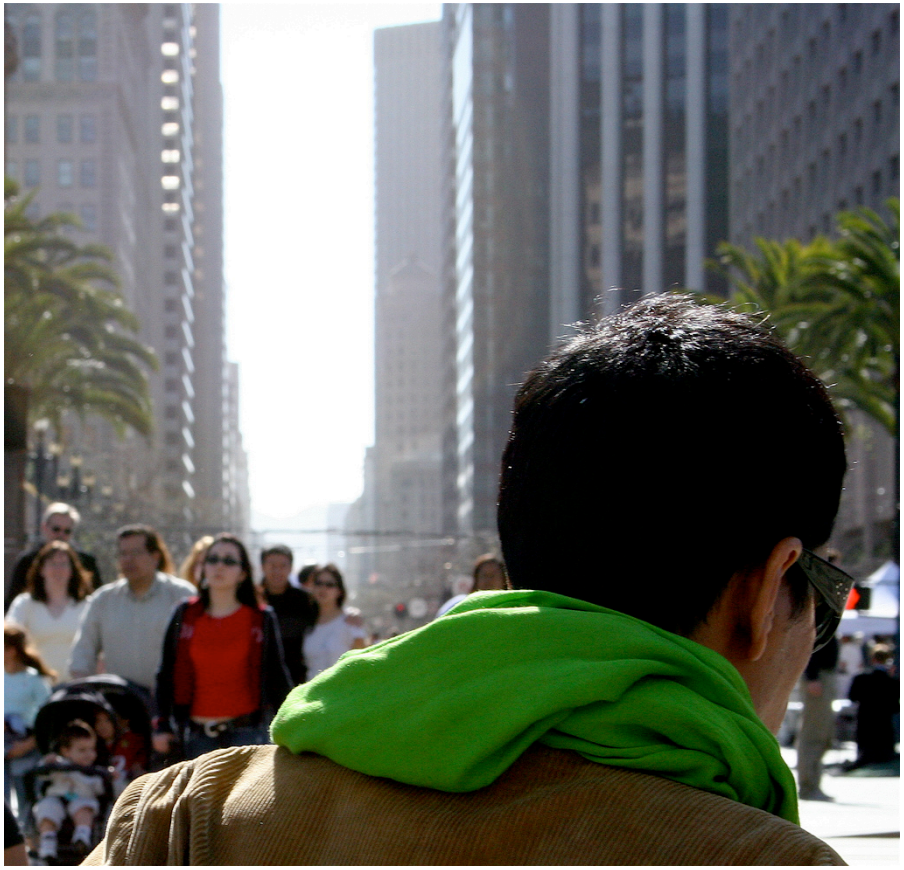


ARBOR NETWORKS

Architecture

The Right Tools for the Right Job

The Right People for the Right Job



OPSEC Team Skill Requirements

The OPSEC Team needs to know:

Everything a Backbone Engineer knows

Everything a Network Management Engineer knows

Everything a sysadmin/webmaster knows

Everything an email postmaster knows

Everything a DNS/DHCP/Addressing Engineer knows

Everything a CERT Engineer knows

Everything an Enterprise Infosec specialist knows

In essence, you're looking for super-engineers who are hybrid Backbone/Security Engineers.

Infrastructure Best Current Practices (BCPs)

- Interface ACLs (iACLs) should be employed at the relevant network edges (peering/transit, customer aggregation edge, etc.) to protect the network infrastructure itself; additional service-specific sections should be used to restrict traffic destined for Internet-facing servers to the ports and protocols associated with the services and applications on those servers.

- The use of GRE – IP Protocol 47 - in these attacks is notable as a common mechanism used by attackers to bypass ACLs that only contain policy statements relating to common protocols such as TCP, UDP, and ICMP; there are 254 valid Internet protocols, and irrelevant protocols should be filtered at the edges via ACLs.

- Additional network infrastructure BCPs such as control- and management-plane self protection mechanisms (rACL, CoPP, GTSM, MD5 keying, et. al.) should also be deployed.

- All network infrastructure devices should be accessible only via designated management hosts, and this access should be facilitated via a dedicated out-of-band (OOB) management network. During high-impact DDoS attacks, a dedicated management network ensures that devices can be managed irrespective of conditions on the production network, and also ensures that vital mechanisms such as flow telemetry and SNMP are uninterrupted, which assures continuing visibility into attack traffic during an incident

Infrastructure BCPs (cont.)

- Flow telemetry such as Cisco NetFlow, Juniper cflowd, and sFlow should be enabled at all network edges, and exported into a collection/analysis system.
- Source-based remotely-triggered blackholing (S/RTBH) is a powerful reaction technique which allows tens or even hundreds of thousands of attacking source IPs (classified via flow analysis, logfiles, etc.) to be rapidly blackholed based upon their source addresses. S/RTBH leverages BGP as a control-plane mechanism to instantaneously signal edge devices to start dropping attack traffic. Flowspec allows for layer-4 granularity – instantaneous ACL deployment via BGP!
- Intelligent DDoS mitigation systems (IDMS) should be deployed in topologically-suitable cleaning centers in order to protect servers/services/applications. They should be emplaced northbound of load-balancers; if an organization insists on placing firewalls and IDS/'IPS' inline in front of servers, protect these stateful DDoS chokepoints and everything behind them!
- Do not place firewalls and IDS/'IPS' in front of servers – they provide no security value whatsoever in server environments where every incoming connection is by definition unsolicited. They are DDoS chokepoints, and degrade the operational security posture of the network and applications.
- Policy should be enforced by stateless ACLs in hardware-based routers/switches!

Host Best Current Practices (BCPs)

- Public-facing servers should be configured in a hardened manner, with unnecessary services disabled, OOB management access, service-specific configuration hardening, IP stack tuning, and other relevant mechanisms.

- Stateless on-server filtering via tcpwrappers is a useful policy-enforcement mechanism; for Web servers, Apache modules such as mod_security and mod_evasive bring additional capabilities.

- The deployment of stateful firewalls or other inspection devices such as IDS/'IPS' in front of Internet-facing servers is contraindicated; as each incoming connection to Internet-facing servers is by definition unsolicited, the stateful inspection adds nothing to the security posture of the servers, and serves to weaken their ability to withstand DDoS traffic due to the limited state-table size of even the largest/fastest firewalls and IDS/IPS on the market today.

  During these particular attacks and many others, firewalls in front of targeted servers were observed to fail while receiving relatively low amounts of attack traffic, thereby enabling the DDoS to succeed in making the servers unavailable with little effort on the part of the attacker

Host BCPs (cont.)

- Load-balancers also instantiate state which renders the real servers behind the load-balancers more vulnerable to DDoS; during these attacks, load-balancers were observed to fail due to state exhaustion as a result of the attack traffic. S/RTBH, flowspec, reverse-proxy caches, & IDMS should be utilized to protect the load-balancer and the real servers behind it.

- DNS infrastructure should be deployed in a modular, bulkheaded architecture, with separation of functions such as authoritative servers, internal resolvers, external resolvers, caching-only resolvers, etc., and should be scaled appropriately by employing techniques such as IPv4 anycast addressing. Flowspec, S/RTBH, DNS server self-defense mechanisms such as RRL, & IDMS should be employed to protect the DNS from deliberate attack and/or collateral damage.

Are We Doomed?

- ***No!*** Deploying existing, well-known tools/techniques/BCPs results in a vastly improved security posture with measurable results.
- Evolution of defenses against these attacks demonstrates that positive change is possible – targeted organizations & defending ISPs/MSSPs have altered architectures, mitigation techniques, processes, and procedures to successfully mitigate these attacks.
- Mitigation capacities are scaling to meet and exceed attack volumes – deployment architecture, diversion/re-injection bandwidth, leveraging network infrastructure are key.
- Automation is a Good Thing, but it is no substitute for resilient architecture, insightful planning, and smart opsec personnel, who are more important now than ever before!

ARBOR NETWORKS

Summary

- The situation today is similar to when Windows XP was the most-used OS, lots of vulnerable devices and not much defense against compromise. This was solved by releasing more resilient software and gradually, the number of vulnerable devices went down. However, we still have vulnerable Windows XP computers connected to the Internet… ☹ . . . and now we have orders of magnitude of more vulnerable IoT devices!
- Bots are becoming more intelligent and have more advanced capabilities. The Windows-based Medusa bot spawns IE browser threads to perform advanced HTTP and HTTP/S attacks. → More intelligence is needed to deal with these attacks – and we have it!
- Defenses must be implemented ***before*** the attacks happen!
- Successful DDoS defense against high-capacity, high-complexity attacks takes place ***every day***!
- ***We know how to do this!***

Thank You!

Roland Dobbins, *Principal Engineer*
<rdobbins@arbor.net>

ARBOR NETWORKS
The Security Division of NETSCOUT