



Breaking the Bank

An Analysis of the 2012 – 2014
'Operation Ababil' Financial Industry
DDoS Attack Campaign

ARBOR[®]
NETWORKS



Roland Dobbins <rdobbins@arbor.net>

Senior ASERT Analyst

+66-83-266-6344 BKK mobile

+65-8396-3230 SIN mobile

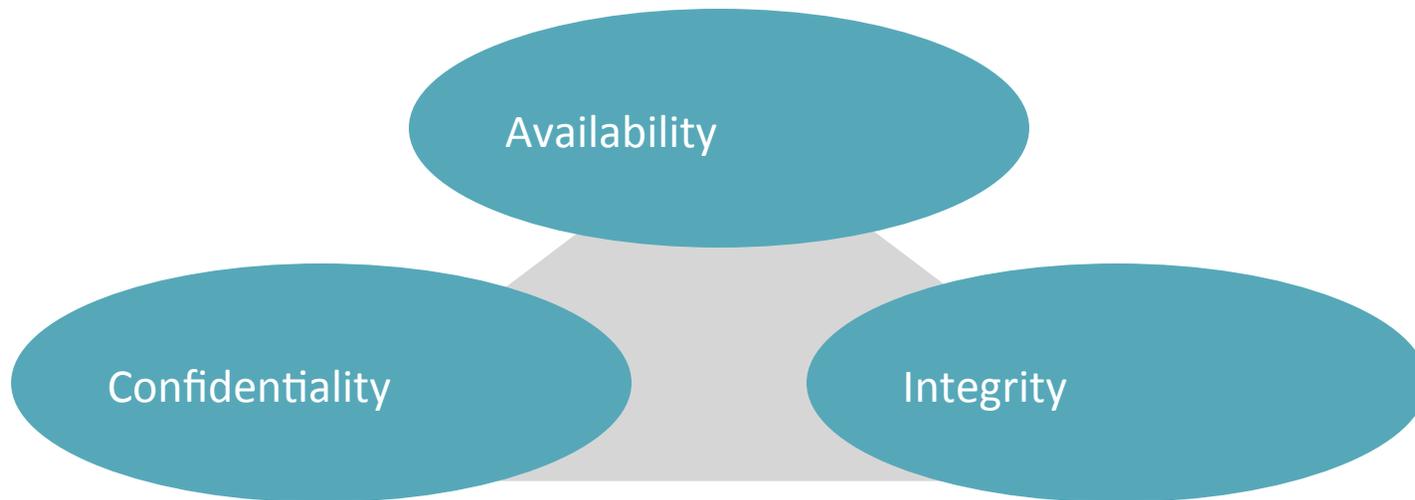
Arbor Public

DDoS Background

What is a **Distributed Denial of Service (DDoS)** attack?

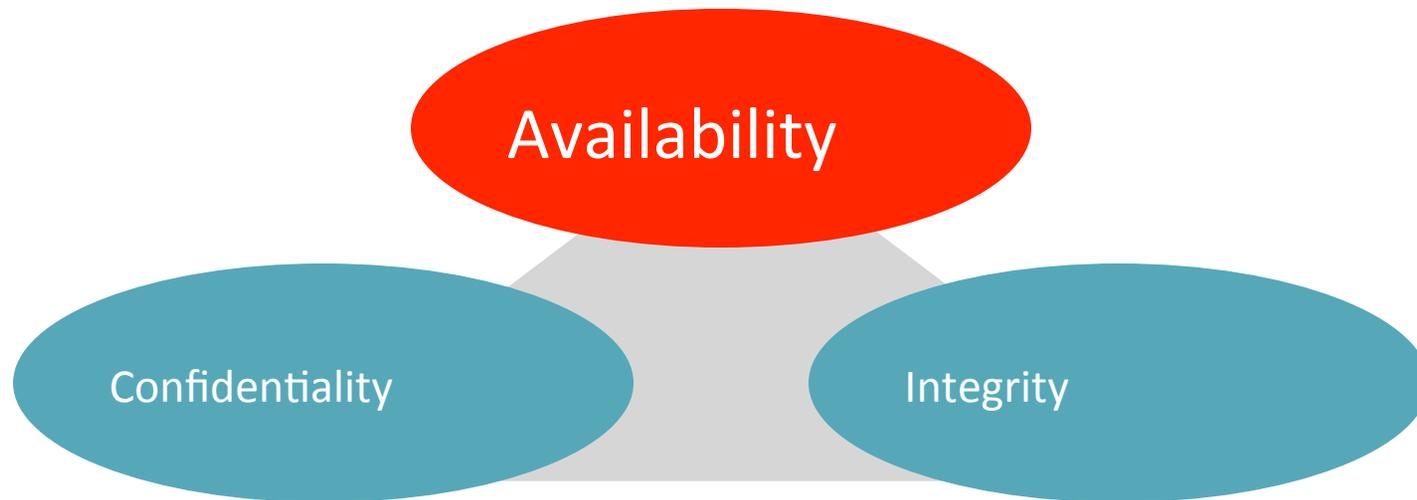
- An attempt to consume finite resources, exploit weaknesses in software design or implementation, or exploit lack of infrastructure capacity
- Targets the availability and utility of computing and network resources
- Attacks are almost always distributed for even more significant effect – i.e., DDoS
- 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!

Three Security Characteristics



- The goal of security is to maintain these three characteristics

Three Security Characteristics



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

'Operation Ababil' DDoS Attacks, AKA 'Triple Crown'

- On 18Sep2012, a purported organization calling itself 'Cyber Fighters of Izz ad-din Al Qassam' posted on Pastebin calling for attacks against Bank of America and the New York Stock Exchange, supposedly in response to a video posted on YouTube offensive to Muslims
- Attack campaign originally christened 'Triple Crown' because three distinct attack tools/methodologies were being used. Industry eventually switched over to attacker sobriquet of 'Operation Ababil'.
- Fifth Week of attack campaign announced via Pastebin on 16Oct2012 - no longer naming targets
- Phase 2 of attack campaign announced via Pastebin on 10Dec2012
- Pastebin post on 8Jan2013 indicates the attacks will be waged for 56 additional weeks
- Pastebin post on 6May2013 indicated pause for supposed Anonymous #OpUSA, which never materialized
- An abortive Phase 4 kicked off unannounced on 23Jul13 – a few hours of attacks that week; a few hours the next week; one attack in mid-August; and then nothing more, so far . . .

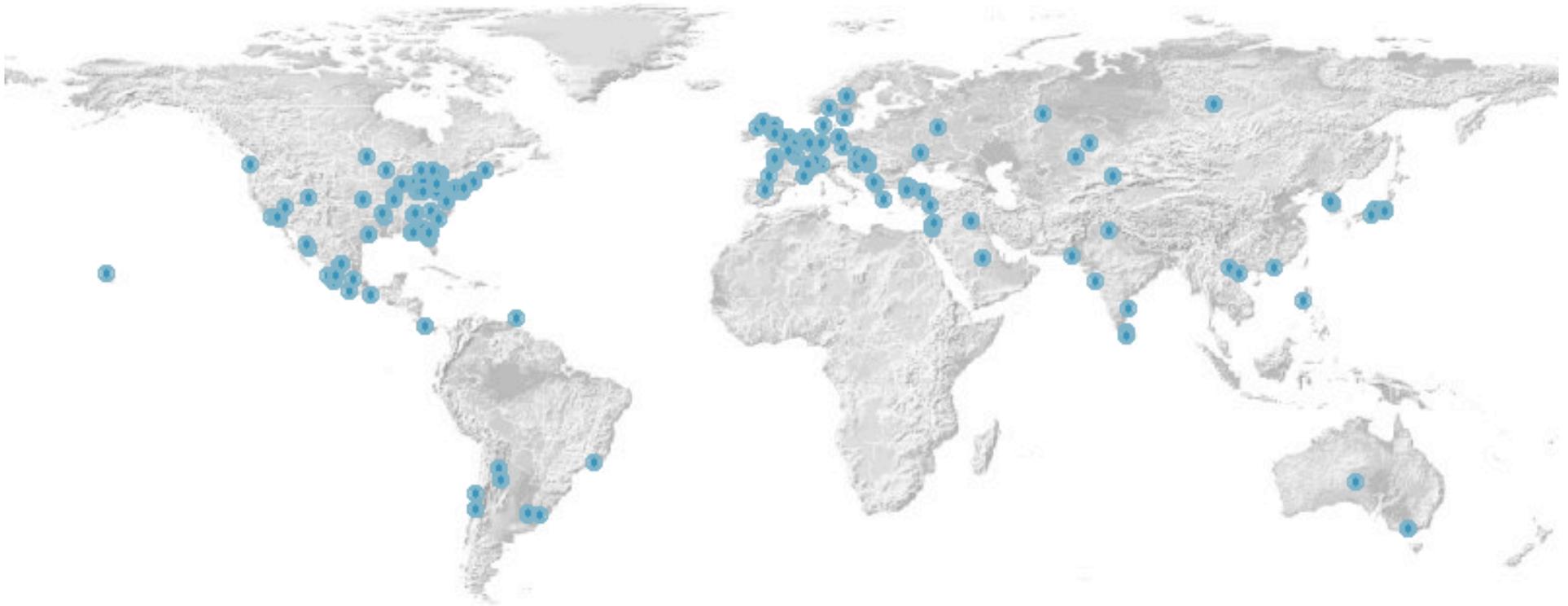
Evolution of Attack Campaign

- **Phase 1 (Sep 2012)**
 - 1-2 banks concurrently attacked, mainly HTTP & HTTP/S combined with malformed DNS flooding attacks
 - Targeting only the largest institutions
- **Phase 2 (Dec 2012)**
 - 3-5 banks concurrently attacked – some HTTP, but more SSL combined with malformed DNS flooding attacks
 - Targeting regional and mid-size institutions
- **Phase 3 (Feb 2013)**
 - 6+ organizations attacked simultaneously, different characteristics for each target, application attacks mostly HTTP/S & malformed DNS
 - Targeting additional institutions such as credit unions and non-customer facing financial services
 - Expanded target base to Europe
- **Phase 4 (Jul/Aug 2013)**
 - A few hours of attacks targeting 2-3 institutions simultaneously, then nothing until mid-August; 1 institution targeted the week of 11Aug13.
 - Somewhat improved attack methodology, UDP/53 traffic directed towards authoritative DNS servers for targeted organizations

Evolution of Attack Campaign (cont.)

- **Phase 5? (28Jan14)**
 - A few hours of attacks targeting 2-3 institutions simultaneously – different attack methodology than observed previously.
 - No announcements on pastebin.com.
 - ‘European Cyber Army’ (ECA) claimed responsibility via Twitter, no way to verify
 - Another group hijacked botnet for its own purposes?

About the Botnet



- Started small, with only a few hundred compromised servers
- Maximum number of hosts ~20,000
- Blacklist currently includes ~3,000 hosts
- Attackers continue adding bots to stay ahead of blacklists, compensate for bots identified and shut down by ISPs, tinkering with bot code

Focused Multi-Stage & Multi-Vector DDoS

- Compromised PHP, WordPress, & Joomla servers
- Multiple concurrent attack vectors
 - GET and POST app layer attacks on HTTP and HTTP/S
 - DNS query app-layer attack, mainly against ISP authoritative DNS servers
 - Floods on UDP, TCP SYN floods on TCP/53 against ISP authoritative DNS servers & target organization Web properties
- Characteristics of this attack campaign
 - Relatively high bps/pps/cps/tps rates per individual attack source
 - Attacks on multiple targeted organizations in same vertical
 - Real-time monitoring of effectiveness
 - Some agility in modifying attack vectors when mitigated
 - Revert to using conventional botnet for SYN-floods, etc. when main attack methodologies are successfully mitigated

Why a Server-Based Botnet?

- Generally **more powerful** machines
- Much **higher Internet transit** bandwidth
- **Hosts not shut down** outside of business hours
- Less chance that administrators will **notice performance issue and investigate**
- Many IDC operators **don't have basic visibility** into their network traffic
- Easy to identify **new hosts to compromise**
- This is nothing new – **the first botnets** in the late 1980s/early 1990s were comprised of servers. It's '**Back to the Future**'!

Primary Attack Tools/Methodologies

- Brobot
 - PHP attack kit, first seen Jan2012. Implements TCP, UDP (malformed DNS query) and ICMP flooding attacks, plus HTTP & HTTP/S GET and POST
 - New variant in Dec2012 implemented the creation of crafted, well-formed DNS queries
- Kamikaze
 - HTTP & HTTP/S DDoS PHP script first used in Sep2012
 - Multi-tier C&C commands sent to 'runners' which pass attack commands to other compromised systems.
- Amos
 - Related to Kamikaze but uses different request template, slightly different User-Agents, and does not implement the cURL functions.
- Additional tools and variants of the above continue to evolve, conventional botnets used on occasion

Multi-vector DDoS, High-PPS/BPS Sources

- Multiple concurrent attack vectors
 - GET and POST application- layer attacks over HTTP and HTTP/S
 - DNS query app-layer attack
 - Floods on UDP, TCP SYN-floods, ICMP and other IP protocols (mainly grossly-malformed DNS packets used as a blunt instrument against Web servers, not DNS servers, until Phase 4, when authoritative DNS servers for targeted organizations were packeted with this traffic)
- Unique characteristics of the attacks
 - Relatively high packet-per-second (pps) and bits-per-second (bps) rates per individual source, relatively low number of sources (not unheard-of, just not the norm)
 - Preannounced attack windows at first, until the defenders were consistently & successfully mitigating the attacks (went longer)
 - Attack volumes were overkill – the targeted sites would've been knocked offline by a tiny fraction of the pps/bps utilized in these attacks, as they were so brittle, fragile, non-scalable, and unprepared. Overkill is quite common in DDoS attacks, but this was an extreme example.

Evidence of Some Sophistication

- Reconnaissance
 - Attackers probing banks and then customizing attacks to the target
- Targeting multiple customer servers
 - HTTP, HTTP/S, authentication subsystems, CGIs, etc.
 - Repeated download of previously-identified large binary files via HTTP/S (.pdf files, .jpgs, et. al.)
 - Repeated GETs/POSTs against non-existent URIs
- Multiple concurrent targets = more stress on upstream mitigation
- Increasing turnover of bots used in attacks
- More frequent/earlier attacks against ISP authoritative DNS servers (not the authoritative DNS servers of the targeted organizations) in earlier phases; attacks against authoritative DNS servers of targeted organizations began in Phase 4
- Began attacking ISP/MSSP network infrastructure directly in Phase 3 – network infrastructure BCPs a must!

Different MO from Most Other DDoS Attacks

Typical DDoS Attacks

- Generally hit-and-run tactics
- Little to no warning
- Attacks peter out as money/interest/attention span runs out
- Use available attack tools

‘Operation Ababil’ Financial Attack Campaign

- Sustained attacks over a long period of time
- Telegraph every move via Pastebin during initial phases
- Substantial & sustained funding
- Continuously evolving attack tools/methods

ISP/MSSP Lessons Learned

- As is quite common, **these DDoS attacks succeeded initially mainly due to the unpreparedness** of the defenders.
- Some ISPs/MSSPs exhibited organizational rigidity; excessive bureaucracy, lack of operational agility; lack of detailed understanding of targeted end-systems characteristics in order to perform optimal countermeasure selection; lack of cross-functional collaboration; **all these inhibited initial defense efforts.**
- Some ISPs/MSSPs exhibited an **incomplete understanding of all available mitigation options**, including full spectrum of countermeasures. Lack of S/RTBH deployment also inhibited initial defense efforts for some ISPs/MSSPs.
- **Capacity models should be re-evaluated** as larger multi-vector, multi-end-customer attacks are more common— initially, a significant proportion of total mitigation capacity lay fallow for some ISPs/MSSPs during these attacks, nor was it dynamically deployed as the attack campaign continued.

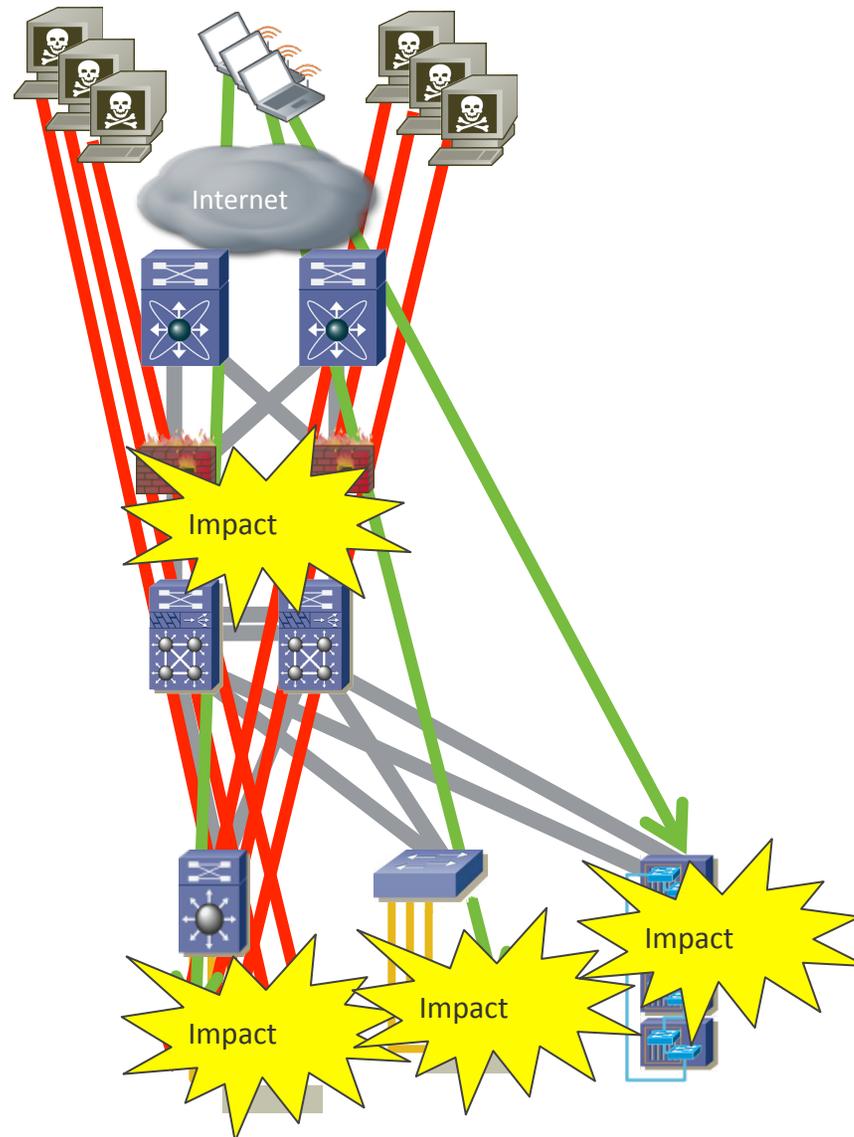
ISP/MSSP Lessons Learned (cont.)

- Some ISPs/MSSPs should work to **increase speed of new technology adoption**, broaden/deepen mitigation education & training, increase inter- and intra-organizational cooperation, fully leverage existing investments in mitigation capabilities
- Some ISPs/MSSPs should work to **customize mitigation tool/countermeasure selection & configuration** based upon specifics of end-customer systems under protection, in response to changing attack methodologies.
- Operationalize and practice with all mitigation tools/countermeasures ahead of time, **be aware of all mitigation options** and utilize as appropriate.
- Exhibit creative thinking during attacks, quickly effectively leverage mitigation vendor recommendations and advice, **remove bureaucratic barriers** to operational agility.
- **Implement anycast diversion** to divert attack traffic into multiple mitigation centers simultaneously, if this hasn't already been accomplished.

Enterprise Lessons Learned

- Firewalls/IPS/Load-balancers **don't offer any protection against DDoS attacks**
 - All targeted organizations have these devices, they are part of the problem!
- ISP/MSSP coverage constraints
 - Resource strain (human, technical) when multiple customers attacked simultaneously
 - Can be slow to upgrade to the latest releases/protections
 - **Need to have detailed knowledge of end-customer systems** under protection
- Enterprises need **DDoS mitigation capabilities both upstream and on-premise**
 - On-premise for direct control and rapid response
 - In-cloud for scale and broad topological coverage of end-customer edge, as well as ISP/MSSP public-facing properties (DNS, etc.)

Targeted Organizations All Had FW/'IPS'/WAF/LB



Enterprise Lessons Learned (cont)

- Attackers were **changing their tactics in real time** as they noticed ISPs/MSSPs effectively mitigating the attacks
- Particular focus on taking down **poorly-written, non-scalable, brittle, fragile banking applications**, mainly utilizing brute-force layer-4/-7 attacks against SSL login subsystems
- Exhaustion of login subsystem resources appeared to cause database and middleware failures – session state appeared to overwhelm middle tier, leading to **apparent middle-/back-tier failures leading to database corruption**, etc.
- We observed this phenomenon in at least two of the attacks against separate banks, during which the **MSSP was highly effective at mitigating the DDoS attack traffic**, but the **banking site still went down due to apparent disruption and corruption** of underlying application/data per the above scenario
- Appropriate network access policy enforcement via stateless ACLs a must – **why allow UDP/53 to Web servers?!**

Enterprise Lessons Learned (cont)

- Very obvious that only a few of the targeted organizations had given much thought/invested many resources in DDoS defense, had rarely (if ever) rehearsed DDoS defense, had **little or no focus on maintaining availability in the face of attack**, had little clue as to how effectively collaborate with ISPs/MSSPs
- This is a gigantic problem across all industry verticals – most **enterprises are simply unaware of/unconcerned with availability**, focus all their ‘security’ resources on mandated compliance measures, none of which include an availability component
- DDoS is essentially a man-made disaster affecting business continuity – why is **DDoS defense not included in disaster preparedness/business continuity planning** efforts, resourcing?
- Why is there **no PCI/DSS availability component**?!

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

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/speccking/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!**

Are We Doomed?

- No! Deploying the existing, **well-known tools/techniques/BCPs** results in a vastly improved security posture with measurable results.
- The evolution of this attack campaign clearly demonstrates that **positive change is possible** – targeted organizations & defending ISPs/MSSPs altered architectures, mitigation techniques, processes, and procedures in order to successfully mitigate these attacks.
- ISPs/MSSPs & enterprises defending against these attacks have learned optimizing for specific attack vectors/methodologies isn't a viable strategy – rather, **optimizing for the servers/applications/services being protected** is the way to go.
- It's important to keep in mind that **IPv6 has all the same issues as IPv4, plus new ones all its own** – and all in hexadecimal! Feature parity, architectural parity, & operational parity are a must!
- Automation is a Good Thing, but it's no substitute for resilient architecture, insightful planning, and plain old elbow-grease – **top-notch opsec personnel** are more important now than ever before!

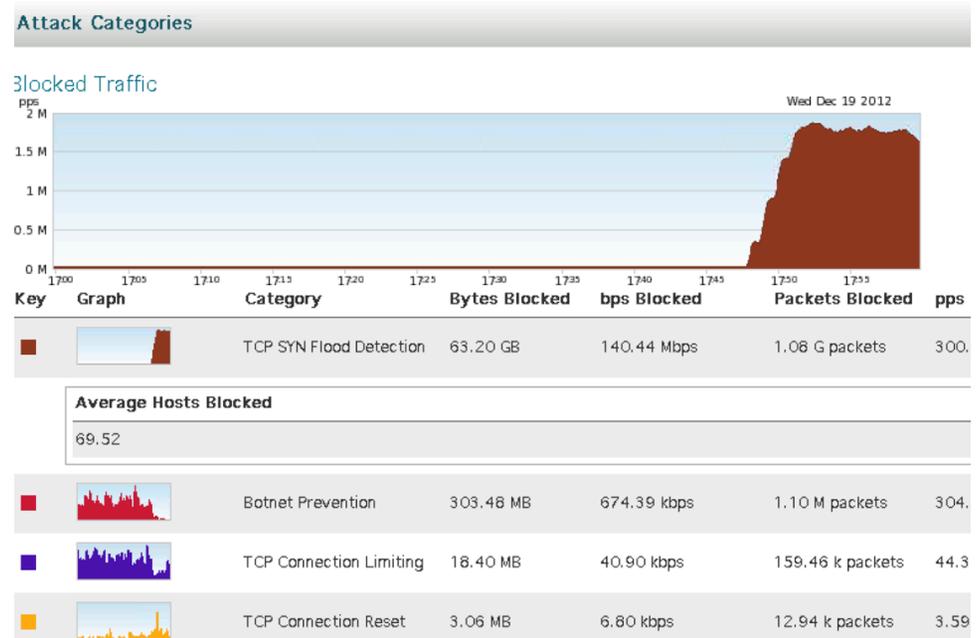
Successful 'Operation Ababil' Attack Mitigation - Coordinated In-Cloud (ISP/MSSP) & On-Premise (End-Customer) Defense

In-cloud mitigation
IDMS



~67Gbps of attack traffic mitigated in upstream ISP/MSSP mitigation center

On-Premise mitigation
IDMS



~2mpps of attack traffic mitigated on-premise by enterprise

References

This presentation:

<http://bit.ly/16DiOuO> - <https://www.box.com/s/ko8lk4vlh1835p36na3u>

Presentations on related topics:

<https://www.box.com/s/4h2l6f4m8is6jnwk28cg>

2009/2010/2011 Arbor Worldwide Infrastructure Security Reports:

<https://www.box.com/s/llwlaowbthppliye2uw>

2012 Arbor Worldwide Infrastructure Security Report:

<http://www.arbornetworks.com/research/infrastructure-security-report>

RFC5635 - S/RTBH

<http://tools.ietf.org/html/rfc5635>

Q&A

This Presentation – <http://bit.ly/16DiOuO>





Thank You!

*Special thanks to Gary Sockrider & Darren Anstee
of Arbor Networks for their contributions to this
presentation.*

ARBOR SERT
Security Engineering & Response Team

ARBOR[®]
NETWORKS



Roland Dobbins <rdobbins@arbor.net>

Senior ASERT Analyst

+66-83-266-6344 BKK mobile

+65-8396-3230 SIN mobile

Arbor Public