ARBOR NETWORKS

The Security Division of NETSCOUT

IoT DDoS Attacks Show The Stakes Have Changed

FEATURING RESEARCH FROM FORRESTER

Quick Take: Poor Planning, Not An IoT Botnet, Disrupted The Internet

IOT DDoS ATTACKS SHOW THE STAKES HAVE CHANGED

Internet-of-Thing (IoT) botnets are not a new phenomenon. Arbor Networks routinely sees IoT botnets comprised of webcams, DVRs, and set-top boxes used to launch DDoS attacks.

In fact, during a recent international event, Arbor Networks, along with our customers, helped mitigate a sustained, sophisticated 540Gbps attack launched by an IoT botnet. This attack started a month before the event and escalated once it began. And nobody noticed.

The reason is clear to us. The defenders knew they'd have their work cut out for them, and prepared accordingly. The key to DDoS protection is *preparation*. The more one knows about the Tactics, Techniques and Procedures (TTPs) of their attackers, the more prepared one is to defend themselves when attacked. To assist organizations in their preparation, Arbor's Security Engineering and Response Team (ASERT) has posted a detailed analysis of the now infamous Mirai botnet including attack vectors and best practices in attack mitigation on their ASERT BLOG. The following is a summary of that Mirai botnet analysis and introduction to Arbor Networks DDoS Protection Solutions.

TACTICS, TECHNIQUES AND PROCEDURES (TTPS)

The original Mirai botnet consists of a floating population of approximately 500,000 compromised IoT devices. Worldwide; relatively high concentrations of Mirai nodes have been observed in China, Hong Kong, Vietnam, Taiwan, South Korea, Thailand, Indonesia, Brazil and Spain.

Devices are subsumed into Mirai by continuous, automated scanning for and exploitation of well-known, hardcoded administrative credentials present in the IoT devices. These vulnerable embedded systems are typically listening for inbound telnet access on TCP/23 and TCP/2323.

Mirai is capable of launching multiple types of DDoS attacks, including SYN-flooding, UDP flooding, Valve Source Engine (VSE) query-flooding, GRE-flooding, ACK-flooding, pseudo-random DNS label-prepending attacks (also known as DNS 'Water Torture' attacks), HTTP GET attacks, HTTP POST attacks, and HTTP HEAD attacks.

MITIGATION TECHNIQUES

The DDoS attack capabilities of Mirai are well-known and can be successfully mitigated by implementing Best Current Practices (BCPs) and by utilizing intelligent DDoS mitigation systems such as Arbor SP/TMS, Arbor APS and/or Arbor Cloud DDoS Protection Services.

IN THIS DOCUMENT

1 IoT DDoS Attacks Show The Stakes Have Changed

5 Research From Forrester: Quick Take: Poor Planning, Not An IoT Botnet, Disrupted The Internet

12 About Arbor Networks

It is possible (and recommended) for network operators to identify likely compromised IoT devices by detecting and classifying outbound/cross bound TCP/23 and/or TCP/2323 activity originating from these devices, and then take steps to isolate those devices, notify their legitimate owners of the problem, and urge them to take corrective action. In order to inhibit scanning for IoT devices, broadband access network operators should implement access-control lists (ACLs) at a situationally-appropriate point in the network topology to prohibit high-port TCP traffic destined for TCP/23 and TCP/2323 on their customer access networks.

All relevant network infrastructure, host/application/service, and DNS Best Current Practices (BCPs) should be implemented by network operators with public-facing network infrastructure and/or internet properties.

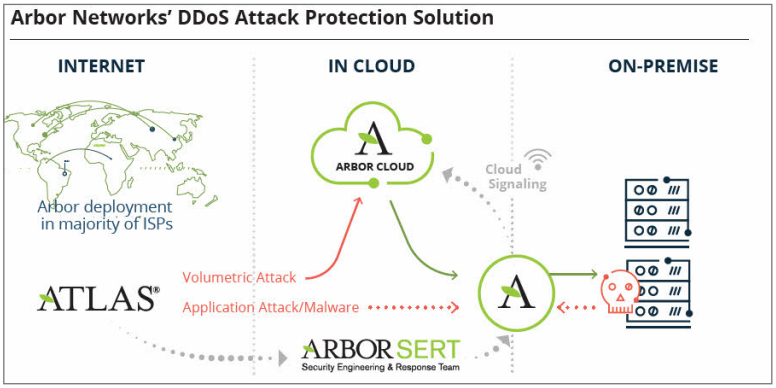
Network operators should export flow telemetry (e.g., NetFlow, IPFIX, et. al.) from their peering/transit/customer aggregation edges and internet data center (IDC) distribution edges to anomaly-detection/traffic visibility systems (such as Arbor SP) which provide the ability to detect, classify and trace back DDoS attack traffic.

Network operators should make use of DDoS mitigation mechanisms such as source-based remotely-triggered blackholes (S/RTBH), flowspec, and/or intelligent DDoS mitigation systems in order to mitigate DDoS traffic sourced from Mirai-based botnets.

INTRODUCTION TO ARBOR'S DDoS ATTACK PROTECTION PRODUCT AND SERVICES:

Due to the multi-vector nature of the Mirai IoT botnet attacks (and others), for comprehensive protection, we recommend a layered approach to DDoS attack detection and mitigation.

For global networks, Arbor SP combines network-wide anomaly detection and traffic engineering with Arbor TMS' carrier-class threat management, automatically detecting and surgically removing only the attack traffic. Customer-facing services remain available while providers actively mitigate attacks.



Arbor Cloud provides fully managed, multi-layer protection from volumetric and application-layer attacks. A powerful feature called Cloud Signaling intelligently links the on-premise mitigation device (Arbor APS) to an upstream/in-cloud DDoS attack protection service (such as Arbor Cloud or an ISP running Arbor TMS) for mitigation. Cloud Signaling significantly reduces the time to mitigate attacks ensuring protection even if your bandwidth becomes fully consumed. Via layered protection, Arbor delivers a comprehensive, industry-leading DDoS protection solution for enterprise networks.

Global Visibility and Threat Intelligence: Arbor Networks Security Engineering and Response Team (ASERT) leverages a 16 year, worldwide deployment of Arbor products and third-party intelligence—otherwise known as ATLAS—to gain unmatched visibility into global threat activity. The global insight derived from ATLAS/ASERT continuously arm all products and services in the form of features, integrated workflows and ATLAS Intelligence Feed (AIF).

For more information regarding Arbor Networks' industry leading DDoS attack protection solutions visit www.arbornetworks.com or contact a local Arbor representative.

FORRESTER®

Quick Take: Poor Planning, Not An IoT Botnet, Disrupted The Internet

Dyn Outage Underscores The Need To Plan For Failure

by Jeff Pollard, Joseph Blankenship, and Andras Cser
with John Kindervag, Stephanie Balaouras, Laura Koetzle, Bill Barringham, and Peggy Dostie
October 24, 2016

Why Read This Quick Take

On October 21, internet users went through a real exercise in one way the internet could die. Critical infrastructure exists on the internet as well as in the real world, and this attack crippled one component of that by targeting the domain name system (DNS). Service provider Dyn came under a massive DDoS attack that left the world unable to connect to popular websites such as Twitter, Reddit, and Spotify, despite the fact that those sites were, in fact, functional. It's a shocking demonstration of the fragility of — and our dependence on — a completely connected world.

Dyn Represented A Massive Single Point Of Failure

At 7:10 a.m. EDT on Friday, October 21, Dyn began monitoring a DDoS attack against its US East Coast infrastructure. Soon after, the world would learn how many sites used Dyn — and solely Dyn — for DNS services. For 2 hours, much of the internet remained inaccessible. By 9:20 a.m. EDT, Dyn resolved the initial attack.[1] At 11:52 a.m. EDT, a series of secondary attacks took place, ending around 6:17 p.m. EDT. In the span of an 11-hour period, the fragility of ubiquitous connectivity was on display. Many of the businesses affected by the attack were unable to recover because they had introduced a single point of failure in their services by relying on a single primary authoritative DNS provider, lacking a secondary authoritative DNS provider.[2] As a result of the attack:

- **Major digital brands suffered disruptions.** Internet-dependent businesses like Etsy, PayPal, and Spotify, among others, experienced major disruptions. Enterprise email was down (Microsoft), software development paused (GitHub), numerous line of business apps were unavailable (Okta), advertising revenue wasn't generated (Reddit/Twitter), and in a twist of irony, outage monitoring services went down, too (PagerDuty).

› **The internet of things (IoT) emerged as a massive attack tool.** It turns out that it's more fun to use your camera to shut down a site than it is to use your camera to watch you. Expect that IoT will make it much easier for hackers to perpetrate DDoS attacks because of the large number of IoT devices plus the relatively primitive OSes on those IoT devices.[3]

The Company Behind The Company Can Impact Your Company

The downstream impact from the attack was felt by companies and their customers, in many cases, without them understanding why they were down. Many hurt by this were sophisticated technology organizations. They started, grew, and emerged as known brands in digital business. They've written posts and have been interviewed about scaling an organization with 10 million users.[4] Despite that sophistication, they disrupted business with poor vendor management and management of third-party risk by — whether directly or indirectly — entrusting their uptime to a single point of failure. It is apparent that:

› **We haven't fully mapped the underlying complexity of digital business.** The DNS is one of the oldest and least tested services of the internet infrastructure — we all just assume it works. Most often it indeed does, but when it does not, it has catastrophic consequences: downtimes, data loss, etc. Digital business depends on DNS, and unfortunately, few firms have conducted a business impact analysis and risk assessment to understand the complex interdependencies the organization has on DNS as well as the business, financial, and operational impacts of an outage.

› **Digital attacks cause damage in the real world.** This attack illustrates that there is no divide between the digital and physical domains.[5] The source of the attack was a set of physical devices infected with malware that led to an outage felt in the digital and physical domains. IoT devices overwhelmed a service provider's physical and electronic infrastructure. Fallout led to disruptions in electronic communication (email and pager), online discussion forums, social networks, human labor (software development), and eCommerce.

› **Cyberwarfare isn't just the domain of nation-states.** The scale, scope, and impact of this attack prove that creating chaos in the 21st century is simply a matter of ideology, not patriotism, politics, or national borders. Companies must build toward resiliency as the barrier to entry for disruption and degradation of digital activity lowers.

› **The very fabric of the internet is under attack.** Our very interconnectedness may be our undoing. Attacks like this one that exploit a weakness in the fragile ecosystem demonstrate how vulnerable it is. In this scenario, a single attack managed to disrupt a site with 82 billion page views in 2015 without directly sending a packet there.[6] Now that DDoS is part of popular vernacular, it's time we addressed the inherent flaws when a decentralized web becomes increasingly centralized. As complex as the internet is, turning to providers that enable digital business is an easy choice — but not always the right one for the organization. CISOs should remind their organizations that closed platforms and service providers present risks for the business, too.

The Intersection Of IoT And DDoS Highlights New Complexities

IoT makers, users, and operators are now participating in and defending against record-setting DDoS attacks, and as Friday, October 21 showed — placing the integrity of the internet at risk. A Chinese manufacturer, Hangzhou Xiongmai Technology, disclosed that it manufactured many of the devices, mostly DVRs and cameras, that were used in Friday's DDoS attack.[7] The malware used in the attack, Mirai, exploited vulnerabilities and weak default passwords in those devices. While newer versions of the firm's devices have been patched, versions prior to September 2015 use older firmware and are still vulnerable. To avoid further — or a cataclysmic outage — there will need to be a number of changes across the 21st century business technology ecosystem from manufacturers to carriers to cloud providers:

- **IoT makers need to insert some basic security requirements into devices.** No IoT device should be able to communicate on the internet without forcing the end user to change the default password. Default passwords should be randomized based on a few factors such as date of manufacture, serial number, and distributor. Devices should also come with a strict egress filtering policy that limits where they can communicate. For example unless the user updates the configuration by default the device should only be able to communicate back to sites owned by the manufacturer. Firmware updates should be signed with a digital certificate.
- **IoT operators in enterprises need to maintain visibility and segmentation.** Enterprise networks should rely on a Zero Trust architecture.[8] That requires segmentation and access control lists. In this case IoT devices should reside on a network segment designated for their use case in the business. Egress filtering policies to limit external communication will prevent them from participating in attacks like the recent DDoS, but also will ensure the enterprise knows exactly where they go, what they share when they go there, and how often it happens.
- **IoT users need to understand their responsibility for their devices.** Security and risk leaders must make sure that acceptable use, bring your own device, and other security and employee policies reflect the reality of IoT device widespread use. End user security awareness training should contain curriculum that explains what is acceptable IoT use and data collection in an enterprise environment — but — should also contain information that educates employees on their role in using IoT devices as a consumer. That includes changing default policies and updating firmware and software when it's available.[9] Managing identities of IoT devices (how and when they can connect to what network, which users are allowed to access them and when) is a critical piece of the IoT security puzzle.
- **Carriers must ante up their DDoS defenses, not just monetize it.** Forced consumer bandwidth caps combined with enterprise sales of DDoS mitigation means these attacks create a conflict of interest for telecoms. Consumers unknowingly participating in a DDoS attack could exceed their caps generating revenue, while the enterprise under attack is forced to pay for DDoS protection from a provider. The anti-consumer opposition to net neutrality from telecoms hinged on network

saturation due to streaming media. As more and more internet consumption occurred it placed backbones at risk. If traffic shaping and bandwidth profiling can reduce the scourge of binge watching streaming series and cat videos the same technical application could apply to DDoS traffic from IoT devices. Carriers want to be part of the data and software economies which requires them to ante up on its defense beyond monetizing DDoS.[10]

Recommendations

Plan For Failure: Make Your DNS Configuration As Secure As Possible

One lesson that we learn over and over is that bad things happen on the internet. The lesson that follows is that any large scale solution is inherently complex and unlikely to happen. That means that CISOs must help themselves and their companies. Here's how:

- **Get a secondary DNS provider and add it to your registrar's list of nameservers.** Automate replication from the primary to the secondary.[11] If a site relied on Dyn and another DNS provider their users don't know it. If a site only relied on Dyn then their users and customers do. If a large portion of your revenue hinges on connectivity then having a single DNS provider creates a massive single point of failure and erases every other redundant architectural decision made.
- **Ask all your DNS providers how they protect themselves from DDoS attacks.** This attack showed the fragility of DNS which is notoriously difficult to secure. After all DNS services are supposed to accept traffic as the "address book" of the internet. DNS providers must provide plans for withstanding various types of DDoS such as direct, reflection NTP, UDP, or API based attacks. Ask for specific thresholds they could withstand along with geographic, service specific, or data center based limits. Determine how often their DDoS and other protections are tested and how they're tested. Use the lessons from business continuity and disaster recovery to understand if a provider's approach is mature. Find out how your DNS provider conducts and responds to findings of penetration testing.
- **If your vendors share an as-a-service single point of failure, so does your business.** Various SaaS, IaaS, PaaS, and IDaaS companies all remained unavailable for hours to their customers despite functioning themselves. If the business and vendors depend on a single DNS provider require that vendors have more than one, and consider vendors using a different set of providers than those used in your business. With cloud if the business and vendors rely on a single cloud provider (e.g., AWS), then consider alternatives with a presence in others (e.g., Google Cloud or Microsoft Azure). By exploring business and vendor overlap with shared infrastructure CISOs can avoid single service points of failure. Ensure that service-level agreements (SLAs) have measurable and enforceable clauses for DNS outages.

› **Re-examine your BCDR procedures with DNS in mind.** Your business continuity and disaster recovery (BCDR) plans, processes and exercises should include primary and secondary DNS switchovers (see above) and responding to service outages caused by cloud platform provider DNS issues. Forrester's clients in some cases have manually defined emergency /etc/hosts file entries (with the appropriate file integrity monitoring) to at least be able to maintain BCDR operations in case of a DNS meltdown.

Endnotes

[1] Source: "DDoS Attack Against Dyn Managed DNS," Dyn, (http://www.dynstatus.com/incidents/nlr4yrr162t8).

[2] Put simply, there are two types of DNS servers, authoritative and recursive. When you try to access a site like Reddit or Spotify, your browser will first ask a recursive DNS server where to find the site. If the recursive DNS server has that information itself, it provides that to your browser. If the recursive DNS server lacks that information, it queries the authoritative DNS server for that site. Dyn suffered an attack on its authoritative DNS services, and these were unable to respond. Source: Chris Frost, "What Is the Difference between Authoritative and Recursive DNS Nameservers?" OpenDNS Blog, July 16, 2014 (http://blog.opendns.com/2014/07/16/difference-authoritative-recursive-dns-nameservers/).

[3] Source: "Mirai Botnet Linked to Dyn DNS DDoS Attacks," Flashpoint, October 21, 2016 (http://www.flashpoint-intel.com/mirai-botnet-linked-dyn-dns-ddos-attacks/).

[4] Source: Derrick Harris, "GitHub: Scaling on Ruby, with a nomadic tech team," Scale, August 27, 2016 (http://medium.com/s-c-a-l-e/github-scaling-on-ruby-with-a-nomadic-tech-team-4db562b96dcd#.zdzuqojhb).

[5] The internet of things (IoT) has evolved beyond a hyped buzzword into commercially available technologies that can significantly improve customer outcomes and deliver business benefits. However, the interlinked set of hardware, software, and ubiquitous connectivity of the IoT ecosystem creates new security challenges and exacerbates legacy security problems. For a summary of the current IoT attack surface, see the "The IoT Attack Surface Transcends The Digital-Physical Divide" Forrester report.

[6] Source: "Reddit in 2015," Upvoted, December 31, 2015 (http://redditblog.com/2015/12/31/reddit-in-2015/).

[7] Source: Michael Kan, "Chinese firm admits its hacked products were behind Friday's DDOS attack," Computerworld, October 23, 2016 (http://www.computerworld.com/article/3134097/security/chinese-firm-admits-its-hacked-products-were-behind-fridays-ddos-attack.html).

[8] There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For today's digital business, this perimeter-based security model is ineffective against malicious insiders and targeted attacks. For an overview of Zero Trust, see the "No More Chewy Centers: The Zero Trust Model Of Information Security" Forrester report.

Zero Trust gives you unprecedented visibility into your digital business, from network packets to applications. Visibility, detection, and prevention work in tandem with one another to secure your firm's most sensitive and valuable data assets. To see how Zero Trust can empower your business, see the "The Eight Business And Security Benefits Of Zero Trust" Forrester report.

[9] The internet of things (IoT) presents huge opportunities for today's digital businesses to use connected objects, sensors, and devices for engaging with customers in new ways and streamlining business operations. However, with its promise also come security concerns. In the coming months and years, identity and access management (IAM) for IoT will become an important security pillar. For a current overview of the current IAM solutions for IoT, see the "Vendor Landscape: Identity And Access Management Solutions For The Internet Of Things" Forrester report.

[10] You can't afford to have your site go down during peak seasons. Unplanned downtime, performance issues, credit card fraud, and DDoS attacks during these critical periods can cost enterprises millions. To avoid the worst, and prepare for attacks before your peak season, see the "Seven Steps To Protect Your eCommerce Website In 2016" Forrester report.

[11] Source: Alex Levin, "How We Survived the Dyn DNS Outage," Sumologic, October 21, 2016 (https://www.sumologic.com/blog-devops/survived-dyn-dns-outage/).

Client support

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

The Security Division of NETSCOUT

Arbor Networks, the security division of NETSCOUT, helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor Networks Spectrum™ advanced threat solution delivers complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of attack campaigns, malware and malicious insiders. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context so customers can solve problems faster and reduce the risks to their business. To learn more about Arbor products and services, please visit our website at arbornetworks.com or follow on Twitter @ArborNetworks. Arbor's research, analysis and insight is shared via the ASERT blog. For a global data visualization of DDoS attacks that leverages our ATLAS intelligence, visit the Digital Attack Map, a collaboration with Jigsaw, an incubator within Alphabet, Google's parent company (NASDAQ: GOOGL).