Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Defend Network and Customers Against IoT-Based DDoS Attacks

By: Stephanie Weagle

Experts have long warned that the inherent lack of security in many of the devices that make up the Internet of Things (IoT) would come back to haunt us. The DDoS events of the past year have brought this concern into sharp focus, by demonstrating just how damaging an IoT-powered botnet can be.

It's no secret that many IoT devices are poorly architected from a security perspective. Many have little or no security in place with simple default passwords making it easy for attackers to take control of them for malicious purposes. This makes them sitting ducks, just waiting to be compromised and enslaved into a botnet for use in DDoS events. In addition, attackers are becoming more creative and using new techniques to wreak havoc with IoT botnets.

While 2016 marked a turning point for DDoS, as attacks reached new heights in terms of both size and complexity. Mirai showed us just how powerful an IoT-powered botnet can really be with the unprecedented attack against DNS provider Dyn just over a year ago. Overnight, the security considerations around connected devices went from being something that security consultants have long warned about into a hot button issue that needs to be addressed.

Internet-based home automation devices, such as video baby monitors, remote thermostat programming, home surveillance and security kits, connected lighting products, etc., are transforming how we manage our day-to-day lives. Remote management of these devices, through smartphones, online portals and-the-like has extended to every home, car, business, building and system in the world – and I'm certain this is only the tip of the iceberg.

Despite its advantages, IoT comes with a host of security disadvantages. IoT devices are often poorly managed, patched and secured, which makes them prime targets for hacker infiltration and takeover. Aside from the personal privacy and security concerns that result from these security gaps, the bigger danger is that these connected devices can be harnessed by hackers for a variety of nefarious purposes; DDoS attacks are prominent amongst them.

These increased threats will mean that defending against DDoS attacks will become a top security priority for any organization that relies on the internet to conduct business. So how can organizations defend against such attacks? In preparing a robust defense against botnets like Mirai it's important to consider how they work. Effectively acting like a giant cloud computer, botnet-driven attacks are launched and then disappear without leaving enough information for victims to trace its origins. This leaves organizations really no choice but to defend themselves at the edges of the network. Legacy out-of-band scrubbing solutions, which require human intervention and reactive countermeasures to block the attack, will not be successful, and using traditional security infrastructure (firewalls, IPS, etc.) will also allow hackers to experiment on your networks undetected, finding vulnerabilities and testing new methods through smaller, hidden attacks.

The reality is that any device, infrastructure, application, etc. that is connected to the internet is at risk for attack, or even more concerning, to be recruited as a bot in an army to be used in DDoS attacks against unsuspecting victims. Botnets, also known as "zombie armies," can be deployed on thousands — if not millions — of connected devices and can wreak havoc - spam attacks, spread malware, or launch DDoS attacks.

There is really no limit to the potential size and scale of future botnet-driven DDoS attacks, particularly when they harness the full range of smart devices incorporated into our IoT. By using amplification techniques on the millions of very high bandwidth capable devices currently accessible, DDoS attacks are set to become even more colossal in scale.

The bottom line is that attacks of this size can take virtually any company offline – a reality that all businesses must be prepared to defend against. The impact of a successful DDoS is far ranging: revenue loss, customer dissatisfaction, and brand damage to name a few. Businesses that rely on internet availability to conduct business or deliver services to their customers cannot deal with DDoS in a reactive manner.

Furthermore, DDoS goes beyond the giant attacks that make the headlines every few months. Before botnets are mobilized, hackers need to make sure that their techniques are going to work. This is usually done using short duration, low volume attacks, which most IT teams wouldn't even recognize as a DDoS attack. Due to their size – the majority are less than five minutes in duration and under 10 Gbps – these shorter attacks typically evade mitigation measures by most legacy and homegrown DDoS mitigation tools, which are generally configured with detection thresholds that ignore this level of activity.

This allows hackers to perfect their attack techniques, while remaining under the radar, leaving security teams blindsided by subsequent attacks. If these techniques are then deployed at full scale with a botnet, the results can be devastating.

Organizations must be better equipped to deal with the inevitable DDoS attack – IoT related, or otherwise. In the early days of DDoS attacks, more than two decades ago, operators handled an attack with a null route; i.e., a remote trigger blackhole. If they detected something going awry, they would look at the victim – the IP that was targeted – and null route everything associated with the victim. This got the attack traffic off the operator's network and stopped the collateral damage against other unintended victims. However, it sacrificed the victim in the interest of keeping the rest of the network viable.

The DDoS mitigation landscape then evolved to a slightly more advanced technique, which involves routing the attack traffic to a scrubbing center where human intervention and analysis is typically required to remove the attack traffic and return the legitimate traffic to its intended target. This process is resource-intensive and expensive. Plus, there's often a lengthy delay between detection of the attack, and when the actual remediation efforts begin.

To keep up with the growing sophistication and organization of well-equipped and well-funded threat actors, it's essential that organizations maintain comprehensive visibility across their networks to instantly and automatically detect and block any potential DDoS incursions as they arise.

Proactive DDoS protection is a critical element in proper cyber security protection against loss of service and data breach activity. This level of protection cannot be achieved with traditional internet gateway security solutions.

The DDoS protection of today requires robust, modern DDoS defenses that will provide both instantaneous visibility into DDoS events, real-time mitigation as well as long-term trend analysis to identify adaptations in the DDoS landscape to deliver proactive detection and mitigation techniques. Automatic DDoS mitigation is available today to eradicate the damage of DDoS and eliminate both the service availability and security impact. The only proper defense is to use an automatic, always-on DDoS mitigation, which can monitor all traffic in real-time, negate the flood of attack traffic at the internet edge, eliminate service outages and allow security personnel to focus on uncovering any subsequent malicious activity, such as data breaches. This type of automatic, always-on protection can come in various forms – either on-premises, or purchased as a security service from an upstream provider. It is only through deploying these real-time solutions that organizations will be able to identify and mitigate the most serious botnet-driven DDoS attacks on their networks in the years ahead.

This type of effective DDoS defense can also be deployed as a premium DDoS Protection as-a-Service (DDPaaS) offering from an upstream internet provider. Carriers are in a unique position to effectively eliminate the impact of DDoS attacks against their customers by surgically removing the attack traffic transiting their networks before flowing downstream. Providing such a service not only streamlines the operations of providers, giving them increased visibility and making their services more reliable, but also drastically reduces the impact of IoT driven DDoS attacks.

Preventing and mitigating the exploitation of the IoT is going to take quite a concerted effort. Device manufacturers, firmware and software developers need to build strong security into the devices. Installers and administrators need to change default passwords and update patch systems – if this is even possible – when vulnerabilities do arise.

The home user must also be educated on best practices in securing their devices against vulnerabilities. The average user of connected devices, whether that be your smart home, smart appliances, smart car or smart office, does not typically pay close attention to software updates or critical patching schedules. They also don't quite understand how these devices are connected or sharing data. IoT devices often have just enough processing power to deliver their required functionality, with security an after-thought at best or often not present at all. Combine this with the fact that access control passwords are often left at their factory defaults, or users choose alternatives which are easy to crack using brute force techniques. The human component is often underestimated as a contributor to an overall lack of security of the IoT.