defense.net

DDoS 2015: Understanding the Current and Pending DDoS Threat Landscape

Whitepaper

By Barrett Lyon
Founder & CTO

DDoS 2015: Understanding the Current and Pending DDoS Threat Landscape

By Barrett Lyon, CTO Defense.net

Executive Summary

The Internet continues to grow exponentially in both number of users and bandwidth capacity to those users. There is also a new type of 'user' on the Internet – the 'smart device'. These devices typically have simple interfaces with no method to look under the hood to see how they're operating or if they have been hacked or exploited.

Smart devices need the Internet to function completely, thus simple tasks like adjusting your home AC unit, monitoring the functionality of your car, tracking your health records, or just changing the temperature on your refrigerator – now depend on the Internet to function completely. Along with the move to smart devices, daily services are relying on connectivity as well. Banking, paying taxes, voting, stock trading, currency trading, calendar coordination, communication, booking travel, almost everything related to business, entertainment, news, and more have become nearly impossible without an Internet connection.

At the same time as our dependence is growing, we're seeing governments fund the creation of smarter cyber weaponry, which will greatly expand the attacking capability of bots. Today's 'in the wild' bot attacking capabilities are still very primitive and feeble. They are not going for the most exact attack possible, however, with the creation of better weapons comes a trickle-down effect which will slowly get these new attacking methods into the hands of script kiddies and incorporated into new bots.

Thus, as crazy as this may sound, we may see a point in the future where your refrigerator's smart OS is hacked and converted to a high-powered botnet used to attack the hosted services that your car depends on for its navigation and music systems. We may see our 'smart' thermostats stop functioning as their CPUs are put to use to attack banking infrastructure, which could cripple a small country's economy. The 'Internet of Things' will be increasingly involved in these attacks as PCs become less interesting to attackers. We will see DDoS attacks grow in size, compute capacity, targets, and intensity – causing major disruptions to Internet access in our modern online-dependent lives.

The Evolution of the Internet: Examining Key Trends

The Internet has evolved significantly since its inception, from a basic network for higher education and research, to a key component (or even

foundation) of society and the economy. It has become our banking center, it's our financial trading interface, our communications system, our primary form of research, our entertainment feed, and our modern day postcard. However, the Internet has been built on a protocol that was designed to scale – but not designed to simultaneously scale AND be secure.

There are several emerging trends that point to an Internet that is becoming much more vulnerable to DDoS attacks. The following sections will examine some of the most significant trends and technology drivers that will shape the future of the Internet over the next few years.

Trend #1. The Exponential Growth of New Users

Key findings from a recent cybercrime study by the UNODC[1] reveal that the diversity of international cybercrime laws, a lack of consensus on the role of evidence 'location', a low capacity for criminal justice, and insufficient cybercrime education and prevention are the main continued problems for combatting cybercrime. Nations with large groups of their populations getting plugged in for the first time will only make this problem worse. These new users don't necessarily have the education on what constitutes a crime on the Internet, and their countries' laws may not be in legally 'in sync' with the rest of the online world yet.

The largest influx of new Internet users is expected from the Middle East and Africa. These newly connected 'netizens' will be entering the Internet community without a background in global law and without the enculturation process that users would get in places like Europe or the United States. Thus, these newly connected user bases may create hot beds containing high numbers of cyber criminals interested in profiting and benefiting from the exploitation of what is now available to them. We saw this happen across Eastern Europe as it was initially plugged in, then Nigeria, and we are now watching it happen with China.

Trend #2. New Motivations: Hacktivism, Vigilantism, and State-Sponsored Attacks

We've seen entirely new motivations behind DDoS attacks over the last ten years. In the past, the main motive was focused around cyber criminals attempting to extort money out of online, time-sensitive businesses. These criminals were trying to shut down businesses at points and times that are very important to that business' operation and extract money out of them for protection. It's basically the old 'mobster protection racket', but attack motivations are now changing significantly.

We've seen 'hacktivism' increase in recent years, which is a group of people (or a single person) that decides to take down an entity of some sort, often for purely ideological or personal reasons. The United States banking infrastructure has been heavily attacked by hacktivists, and so has PayPal, and it's all because their business practices angered someone for some reason. This is a phenomenon that has increased over the last ten years, and we're going to see this continue to grow.

[1] http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Internet 'vigilantism' is a little different. This is when you see somebody taking the law into their own hands and deciding to make something happen. We've seen actual civil wars break out and the vigilantes end up attacking one side or the other, thinking that they are doing something for the greater good. This is not necessarily a separate phenomenon from hacktivism, but it's very focused, since people believe they are doing the right thing. They are not trying to silence a business, they are trying to promote a larger cause outside of the Internet.

Vigilantism also consists of state-sponsored attacks, where one country decides to attack another country through its Internet resources. This type of attack can have very powerful results, such as the 2007 cyber attacks against Estonia's banking system[2]. The country's Internet connections were severed, which crippled the Estonian banking system's ability to conduct wire transfers and clear banking transactions. That vigilante attack could have been a state-sponsored attack, or it could have been Russia creating a smokescreen around what they were actually trying to do. But it's hard to tell which makes this motive more elusive. These trends are very disturbing and dark, and we're going to see more of them over the next few years.

Trend #3. Military and Commercial Technologies Will Be Leveraged by Attackers

There is a long-standing history of military designs being demilitarized and passed down to society, including GPS, ARPANet, as well as the Internet itself. The same is true for weaponry. Although traditional weapons like Drones don't necessarily end up in the hands of everyone, some of the concepts and designs used in these military weapons do inevitably show up in civilian devices and applications.

Today's cyber weapons are pretty basic. With the exception of testing tools created by companies like Ixia, most botnet software is rather simplistic. In the past, a single person or a couple of people have created most attack weapons. These individuals were not necessarily the world's greatest programmers, and they were often working on these projects for their own interests.

Amazing works of software are typically not created by one or two people, but by advanced project management styles and huge teams. For example, it is rumored that 1,800 developers work on Apple IOS at any given moment. In contrast, Low Orbi Ion Cannon (LOIC) is an open source network stress testing tool that has been adopted to become a DDoS attack application. It was originally developed by a hacker – an 18-year-old developer by the name of Praetox in Oslo, Norway.

If an 18-year-old Norwegian can develop a tool that enables groups of people to launch attacks at targets like the Church of Scientology, the DoJ, and banks, imagine what a group of seasoned developers could create. If the commercial and military software development styles common in Silicon Valley are applied when building new cyber weapons

[2] http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/

going forward, the results may well be staggering. We will see new weaponry technologies that have an impact many orders of magnitude greater per-user than any weaponry in use or being developed today.

With newer attack vectors, the ability to mitigate such attacks will become much more difficult, processor-intensive, and bandwidth-intensive. We will also eventually see these new weapons and techniques dissimilate globally.

Trend #4. Open Source Tools Will Make Hacktivism Easier

Open source software tools are not only facilitating the development of many innovative and valuable enterprise applications, they are also making hactivism much easier. Current attack tools are very underpowered, however, we are now seeing a new trend in software development outside of state sponsorship.

LOIC was originally released as an open source testing tool. It was later adopted as a simple tool that Anonymous Hackers uses to push its agenda via hacktivist attacks towards different entities. Regardless of the tool's effectiveness, it's clear that it has been re-written and re-tooled several times over a small community of developers. Open source tools with a community behind them could end up becoming a hot bed of design and creation for new attack weapons, and at the same time, very difficult to remove from the Internet.

Trend #5. Mitigation against Complex Attacks

As mitigation devices become common components of the enterprise network, cyber weapons will also become focused on bypassing such hardware. There are more discussions every day about DDoS mitigation bypassing on Twitter, DDoS forums, and internal discussions behind closed walls.

Over time, it may not be who has the largest botnet, but who has the smartest and most advanced botnet instead. For example, we know that a lot of attack mitigation hardware uses a form of SYN cookies for its defenses. However SYN cookies don't work well in asymmetric mode. Thus, there are new forms of SYN mitigation in place that make poor assumptions about traffic flow, and they can in turn be used against the mitigation device to cause DDoS attacks purely based on the hardware's functionality. Eventually, these flaws will be discovered and exploited.

One recent and highly publicized example of this is a SYN reflection attack, where mitigation hardware responds to SYN packets with a SYN-ACK, regardless if the SYN was generated with a real computer or not. When the SYN-ACK is sent to the spoofed source IP address, it could be used by attackers to target another network, turning the DDoS mitigation device into a DDoS reflection device.

Trend #6. The Migration to IPv6 Will Not Fix the Problems

IPv6 is being touted as a more secure networking protocol to replace IPv4. This misnomer is caused by the fact that IPv6 supports IPsec; however, most IPv6 deployments do not employ IPsec. Trusting that encryption will solve all of the problems of IPv4 is not a good assumption.

Some security experts believe that security is not done at layer 3 (referring to the OSI model). Other networking experts (including the author) strongly disagree. But most do agree that scale, performance, and availability are core to security. If an application or service is not available, then the application is not secure. Security involves every layer of network, especially layer 3! Unfortunately layer 3 has been ignored in protocol design and will continue to be one of the many layers of DDoS, regardless of IPv4 or IPv6.

In fact, the IPv6 protocol uses new transport layer protocols which are the focus of most IPv4 attacks. Not only will we still have TCP and UDP, we will now get additional avenues for attack, like DDCP, SCTP, and RSVP. These new protocols will introduce entirely new angles of attack based on their implementations. Regardless of the DDoS attacks via new transport layer protocols, we also will see the same attacks to the application layer.

The largest issue with IPv6 is the fact that there are a lot more IP addresses that can be used to spoof attacks from. IP addresses on IPv4 are limited to a manageable range and memory on routers, load balancers, firewalls, and PCs. They can all deal with the address ranges of IPv4. But IPv6 maxes out all of our memory and makes it nearly impossible to defend against large ranges of spoofed attacks.

Trend #7. The Internet of Things: Will My Thermostat Attack My Bank?

According to ABI Research[3] , more than 30 billion devices will be wirelessly connected to the 'Internet of Things' by 2020. These are common household devices that we've been using most of our lives: Our TVs, stereo systems, cars, thermostats, sprinkler controllers, baby monitors, and many more. They are now becoming 'smart' with their own IP addresses and a plug-and-play interfaces. These devices with new Internet-connected interfaces pose a significant threat going forward.

With no or limited user interfaces on these devices, it makes them very difficult to diagnose and 'disinfect.' We have to implicitly trust that the device manufacture has secured the device and will continue to provide security patches and updates to the device. These devices are introducing entirely new waves of unprotected and uncontrollable operating systems. These feeble device operating systems don't run any anti-virus applications, and they don't run the security tools that you're used to seeing on your PCs. As a result, you have no control over attacks from these devices. Thus, more devices will proliferate that may have far fewer safety checks.

[3] http://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne

In the past, 'smart devices' (such as network printers) have been exploited, but their processors and network connections were not powerful enough to be used for anything serious. However, the new Nest Smart Thermostat has a 600MHz to 1GHz+ CPU and has a high quality network deriver. The same thing that makes the controller able to process what patterns and usage a consumer likes is also very helpful for creating botnets.

> "Nearly half of all IP traffic will originate with non-PC devices by 2017. In 2012, only 26 percent of consumer IP traffic originated with non-PC devices, but by 2017 the non-PC share of consumer IP traffic will grow to 49 percent. PC-originated traffic will grow at a CAGR of 14 percent, while TVs, tablets, mobile phones, and machine-to-machine (M2M) modules will have traffic growth rates of 24 percent, 104 percent, 79 percent, and 82 percent, respectively[5].

In addition to smart devices, servers have new remote management interfaces such as IPMI that are heavily vulnerable. At least 100,000 of these Internet-connected devices now have hardware that is vulnerable to remote attacks[4].

Thus, as unlikely as this may sound, we may see a point in the near future where your thermostat's OS is hacked and converted into a high-powered bot used to attack the hosted services that your car depends on for its navigation and music systems. We may see our 'smart' TVs stop functioning as their CPUs are put to use to attack video services such as Netflix, causing the Internet-connected video service to go dark. Or worse, they could be used to attack banking infrastructure which could cripple a small country's economy.

The Internet of Things will be involved in more attacks as PCs become less attractive to attackers. We will see DDoS attacks grow in size, compute capacity, targets, and intensity, causing major disruptions to access in our modern, online-dependent lives.

Trend #8. Increasing Dependency on the Internet Increases Risks

The Internet of Things is becoming more popular and users are depending on their smart devices more each day. The Internet of Things also heavily depends on hosted cloud services. For example, the Tesla Model S uses an Internet-connected service to update the car's entire computer and electronics systems, including maps and the batteries' controller systems. Unknowingly, the owner of a Tesla Model S now depends on this hidden service to keep his or her car functioning properly.

Nest Thermostats use Nest's cloud computing service to link the controller to iPhone apps and to crunch 'big data' in order to make the best decisions on how to operate your home's HVAC. Again, this device is reaching out to the Internet to function and thus increasing the user's dependency on connectivity.

We see this trend outside of the Internet of Things as well. The dependency on the Internet is growing at every level, including banking, stock trading, medical and healthcare, education, communications,

[4] http://arstechnica.com/security/2013/08/remote-admin-tool-imperils-servers/?
[5] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

entertainment, etc. This higher dependency on a network that's DDoS-prone virtually guarantees that DDoS attacks will be bigger part of everyday life in the near future.

Trend #9. New Targets: The Corporate Internet Connection

Beyond just attacking web sites and services, there's an entirely new unexplored attack vector: The office Internet connection. Corporate headquarters' Internet connections are often the lowest rung of a company's IT service offerings. They are typically underpowered, protected by devices prone to DDoS (they can't handle small packets), and often forgotten about until they stop working. They are also easy to pinpoint. Many companies continue to allow embedding of their office IP addresses in email, and a bounced email message to a company that hosts its own mail servers will reveal the office's IP space and allow for quick lookups in BGP (border gateway protocol) to expose all of that corporation's IP addresses associated with specific locations.

Since office Internet connections are typically underpowered, they are a prime target for a small yet highly effective DDoS attacks. The ISPs that offer this kind of Internet are also ill-prepared for DDoS, and thus small attacks would be very effective. Imagine if your office building no longer had Internet. Could you conduct business efficiently and effectively? Chances are no. Chances are your office uses VoIP for phones, thus the phones would be down. Chances are your office needs a variety of Internet third-party applications that are all then inaccessible. Chances are you'll need email to communicate to your customers. Chances are your company does not allow you to use tethering with your computer. Thus, if your corporate Internet connection is attacked, your corporation is effectively useless. If the attack is calculated and done with very exact methods, a building that employs thousands of people would be rendered dead.

Trend #10. APIs, CDNs, and Cloud Services: Soft, yet Complicated Targets

According to a recent Cisco study, content Delivery Networks (CDNs) will carry over half of all Internet traffic in 2017[6]. More than half (51 percent) of all Internet traffic will cross content delivery networks in 2017 globally, up from 34 percent in 2012. There are currently only a few successful CDNs, which basically puts a couple of companies holding a large part of the Internet's egress traffic – making them a very interesting target. Among those networks that we classify as a CDN include Google's YouTube, Gdrive, and the file attachment network for Gmail.

CDNs can egress or transmit many terabits-per-second of data out of their networks, but the same is not true for traffic into their networks. CDNs are designed around pushing a lot of large packets quickly in one direction. Based on the architecture to YouTube, LimeLight, Akamai, and BitGravity – they are highly vulnerable to DDoS attacks. DDoS could cripple these services if the attack was aimed at the right location on the CDN. Google

[6] Cisco Visual Networking Index: Forecast and Methodology, 2012–2017 http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

is notorious for building bulk cheaply, which affords them the ability to give away storage, video, etc. However, the same switches that push cheap bits out are not always the ones that can mitigate against them on the way in. The same is true with their software PC-based load balancers.

In Defense.Net's labs, testing with modern driver and interface technology on Linux, we've seen flaws in many high-end software development strategies. Linux can only handle about 5Gbps of small packets when accessing large arrays of memory before a PC fails over, yet they run line rate with big packets.

'The bigger they are, the harder they fall' seems to be true in networking as well. A successful attack will be difficult to analyze, locate, and mitigate against due to its layers of abstraction and sheer size. Live events are also very timely and offer a very good target to attack.

Trend #11. Cloud Dependencies: One Service Could Topple Many

For the first time in history, we are seeing a virtual overlapping dependency on physical and virtual infrastructure that can potentially impact a company's business flow without any oversight. In the past, an insurance company would own and operate its own servers and services that process premium transactions, deposits, and call centers. Now these same interfaces are operated by many layers of technology and by design, are completely abstracted.

Many enterprises now utilize cloud services for things ranging from customer support, databases, phone services, API calls for geographical lookup, push notifications to smart phone applications, email, wiki and data repositories, data storage, calendaring, etc. Developers can easily integrate external services, creating a web of overlapping dependencies on abstracted infrastructure and code. For example, many companies use services such as ZenDesk for support operations. Some companies utilize the ZenDesk API to gather ticketing and support details for their customers. At the same time, the companies' sales group may integrate with SalesForce.com to cross-reference that data with sales. They may use a shared authentication system, like OAUTH2 from Google, and an outsourced VoIP provider along with an outsourced server farm.

We are already seeing this happen across the board. Google experienced a complete blackout outage for five minutes in August 2013, which caused a reported 40% drop in overall Internet traffic[7]. G-drive, Google Search, YouTube, Gmail, and all associated APIs were offline. The five-minute outage caused businesses that are highly integrated with Google Apps to halt. Sites that are linked to Google Analytics and ad displays were not loading properly.

When all cloud services are operating as advertised, the experience should be pretty good. However, if any of the abstracted layers fall ill,

[7] http://news.sky.com/story/1129847/google-outage-internet-traffic-plunges-40-percent

it could cause serious business impacts across an enterprise without any clear understanding of how all of the services fit together and works. This makes cloud services prime targets for DDoS attacks and creates unknown impacts to the businesses that have created unknown dependences on unknown and abstracted infrastructure.

Summary

While cyberattacks are evolving and growing, so is the technology that stops them. The best minds in tech are working on state-of-the-art defenses to protect our critical infrastructure and develop new techniques to stay two steps ahead of the attackers. At the same time, industry associations are being formed to share and compare notes on recent attacks and review defensive strategies.

The most important element to overcome is the “it could never happen to me” feeling by many businesses. Without implementing protective measures in advance, these businesses and organizations will be the most at risk when the day comes and they are the target of a cyber-attack.

Defense.Net employs some of the top thinkers in this area and is devoting all of its time designing solutions that can address the mounting DDoS threats of today, and those expected in the years to come. To find out more, visit us on the web at **www.Defense.net**