Geoff Huston
September 2016

DDOS Attackers – Who and Why?

Bruce Schneier's recent blog post, “Someone is Learning How to Take Down the Internet” (https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html), reported that the incidence of DDOS attacks is on the rise. And by this he means that these attacks are on the rise both in the number of attacks and the intensity of each attack. A similar observation was made in the Versign DDOS Trends report for the second quarter of 2015 (https://www.verisign.com/assets/report-ddos-trends-Q22016.pdf), reporting that DDOS attacks are becoming more sophisticated and persistent in the second quarter of 2016. The Verisign report notes that the average attack size is 17Gbps, with a number of persistent attacks of the order of 100Gbps or greater. The number reported is 75% larger than the comparable period of a year ago. To quote from the report: "Verisign’s analysis shows that the attack was launched from a well-distributed botnet of more than 30,000 bots from across the globe with almost half of the attack traffic originating in the United States." The State of the Internet report from Akamai for the second quarter of 2016 paints a disturbingly similar picture: they observed a 129% increase in DDOS attacks over the same period in 2015, with increases in NTP reflection attacks and associated UDP flooding attacks.

The obvious question I have when reading these reports is "Who is behind these attacks, and why are they doing it?"

There has been a visible evolution of malice and hostility on the Internet. The earliest recorded event that I can recall is the Morris Worm of November 1988 (https://en.wikipedia.org/wiki/Morris_worm). This was a piece of self-replicating software that operated in a manner similar to many biological viruses - once a host was infected, the host tried to infect other hosts with an exact copy of its own code. The author, Robert Morris, was evidently a curious graduate school student. This was perhaps the first public Internet example of the ‘heroic hacker’ form of attack, typified by apparently pointless exploits that have no obvious ulterior motive other than flag planting or other forms of discovery. A public declaration that "*I was here*" appeared to the motivation that was the primary objective of many of these hacker exploits.

However, this situation did not remain so for long. While the task of finding new attack vectors was a challenging task that involved some considerable expertise, it was quickly observed that the level of mediation of previously discovered vulnerabilities was woefully small. As long as the vulnerabilities remained unfixed, the attacks could simply be repeated, and pretty quickly much of this work was packaged into scripts. This resulted in a new wave of attacks was typified by so-called 'script kiddies’ who ran these attack scripts without detailed knowledge of precisely how they exploited vulnerabilities in host systems. While it’s debatable, it appears in retrospect that the motive of the script kiddies was still predominately flag planting.

The next step in this unfortunate story was the introduction of money, and predictably where money flows, then crime follows soon after. Script authors rapidly discovered that they could sell their attack scripts, so that what was once a hobby turned into a profession. Equally the potential attackers found that they could turn the threat of an attack into a monetary opportunity: launch a small attack and threaten a larger and more prolonged attack unless the victim paid up.

There is no doubt that this criminal component of attack activity persists on the Internet today, but it is increasingly difficult to reconcile the level of expertise and capability that lies behind some of these large scale attacks on criminal activity alone. There is now some common belief, without much in the way of direct corroborative evidence from public sources, that so-called state-based actors are a new entrant who may be behind these highly sophisticated attacks. For example, while public information is scant on this topic, there is a strong suspicion that the "Stuxnet" computer worm was a joint US-Israeli developed effort (https://en.wikipedia.org/wiki/Stuxnet).

When the finger of suspicion points to state-based actors it is tempting to point to some foreign or alien "them" as the attacker. In the West it may well result in suspicion of the activities associated with some ill-defined Chinese or Russian agencies who are supposed to harbour some general malign intent to the West. Equally, it is easy in this age of concern over terrorism to point the finger of suspicion at a number of states that are seen as either failed nation states or are suspected as being sponsors of terrorism. But does it really make any sense to mount these attacks if you are a state actor? Sure, it may cause some short term disruption, but what strategic objective is fulfilled by such actions if the attacker is indeed a nation state?

Bruce Schneier puts forward the proposition that it's possible that these attacks represent a learning exercise: "the size and scale of these probes -- and especially their persistence -- points to state actors. It feels like a nation's military cybercommand trying to calibrate its weaponry in the case of cyberwar. It reminds me of the US's Cold War program of flying high-altitude planes over the Soviet Union to force their air-defense systems to turn on, to map their capabilities."

But it seems to me that such attacks tend to be self-defeating for the attacker. It's a common human reaction that we tend to fix what's broken. So when your front door is bashed down you then have a strong motivation to not only repair the door, but replace it with a stronger door that won't be so readily broken in future. When your online service infrastructure is under attack, then after the attack is over it is likely that the victim will invest in a more resilient service infrastructure. What these attacks are actually achieving as an outcome is incenting additional private investment in defending common service infrastructure. So if the purpose of these attacks is to probe the levels of defensive capability, then the result is that the victims have a strong desire to invest in greater level of defensive capability, which is hardly a desired result on the part of a potential attacker.

In such a light there are other explanations that could point to a slightly different motivation for these hostile probing attacks than a learning exercise to expose potential points of vulnerability in national cyber infrastructure. There is no doubt that much of the concern coming from the various national cybersecurity bodies is the lack of private investment in robust service infrastructure. And while exhortation is fine, we humans tend to be extremely poor assessors of risk when it is presented to us in theoretical terms. Warning folk that their service infrastructure is at risk of being attacked is readily discounted, while actually demonstrating these vulnerabilities by attacking someone produces a vastly different outcome, particularly by the victim! If we really wanted to have local actors to decide to invest more of their effort, time and resources in defensive infrastructure, then subjecting them to a robust stress test under true attack conditions might well be the best way to achieve that outcome!

Now most of us, including myself, just don't know who is launching these attacks. And we don't know why they are doing it. And those who may know just aren't talking. So all this is just conjecture. But what is not so abstract is the observation that the result of these attacks is not entirely bad. We are acutely aware these days that we need to think about operating services in a hostile environment, and deploy services in a manner that is resilient to today's forms of attack. And if that is one outcome of these attacks, then whoever the attackers may be or whatever their motivations may be, this particular result can be seen as a positive one. I'm not condoning these attacks in any way, but it does seem that some of the outcomes from these attacks are not entirely bad. If state-based actors are behind some of these attacks then it is entirely possible, as Bruce Schneier wonders, that this is a hostile activity intended to probe our defensive capability. But we just don't know, and another supposition is that some of these attacks could represent “friendly fire” from our own state, intended to make us take online security seriously enough to invest in real defensive deterrents for our online service infrastructure.

Irrespective of precisely what has prompted us to make this investment, we actually are investing in a more resilient Internet, and operating a service infrastructure that is intended to be capable of shrugging off many of the most common attack vectors. There is a viable business opportunity in providing highly resilient content delivery services that are engineered to withstand current brute force DDOS attacks and those businesses have customers who recognize the value that they offer. We may not be able to clean up all the open DNS resolvers, NTP agents and other elements that are exploited to create the bot armies. Cleaning up the legacy of all but forgotten connected devices that are coercible to operate in hostile ways is apparently a task that is way beyond us. But that need not be the end of the Internet. We can field services in a way that can deflect the consequent attacks that leverage this legacy of neglect. We understand how to provide service even through the most intense period of attack. And these days many service providers see the commercial benefit in investing in such measures as part of the cost of providing a robust service on the Internet.

And perhaps well we balance it all up, that’s a net beneficial outcome for all of us!

Author

Geoff Huston B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region. He has been closely involved with the development of the Internet for many years, particularly within Australia, where he was responsible for building the Internet within the Australian academic and research sector in the early 1990's. He is author of a number of Internet-related books, and was a member of the Internet Architecture Board from 1999 until 2005, and served on the Board of Trustees of the Internet Society from 1992 until 2001 and chaired a number of IETF Working Groups. He has worked as an Internet researcher, as an ISP systems architect and a network operator at various times.

www.potaroo.net

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.