Are the Days of "Booter" Services Numbered?

Published: 2016-10-27 · Archived: 2026-04-05 19:23:05 UTC

It may soon become easier for Internet service providers to anticipate and block certain types of online assaults launched by Web-based attack-for-hire services known as "booter" or "stresser" services, new research released today suggests.

The findings come from researchers in Germany who've been studying patterns that emerge when miscreants attempt to mass-scan the entire Internet looking for systems useful for launching these digital sieges — known as "distributed denial-of-service" or DDoS attacks.

To understand the significance of their research, it may help to briefly examine how DDoS attacks have evolved. Not long ago, if one wanted to take down large Web site, one had to build and maintain a large robot network, or "botnet," of hacked computers — which is a fairly time intensive, risky and technical endeavor.

These days, however, even the least sophisticated Internet user can launch relatively large DDoS attacks just by paying a few bucks for a subscription to one of dozens of booter or stresser services, some of which even accept credit cards and PayPal payments.

These Web-based DDoS-for-hire services don't run on botnets: They generally employ a handful of powerful servers that are rented from some dodgy "bulletproof" hosting provider. The booter service accepts payment and attack instructions via a front end Web site that is hidden behind Cloudflare (a free DDoS protection service).

But the back end of the booter service is where the really interesting stuff happens. Virtually all of the most powerful and effective attack types used by booter services rely on a technique called traffic **amplification** and

reflection, in which the attacker can reflect or "spoof" his traffic from one or more third-party machines toward the intended target.

In this type of assault, the attacker sends a message to a third party, while spoofing the Internet address of the victim. When the third party replies to the message, the reply is sent to the victim — and the reply is much larger than the original message, thereby amplifying the size of the attack.

To find vulnerable systems that can be leveraged this way, booters employ large-scale Internet scanning services that constantly seek to refresh the list of systems that can be used for amplification and reflection attacks. They do this because, as research has shown (PDF), anywhere from 40-50 percent of the amplifiers vanish or are reassigned new Internet addresses after one week.

Enter researchers from **Saarland University** in Germany, as well as the **Yokohama National University** and **National Institute of Information and Communications Technology** — both in Japan. In a years-long project first detailed in 2015, the researchers looked for scanning that appeared to be kicked off by ne'er-do-wells running booter services.

To accomplish this, the research team built a kind of distributed "honeypot" system — which they dubbed "**AmpPot**" — designed to mimic services known to be vulnerable to amplification attacks, such as DNS and NTP floods.

"To make them attractive to attackers, our honeypots send back legitimate responses," the researchers wrote in a 2015 paper (PDF). "Attackers, in turn, will abuse these honeypots as amplifiers, which allows us to observe ongoing attacks, their victims, and the DDoS techniques. To prevent damage caused by our honeypots, we limit the response rate. This way, while attackers can still find these ratelimited honeypots, the honeypots stop replying in the face of attacks."

In that 2015 paper, the researchers said they deployed 21 globally-distributed AmpPot instances, which observed more than 1.5 million attacks between February and May 2015. Analyzing the attacks more closely, they found that more than 96% of the attacks stem from single sources, such as booter services.

"When focusing on amplification DDoS attacks, we find that almost all of them (>96%) are caused by single sources (e.g. booters), and not botnets," the team concluded. "However, we sadly do not have the numbers to compare this [to] DoS attacks in general."

Many large-scale Internet scans like the ones the researchers sought to measure are launched by security firms and other researchers, so the team needed a way to differentiate between scans launched by booter services and those conducted for research or other benign purposes.

"To distinguish between scans performed by researchers and scans performed with malicious intent we relied on a simple assumption: That no attack would be based on the results of a scan performed by (ethical) researchers," said **Johannes Krupp**, one of the main authors of the report. "In fact, thanks to our methodology, we do not have to make this distinction upfront, but we can rather look at the results and say: 'We found attacks linked to this scanner, therefore this scanner must have been malicious.' If a scan was truly performed by benign parties, we will not find attacks linked to it."

SECRET IDENTIFIERS

What's new in the paper being released today by students at Saarland University's Center for IT-Security, Privacy and Accountability (CISPA) is the method by which the researchers were able to link these mass-scans to the very amplification attacks that follow soon after.

The researchers worked out a way to encode a secret identifier into the set of AmpPot honeypots that any subsequent attack will use, which varies per scan source. They then tested to see if the scan infrastructure was also used to actually launch (and not just to prepare) the attacks.

Their scheme was based in part on the idea that similar traffic sources should have to travel similar Internet distances to reach the globally-distributed AmpPot sensors. To do this, they looked at the number of "hops" or Internet network segments that each scan and attack had to traverse.

Using trilateration –the process of determining absolute or relative locations of points by measurement of distances — the research team was able to link scanners to attack origins based on hop counts.

These methods revealed some 286 scanners that are used by booter services in preparation for launching amplification attacks. Further, they discovered that roughly 75 percent of those scanners are located in the United States.

The researchers say they were able to confirm that many of the same networks that host scanners are also being used to launch the attacks. More significantly, they were able to attribute approximately one-third of the attacks back to their origin.

"This is an impressive result, given that the spoofed source of amplification attacks usually remains hidden," said **Christian Rossow** of Saarland University.

Rosso said the team hopes to conduct further research on their methods to more definitively tie scanning and attack activity to specific booter services by name. The group is already offering a service to hosting providers and ISPs to share information about incidents (such as attack start and end times). Providers can then use the attack information to inform their customers or to filter attack traffic.

"We have shared our findings with law enforcement agencies — in particular, Europol and the FBI — and a closed circle of tier-1 network providers that use our insights on an operational basis," the researchers wrote. "Our output can be used as forensic evidence both in legal complaints and in ways to add social pressure against spoofing sources."

ANALYSIS

Even if these newly-described discovery methods were broadly deployed today, it's unlikely that booter services would be going away anytime soon. But this research certainly holds the promise that booter service owners will be able to hide the true location of their operations less successfully going forward. and that perhaps more of them will be held accountable for their crimes.

Efforts by other researchers have made it more difficult for booter and stresser services to accept PayPal payments, forcing more booters to rely more on Bitcoin.

Also, there are a number of initiatives that seek to identify a handful of booter services which resell their infrastructure to other services who brand and market them as their own. Case in point, in September 2016 I published an expose on vDOS, a booter service that earned (conservatively) $600,000 over two years helping to launch more than 150,000 DDoS attacks.

Turns out, vDOS's infrastructure was used by more than a half-dozen other booter services, and shortly after vDOS was taken offline most of those services went dark or were dismantled as well.

One major shift that could help to lessen the appeal of booter services — both for the profit-seeking booter proprietors and their customers — is a clear sign from law enforcement officials that this activity is in fact illegal and punishable by real jail time. So far, many booter service owners have been operating under the delusion or rationalization that their services are intended solely for Web site owners to test the ability of their sites to withstand data deluges. The recent arrest of two alleged Lizard Squad members who resold vDOS services through their own "PoodleStresser" service is a good start.

Many booter operators apparently believe (or at least hide behind) a wordy "terms of service" agreement that all customers must acknowledge somehow absolves them of any sort of liability for how their customers use the service — regardless of how much hand-holding and technical support they offer those customers.

Indeed, the proprietors of vDOS — who were arrested shortly after my story about them — told the *Wall Street Journal* through their attorneys that, "If I was to buy a gun and shoot something, is the person that invents the gun guilty?"

The alleged proprietors of vDOS — 18-year-old Israelis **Yarden Bidani** and **Itay Huri** — were released from house arrest roughly ten days after their initial arrest. To date, no charges have been filed against either men, but I have reason to believe that may not be the case for long.

Meanwhile, changes may be afoot for booter services advertised at **Hackforums[dot]net**, probably the biggest open-air online marketplace where booter services are advertised, compared and rated (hat tip to @MalwareTechblog). Earlier this week, Hackforums administrator **Jesse "Omniscient" LaBrocca** began restricting access to its "stressers" subsection of the sprawling forum, and barring forum members from advertising booter services in their user profiles.

"I can absolutely see a day when it's removed entirely," LaBrocca said in a post explaining his actions. "Could be very soon too."

Hackforums administrator Jesse “Omniscient” LaBrocca explaining a decision to restrict access to the “stressers” portion of the Hackforums marketplace.

My worry is that we may soon see a pendulum shift in the way that many booter services operate. For now, the size of attacks launched by booter services is somewhat dependent on the number and power of the back-end servers used to initiate amplification and reflection attacks.

However, I could see a day in the not-too-distant future in which booter service operators start earning most of their money by reselling far more powerful attacks launched by actual botnets made from large networks of hacked **Internet of Things** (IoT) devices — such as poorly-secured CCTV cameras and digital video recorders (DVRs).

In some ways this has already happened, as I detailed in my January 2015 story, Lizard Stresser Runs on Hacked Home Routers. But with the now public release of the source code for the Mirai botnet — the same malware strain that was used in the record 620 Gbps DDoS on my site last month and in the widespread Internet outage last week caused by an attack against infrastructure provider **Dyn** — far more powerful and scalable attacks are now available for resale.

A copy of the paper released today at the ACM CSS conference in Vienna is available here (PDF).
