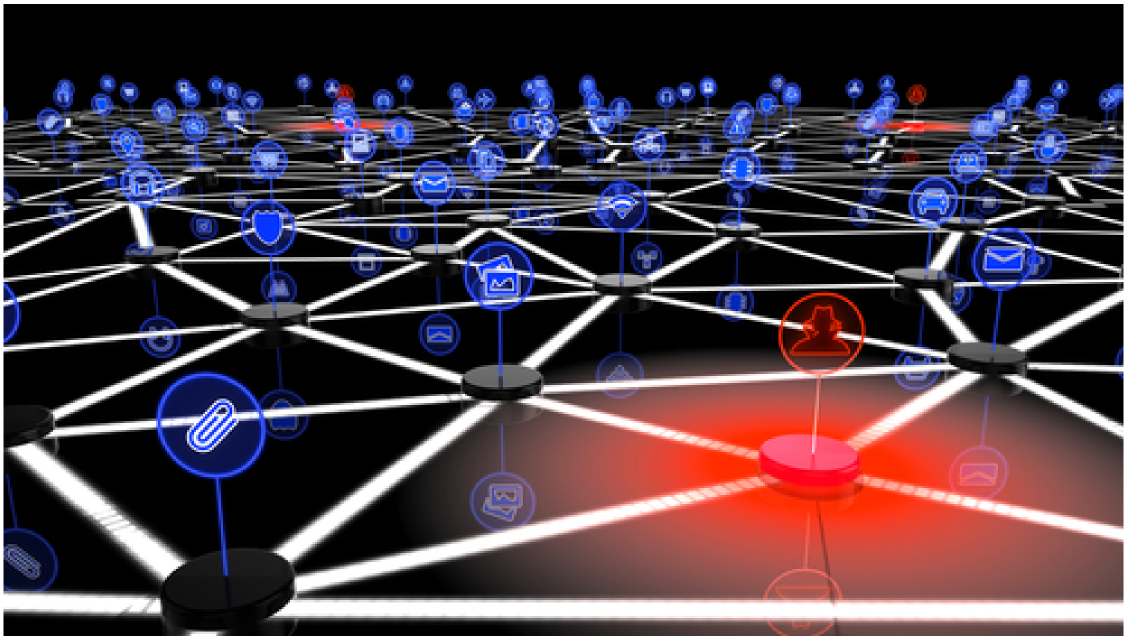
KrebsOnSecurity Hit With Record DDoS

krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.



The attack began around 8 p.m. ET on Sept. 20, and initial reports put it at approximately 665 Gigabits of traffic per second. Additional analysis on the attack traffic suggests the assault was closer to 620 Gbps in size, but in any case this is many orders of magnitude more traffic than is typically needed to knock most sites offline.

Martin McKeay, Akamai's senior security advocate, said the largest attack the company had seen previously clocked in earlier this year at 363 Gbps. But he said there was a major difference between last night's DDoS and the previous record holder: The 363 Gpbs attack is thought to have been generated by a botnet of compromised systems using well-known techniques allowing them to "amplify" a relatively small attack into a much larger one.

In contrast, the huge assault this week on my site appears to have been launched almost exclusively by a very large botnet of hacked devices.

The largest DDoS attacks on record tend to be the result of a tried-and-true method known as a DNS reflection attack. In such assaults, the perpetrators are able to leverage unmanaged DNS servers on the Web to create huge traffic floods.

Ideally, DNS servers only provide services to machines within a trusted domain. But DNS reflection attacks rely on consumer and business routers and other devices equipped with DNS servers that are (mis)configured to accept queries from anywhere on the Web. Attackers can send spoofed DNS queries to these so-called “open recursive” DNS servers, forging the request so that it appears to come from the target’s network. That way, when the DNS servers respond, they reply to the spoofed (target) address.

The bad guys also can amplify a reflective attack by crafting DNS queries so that the responses are much bigger than the requests. They do this by taking advantage of an extension to the DNS protocol that enables large DNS messages. For example, an attacker could compose a DNS request of less than 100 bytes, prompting a response that is 60-70 times as large. This “amplification” effect is especially pronounced if the perpetrators query dozens of DNS servers with these spoofed requests simultaneously.

But according to Akamai, none of the attack methods employed in Tuesday night’s assault on KrebsOnSecurity relied on amplification or reflection. Rather, many were garbage Web attack methods that require a legitimate connection between the attacking host and the target, including SYN, GET and POST floods.

That is, with the exception of one attack method: Preliminary analysis of the attack traffic suggests that perhaps the biggest chunk of the attack came in the form of traffic designed to look like it was generic routing encapsulation (GRE) data packets, a communication protocol used to establish a direct, point-to-point connection between network nodes. GRE lets two peers share data they wouldn’t be able to share over the public network itself.

“Seeing that much attack coming from GRE is really unusual,” Akamai’s McKeay said. “We’ve only started seeing that recently, but seeing it at this volume is very new.”

McKeay explained that the source of GRE traffic can’t be spoofed or faked the same way DDoS attackers can spoof DNS traffic. Nor can junk Web-based DDoS attacks like those mentioned above. That suggests the attackers behind this record assault launched it from quite a large collection of hacked systems — possibly hundreds of thousands of systems.

“Someone has a botnet with capabilities we haven’t seen before,” McKeay said. “We looked at the traffic coming from the attacking systems, and they weren’t just from one region of the world or from a small subset of networks — they were everywhere.”

There are some indications that this attack was launched with the help of a botnet that has enslaved a large number of hacked so-called “Internet of Things,” (IoT) devices — routers, IP cameras and digital video recorders (DVRs) that are exposed to the Internet and protected with weak or hard-coded passwords.

As noted in a recent report from **Flashpoint** and **Level 3 Threat Research Labs**, the threat from IoT-based botnets is powered by malware that goes by many names, including "Lizkebab," "BASHLITE," "Torlus" and "gafgyt." According to that report, the source code for this malware was leaked in early 2015 and has been spun off into more than a dozen variants.

"Each botnet spreads to new hosts by scanning for vulnerable devices in order to install the malware," the report notes. "Two primary models for scanning exist. The first instructs bots to port scan for telnet servers and attempts to brute force the username and password to gain access to the device."

Their analysis continues:

"The other model, which is becoming increasingly common, uses external scanners to find and harvest new bots, in some cases scanning from the [botnet control] servers themselves. The latter model adds a wide variety of infection methods, including brute forcing login credentials on SSH servers and exploiting known security weaknesses in other services."

I'll address some of the challenges of minimizing the threat from large-scale DDoS attacks in a future post. But for now it seems likely that we can expect such monster attacks to soon become the new norm.

Many readers have been asking whether this attack was in retaliation for my recent series on the takedown of the DDoS-for-hire service vDOS, which coincided with the arrests of two young men named in my original report as founders of the service.

I can't say for sure, but it seems likely related: Some of the POST request attacks that came in last night as part of this 620 Gbps attack included the string "freeapplej4ck," a reference to the nickname used by one of the vDOS co-owners.

Update Sept. 22, 8:33 a.m. ET: Corrected the maximum previous DDoS seen by Akamai. It was 363, not 336 as stated earlier.