Forbes

Thomas Fox-Brewster Forbes Staff

I cover crime, privacy and security in digital and physical forms.

SECURITY 9/25/2016 @ 10:00AM | 41,031 views

How Hacked Cameras Are Helping Launch The Biggest Attacks The Internet Has Ever Seen

The Rio Olympics was targeted with epic DDoS attacks, but shrugged them off. But attacks are getting bigger, sites are falling and voices being silenced. / AFP / Odd ANDERSEN (Photo credit should read ODD ANDERSEN/AFP/Getty Images)

Brian Krebs knows what it's like to face intimidation from hackers. The independent reporter has had a SWAT team called to his house by subjects of his investigations. One sent threats via flowers shaped in a cross, the kind one orders for a funeral. But he's never been on the wrong end of a record-breaking digital attack like he was this week when an epic amount of traffic – somewhere between 600 gigabits per second and 700Gbps – took his website offline.

Such was the size of the hit, known as a distributed denial of service (DDoS), the security company protecting Krebs' site – Prolexic, owned by Akamai – could no longer justify supporting KrebsOnSecurity.com. The economics made it infeasible: Akamai had to suck in all that data at a huge cost, and as Krebs wasn't paying for the service, the firm had to

make a call. Krebs doesn't blame them. "I'm most concerned about not having the attack blow back on my original provider," he told me. The site is now back up, thanks to Google's Project Shield service designed to protect human rights activists and journalists from DDoS-powered censorship.

But Krebs isn't alone in being targeted. He's one of many victims of the same hacker crew, FORBES understands. The unnamed individual or group has, in the last five days, launched other huge attacks across the internet. French hosting giant OVH said it had been hit by an even greater attack, at more than 1100Gbps, though this was not independently confirmed. Gaming companies, including Blizzard, have been disrupted by sizeable DDoS hits, though the studio behind massively popular shooter Overwatch creator hasn't clarified just how big its hit was.

How hackers generate such power

FORBES was told by two sources familiar with the attacks that the botnets are made up of tens of thousands of Internet of Things (IoT) devices, including unsecure routers, digital video recorders (DVRs) and connected IP cameras. Such IoT machines have been shown widely vulnerable to simple hacks, meaning the bot masters are easily able to build up vast networks of compromised systems to send extraordinary volumes of traffic to a chosen target. But connected cameras have proven especially attractive to hackers. Founder of OVH, Octave Klaba, said one of the botnets that struck his company consisted of 145,607 cameras and DVRs. Just this summer, a botnet of 25,000 CCTV cameras was used to initiate significant attacks across the world.

The majority of traffic in the latest attacks has come from Asia, in particular China, South Korea, Taiwan and Vietnam, though it's unclear where the hackers themselves hail from. One source familiar with the attacks said they were being perpetrated either by an individual or a group that's flexing its muscles and testing its capability.

The same source said the botnets are being sold as "booters," rentable DDoS services much like the one Krebs reported on this month, vDos, which resulted in the arrest of two individuals in Israel. Lizard Squad, the crew responsible for the infamous Christmas 2015 Xbox and PlayStation network outages, has built up significant botnets to power their booter, the LizardStresser. Many others hoping to earn as much or more than the vDos crew – a reported $600,000 over two years - have done the same. Krebs suspects his site was knocked out by someone linked with vDos. "I don't think there's any question," he told me. "Some of the people who are aligned with that service have built enormous botnets."

Whoever they are, the hackers perpetrating the humongous attacks have used some old tricks to generate unprecedented levels of malicious traffic. They've reverted to a somewhat

esoteric form of shifting data at terrifying speeds, using what's known as Generic Routing Encapsulation (GRE). GRE is used in a similar way to Virtual Private Networks: to provide "tunnels" into a business network. But whereas VPNs are encrypted, GRE tunnels aren't.

As it's a less-familiar protocol, many don't configure their security systems to deal with GRE traffic. Tom Paseka, engineer at content delivery network and anti-DDoS supplier CloudFlare, said GRE was being used as it can bypass poorly-setup firewall filters. "GRE is protocol 47 and would be able to still be transmitted past firewalls that aren't looking for it, or don't explicitly block other traffic or protocol types," he told me.

Just this summer, official sites of the Rio Olympics were targeted with a GRE-based DDoS, which reached up to 540Gbps. Anti-DDoS vendor Arbor Networks noted in a blog post it was the longest 500Gbps-plus DDoS attack it had ever witnessed. Again, hacked IoT devices were used to generate that power. But the sites remained online. The Olympic organizers were prepared.

The internet 'has to act'

Major network providers and DDoS mitigation firms have, evidently, struggled to withstand the levels of traffic produced by the attackers. Though Krebs was receiving *pro bono* assistance from Akamai, Blizzard and OVH paid for their services and still saw disruption.

The subsequent concern is the eventual impact: criminals have the ability to censor the web, as in the case of Krebs. They could also silence human rights organizations or protesters. They could demand ransoms from businesses. And, in delivering such sizeable attacks, there is collateral damage: any organization served on the same infrastructure as a target could be inadvertently knocked offline.
Even networks sat next to those where a DDoS is initiated will suffer, warned Arbor Networks principal engineer Roland Dobbins. "The collateral damage footprint can be quite broad and deep. In many cases, collateral damage inflicted on bystander organizations and disruption of their internet traffic is even greater than the direct effects on the actual targets of the attack," he added.

CloudFlare, for instance, has had to cope with some disruption from the attacks on Akamai-protected properties. "We've seen some congestion and packet loss on networks we share with the Akamai scrubbing centers [where traffic is spread out across servers to reduce the load], but nothing serious," said CloudFlare CEO Matthew Prince, before claiming his company had dealt with similar attacks to its rival.

And nation states aren't afraid of flexing their muscles. Security expert Bruce Schneier warned earlier this month, via a somewhat opaque article entitled *Someone Is Learning*

How To Take Down The Internet, that governments were testing the stability of the net's backbone with DDoSes. Whilst that development isn't new (DDoS experts told me it's been going on for 20 years or more) the inability of web providers to cope with such traffic is a worrying, emergent development in the narrative of global online security. Even the most confident of DDoS defenders fear the days when 1 terabits per second (Tbps) attacks are commonplace.

Action, therefore, needs to be taken, both at the internet service provider (ISP) level and across IoT device makers, said Dobbins. The former will require ISPs across the world to combine efforts in shutting off access from infected machines. The latter will need vendors to cease bad practice, such as leaving easily-guessable default passwords like "admin" running on commercial products, said Dobbins.

"ISPs and enterprises who purchase such devices should insist on adherence to well-known industry security practices of this nature, and should test any IoT-type devices they're considering purchasing in order to validate that those devices are secure by default, and can't be abused to launch DDoS attacks or be compromised in others ways."

ISPs have another critical role to play, added Dobbins, one that will require a degree of altruism. "It's imperative that all internet-connected organizations – especially ISPs – have sufficient visibility into internet traffic ingressing, egressing, and traversing their networks so that they know when DDoS attack traffic is present on their networks, and work to mitigate it promptly."

"It's in the best interests of network operators to treat DDoS traffic leaving their networks just as seriously as DDoS traffic entering their networks."

Krebs, meanwhile, remains anxious about the current status quo. "Somebody compared it to testing the Death Star on the Millennium Falcon. It's a good analogy."

Tips and comments are welcome at TFox-Brewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail. Get me on Twitter @iblametom and tfoxbrewster@jabber.hot-chilli.net for Jabber encrypted chat.

The Conservative Alternative To Donald Trump Isn't Gary Johnson -- It's Evan...

The Most Expensive Home Listing in Every State 2016

The 20 Most Prestigious Internships For 2017