DDoS Botnet Strategy: Rise Of The Appliances!

Remember those early carefree days of the Internet? Dial-up modems? Funny Flash animated videos? Really cruddy looking websites?

Gone, gone, gone; along with any sense of security or privacy you might have harbored while slowly surfing that crazy new thing we used to call the Information Superhighway…

Not only are data theft, malware and ransomware attacks, phishing schemes and Point of Sale breaches all commonplace, but something far scarier – and larger in scale and scope – is definitely afoot.

Like in a cheesy sci-fi movie, the world's "smart" (or more precisely, "connected") Internet of Things (IoT) appliances are being marshalled by evil overlords and pitted against us, leaving huge swaths of the Internet overwhelmed and smoldering offline in their path. Connected home security sensors, webcams, DVRs and other appliances (as discussed in an earlier DEFEND piece on the Mirai botnet here) often don't have very strong security built into them and thus can be easily taken over, controlled remotely and aggregated into a massive army of data attackers.

I recently did a radio play about appliances becoming sentient, banding together and turning against us. Let's just say it didn't end well for humanity.

Increasingly, over the last few months, real life has started to imitate art as a spate of concentrated, progressively powerful botnet-fueled Distributed Denial of Service (DDos) attacks has brought large chunks of the Internet offline.

With the public release of the code for the straightforward but effective Mirai botnet about a month ago, today, almost any hacker, regardless of talent or experience, can mount a serious and exceptionally disruptive botnet-fueled DDoS attack by finding and controlling any number of the millions of essentially unprotected IoT devices now sitting in our homes and/or offices.

In late September, Brian Krebs' site KrebsOnSecurity was targeted. In that attack, the data flood reached over 600 gigabits per second, which simply hadn't been seen before, certainly not in more traditional DNS reflection or amplification style attacks. About a week later, it was French webhosting provider OVH that was attacked by a botnet of over 150,000 IoT devices. During that attack, the torrent hit over 1 terabit per second. Last Friday (October 21st), it was a well-orchestrated, highly concentrated attack on Dyn, an Internet service provider based in Manchester New Hampshire, with attacks emanating from millions of IP addresses collectively reaching a bit rate of 1.2 trillion bits of data per second, bringing the Dyn servers down and Twitter, Amazon, Spotify, Netflix, HBO, PayPal, and others with them for most of the East Coast of the United States (and elsewhere) for a large portion of the day.

“Hmm,” you say, “couldn’t binge-watch The Walking Dead for a few hours? So what?” Well, while Friday’s coordinated mass outage might have been more of an inconvenience and a show of strength, the storm clouds are looking pretty ominous here. Many analysts think that the uptick in scale and scope of recent DDoS attacks is all warm-up for the big one – taking down the Internet. Why someone would want to wipe out the Internet is another question – ransom, fame, revenge – that may very well become crystal clear in the event that these “tests” are in fact practicing for a major anti-Internet event.

Late-breaking information is pointing to an odd confluence of attackers working together. The first “hit” on Friday looks to be a possible revenge attack from fans of WikiLeaks founder Julian Assange, whose Internet access was famously cut off by the Ecuadoran Embassy not long ago. A hacking collective called NewWorldHackers claimed it passed the baton to the group Anonymous for the second round of attacks to send a rebuke to Russian hackers and their meddling in the U.S. elections this year. How bringing down American sites hurts the Russians is beyond my ken, but then again, so many things are that I’m happy to leave it right there.

Whatever the underlying grudge here, if there really is one, there’s almost definitely more trouble brewing. Cyberspace is looking increasingly like the Wild Wild West, and the things we take for granted (like Internet stability and guaranteed connectivity) today may very well be harder to come by tomorrow.

Time will tell whether we’ll be able to lock down our IoT devices and prevent a mass cyber-calamity, or if we’ll all end up like the defenseless civilians ducking for cover while superheroes and villains battle it out and destroy our “city” in the latest action movie.

In the meantime, sleep with one eye open Vladimir Putin, and back up your data everyone!