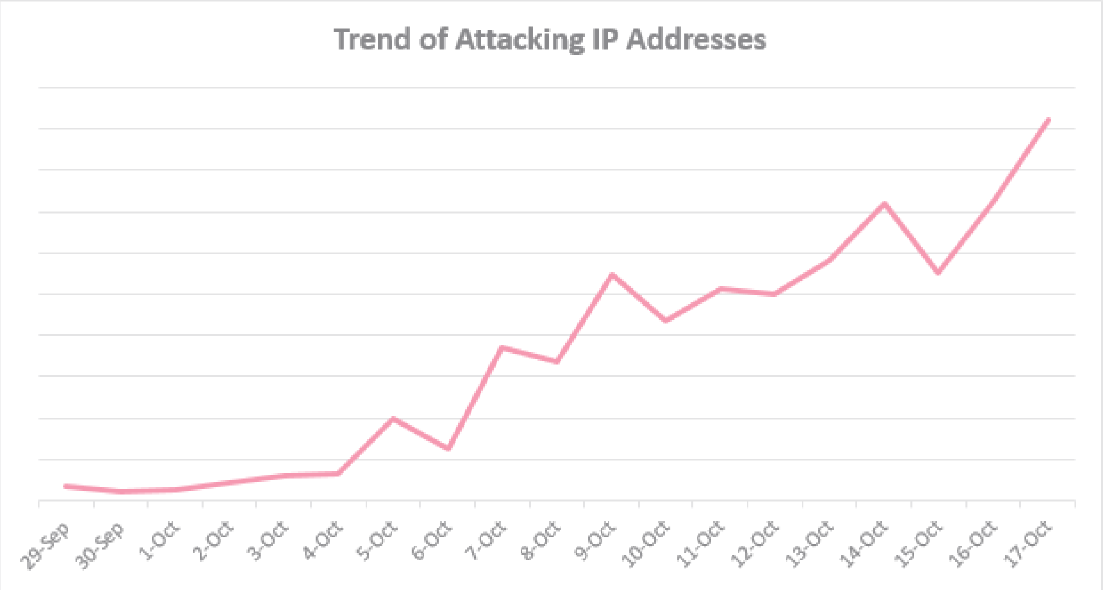
Reaper: Calm Before the IoT Security Storm?

krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm



46 thoughts on “Reaper: Calm Before the IoT Security Storm?”

1. *Sam* October 23, 2017
   Thanks for this info Krebs, as always.

2. *Chris* October 23, 2017
   My kingdom, my kingdom for a y-axis label on the first CheckPoint plot!

   The rest of the article is certainly concerning, but without scale and labeling, all we know from that graph is that something is going up on a daily basis.

   1. *John* October 24, 2017
      His kingdom, his kingdom for an x-axis label on the first CheckPoint plot!

   2. *John* October 24, 2017
      His kingdoom! Her kingdoom for an x-axis labull on th second CheckPoint plot! meaningless comments!

   3. *PattiM* October 25, 2017
      That was exactly my first thought – unlabeled graphs can’t be interpreted.

3. *Wajdi* October 23, 2017
   Have researchers been able to identify C&Cs and involved domain names ?

4. *Ben* October 23, 2017

   We need a “patch or die” worm.

   Recruits a botnet of unpatched and unpatchable devices, then permanently bricks every single one.

   A few rounds of that and the message might sink in.

   I am not recommending anyone does this because they will go to prison, but I still wish someone would.

   1. *Robert* October 23, 2017

      Ben, you’re not the 1st 1 to wish 4 such. Problem is, the Gov’t doesn’t seem to care, manufacturers of the IoT devices don’t seem to care, ISP don’t seem to care, people who own the devices don’t seem to care, yet everyone gets all bent out of shape when things go wrong. Well, do something about the problem “before” it becomes a problem! Patch, change passwords, buy more reliable Iot’s. But I do hope some 12 yr old decides to stop the problem (he won’t go to jail, will he?).

      I’ve noticed more probes of my ports for a few months, nothing major like last year though. But I’m seeing lots of probes from w/i the US (probably slaved PC’s), including one I never saw in a decade of probe logs – Microsoft Media Server (MMS). I’m getting port probes way beyond just telnet, maybe something is up.

      1. *SeymourB* October 24, 2017

         Unfortunately thanks to widespread use of netnannies and similar childproofing our 12 year olds aren’t as technical as the generation before them.

         When you shove them into padded rooms for their entire childhood, you can’t be surprised that all they know are padded rooms.

      2. *Deb* October 26, 2017

         As long as people are making money, they will not care

2. *Paul* October 23, 2017
   brickerbot may interest you

   1. *Robert* October 24, 2017
      Paul – “brickerbot may interest you”

      Just did a bit of reading on Brickerbot. I can see the carnage it could cause as it doesn’t discriminate between an unsecured but vital piece of equipment in a hospital and the average IoT camera. Both get bricked.

      “Strong password protection” is the key that manufacturers can offer consumers of IoT devices, unlocking such a device would require the same key, much harder to do.

      I have no IoT dog in this fight so I don’t care but it can still affect me via, say, that hospital device if I’m a patient! I hope that if anything good comes out of this new mess, it’s that manufacturers and end users will finally take steps to help prevent Webageddon from making the Internet useless for everyone.

      I reacted to the Equifax breach by freezing my credit with all potential access points for the bad guys. Better to do something now rather than wait and see if I’m going to be affected. Something about a ounce of prevention being worth a pound of cure.

      If I do buy an Iot device, you can be sure it will be one that offers strong password protection, one that at least tries to prevent the pound of cure approach. More expensive up front perhaps, but cheaper in the long run.

      1. *v.cardwell* October 30, 2017
         It will do nothing. they are using the smart meter on your house to control anything in it. I know because I have been dealing with it involuntarily for about 17 years (since 2004). I have a iPhone 6s with sprint service, Verizon home internet suite with security and still they are either not interested in things they can fix then and there so the gapping security hole gets ignored to a Krebs-like security researcher finds and then reports the problem. I’ve sent the screenshot of the “springboard” on my iPhone and they were stumped. the actual springboard icon is missing. I tried to explain that the ITouch feature is not working correctly never heard anything yet.

5. *Scott* October 23, 2017
   I wish you well with the web site changes.

   Oh and thanks for the article as well.. Appreciate the work you do.

6. *Bryn Gerard* October 23, 2017
   Two of my clients suffered their DVR’s being recruited to the Mirai Botnet earlier this year. AVTECH have been unresponsive and as a short-term fix, unexpected ports were configured prevent the devices being compromised. Each compromised device had an IP address applied in the 10.*.*.* range (I can’t remember the actual configuration). The devices went off line and the performance, even at the local console was severely degraded. The problem for my clients is that they require access to these DVR’s as a key business requirement. They haven’t been hacked since the ports were changed but reading further I see that the new variant of this attack no longer requires the admin password to commandeer the device. Does anyone know if it is possible to detect if they have been compromised?

7. *Rich A* October 23, 2017
   Reconsider cheering on brickerbot!
   There probably is no economic answer to unsecured devices, except to disable them.
   https://arstechnica.com/information-technology/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/

8. *Robert Scroggins* October 23, 2017
   What port(s) do IOTs use? Perhaps something could be done to beef up security at that level.

   Thanks, Brian!

   Regards,

   1. *somguy* October 24, 2017
      Short non technical answer:
      They use all ports.

      That’s not a solution.

9. *Winston* October 24, 2017
   How vulnerable are self-funded and installed Orwell Telescreens Amazon Echo, Echo Look, Tap, etc. to hacking? Did they do the smart things security-wise?

   1. *Winstom* October 25, 2017
      Looks like we’re going to see a familiar face on the IoT vulnerability subject next week on Vice channel’s Cyberwar series.

      1. BrianKrebs *Post author*October 25, 2017
         Yup, recorded that in late spring. Will be great to see what they’ve done with it. I’ve enjoyed the series.

10. *Chris* October 24, 2017
    @kerbonsecurity did you ever follow up on the 503C you where thinking of setting up in 2016? ‘The Center for the Defense of Internet Journalism’ for those in the journalism community that may require protection from large attacks such as the one you endured?

    Thanks,

11. *Dan* October 24, 2017
    Hi Brian, thanks for the article !

    Just as a note: “CheckPoint” is two words, “Check Point”.

12. *Richard Stein* October 24, 2017
    Please add a vertical axis scale to the graph of “Trending Attack IP Addresses.” Would like see order of magnitude – use log-scale.

    1. *Lori* October 24, 2017
       Since several people have commented on this, I went to Check Point to find their graph – and they do not have a vertical axis on it, so it would be difficult for Brian to provide one. Looks like it is Check Point that needs to define the scale on their graph.

13. *Jerry* October 24, 2017
    It appears a firmware update is available for the Linksys e1500 router after the identified vulnerabilities. Hopefully it can mitigate these vulnerabilities. Thanks for bringing this to our attention Mr Krebs.

14. *Bob* October 24, 2017
    If this is big enough and does enough damage, it might be the wake up call that is needed to get the everyone to take IOT security seriously.

15. *Mike* October 24, 2017
    Wow, that chart! The one from Checkpoint… It's so… Meaningless.

    I see horizontal lines, but they don't mean anything.

    While other readers comment that the article is good, it's slop like this (and previous editing problems) that make me stop reading and just skip for the point. Get it together Krebs, and hire an editor.

    1. *SeymourB* October 24, 2017
       More than likely it was intentionally left off by CP so the authors couldn't use it to determine the source(s) of their data.

       Whatever amount they note will not accurately match the real-world installations, so by correlating groups of systems you can do simple math to determine which groups CP has access to and shut down their insight into your botnet.

       Unless you're paying Brian to provide you with information, you're not in a position to make demands. Its kind of like people who use an open source project then make demands to the author – sorry but it doesn't work that way.

       1. *Margaret* October 24, 2017
          Thank you Seymour!!!!! I agree with you. Brian does a great service for us… maybe we need to exert a little of our own effort to get a better understanding rather than putting a demand we have no right to do on Brian.

    2. *J. W.* October 24, 2017
       Complain to Checkpoint, not Krebs. It's identical to what's on the Checkpoint site, as noted.

    3. *Louise* October 24, 2017
       The CheckPoint graph offers a rough summary of number of sources of infection worldwide.

       The Y-axis represents number of organizations infected, with increments of 100,000, and the X-axis is the time over which this was discovered, starting "the last few days of September." September 29th is the first coordinate labeled.

       1. *Nobby Nobbs* October 25, 2017
          Thanks for that, Louise. That helps a lot.

          Thanks for keeping an eye on this, Brian. I wonder about "smart" tvs, seems like they could be similarly vulnerable. And the lucky hacker might get an earful of archived voice commands…

16. *GlenR* October 24, 2017
    Brian,
    Thanks for the very thought provoking post.
    You have prompted me to start investigating yet another IoT device in my home. The satellite receiver in my living room advertises itself as a WiFi connection point. I have no idea of its security settings, who can see it, who it talks to, or who can access it….

    1. *Gary* October 25, 2017
       At the very least, find the default password and change it. Ideally if you don't use the WAP, disable it.

17. *Brian Failkrebs* October 25, 2017
    Y AXIS LABEL WHY YOU NO HAVE?!?!?!?!?!?!?!

    graph fail. with great fail. in the fail fail.

    1. *Michael Dortch* October 25, 2017
       Always a good idea to read through the earlier comments before posting yours. Might save you a bit of time. Also embarrassment. 🙂

18. BrickerBot sounds interesting, but I agree with the comment against it. There are better and safer ways to "fix" the Internet.

    I would rather see a bot that finds a problem send a notice to the tech contact on the domain name (if there is one), and record the date and time of the problem. After some period of time the bot can return to see if the problem has been fixed, and if not contact the other domain contacts.

    If there is no domain involved, then using IP WHOIS the person or organization for the IP block can be notified. Failing that, I would try The upstream provider. At some point if the problem is not fixed and especially if an IP range contains many problems, that segment should be isolated or added to a black list.

    If we can't fix this, I foresee a future where we have two Internets, one public and one private. The private Internet will be something we pay for where the providers have a way to enforce any rules they see fit to establish. On it, you can expect to be really safe and unoffended with no parental restrictions needed.

19. *Reader* October 26, 2017
    With regard to IOT, no problem for me: I've never trusted the idea of remote access of stuff in my home. If I can remote control, someone else can remote control.

    Our government and utility providers should also remember that if they can remote control something, bad guys can remote control, too.

    Brian, please don't make this site adaptive to devices. I REALLY HATE WHEN WEBSITES feed me their mobile versions, even when I'm using a small screen. And one thing I have liked on this site is that it works perfectly, identically, and consistently with or without Javascript.

20. *PCar* October 26, 2017
    Thanks for the heads up! I did not see Apple's AirPort Listed, so for this I am thankful! It never hurts to be watchful, especially with the current WPA2 Threat, which is mild as compared to your report above! The hit just keep on rolling! Thank heaven for krebsonsecurity.com !

21. *Robert* October 26, 2017
    Considering the new push for money from Amazon with their "Amazon Key", I wonder how long before it becomes a "prime" (pun intended) target for hackers. Not on my wish list but I'm sure the NSA would like all of us to have one, would make it so much easier to keep an eye/ear on us 😉

22. *dcmargo54* October 27, 2017
    Haven't even read the article yet. I just love the little IT men in the pic.

23. *Bob Williams* October 28, 2017
    For God's sake, Brian. "Impactful" is not a word. Your English teacher would have slapped you. Degradation by respected journalists of the English language is as slippery a slope as our slide into the cyber netherworld.

    -Bob

    1. *BrianKrebs Post author*October 28, 2017
       Bob,

       There's nothing incorrect about the word impactful. Can't help it if someone told you some time ago that it was not a word, but I assure you it is. Languages are living organisms that change over time. Maybe if your own vocabulary wasn't so fossilized, you'd recognize this. Merriam-Webster agrees it's a word, btw: https://www.merriam-webster.com/dictionary/impactful

Comments are closed.