Security strategies for defense against botnet infections

By Matthijs Bijman, Max Pigmans, Daniël Vos, Rens Heddes

Introduction

The rise of the Internet of Things (IoT) has lead to widespread use of cheap, poorly secured devices. The volume of and lack of security present in these devices has made them a common vehicle for distributed denial of service (DDoS) attacks performed by botnets. In recent years, several high profile DDoS attacks originated from the Mirai IoT botnet. Since these botnets are mostly used for DDoS attacks or sending spam/phishing emails[1], the owners of these devices do not bear the damages and thus have low incentives to secure their devices[2]. Consequently, most mitigation strategies against botnet attacks are designed for the victims of such attacks[3][4].

Another important actor in the scenario of botnet attacks is the internet service provider (ISP). ISPs are influenced by the Mirai botnet in a few different ways.

First of all, their infrastructure is used for the traffic to and from IoT devices, including scanning, TCP floods, spam e-mails, etc. This causes an increase in bandwidth on their network which can result in additional costs if the ISP must improve their infrastructure to cope with the increased bandwidth.

Secondly, if the network (and specifically the set of IPs) maintained by the ISP becomes commonly known and marked as infected, this will lead to a worse experience for their customers. They may be blacklisted by various services, be required to complete CAPTCHAs very often, etc. This all may lead to customers switching providers.

Lastly, an ISP may face legal consequences if their network commonly participates in DDoS attacks. They may be held responsible for not taking action against the infected devices, especially if they are known to be aware of the problem.

An ISP may therefore be affected in several ways by botnet infections in their network. We will focus our analysis on the impact on infrastructure, since it is the most quantifiable impact, and in our opinion most significant one. In this report we will first discuss why ISPs are the problem owner and how they may affect the issue. We then discuss a metric that can be used to measure security performance. We follow this with a discussion on the strategies available to the ISP, other actors involved, and finally a calculation of the value of applying one of the strategies.

Problem Owner

We believe that internet service providers can be considered one of the problem owners. ISPs are victims of the mirai botnet in various ways, as discussed in the introduction. This means they will benefit from reducing the risk of the problem.

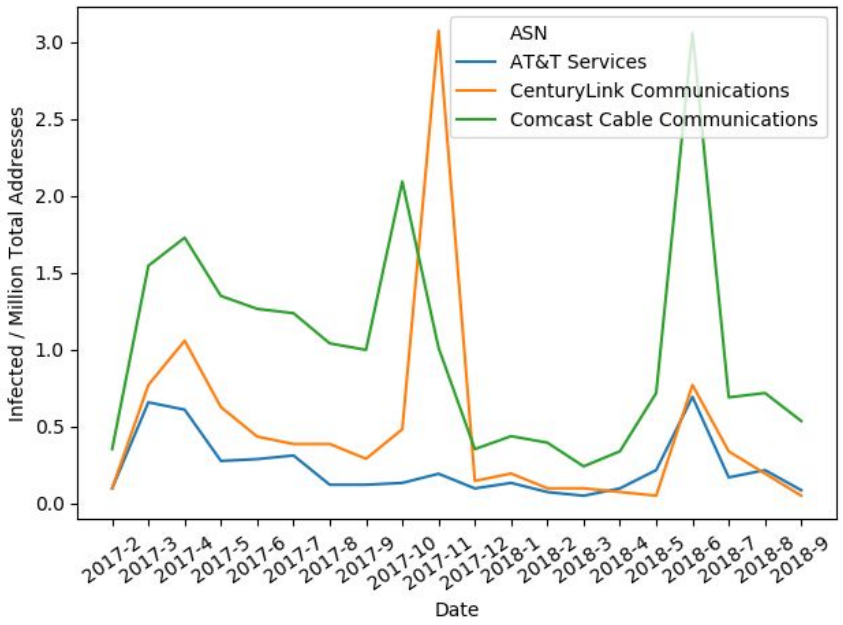
Furthermore, ISPs are likely to be knowledgeable about botnet activity on their network and aware that this causes possible issues, unlike e.g. device owners[2]. They can also measure their performance through the dataset, unlike companies or end-users. This means that they are not only in a position to benefit from the issue being dealt with, they are also aware that the issue exists and could be dealt with.

Finally, due to their control of the network they have the ability to take action against the issue, giving them several strategic options to deal with the problem. These options are further discussed in the section *Risk Strategies for Problem Owner*.

For these reasons, we choose ISPs as the problem owner.

Measuring Security Performance

In order to determine how effective any risk strategies are, we need some method of measuring the performance of our security. We will base this on the metric of “Number of infected IP sightings over time”, as we obtained from the dataset last week. In order to see if we can compare security performance between ISPs, we adjust the metric such we calculate the number of infected devices per ISP. For this comparison, we chose to compare AT&T, CenturyLink and Comcast. We compared AS209, "CenturyLink Communications", with AS7018, "AT&T Services", and AS7922, "Comcast Cable Communications". These have 20,809,984, 83,883,008, and 71,195,904 IP’s respectively, which we used to normalize the number of infections found.



Number of infections per million addresses in various ISP ASNs

The metric is shown in the above image. We plot new Mirai infections per month, per ASN. The number of infected packets over time from our dataset can be interpreted as the infection rate of the mirai botnets. The peaks and valleys in the graph show differences in security performance worldwide. We see several peaks and valleys that are shared between all three, although with different magnitudes. The existence of this trend in all three lines indicates that this is likely related to a change in attacker tactics, and not the security decisions of the ISPs.

Where we do see a security difference between ISPS is in the large peak around October-November 2017. As discussed by Bailey et al., these peaks tend to occur when new exploits are used by the Mirai botnet to infect more machines[6]. While both Comcast and CenturyLink spike up drastically around this time, we see nearly no effect on AT&T's network. The initial and later spikes do appear in AT&T's network. This could indicate a different security policy at the time, or different devices being used that are not vulnerable to the same exploit. Another observation from the graph is that Comcast generally appears to have longer runoffs after each peak than the other two ISPs, which could again be due to differences in policy.

By looking at the above metric the IT admin can get a sense of security performance in the company. One potential issue with this metric is that we it can sometimes be hard to differentiate between moments where less infections take place due to better security, and moments where less attacks take place because of the attacker changing strategy. While we can sometimes see clear peaks and valleys across all ISPs, during less extreme instances we do not know which is the cause of our performance.

Risk Strategies for Problem Owner

The strategies available to the ISP can be subdivided in 4 categories: accepting the risk, transferring the risk, mitigating the risk, and avoiding the risk. In this section we will discuss the feasibility of each of these strategies for our problem owner, and choose the most applicable strategy to analyse in depth. As mentioned before, we focus our analysis on the issue of infected devices impacting the infrastructure.

Risk Acceptance
Risk Acceptance implies accepting the risk for what it is, and deciding that carrying the risk is better than taking steps to transfer, mitigate, or avoid the risk. This can be a sound approach when the risk is very low, or the cost of e.g. mitigation would be too high.

For our ISP, this may be a possible strategy depending on the context of the business. A small, localized ISP may consider the likelihood of devices participating in a DDoS attack insignificant, and the impact low. A large ISP however will not be able to accept the risk, because the impact of an attack on such critical infrastructure will be high. We consider this strategy infeasible for our scenario due to this.

Risk Transfer
Risk Transfer implies moving the risk to another actor, such as an insurance company. Often this is done to exchange a high-impact but low-likelihood risk for a more predictable cost, such as an insurance premium. When an incident takes place, the insurance can be materialized in the form of direct financial compensation, or immaterial aid such as a security assessment, cyber forensics, PR assistance, etc.

Aid in the form of PR assistance, forensics, etc. can be valuable for an ISP, who will likely not have all the necessary expertise in-house. Therefore risk transfer may be an applicable strategy to reduce the impact of attacks on their brand. Reducing the impact on their infrastructure through transferring the risk is not feasible, because the impact cannot be changed after an attack happens.

Risk Avoidance
Risk Avoidance implies avoiding the risk entirely by removing the source of the risk, such as a business activity in a specific country. In this case this would only be possible if the ISP was not connected to the internet, which is of course not possible. This strategy is therefore not feasible.

Risk Mitigation
Risk Mitigation is reducing the risk by implementing additional controls, either lowering the likelihood or limiting the impact. This is a feasible strategy for the ISP, but it is not easy to implement.

Examples of technicals controls that can be used:

- Filtering software to scan traffic for DDoS packets to protect customers and block attacks.
- Updating customer routers to become resistant against typical Mirai scans.

Examples of organisational measures that can be used:

- Crisis protocols to initiate when DDoS attacks take place to consider immediate reaction such as filtering/blocking traffic.
- Contracts with other ISPs to allow rerouting traffic if the infrastructure cannot handle a DDoS attack.

Risk mitigation may be effective in our scenario, as it can directly lead to better service for customers. Influencing traffic can also have negative effects, e.g. when packets are wrongly blocked, so this is an additional risk that may need to be analyzed.

Conclusion
From our analysis, risk mitigation and risk transfer are two applicable strategies for the ISP. Accepting the risk is not possible, because the impact of large DDoS attacks is too high. Avoiding the risk is also not possible, because it would imply stopping all business.

The best strategy should be a combination of mitigation and transfer. This is because mitigation will lead to better service to customers, while transfer is effective when an attacker still manages to impact the network. We will discuss the exact effectivity of mitigation in more detail later.

Other Actors

Due to the distributed nature of botnets, there are several other actors that have some relation to the security issue. Any actor that has influence on the operations of the botnet (DDoS) and its existence (infected devices) could influence the issue. We briefly discuss below 5 other actors that we believe are most relevant to the problem.

- *IoT device owners* impact the problem by having their devices become part of the botnet, since they likely do not know and/or care about being infected. Device owners generally employ two main methods of dealing with the risk of being infected. Firstly, they can mitigate the risk by updating their IoT devices to the newest firmware and changing from default passwords. Secondly, they can accept the risk and keep using unsafe IoT devices. While they could stop using insecure IoT devices to avoid the risk altogether, this is generally not done because the device owners face few consequences and may be entirely unaware of the problem. Because of this, the risk is usually accepted, which means other actors must deal with the problem[2].

- *Governments* can indirectly influence the botnet problem through legal and policy decisions. For instance, forcing risk mitigation by making policies to make sure device manufacturers use properly randomized default login credentials for each device, or obligate ISPs to actively stop malicious traffic. While governments could also avoid the risk by banning insecure IoT devices, this is not feasible. It is however feasible for the government to accept the risk by doing nothing.

- *Device manufacturers* influence the botnets by selling insecure devices. Manufacturers can influence the risk in two ways. Firstly they could improve their security by configuring strong default passwords, by for example randomizing them for each device. This would mitigate the main method of Mirai to infect new devices. Alternatively, and common in practice, is that they simply accept the risk and keep selling insecure devices. Making them more secure often leads to less intuitive or user-friendly products, which is a more important factor than security. Manufacturers can not avoid the risk since selling the devices is their core business.

- *DDoS attack victims* are directly impacted by the Mirai botnets by being the target of an attack, which is likely to make their service unavailable. They can impact the problem in a few different ways. Firstly purchase a DDoS protection service to transfer the risk to the protection company. Secondly they can accept the risk and just let their service become unavailable during an attack. Risk avoidance is likely not possible because most targets use their internet service for their core business.

- Finally, the *attacker* is obviously involved, but has goals opposite to that of the IT admin and is therefore very unlikely to take action to address the risk in any way but accepting it.

Mitigation

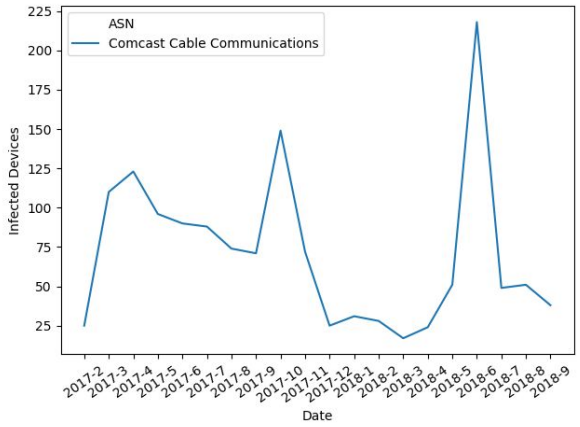
We will discuss the mitigation from the perspective of Comcast, a large ISP in America. As discussed before, we consider the fact that their infrastructure must deal with additional traffic generated by the machines during DDoS attacks to be the most significant issue for an ISP. We assume that the ISP provides routers to its clients. Routers are one of the primary target devices of Mirai [5].

We will first analyse the number of infections in a typical ISP network to understand the size of the problem. We then gather data about the commonality of DDoS attacks, and the size of the traffic sent by a typical infected device during a DDoS attack. From this we compute the botnet data sent in the ASN as a whole. Using an estimate of the price of transmitting data for ISPs we compute the costs caused by infections in the network, normalized to the number of devices. We then determine the cost and effectiveness of mitigation measures, and compute a ROSI.

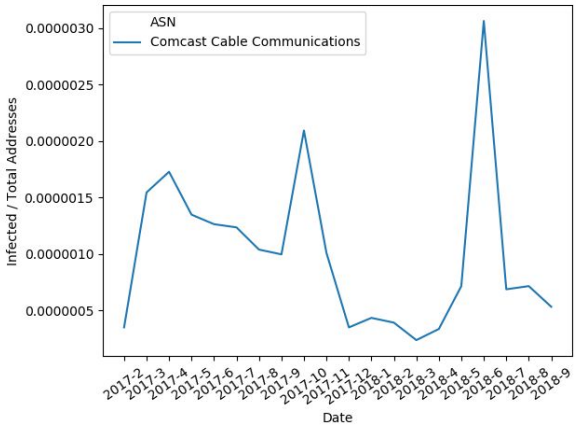
A typical ISP network

We have chosen a large ASN from the dataset known to correspond to Comcast as context for our calculations: AS7922 “Comcast Cable Communications”. We will assume that this ASN represents a significant portion of the Comcast customer base. We know the size of this ASN to be 71,195,904 IP-addresses [7], of which a large portion are likely addresses that may be infected by Mirai, since PCs and other connected devices often share a single IP address behind a Router/NAT-device.

From the dataset, we have discovered the number of infected hosts within the ASN over time and have visualized this, also normalized by Comcast ASN size, below:



Infected devices in Comcast ASN



Infected devices in Comcast ASN (normalized)

DDoS attacks and data costs

According to Fong et al. [8]**,** the average amount of bandwidth used by an infected device during an hour of a UDP flood DDoS attack is 6.8 GB. According to Antonakakis et al [10], the number of ddos attacks performed by the mirai botnet is 15,194 in a 5 month period, which equates to approximately 36,000 annual DDoS attacks by Mirai botnets. According to Kaspersky securelist[9], the average DDoS attack in the fourth quarter of 2018 is 218 minutes, the standard deviation was roughly 70 minutes. However, not each infected device takes place in each DDoS attack. We will estimate the ratio of participating devices based on available numbers during the large KrebsOnSecurity attack. At the time, around mid September 2016, Antonakakis et al. [10] estimate that there were around 275,000 infected devices in the Mirai botnet. According to a retrospective by Brian Krebs [11], around 24,000 unique devices participated in the attack. This would give a ratio of $\frac{24{,}000}{275{,}000} = 0.087$ chance for a device to participate in an attack. We consider this to be on the upper end of chance, since this was a very large attack and most attacks are much smaller. However, since we lack data on this we will consider a normal distribution

centered around this value. Combining these numbers we compute the total data usage in the ASN per infected device:

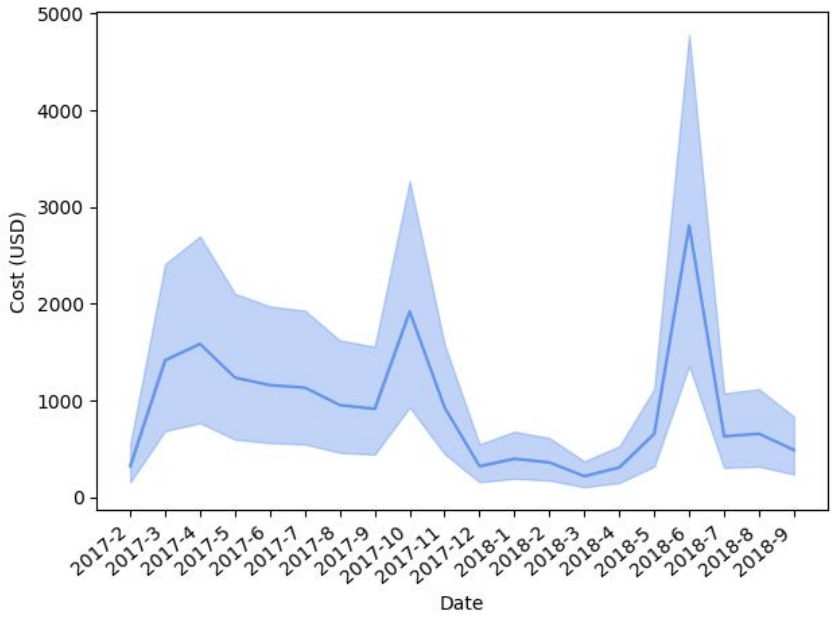
$$annual\ DDoS\ attacks\ *\ average\ DDoS\ duration\ *\ hourly\ DDoS\ data\ rate\ *\ participation\ chance$$
$$= 36000\ *\ \frac{218 \pm 70}{60}\ *\ 6.8\ *\ 0.087 \pm 0.025\ = 84,521 \pm 47,083 GB\ per\ year\ per\ device$$

Since in our analyses we look at Mirai infections and costs on a monthly basis we should also calculate the monthly DDoS GB usage per device:

$$84,521 \pm 47,083 GB\ per\ year\ per\ device\ /\ 12\ = 7,043 \pm 3,923\ GB\ per\ month\ per\ device$$

Cost for the ISP

With the data usage in the ASN, we now only need an estimate for the cost per quantity of data to compute the cost for the ISP caused by infected devices. The cost of transferring data is a difficult value to estimate, because internet traffic costs and contracts are usually decided over bandwidth, which is the maximum data transfer rate per unit of time. As long as all data of the DDoS attack fit within the bandwidth negotiated between the ISP and higher tier ISPs, there will be no issues transporting the data. The attacks may still lead to costs however, either through simple operational costs such as electricity costs, or by leading the ISP to increase the capacity of the network. To compute a rough estimate of the operational costs, we take the consumer costs of 50Gb, which is 10$ for Comcast Xfinity[12]**,** and assume that the ISP has a profit margin of roughly 99%. This means 1Gb costs them 0.002$ to transfer. The total cost of the infected machines in the ASN then becomes:



Costs of the losses (in USD) that Comcast can incur per month. The middle line is the expectation, the blue area represents one standard deviation away from the expectation.

Mitigation options

One way of mitigating the risk of the botnet problem for Comcast is patching the modem/routers of their subscribers. Comcast is a provider which has the router as a service included in its subscription. Most of the subscribers use the routers supplied by their ISP, therefore Comcast can update the software on the provided and already installed routers at the subscribers to filter and block malicious botnet traffic and thereby stop DDoS traffic from entering Comcast's network infrastructure and thus reducing the loss incurred by a DDoS attack.
Comcast's ASN contains 71,195,904 IP-addresses of which most will be routers so let us assume that half of these IPs are routers: $71,195,904 * 0.5 = 35,597,952$. Assuming it costs Comcast approximately 0.001 USD to update a router, then patching all Comcasts's routers would cost approximately $35,597,952 * 0.001 = 35,598\ USD$. Since the Mirai botnet simply guesses passwords to get control over a device, we assume the patch will be 99% successful in blocking Mirai infections.

ROSI

Now that we know the losses that Comcast can incur over time, the costs for a mitigation option and its success rate, we can calculate the Return on Security Investment (ROSI) for this mitigation option. Since the cost follows a probability distribution, we will calculate the ROSI three times, once for the expectation (middle blue line in cost plot), once for one standard deviation higher (upper blue line in cost plot) and once for one standard deviation lower (lower blue line in cost plot). The ROSI is given by the formula:

$$ROSI = \frac{Cost\ of\ Losses * Mitigation\ Ratio - Cost\ of\ Solution}{Cost\ of\ Solution}$$

Since our loss cost estimates are given as a time series, we will look at a time horizon from 2017-2 until 2018-9 and sum up the losses in this time interval. Our three ROSI estimates are then:

$$ROSI_{Expected} = \frac{17,952 * 0.99 - 35,598}{35,598} * 100\% = -50.1\%$$

$$ROSI_{Lower} = \frac{8,685 * 0.99 - 35,598}{35,598} * 100\% = -75.8\%$$

$$ROSI_{Upper} = \frac{30,532 * 0.99 - 35,598}{35,598} * 100\% = -15.1\%$$

From the ROSI estimates we can see that the return on investment is negative in all cases, therefore it would not be wise to invest in this mitigation for countering these losses alone.

Other potential costs

Clearly the costs of infected devices in the network are very low for the ISP. This corresponds to our earlier hypothesis and general knowledge, that the victims of DDoS attacks bear the largest cost by far. ISPs are therefore not incentivized to combat the issue. In this section we discussed the costs of the increased bandwidth usage, but we also mentioned a few other issues that may lead to costs, including reputation damage leading customers to switch, or legal issues causing fines.

We do not believe that customers are, on average, knowledgeable enough to know about the issues caused by botnet infections, nor do we expect them to switch providers due to the rare issues caused if their router is infected while they are unable to fix this without help from their ISP. We therefore do not expect this to be a more significant issue than the bandwidth usage.

We also do not believe that legal issues are a significant cost, since no existing cases of legal action against ISPs for not filtering DDoS attacks could be found.

Conclusion

We identified ISPs as the problem owner for infected devices in their network since ISPs would benefit from removing the problem, have the possibility to influence the problem, have the awareness that the problem exists. We discuss a metric based on the dataset that the ISP can use to measure their performance of dealing with infections. The main cost for the ISP was analyzed to be the additional load on their infrastructure. We analyzed possible strategies an ISP could apply to fix the problem, and concluded that mitigation was the most effective approach. We calculated the various costs the problem created for the ISP based on the infection rate of the dataset, as well as the solution costs. The resulting ROSI shows us that it is not worthwhile for the ISP to attempt to solve the problem. This aligns with our expectations, since the actor with the most significant costs from a DDoS attack are the victims of the attack. The variable costs of data transfer for the ISP are generally very low, since most of their investments happen in creating the infrastructure, i.e. constant costs. Our final recommendation for an ISP purely considering the economic aspect is to not invest in fixing this problem.

References

[1] Yury Namestnikov, “The economics of Botnets”.

[2] James A. Jerkins, “Motivating a Market or Regulatory Solution to IoT Insecurity with the Mirai Botnet Code”.

[3] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013.

[4] M. Özçelik, N. Chalabianloo and G. Gür, "Software-Defined Edge Defense Against IoT-Based DDoS," *2017 IEEE International Conference on Computer and Information Technology (CIT)*, Helsinki, 2017, pp. 308-313.

[5] Biggs, John (Oct 10, 2016). "Hackers release source code for a powerful DDoS app called Mirai". TechCrunch. Retrieved 19 October 2016.

[6] Bailey, M., Cooke, E., Jahanian, F., Xu, Y., & Karir, M. (2009, March). A survey of botnet technology and defenses. In *2009 Cybersecurity Applications & Technology Conference for Homeland Security* (pp. 299-304). IEEE.

[7] ipinfo.io on AS7922 Comcast Cable Communications, LLC. Retrieved on October 5th, 2019 from https://ipinfo.io/AS7922

[8] Fong, K., Hepler, K., Raghavan, R., & Rowland, P. (2018). rIoT: Quantifying Consumer Costs of Insecure Internet of Things Devices. University of California Berkeley, School of Information Report. Retrieved from: https://groups.ischool.berkeley.edu/riot

[9] Kaspersky Securelist. (2019, Feb 7). DDoS attacks in Q4 2018. Retrieved from https://securelist.com/ddos-attacks-in-q4-2018

[10] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J. & Kumar, D. (2017). Understanding the mirai botnet. In *26th USENIX Security Symposium (USENIX Security 17)* (pp. 1093-1110).

[11] Krebs, B. (May, 2018). Study: Attack on KrebsOnSecurity Cost IoT Device Owners $323K. Retrieved from https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/

[12] cabletv.com. Comcast Xfinity Internet Plans. Retrieved on October 5th, 2019 from https://www.cabletv.com/xfinity/internet