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 and lack of security present in these devices has made them a common vehicle for DDoS attacks performed by botnets. In recent years, several high profile DDoS attacks originating 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].

A specific example of such a victim is an IT admin of a company with IoT devices as part of their network. The IT admin is incentivized to keep their network free network free of infected software to prevent private data from being leaked from within their network, and to prevent further spread of infected software within their system. In this report we will clarify what security strategies such an IT admin can apply to prevent the company network from becoming infected.

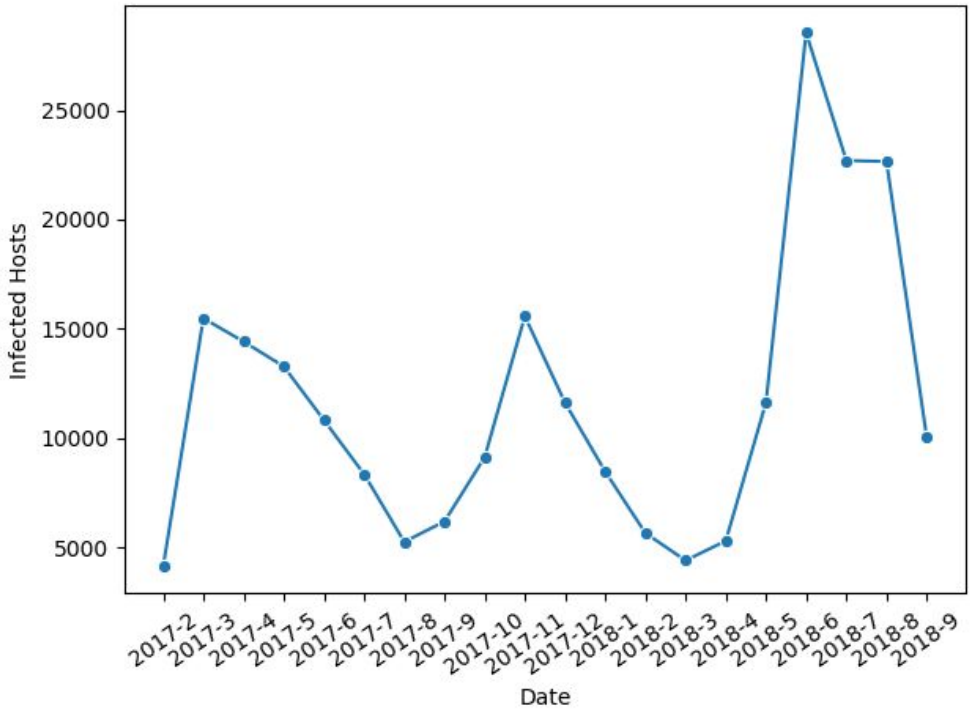
Problem owner

We believe that the IT admin is the primary problem owner. The IT admin is both aware of the problem and has an incentive to deal with it, since botnet infections pose a danger to the company. He also has a large potential impact on the problem. For example, the IT admin can mitigate the risk of infection without requiring drastic changes to the company, such as the removal of devices altogether. The first of these mitigation strategies is patching vulnerable devices, rendering them safe from infection. Additionally, or when patches are not available, the IT admin can try to defend on a network level. He can do this by either disconnecting the IoT devices from the internet altogether, although this might not always be possible, or by filtering Mirai-like packets [8] completely.

Because the IT admin is aware of the problem, incentivized to address it, and capable of doing so we consider him to be 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.



The metric is shown in the above image. We plot new Mirai infections per month. The number of infected packets over time can be interpreted as the infection rate of the mirai botnets. The peaks and valleys in the graph show differences in security performance worldwide. A similar metric but limited to the IT admin’s company works similarly. We see the spikes in november 2017 and june 2018, which share some similarities with the spike discussed in size analysis of the mirai botnet in [9]. That case was a new exploit that was used by the mirai botnet to infect more devices, a similar thing could be the case for the peaks in november 2017 and june 2018.

By looking at the above metric, and ideally comparing it to the same metric containing only infections in the company itself, the IT admin can get a good sense of security performance in the company. One potential issue with this metric is that we cannot differentiate with the given dataset between moments where less infections take place due to better security, and moments where less attacks take place because of the attacker instructing the botnet to not infect. This only works as a good indicator of security performance if the influence from other factors than security are consistent, which we do not know in the case of botnets.

Risk Strategies for Problem Owner

The strategies available to the IT admin can be subdivided in 4 categories: accepting the risk, transferring the risk, mitigating the risk, and avoiding the risk.

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 IT admin, accepting the risk is not a feasible approach. The likelihood of an infection is very high, as shown by the increasing number of infected IoT devices worldwide. Moreover, the impact of an infection can be high, since the confidentiality and integrity of personal data may be affected. This exact risk depends on the types of IoT devices, and the specific adverserial actor.

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. Insuring cyber risk is generally difficult, and we believe that in this case insuring against botnet infections is not feasible. The damages caused by an infection are not easily quantifiable with certainty, so finding an insurer willing to cover this risk may not be possible.

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 IT admin. There are many ways in which the risk of a botnet infection can be mitigated:

- Proactive technical controls, such as firewalls, can block malicious packets and reduce the likelihood.
- Reactive technical controls such as Intrusion Detection Systems (IDS) can monitor the network for suspicious traffic, and spot devices that have been infected to reduce the impact.
- Organizational controls can ensure that devices do not have easily guessable or default passwords, to reduce the likelihood.
- Organizational controls including protocols to clean up infections to reduce the impact.

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 imply removing IoT devices from

the company network entirely. We do not think this is feasible, because the IoT devices may be a critical piece of infrastructure.

Conclusion
We think Risk Mitigation is the most feasible strategy for the IT admin. This is because the Mirai botnet is mostly a threat to unsecured devices, which can be mostly fixed with technical and organizational controls. Other strategies are less feasible due to the intangible damages caused and widespread occurrence of botnet infections.

Other actors

Due to the distributed nature of botnets, we identify quite a few other actors that have some relation to the security issue. Any actor that has influence on the botnets operations and existence could influence the issue.

- Within the IT admin's company, *other company employees* can impact the IT admin's capability to address the issue. For example, management imposes budget restrictions and directs overall company direction. This can impact the options available to the IT admin.
- The *employees who rely on these IoT devices* to do their job likely have a say in which devices they use, and generally will care more about their job than overall security.
- *IoT device owners outside the company* impact the problem by having their devices become part of the botnet, since they likely do not know and/or care about being infected.
- *ISP's* are involved since the botnet traffic passes through their infrastructure. They could attempt to filter out Mirai-like packets, but are generally not impacted themselves directly, so have little incentive to do so.
- *Governments* can indirectly influence the botnet, through legal and policy decisions.
- *Device manufacturers* influence the botnets ability to spread by creating more secure devices.
- Finally, the *attacker* is obviously involved, but has goals opposite to that of the IT admin.

Other risk strategies (TODO)

Plan: For each of the actors listed above, list what risk strategies they currently commonly employ.
E.g. (but not in table format)

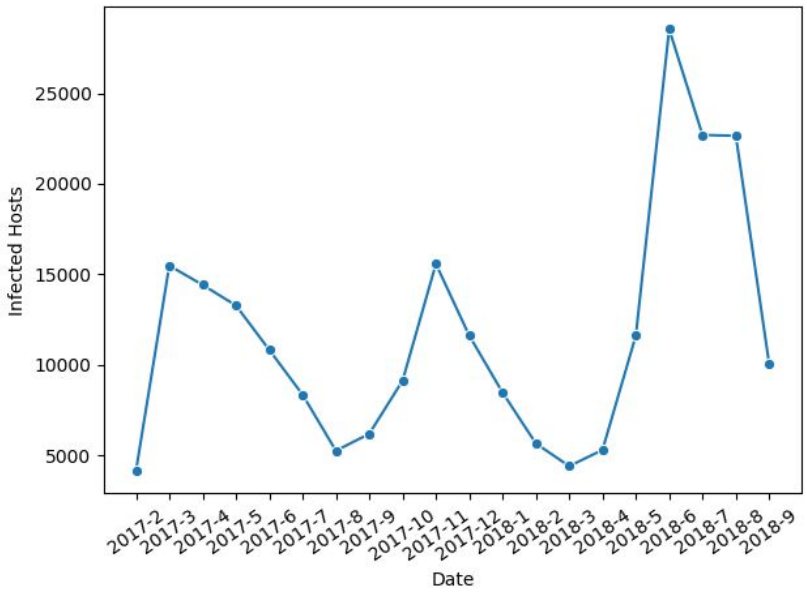
	Acceptance	**Transfer**	**Mitigate**	**Avoid**
Government	Not a priority to government	No	Implement regulation so to encourage secure devices and/or fixing infections	Ban insecure devices

Mitigation

The Mirai botnet infects primarily devices such as network cameras and routers [6], therefore in estimating the number of vulnerable devices worldwide we will look at the amount of these devices that are in use.

The amount of installed network cameras is growing quickly since 2012 [5], namely in 2012 there were about 19,000 and in 2016 118,000. The last information on installed cameras we could find was from 2016 however. If we continue the trend that we see from 2012 until 2016 we can estimate the amount of installed network cameras to be approximately 170,000.

Next we estimate the amount of home routers that are in use worldwide. We can make an assumption that behind every router there will be on average 4 people. Since there were about 4 billion internet users in 2018 [7] we estimate that there are approximately 4 billion / 4 = 1 billion home routers active. Given that there exist many more home routers worldwide than there are network cameras installed we can, for now, ignore the installed camera estimate and use that there exist approximately 1 billion devices that are vulnerable to the Mirai botnet.



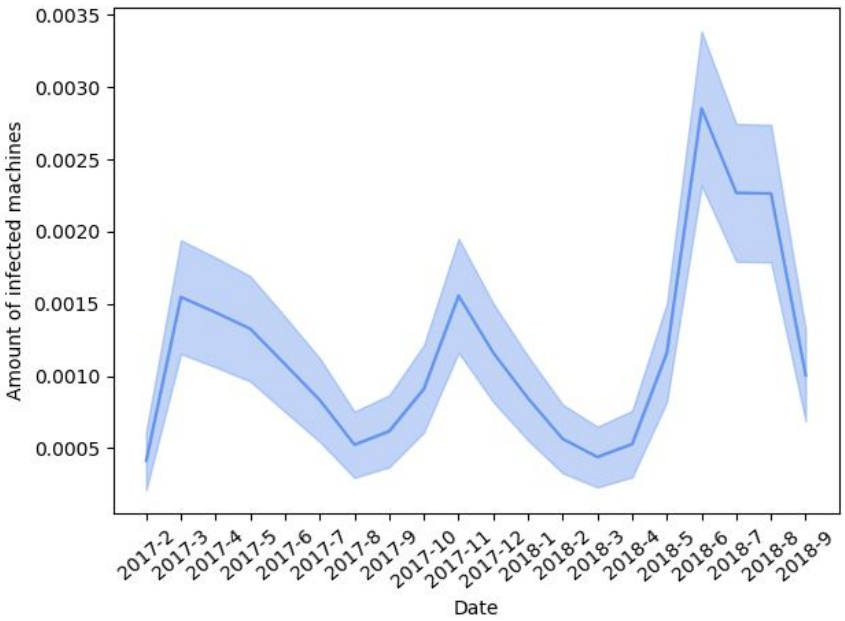
Given the previous estimate and our metric showing Mirai's amount of newly infected hosts over time (figure above), we can roughly predict the likelihood of a vulnerable device being infected by Mirai over time. We assume that the likelihood of infection is directly proportional to the amount of devices that are being infected at that time so we estimate the likelihood following:

$$P(device\ infected) = \#infections / \#devices$$

Although we can now estimate the probability and possibly costs of a device being infected, our actor (a company) will likely run many more devices than one, devices that each have a chance of being infected. Assume that our actor runs 100 vulnerable devices within their company, we will get the following binomial distribution at each time interval:

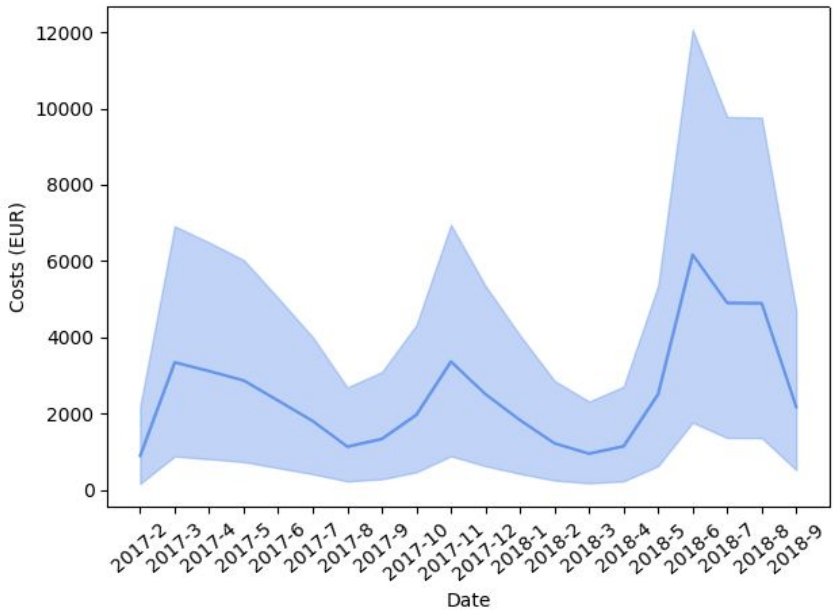
$$B(100,\ P(device\ infected))$$

Below we plot the expected amount of infected machines (out of 100) over time, with the blue region being one standard deviation from the expectation.



We can see that since the probability of infection is so low, the amount of our 100 devices that we can expect to be infected is also very low. The plot below becomes more interesting when we factor in the potential costs/damages for the company. The direct costs associated with increasing resource use by infected devices is not significant, research has estimated this to be about 13.50 EUR per device [10]. However, we can imagine that if a company's router is infected by Mirai and it handles private data, then the company might also incur damages from e.g. a data breach or man-in-the-middle attack [11].

It is very hard to put an accurate number on the cost of having a router hacked since there are so many possible attack vectors but each not being very likely, therefore we will estimate the costs with a probability distribution. Malware infections were the most costly type of cyber attack in 2017 [12] costing on average 2,364,806 USD = 2,161,409 EUR for companies but varying by incident (3.82 million USD = 3.49 million EUR and 1.24 million USD = 1.13 million EUR are also reported). We model this distribution of costs by a normal distribution with mean 2,161,409 EUR and standard deviation 1.40 million EUR. In the plot below we visualize the expected costs over time by multiplying our distribution over number of infected machines from the previous plot by the distribution of costs per infected machine.



Now say that it is 2017-9, we want to mitigate this risk as a company and we decide to use a firewall for mitigation that can block 95% percent of infections. The firewall itself costs 30,000 EUR per year. We can use the costs that we have determined to compute an approximation of the ROSI (Return on Security Investment), it is given by the following formula:

$$ROSI = \frac{ALE * mitigation\ ratio - solution\ cost}{solution\ cost}$$

Where ALE is the annualized loss expectancy. We know the mitigation rate (95%) and the solution cost (30,000 EUR) and we can calculate the ALE by integrating over the 12 months cost expectation following 2017-9. Summing the cost expectations in the period 2017-9 until 2018-9 results in an ALE of 32,819 EUR. Therefore the ROSI of our proposal of mitigation by purchasing a firewall is:

$$ROSI = \frac{32{,}819 * 0.95 - 30{,}000}{30{,}000} = 0.039\%$$

With the resulting ROSI of 0.039% the company does not lose money on the mitigation, however the investment returns are so minimal that ROSI alone is not enough justification for spending on this solution. The company needs to evaluate if they want to put in the working hours needed to set up this firewall solution for the sake of security itself.

Conclusion (todo)

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] Rise of Surveillance Camera Installed Base Slows. (2016, May 9). Retrieved from https://www.sdmmag.com/articles/92407-rise-of-surveillance-camera-installed-base-slows.

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

[7] Dubras, R., Underwood, L., Valentine, O., & Lore Oxford. (2018, January 30). Digital in 2018: World's internet users pass the 4 billion mark. Retrieved from https://wearesocial.com/blog/2018/01/global-digital-report-2018.

[8] Bad Packets Mirai database, https://mirai.badpackets.net/about/

[9] 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.

[10] Chirgwin, R. (2018, May 19). Mirai botnet cost you $13.50 per infected thing, say boffins. Retrieved from https://www.theregister.co.uk/2018/05/09/berkeley_boffins_infect_things_with_mirai_in_a_good_cause/.

[11] Atwood, J. (n.d.). Coding Horror. Retrieved from https://blog.codinghorror.com/welcome-to-the-internet-of-compromised-things/.

[12] Ponemon Institute LLC, Accenture. (2017). *2017 COST OF CYBER CRIME STUDY*. Retrieved from

https://www.accenture.com/t20170926t072837z__w__/us-en/_acnmedia/pdf-61/accenture-2017-costcybercrimestudy.pdf