Does the joint effort make a difference

The role of joint efforts in the Mirai botnet mitigation process

Radinka Yorgova

1 Abstract

This report is provoked by the data mirai badpackets [1]. First we define the main security issue raised from the data and list the first few attacks based on Miray botnet as an evidence for the importance of the security problem. Then we discuss briefly the possible problem owners, strategies, costs and benefits in order to give a general idea for the complexity of the problem to mitigate the security issue. Further we go through few extensive studies on the same security issue. To be able to analyse the relation between the different initiatives against the Mirai botnet spread we introduce a new measure. Data analysis proves that there is a relation between the infection rate per country and the joint effort in the mitigation process coming from different organizations on national and international level.

2 Introduction

The security issue which raises from the mirai badpackets [1] dataset is the spreading of the Mirai malware by infecting new IoT (Internet of Things) devices and increasing the size of the corresponding botnet. Each infected device becomes a remotely controlled bot which scans the Internet for other vulnerable IoT using bruteforce attack, like a table with default factory login passwords, to get the Mirai malware on the target device. Then the infected bots synchronized all together, can be used by the botnet owner to perform different types of attacks such as Distributed Denial of Service (DDoS), spam or phishing campaigns.

Here are the first few Mirai attacks:

- September 21st, 2016, few massive distributed denial-of-service (DDoS) attacks temporarily crippled Krebs on Security. According [4] the initial attack on Krebs exceeded 600 Gbps in volume which is among the largest on record.

- September 21st, 2016, DDoS attack on a security researcher's blog website with the record of 620 Gpbs stream [3].
- October 21st, 2016, Dyn, an infrastructure vendor, which serves Internet's top giants, such as Netflix and Twitter, has been attacked by a series of DDoS attacks [2].
- October 26th, 2016, Mirai has enabled unsophisticated adversaries to deliver more than 1.1 Tbps of malicious traffic to the French Internet Service Provider, OVH, on simultaneous DDoS attacks [7].

It is known that Mirai malware targets are mostly CCTV cameras, DVRs, and home routers. The source code for Mirai has been published by its author on github.com website as an open source around October 10th, 2016 [6]. Since the release the number of IoT infected devices has doubled in just two weeks. So now, after the creators have stopped, there are still attackers who use or even more - evolve this code. Therefore the security issue remains and security threats are still among the most urgent.

Mirai botnet can also cause a number of issues not directly related to security concerns, such as losses in computational powers of systems, waste of power, latency and bandwidth issues. In [5] the authors consider a different aspect of IoT botnet - the risk to manipulate the power demand in the grid. The high wattage devices, such as air conditioners and heaters, give an unique ability to adversaries to launch large-scale coordinated attacks on the power grid. This is a new class of potential attacks on power grids via IoT that can use a botnet like Mirai in order to manipulate the power demand in the grid. This aspect in fact raises the level on the security threats.

A very recent report [20] shows that smart irrigation systems, a new type of green technology and IoT device can be used by attackers to target urban water services. The authors present a distributed attack model using a botnet of commercial smart irrigation systems. They calculate that a standard water tower can be emptied in an hour using a botnet of 1,355 sprinklers and a flood water reservoir can be emptied overnight using a botnet of 23,866 sprinklers.

These examples show that the mitigation of the considered security issue needs a broad and urgent consideration.

Further in this report we discuss briefly possible problem owners of the security issue, their mitigation strategies, costs and benefits connected to a security investment.

Then in Section 4 we make an overview of few extensive research reports concerning our security issue. Thereafter we define the main research question, objectives and hypothesis. The last section contains our research in few steps: observation, new measure, data analysis and results. At the end we discuss the results and open questions for further research.

3 Problem owners, strategies, costs and benefits

The problem owner of the main security issue discussed above is the person or persons who are responsible or who are most affected by this issue. Possible problem owners are the owners of the infected IoT devices, the manufacturers of these devices, the Internet Service Providers (ISP's) with a large number of bots in their network, and the government. For each of them, beside the ISP's, we discuss shortly their strategy for mitigating the security risk, costs and benefits. The ISPs are described in more details in order to give a general idea for the complexity of the problem for increasing the security level in order to mitigate the the security issue, namely spreading of the Mirai malware.

Owners of infected IoT devices: they are not all likely to take steps against the botnet. In most of the cases they are not aware that their devices are compromised, would not know how to clean them up, and moreover their loss is mainly slightly slower device. Therefore their risk strategy most often is a risk acceptance. The strategy could be different if the botnet has been used for spreading ransomware, when the loss is much higher.

There are still owners who are willing to mitigate the risk of the botnet. On [8] there are listed few steps which one can apply in order to clean up the IoT. All the steps beside one are risk mitigation steps. The exception is discontinuing the use of the infected device which can be classified as risk avoidance.

Device manufacturers of the infected IoT: due to the fact, that more and more IoT devices are purchased, there is a bigger threat for the botnets to increase their size. The manufacturers of these IoT devices need to take more security measurements to prevent attackers from infecting their devices [9]. All of the measures will be risk mitigating. A simple action would be to stop using a default login. Of course, there always will be some manufacturers which will not take these steps, in which case we have risk acceptance.

In contrary to the need of increasing the security level of the IoT, device manufacturers do not have incentives to make security investments implementing security measurements. That is because such an investment will bring them only costs with relatively little benefit and at the same time they are not victims of a botnet attack. Unless this becomes mandatory by law/regulations, which can create incentives for the manufacturers.

ISP's floated with infected devices: ISP's are security providers, as their core business is IT and security comes second to their core business. Therefore their decisions are business-driven. Here are few possible risk strategies for the ISPs as a problem owner:

- Risk reduction - Investing in detection and blocking of malicious traffic, reducing the security issue and decreasing the loss incurred by the security issue.

- Risk reduction - Investing in awareness campaigns of malware infections for device owners, thus tackling the source of the problem and reducing the security issue.

- Risk reduction - Initiating information sharing between the ISP on a

national level. Information disclosure helps in remedying information asymmetries.

- Risk acceptance - Doing nothing against the spread of the malware, accepting the risk; accepting increased cost and possible reputation damage.

- Risk transfer - Charging costumers based on the traffic they generate, thus transferring the risk of extra traffic related cost. This does not address the risk of reputation damage which in this case is accepted.

- Risk transfer - Seek insurance for any botnet/malware related damages, thus transferring the risk to an insurer.

Risk avoidance is not an option for the ISP as the security issue is embedded in their core business: providing Internet access.

Implementing the first risk reduction strategy for mitigation the risk of Mirai malware brings different type of costs. In [10] we see a good overview of the general costs and benefits for IT and Non-IT companies which choose to make a security investment (Figure 1).

Figure 1: Comparison of IT and Non-IT costs and benefits

Security Strategy	IT Impacts	Non-IT Impacts
Proactive	• Cost: Cutting-edge hardware and software (likely more expensive than well-established solutions) • Cost: Information gathering, installation, debugging, and maintenance costs (labor)	• Cost: User inconvenience
	• Benefit: Decreased need for reactive labor	• Benefit: Regulatory and reputation benefits • Benefit: Fewer business interruptions
Reactive	• Cost: Infrastructure (mostly labor) resources needed to respond quickly and effectively • Cost: Resources (labor) needed to repair damaged systems and data	• Cost: More events, and thus a likely increase in down time • Cost: Potential damage to reputation
	• Benefit: Decreased investments in proactive (risky) solutions	• Benefit: User convenience • Benefit: Flexibility to accommodate diverse business environments

When an ISP decides to implement this security investment, this could result in the following costs:

- **direct costs**

- costs for acquisition of the detection and blocking hard- and software on *end users*. They are mainly *one time cost*;

- costs for acquisition of Network Intrusion Detection Systems (IDS). This system is for *the ISP use* and also *one time cost*;

- costs for installation and maintenance of the security system (mainly labor hours)- *one time cost*;

- costs for maintenance of the security software/hardware (mainly labor hours)- *continuous*;

- costs for training of the employees and the change of protocols- *continuous*.

- **indirect costs**

- forgotten passwords after enforced changes (time lost);

- incompatibilities between security mechanisms;

- missed opportunity costs costs because of enforce confidentiality of information (denied access to information) that is relevant for business decisions and because of this missed opportunities.

The ISPs themselves are not the victim of such botnet attacks. We have listed the costs connected to a security investment implementing the first strategy. In Figure 1 we see that the benefits are minor in comparison to the costs. The main benefit for the ISP is prevention of a potential reputation damage. Therefore the ISPs do not have incentives to implement such a security investment, unless to tackle this security issue becomes mandatory by law/regulations.

Government - the government cannot influence the botnet spreading directly, except for their own infected devices, but they can make a difference indirectly. We saw that ISPs and device manufacturers do not have incentives to implement the security investments. The government have the authority to introduce additional regulations and to initiate changes in the law which oblige the manufacturers to secure their products and the ISP's to secure their network against botnet malware spread [11]. Then ISPs and device manufactures are enforced to apply security investments. This is also called indirect intermediary liability.

An example of this, is the blocking of port 23 at nighttime by the Korean government. These actions of the government will also be a risk mitigating strategy.

The government itself can be a victim of botnet attacks but besides that, the government has the responsibility to ensure the security of the network ecosystem. An indirect benefit for the government is better reputation.

Attackers - the attackers play also a very important role in the spreading of the botnet, but they are the creator of the security issue and therefore they are not considered in this report.

4 Literature overview

Now having the security issue and the description of the complexity of the problem in regards to the main actors and their mitigation strategies, we will go through few publications which are focused on the same security issue.

Since 2005, the security community has been working to understand, mitigate, and disrupt botnets. Since the first DDoS attack by Mirai (late 2016), it has been in the front line of the studies. Researchers have collected measurements about which networks are stable against malware like Mirai, which are not; how do they differ; how can this security issue be mitigated. There is a large amount of publications on this security issue. In general the studies go into *technical* and *not technical* category. Regarding the first type there are many working groups from the academy as well as from the industry which research is focused on creating new devices or software for detecting and blocking malware which main targets are IoT. An example for such a project is the new device Manufacturer Usage Description (MUD) - an authoritative identifier of IoT devices on the network. It allows manufacturers to expose the identity and intended use of their devices. It provides network operators with a tool to limit the network access of IoT devices. The MUD allows a vendor to specify the network access requirements of a device. In fact, MUD is a direct protection of the device against a mileware like Mirai and therefore a tool for mitigation of our security issue.

Recently Schutijse has published the results of his study over MUD[13]:

- it is possible to successfully generate profiles that can be applied to devices (i.e. enforcing a profile and prevention are verified);

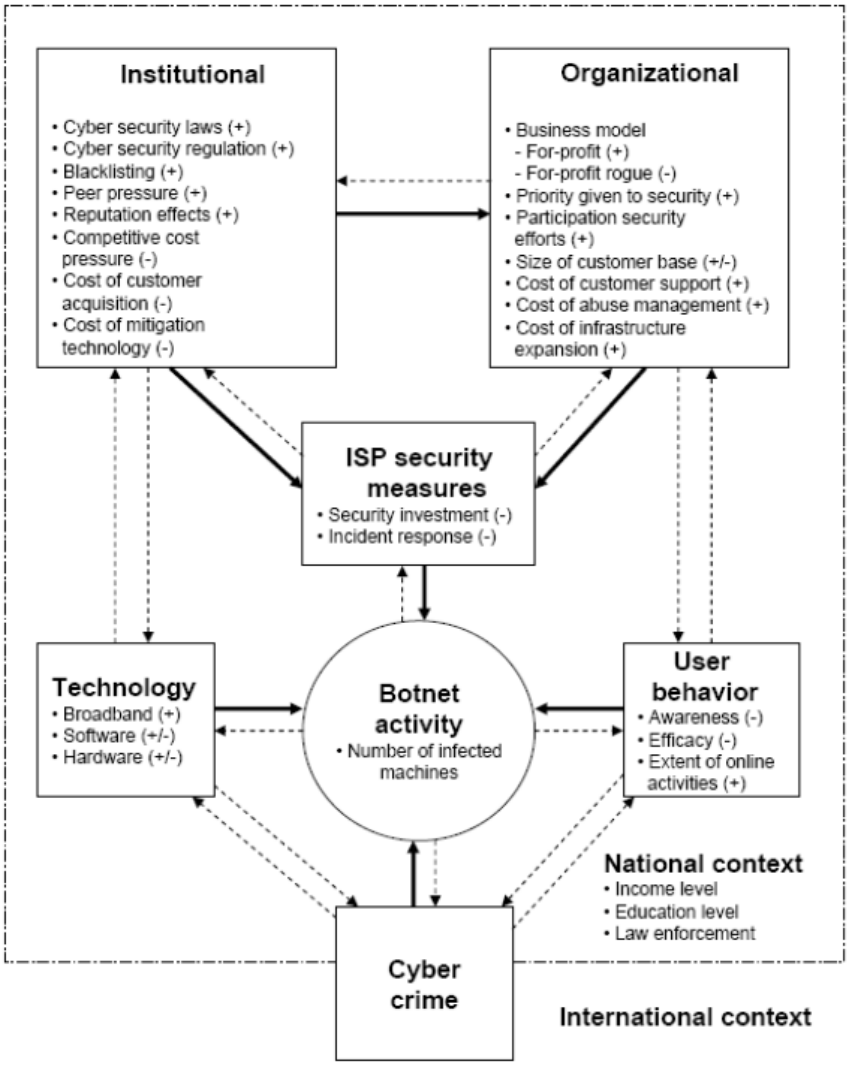
- it reduces the chances of being hacked and being misused in DDoS attacks.

Since in our report we focus on the data [1], we are more interested in the studies with analytical findings.

In the literature it is acknowledged that ISPs can play an important role in botnet mitigation process, since ISPs are well positioned to detect malicious traffic in their networks and to block/disconnect the devices-source of this traffic. Measures towards the end internet users, such as awareness and information campaigns, in general are useful but insufficient. So, the strategy for more effective mitigation points towards the ISP's. There are several thousand ISPs worldwide but the largest ones are around 200.

Van Eeten, Bauerb et al. [15] study extensively the role of ISP's in botnet mitigation process. They show that across the 40 countries, around 80% of the infected machines are located in a network which are hosted by well-known ISP's. So, ISP's indeed have a high influence and can be a potential control point for detecting the botnets. Their quantitative analysis shows clearly that ISPs do influence the botnet mitigation, applying organizational and institutional incentives.

Figure 2: Conceptual framework



The Figure 2 is their "stylized model of the factors that influence botnet activity: the security measures adopted by an ISP, the level and virility of cybercriminal attacks, technological factors, and user behavior."

It is clear that the ISP's security measures are dependant of factors related to the institutional and organizational environments. There is a connection between the different factors but also they are influenced by the ISP's security efforts and so, they co-evolve over time. For example, security measures may

reduce botnet activity but also to activate the cybercriminals to find new attack vectors.

The analysis is based on multi factors, namely:

- Effects of ISP size;
- Cable vs. DSL providers;
- Effects of regulations: Cybercrime Convention member;London Action Plan member
- Effects of piracy;
- Effects of user education;
- Effects of average revenue per user (ARPU);
- Effects of bandwidth.

From these factors the last two have no significance. The results from their regression model are that the parameters: total number of subscribers of the ISP, cable service provision status, membership in the Cybercrime Convention, education levels of users and piracy rate, are factors mitigating the botnet activity.

A follow up of this study is presented by Pijpker and Vranke [16]. They claim that the analysis in [15] is mainly quantitative and present their qualitative analysis of the role of ISPs in the Netherlands. The study outcome is a reference model of security measures for botnet mitigation that ISPs can apply. The model has all five steps according to the five stages in the anti-botnet lifecycle: prevention, detection, notification, remediation, and recovery. This study is validated by semi-structured interviews with a representative sample of Dutch ISPs. Based on those data it is identified which measures actually have been executed by ISPs, and why other measures have not been (yet). The outcome is that ISPs focus on prevention and notification towards customers, i.e. on individual bots. There are little incentives for the ISPs to implement further measures for detection, remediation, and recovery. This fact actually is recognized in most of the publications on the same security issue. Another finding in [16] is: "although ISPs do cooperate in various ways, there still is room for improvement, particularly in the sharing of information on botnet infections and mitigation practices with stakeholders and peer ISPs".

Another extensive study/overview on the security issue raised by Mirai botnet is [14]. This work presents the use of many different well-established botnet measurement perspectives, in concern to the IoT security. The authors analyze how Mirai botnet has emerged, its structure, methodology and evolution. An overview of the most powerful DDoS attacks by Mirai are discussed. "We argue that Mirai may represent a sea change in the evolutionary development of botnets—the simplicity through which devices were infected and its precipitous growth, demonstrate that novice malicious techniques can compromise enough low-end devices to threaten even some of the best-defended targets." This statement makes it clear how much the level on the security threats is raised by the botnet Mirai. The study makes also a survey of the known solutions for mitigation the botnet. It also adds own proposals for combating the Mirai botnet, and IoT botnets in general.

In another recent publication [12] the author discusses the role of the ISPs. A list with the following different hypotheses is presented:

- the role of ISPs as intermediary in botnet mitigation;
- it is proposed that ISP should be bear the costs of DDoS attacks originating in their network;
- ISPs should be considered liable (at least partially), because they control the gateway through which malware is diffused.

The author argues: "Nevertheless, it is important to notice that ISPs are already involved in the mitigation of several Internet problems, from phishing and spam to major botnet takedown, from blocking offensive material to infrastructure resilience. Despite they clearly have a central role in Internet security, ISPs cannot be responsible for the security of the whole ecosystem."

We agree with this and argue that the mitigation of the spread of the Mirai malware should be a join responsibility between all the actors involved in the ecosystem of IoT devices and in the whole internet ecosystem in general.

5 Research question and Hypothesis

The key role of the ISP's in the mitigation process against the Mirai botnet, and in botnet spread in general, is the focus on many studies and published research results.

Here we argue that the mitigation process would be more effective when every actor except the attacker is actively involved by one or another way in enhancement of the security level in the complete network.

In this report we take the complexity of the internet ecosystem and observe the impact of the collaborated work in the mitigation process on the Mirai botnet spread.

5.1 Research question

The research question is: Does the joint effort make a difference? Or more precise which collaborations, initiatives, joint projects are successful in the mitigation process and in what extent.

5.2 Research objects and observations

Possible joint efforts could be:

1. Collaborations in mitigation **spreading** the Mirai botnet, based mainly on controls:

   - introducing certifications and standards corresponding to the current required cybersecurity level for the devices on the market;

- initiating changes/creating law on 'Polluter Pays Principle' similar to security breach reporting law (if personal data has been compromised the company where that has happened must inform the customer);

- sharing security information - central point for global operational communication and coordination between network operators;

- introducing policies for publishing the information about compromised devices, sources for malicious traffic, etc;

- increasing the security level on manufacturing process - less vulnerable devices on the market (incentives by legislation and control);

- improving the update procedure on the existing vulnerable IoT in the network /vendors, ISP/;

- awareness campaign for the end users- when there is an asymmetric information - bring it to the end users;

- active end users in respond to required updates/instractions provided by ISPs or governmental institution;

- stop using piracy software - legislation and control;

- continuous monitoring of the network for vulnerable devices and provide an update or restrict their access;

- internet traffic control for malicious packets.

The listed activities involve many different actors: governmental and control institutions; vendors of IoT, manufacturers, ISPs, end users etc.

2. Collaboration **during attacks** through the botnet:

   - synchronized operation mitigating the losses, tracking the controller of the attack and cut off access.

Here are two examples of successful operations against botnet as a result of joint efforts:

- 29 November 2017, the Federal Bureau of Investigation (FBI) together with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust and private-sector partners, dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue). Steven Wilson, the Head of Europol's European Cybercrime Centre: "This is another example of international law enforcement working together with industry partners to tackle the most significant cyber criminals and the dedicated infrastructure they use to distribute malware on a global scale. The clear message is that public-private partnerships can impact these criminals and make the internet safer for all of us."

- this operation comes a year after another successful operation, 30 November 2016, 'Avalanche' botnet dismantled after a four-year project by an international collaboration.

There are many collaborations in practice between different parties towards mitigation the security issue. Here are three recently published reports about collaboration between the academy and industry:

- SIDN Labs and the MS project by Caspar Schutijser: Towards automated DDoS abuse protection using MUD device profiles [13];
- warning signal from research groups exploring new vulnerabilities:
  - BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid [5];
  - Smart irrigation systems, a new type of green technology and IoT device can be used by attackers as a means of attacking urban water services [20].

In this report we are especially interested in the organizations which have the botnet mitigation in their priority list with activities. The reason is that a country being a member of an itiniative/organization we can use as a measure in order to analyse the difference in the security performance between the countries.

- Organizations against botnet - national and international:

- London Action Plan (LAP) or The Unsolicited Communications Enforcement Network (UCENet) since 09 Sep 2016: a framework of 29 countries for international cooperation in enforcing spam-related legislation and addressing similar cyber-challenges such as online fraud, malware, phishing and dissemination of viruses [1].

- National Anti-Botnet Initiative (ABI): in 14 countries and AbuseHub in 1 [18].

- The Council to Secure the Digital Economy (CSDE): companies from the ICT sector to combat cyber threats through collaborative actions. Its first priority - anti-botnet activities (May 2018)[2].

- North American Network Operators Group (NANOG).

- Pacific Cyber Security Operational Network (PaCSON): April 2018, 20 participants from 14 countries[3].

- NATO Cooperative Cyber Defence Centre of Excellence [4].

- Messaging Malware, Mobile and Anti-Abuse Working Group (M^3AAWG)[5]: is an international information technology industry forum that works to reduce the threat from bots, malware, spam, viruses, DoS attacks and other online exploitation'.

- Advanced Cyber Defence Centre (ACDC): EU 2013-2015, 28 partners from 14 countries[6].

- The European Union Agency for Network and Information Security (ENISA)[7].

[1] https://www.ucenet.org/history/
[2] https://securingdigitaleconomy.org/
[3] https://www.cert.gov.au/news/pacific-cyber-security-operational-network
[4] https://ccdcoe.org/
[5] https://www.m3aawg.org/
[6] https://www.botfree.eu/en/aboutus/information.html
[7] https://www.enisa.europa.eu/

- Australian Cyber Security Centre (JCSC)- a partnership between business, government, academia and other key partners to enhance collaboration on cybersecurity[8].

- European Cybercrime Centre (EC3) at Europol (Jan 2003)[9].

5.3 Hypothesis

Hypothesis: The cyber security performance of each country against the Mirai botnet spread is positively related (has direct variation) to the Institutional power in the country, to presence of awareness and respond by the end users of IoT, to presence of international collaboration and national initiatives in the mitigation process.

This can be considered as a negative relation (inverse variation) between the infection rate and the listed factors.

6 Data, Methodology and New Measure

The dataset [1] consists of 233 629 entries with the following information for each entry:

- IP address - IPv4 address which shows behavior of infection;
- Autonomous System (AS) - The name of the subnet to which the IP address, usually the name of the organization that owns the AS;
- Country - The country where the AS and IP address is registered;
- ASN - Autonomous System Number;
- Date First Seen - The time the IP was first seen to have been infected.

From the dataset we can aggregate the new infections per country per unit of time, 7 days in out case. The *infection rate over time* is these aggregated values divided by the total number of IP addresses [19] in this country, whereas the *infection rate* per country is the total number of infections from the dataset per country over the total number of IPs in it.

To measure the Institutional power in the country we use the Global Cybersecurity Index (GCI) calculated by the International Telecommunication Union. The report [21] presents the methodology which is used. Here we cite the brief description of the five pillars applied:

"1. Legal: Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.

2. Technical: Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.

3. Organizational: Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.

[8] https://cyber.gov.au/

[9] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

4. Capacity Building: Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.

5. Cooperation: Measured based on the existence of partnerships, cooperative frameworks and information sharing networks."

The characteristic awareness and respond by the end users of IoT is partly captured by the same GCI index but also partly by the GDP per Capita (Gross domestic product). For a country with higher income the legislative responsibility in general is higher and the awareness to lose more is a natural incentive to contribute for increasing the cybersecurity level.

The international collaboration and national initiatives are projection of the membership in the organizations listed in the previous subsection. They are UCENet, ABI, CSDE, PaCSON, NATO CCDCE, M^3AAWG, ENISA, JCSC, EC3.

First we perform quantitative analysis and then statistical linear regression analysis.

From the dataset there is no information whether or not the machines behind those IP addresses are currently infected. Therefore we focus on the new infections, i.e. on the spread, and not on the total size of the botnet. We assume that the data given by the source are reliable and we do not take into account possible abnormalities caused by it.

6.0.1 New infections observed over time

Our first metric is an overview of the total spread of the Mirai malware over time (Figure 3). It presents the aggregated numbers of newly observed infections over time of one week. Security breaches such as the router vulnerability at the Telmex in *April 2018* [17] are clearly visible.

6.0.2 Infections per country

Here we consider the total infection rate per country. In Figure 4 the highest 30 infection rates are plotted, i.e. the worst results. Details are included in the appendix. From this metric we can conclude that there is a large difference between the security level in the network per country.

Figure 3: Aggregated number of new infections per 7 days

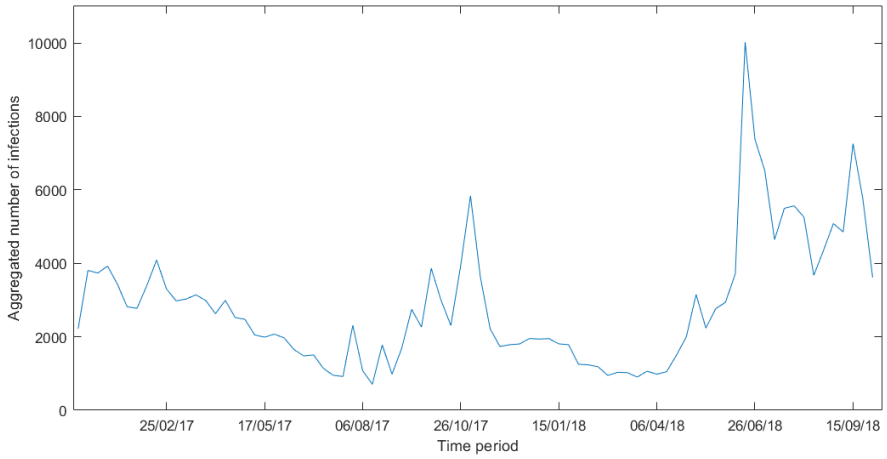
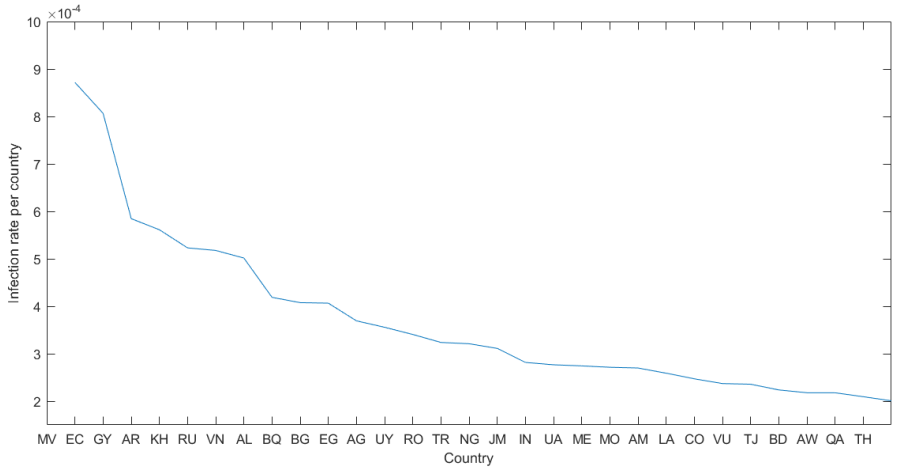


Figure 4: Aggregated number of new infections per country

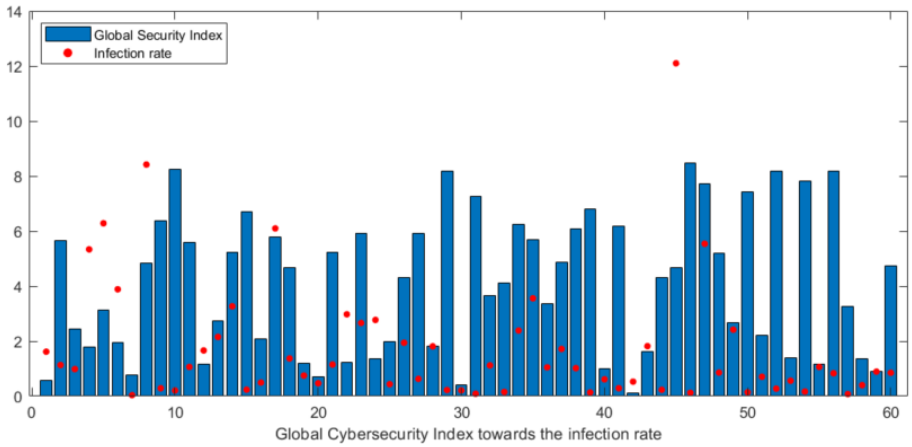


These two figures show the spread behaviour of the Mirai malware and the difference in the security performance per country. Now we will look into the factors which we argue that influence this difference. The factors are:

- Global Cybersecurity Index (GCI)
- GDP per Capita
- Anti-Botnet Initiative (ABI)

- UCENet (former London Action Plan)
- Pacific Cyber Security Operational Network
- M^3AAWG
- NATO Cooperative Cyber Defence Centre
- ENISA and EC3
- JCSC, NANOG

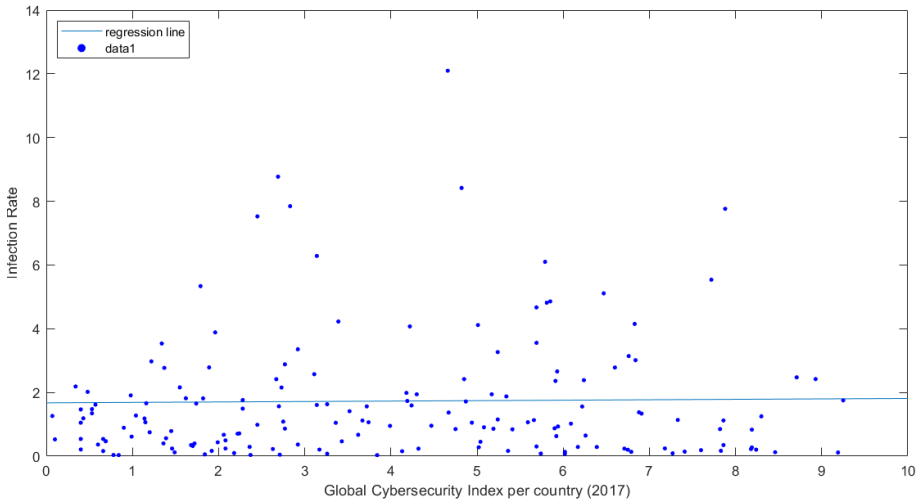
Figure 5: Scatterplot of the Infection rate and GCI per country



Lets us first consider the Global Cybersecurity Index. We expect that it should have an inverse variation with the infection rate, i.e. higher security corresponds to a lower infection rate. Figure 5 shows both measures for the first 60 countries ordered by name. A table with the data for all 190 countries is attached in the appendix. Clearly there is a correlation between the values for the Index and the infection rate. For the majority of the countries the high GCI corresponds to a low infection rate.

A simple linear regression does not lead to a significant match (Figure 6 for all 190 countries). Therefore we consider the factors together in a multiple linear regression model.

Figure 6: Scatterplot of the Infection rate and GCI per country



The first two factors (GCI and GDP) combine a large list of other factors and we leave them separately. Their values are published and available. For the other factors we need to define a methodology of measurement.

The Anti-Botnet Initiatives are studied in [18]. We use the results directly as follows: the countries with a long term Anti Botnet Initiative we index with 5, the recent once with 2.

Group	Country Codes	index
Mature ABI	AU, DE, IE, JP, KR , FI, NL	5
Recent ABI	BE, ES, HR, RO, IT, FR, PT, US	2

For the 29 countries members of UCENet (former London Action Plan) an index 1 is assigned.

For the members of the very recent Pacific Cyber Security Operational Network (May 2018) we use index 0.5.

The next factor, M^3AAWG, has 29 full members in 6 countries. Each member we weight with 1/29 influence index on the mitigation process against of Mirai Botnet spread. Then we have the following:

Country Codes	index
DE, JP, IL	0.0345
FR	0.0690
UK	0.1379
US	0.6897

The factors JCSC and NANOG, both in US, we weight with 3 and add this index to the Anti-Botnet Initiative. Therefore the index for US there is also 5.

There are three more factors listed: if a country is a member of NATO Cooperative Cyber Defence Centre, of The European Union Agency for Network and Information Security and of European Cybercrime Centre (EC3) at Europol. For each membership we assign an index 1 to the corresponding country.

7 Results

Now we have all the data and can perform the analysis. Some of the organizations have no common members, or exactly the same members, therefore we combine some of the indexes. The grouping is as follows:

- ABI, LAP, PaCSON, M^3AAWG and ISP organizations, denoted by ABI_index
- ENISA and EC3, denoted by EU_index
- NATO, denoted by NATO_index.

Combined by this way we first look into the correlation matrix in order to insure that there are no factors used in the regression model which are highly correlated.

Table 1: Correlation matrix of the factors

	GCI	GDP	ABI_index	EU_index	NATO_index
GCI	1.0000	0.5766	0.4479	0.6961	0.3989
GDP	0.5766	1.0000	0.5407	0.5178	0.4496
ABI_index	0.4479	0.5407	1.0000	0.3831	0.3574
EU_index	0.6961	0.5178	0.3831	1.0000	0.4731
NATO_index	0.3989	0.4496	0.3574	0.4731	1.0000

As we see in Table 1 all the factors are with correlation less than 0.75. Therefore we include all of them in the model.

For the multiple linear regression model we use MATLAB. The results of the model with all five factors are shown in Table 2

Table 2: Results Linear Regression Model with five factors

	Estimate	p-Value
Intercept	1.01730	3.145e-09
GCI	0.11378	0.04081
GDP	-0.01424	0.07299
ABI_index	-0.11623	0.13421
EU_index	0.02682	0.92704
NATO_index	-0.20328	0.22053

The p- values of the last three factors are far above the statistically significant level of 0.05. The 4-th factor has the highest p-value. Removing it from the model does not improve the solution. Therefore we use another approach. Similarly to the factors GCI, GDP which combine many other factors we merge the last three factors in one and name it ABI_EU_NATO_index. The exact values are included in the Appendix. The results of the model with the new combination of factors are:

Table 3: Results Linear Regression Model with three factors

	Estimate	p-Value
(Intercept)	1.01300	2.9856e-09
GCI	0.12685	0.00908
GDP	-0.01427	0.07097
ABI_EU_NATO_index	-0.12380	0.04798

The second factor still has too high p-value. At last we consider only the factors Global Cybersecurity Index and our joint ABI_EU_NATO_index.

The linear regression model results into:

Table 4: Results Linear Regression Model with three factors

	Estimate	p-Value
(Intercept)	1.00200	5.0243e-09
GCI	0.09949	0.03172
ABI_EU_NATO_index	-0.17483	0.00201

The received p-value of the first factor is not very small but fit in the significant level. Therefore we can conclude that from all the considered factors these two are the most related to the cybersecurity performance of each country and respectively to the mitigation process in the Mirai botnet spread.

8 Conclusions and open questions

Hypothesis: The cybersecurity performance of each country against the Mirai botnet spread is positively related (has direct variation) to the Institutional power in the country, to presence of awareness and respond by the end users of IoT, to presence of international collaboration and national initiatives in the mitigation process.

Based on the outcome of the last model we can conclude that the first part of our hypotheses should be rejected because the Global Cybersecurity Index has a positive relation to the infection rate (the coefficient is 0.099496) even though the coefficient is very small. Again based on the results, the second part of our hypotheses can be accepted. The value of the coefficient is -0.17483, and the p-value is less than 0.05, which makes the factor significant. According

the coefficient we can conclude that the infection rate decreases with increasing of our new index ABI_EU_NATO_index which measures the joint efforts: the presence of awareness, the respond by the end users of IoT, to the presence of international collaboration and national initiatives in the mitigation process.

After all we attain that the cybersecurity joint efforts lead to a better performance in the mitigation process against the Mirai botnet.

Limmitations: The limited time and language barrier to study the existing AntiBotnet Initiatives in each country makes the result in a sense uncomplete. There is a room to extend the coefficient and include more organizations and centers on international and national levels.

References

[1] Mirai-like Botnet: Bad Packets Report, https://mirai.badpackets.net/, accessed 13 Sep 2018

[2] Ddos attack that disrupted internet was largest of its kind in history, experts say. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[3] Hacked cameras, dvrs powered todays massive internet outage. https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

[4] B. Krebs, Krebsonsecurity hit with record DDoS, https://krebsonsecurity.com/2016/09/krebsonsecurity-hitwith- record-ddos/.

[5] BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, Saleh Soltan, Prateek Mittal, and H. Vincent Poor, 27th USENIX Security Symposium, August 15–17, 2018.

[6] Anna-senpai, Mirai Source Code on GitHub, September 2016, Source: https://github.com/jgamblin/Mirai-Source-Code

[7] R. Millman, "OVH suffers 1.1Tbps DDoS attack," in News, SC Magazine UK, 2016. [Online]. Available: http://www.scmagazineuk.com/ovh-suffers-11tbps-ddos-attack/article/524826/. Accessed: Oct. 24, 2016.

[8] NJCCIC (2018) "Botnets". https://www.cyber.nj.gov/threat-profiles/botnets/#STRATEGIES-TO-PREVENT-AND-MITIGATE-POTENTIAL-IOT-COMPROMISE

[9] Bill Hull. (2018). IoT risk and the smart factory: Building cyber resilience

[10] Gallaher, M. P., Rowe, B. R., Rogozhin, A. V., & Link, A. N. (2006). Economic Analysis of Cyber Security. RESEARCH TRIANGLE INST (RTI) RESEARCH TRIANGLE PARK NC.

[11] Howard Solomon. (2018). Governemts should use buying, regulatory power to fight botnets: Expert.

[12] Luigi Tuttobene, Private and Public Information Disclosure to Improve Cybersecurity, May 2018, MsThesis

[13] Caspar Schutijse, Towards automated DDoS abuse protection using MUD device profiles, Aug 2018, MsThesis

[14] Antonakakis, Manos, et al. "Understanding the mirai botnet." USENIX Security Symposium. 2017.

[15] M. van Eeten, J. Bauer, H. Asghari, S. Tabatabaie and D. Rand, The role of Internet Service Providers in botnet mitigation: an empirical analysis based on spam data, Workshop on the Economics of Information Security (WEIS), 2010.

[16] L. Pijpker, H. Vranken, The Role of Internet Service Providers in Botnet Mitigation, European Intelligence and Security Informatics Conference, 2016.

[17] Zack Whittaker, "Over a million vulnerable fiber routers can be easily hacked", https://www.zdnet.com/article/over-a-million-vulnerable-fiber-routers-can-be-easily-hacked/, accessed 5 Oct 2018.

[18] M van Eeten, Q Lone, G Moura, H Asghari, M Korczyński, Evaluating the Impact of AbuseHUB on Botnet Mitigation, May 2016, https://arxiv.org/pdf/1612.03101.pdf

[19] https://www.ip2location.com/reports/internet-ip-address-2017-report

[20] B. Nassi, M. Sror, I.Lavi, Y. Meidan, A. Shabtai, Y. Elovici, Piping Botnet - Turning Green Technology into a Water Disaster, (6 Aug 2018) https://arxiv.org/abs/1808.02131

[21] International Telecommunication Union (ITU). "Global Cybersecurity Index (GCI) 2017", www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Appendix

Country	infection rate	GCI	Country	Infection rate	GCI
AD	0.0108	0	DE	9.1176e-04	43.4900
AE	0.0075	39.1300	DJ	0.0041	1.8800
AF	0.0066	0.5700	DK	0.0019	55.2200
AG	0.0356	14.1700	DM	0.0035	6.9900
AL	0.0419	4.3200	DO	0.0121	6.3300
AM	0.0259	4	DZ	0.0016	3.9600
AO	2.4345e-04	3.3300	EC	0.0807	5.8900
AR	0.0561	13.0400	EE	8.1687e-04	18.1900
AT	0.0019	45.4400	EG	0.0369	3.0100
AU	0.0014	51.3600	ES	0.0057	27.1800
AW	0.0218	0	ET	0.0161	0.7400
AZ	0.0071	4.0800	FI	9.4861e-04	44.5800
BA	0.0111	4.9400	FJ	0.0047	4.9700
BB	0.0144	15.5400	FR	0.0018	37.9700
BD	0.0218	1.4700	GA	0.0037	6.6100
BE	0.0016	41.7900	GB	0.0011	40.5300
BF	0.0033	0.6100	GD	0.0071	9.6500
BG	0.0407	7.7600	GE	0.0055	3.7900
BH	0.0091	20.2400	GF	0.0031	1.0000e-03
BI	0.0050	0.2900	GH	5.0667e-04	1.4900
BJ	0.0031	0.8000	GI	0.0041	1.0000e-03
BM	7.7514e-04	2.1700	GM	0.0027	0.4500
BN	0.0077	29.6000	GN	0.0059	0.8000
BO	0.0198	3.1300	GQ	0.0090	1.0000e-03
BQ	0.0408	0	GR	0.0057	18.0900
BR	0.0177	8.5800	GT	0.0079	4.0600
BS	0.0185	29.1700	GU	0.0086	1.0000e-03
BT	0.0029	2.7200	GY	0.0585	4.4600
BW	0.0129	6.8200	HK	0.0171	46.3100
BY	0.0042	5.2800	HN	0.0134	2.2500
BZ	0.0121	4.3900	HR	0.0058	12.4300
CA	0.0015	42.8700	HT	0.0036	0.7600
CG	0.0014	1.3600	HU	0.0125	12.8700
CH	5.9347e-04	80.5600	ID	0.0106	3.5400
CI	0.0020	0	IE	0.0014	55.2900
CK	0.0121	0	IL	0.0089	37.2700
CL	0.0075	13.6100	IN	0.0277	1.8200
CM	0.0010	1.3600	IQ	0.0079	4.7700
CN	0.0159	8.6900	IR	0.0070	5.4000
CO	0.0237	5.8300	IS	2.2102e-04	60.8300
CR	0.0070	11.0400	IT	0.0043	31.0200
CW	0.0052	0	JE	0.0038	1.0000e-03
CY	0.0114	23.7200	JM	0.0282	4.7500
CZ	0.0068	18.1600	JO	0.0192	3.9800

Country	infection rate	GCI	Country	Infection rate	GCI
JP	0.0075	38.5500	NP	0.0072	0.7900
KE	5.4910e-04	1.4400	NZ	0.0016	38.9700
KG	0.0104	1.1300	OM	0.0165	14.4400
KH	0.0523	1.2300	PA	0.0161	13.1000
KM	0.0098	0.7600	PE	0.0071	5.9700
KN	0.0036	16.0300	PH	0.0062	3.6600
KR	0.0057	28.3800	PK	0.0064	1.5800
KW	0.0085	31.4300	PL	0.0104	12.7100
KY	0.0106	0	PR	0.0066	0.8200
KZ	0.0094	7.8900	PS	0.0099	1.0000e-03
LA	0.0247	0	PT	0.0060	19.8200
LB	0.0026	8.3100	PW	0.0098	12.5300
LC	0.0090	8.7800	PY	0.0109	3.9200
LK	0.0115	3.8400	QA	0.0209	61.0700
LR	7.9932e-04	0.3800	RE	0.0012	1.0000e-03
LT	0.0030	15.2000	RO	0.0324	9.9700
LU	8.8487e-04	70.2600	RS	0.0171	5.1800
LV	0.0092	14.7400	RU	0.0518	9.2300
LY	0.0048	6.5400	RW	5.2633e-04	0.7200
MA	0.0056	2.8600	SA	0.0020	20.0800
MC	0.0020	0	SC	3.7882e-04	14.1800
MD	0.0132	2.1800	SD	3.0637e-04	2.3800
ME	0.0271	7.3500	SE	0.0076	52.5900
MG	0.0023	0.4000	SG	0.0117	54.5300
MK	0.0130	4.8800	SI	0.0031	22
ML	0.0024	0.7700	SK	0.0045	16.6100
MM	0.0015	1.1900	SL	0.0052	0.5100
MN	0.0118	3.2900	SM	0.0110	1.0000e-03
MO	0.0270	0	SN	0.0107	0.9500
MP	0.0055	0	SO	0.0146	1.0000e-03
MT	0.0063	23.8100	SR	0.0144	6.0200
MU	0.0083	10.1400	ST	0.0070	1.7700
MV	0.0872	9.5700	SV	0.0016	3.5600
MW	2.3642e-04	0.3200	SX	0.0083	1.0000e-03
MX	0.0186	8.6100	SY	2.4947e-04	1.0000e-03
MY	0.0161	9.6500	SZ	0.0056	2.9600
MZ	0.0045	0.4200	TG	6.4080e-04	0.6100
NA	0.0011	4.6000	TH	0.0201	5.9600
NC	0.0061	1.0000e-03	TJ	0.0224	0.9900
NE	0.0021	0.3600	TN	0.0157	3.5000
NG	0.0311	1.0000e-03	TR	0.0321	10.9300
NI	0.0016	2.0800	TT	0.0127	15.3500
NL	0.0013	46.1800	TW	0.0143	1.0000e-03
NO	0.0023	75.9900	TZ	0.0014	0.9100

Country	infection rate	GCI	Country	Infection rate	GCI
UA	0.0274	2.3900	VG	0.0032	1.0000e-03
UG	0.0011	0.6000	VN	0.0502	2.1700
US	7.6405e-04	58.2700	VU	0.0236	2.9200
UY	0.0341	15.2500	YE	0.0084	1.0000e-03
UZ	0.0058	1.9800	ZA	0.0019	5.4300
VC	0.0186	1.0000e-03	ZM	0.0024	1.3000
VE	0.0104	1.0700	ZW	0.0011	0.9100

Country	AB_index	EU_index	NATO_index	Country	AB_index	EU_index	NATO_index
AE	0	0	1	KE	0	0	1
AF	0	0	1	KR	7	0	1
AL	0	0	1	LT	1	2	1
AT	0	2	1	LU	0	2	1
AU	7.5000	0	1	LV	1	2	1
AZ	0	0	1	MA	0	0	1
BD	0	0	1	ME	0	0	1
BE	3	2	1	MN	0	0	1
BG	0	2	1	MT	0	2	1
BR	1	0	1	MU	0	0	1
BW	0	0	1	MX	1	0	1
CA	1	0	1	MY	1	0	1
CH	2	0	1	NG	1	0	1
CK	0.5000	0	0	NL	7	2	1
CL	1	0	0	NO	1	0	1
CN	1	0	1	NZ	1.5000	0	1
CO	0	0	1	PA	0	0	1
CR	0	0	1	PK	0	0	1
CY	0	2	0	PL	0	2	1
CZ	0	0	1	PT	3	2	1
DE	6.0345	2	1	PW	0.5000	0	0
DK	1	2	1	QA	0	0	1
EE	0	2	1	RO	2	2	1
EG	0	0	1	RS	0	0	1
ES	3	2	1	RU	0	0	1
FI	7	2	1	SA	0	0	1
FJ	0.5000	0	0	SE	1	2	1
FR	2.0690	2	1	SG	0	0	1
GB	1.1379	2	1	SI	0	2	1
GD	0	0	1	SK	0	2	1
GE	0	0	1	TR	0	0	1
GM	0	0	1	TT	0	0	1
GR	0	2	1	UA	0	0	1
HK	1	0	0	UG	0	0	1
HR	2	2	1	US	9.6897	0	1
HU	1	2	1	VU	0.5000	0	0
IE	7	2	1	ZA	1	0	1
IL	0.0345	0	1	ZW	0	0	1
IN	0	0	1	JM	0	0	1
IS	0	0	1	JO	0	0	1
IT	2	2	1	JP	7.0345	0	1

Table 5: M^3AAWG group full members

Members	Country
1 & 1 Internet SE	Germany
Agora Inc.	US
Akamai Technologies	US
Apple Inc.	US
Campaign Monitor	US
Cisco Systems, Inc.	US
CloudFlare, Inc.	US
Cyren	Israel
dotmailer	United Kingdom
eDataSource	Inc US
ExactTarget Inc.	US
IBM	US
iContact	US
Internet Initiative Japan (IIJ)	Japan
Liberty Global	United Kingdom
Listrak	US
Litmus	US
Marketo, Inc	US
McAfee	US
Mimecast	United Kingdom
Oracle Marketing Cloud	US
OVH	France
PayPal	US
Rackspace	US
Spamhaus	United Kingdom
SparkPost	US
Splio	France
Symantec	US
USAA	US