Mirai and The Future

Forecasting the DDoS Landscape in 2017

December 5, 2016

digital shadows_

Table of Contents

Executive summary

Since the release of the Mirai source code, the tactic of DDoS has gained notoriety and has been portrayed as a "digital nuclear attack" and "zombie apocalypse" by elements of the press. Of course, the reality lies short of that with the potential impact of DDoS dependent on the type of threat actor you face, your geography, industry and how well you are placed to deal with the threat.

Aside from opportunistic attacks launched for the fun of it – or the "lulz" – there are three main motivations for threat actors looking to use DDoS as a tactic: protests by hacktivists, extortion by cyber criminals and geopolitical by nation state affiliated actors. This paper uses the cone of plausibility technique to look across current trends, identify drivers that look to impact these trends throughout 2017, and outline three different scenarios: a probable, a plausible and a wild card option. These forecasts can be used to help you understand the probable and plausible threats posed by DDoS in 2017, as well as the types of things organizations need to think about in order to prepare for such threats.

There has been no shortage of news surrounding Mirai over the past several months. The release of its source code has caused a considerable evolution of the DDoS landscape, and it is important to understand the continuing development of botnets at a broader level. However, it is equally important not to lose sight of other DDoS threats that will continue to pose a threat to organizations and understand how prepared you are for this particular tactic.

Using this forecasting technique allows us to put Mirai into context, consider how the DDoS landscape will evolve over the next year and align security processes accordingly.

Mirai has dominated the headlines

On September 30, 2016, a user on hackforums[.]net publically released the source code for Mirai. Mirai malcode exploits Internet of Things (IoT) devices and is used as a platform for launching DDoS attacks. Since that time, attacks against Krebs on Security, OVH and DynDNS have all involved, at least in some part, the use of the Mirai botnet. These attacks – in particular against DynDNS that caused several high profile sites to go down – generated significant disruption and widespread media attention.[1] However, despite some spurious claims from groups such as New World Hackers,[2] the actors and motivations behind these attacks remain unknown.

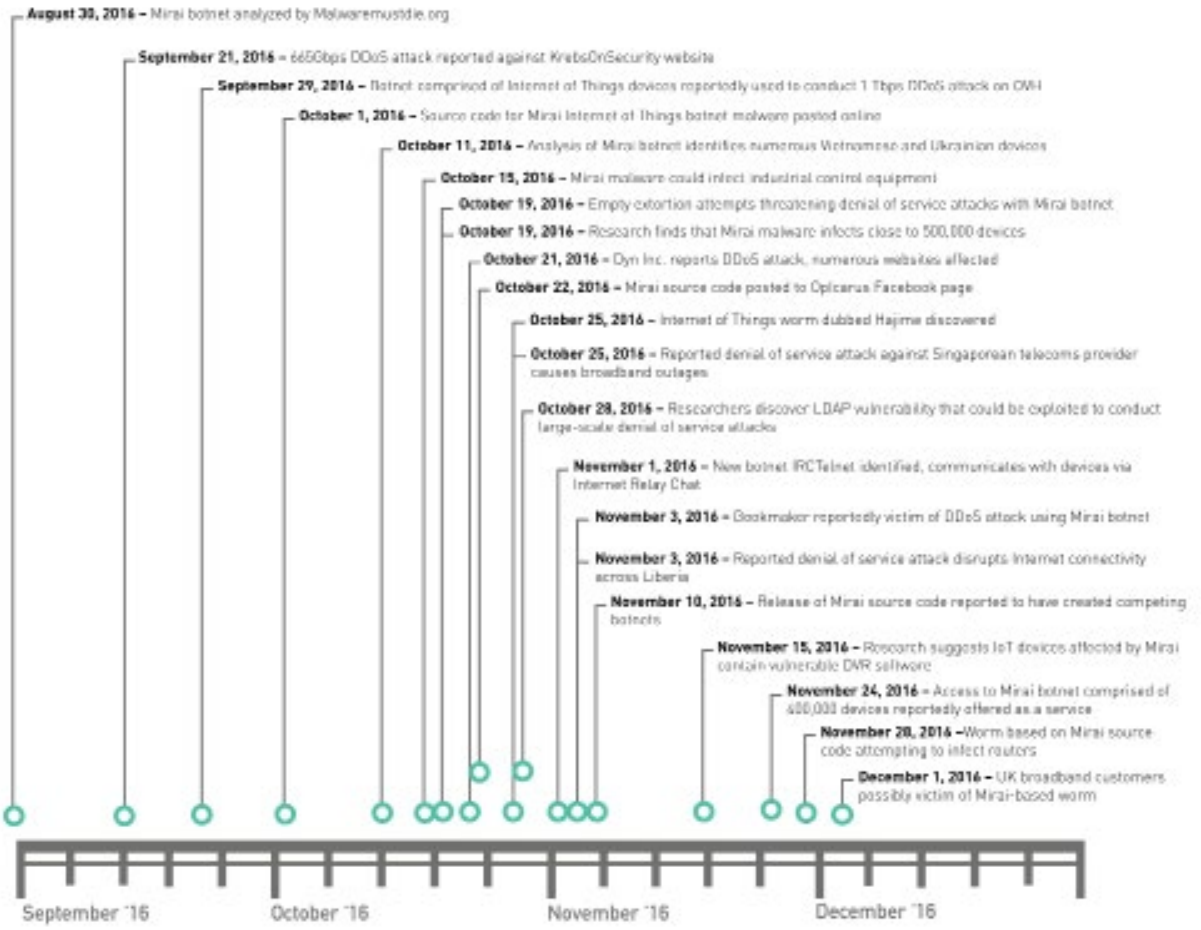
The availability of the Mirai DDoS source code is yet another example of the lowering of barriers to entry for malicious activity. While the public release of the source code may have led to an increase in opportunistic attacks, there are traditionally three main motivations for actors using DDoS as a tactic: online protest, extortion and political gain.

Mirai translates from Japanese as the "future", but how is it set to change the DDoS landscape in 2017? By looking at trends from 2016 and outlining factors that may change the landscape, it is possible to outline different scenarios for each of these motivations. Understanding the various scenarios enables organizations to develop plans that will minimize the impact of denial of service attacks against their services.

The Mirai malware

Mirai is a Linux malware variant specifically developed to enslave IoT devices into botnets that can then be used to launch DDoS attacks. Mirai initially spread by scanning for IoT devices operating Telnet, and then used default credentials in an attempt to brute-force access to the device. Botnets of cameras, DVRs, routers, or other internet-connected hardware can be used to execute a range of DDoS attacks.[3] In addition to being able to send packets from an infected device, Mirai has an additional notable functionality. Following installation, the malware executes scripts which kill any other processes on the device which use ports associated with HTTP, SSH or Telnet, and conducts a memory scrape in an attempt to remove any other malware installed on an infected device. Figure 1 shows the timeline of Mirai activity.

Figure 1: A Timeline of Mirai activity, from August to December



• Mirai was first identified in August 2016 and soon gained notoriety after a Mirai botnet was used to launch a DDoS attack against the website of security blogger Brian Krebs. This attack, in which the traffic volume peaked at 620Gbps, successfully rendered the website unavailable for an extended period of time and resulted in Akamai suspending its pro bono provision of DDoS protection services to Krebs on Security.[4] Akamai reportedly ascertained that the botnet used to target Krebs on Security was compromised of IoT devices,[5] and it was later reported that this botnet was compromised of devices infected with Mirai.

• On September 22 and 23, 2016 it was reported that the French internet service provider (ISP) OVH had been targeted with a DDoS attack with a peak traffic volume of 1Tbps, making it the largest attack ever recorded, using a botnet of IoT devices infected with Mirai.[6]

• On September 30, 2016, a user on HackForums using the name "Anna-senpai" added a post featuring links to pages on file hosting sites where the source code for Mirai could be freely downloaded. Anna-senpai, who claimed to be the author of Mirai, professed that the Mirai source code was released in response to heightened scrutiny of IoT botnets. Anna-senpai acknowledged the link between Mirai and the DDoS attack on Krebs on Security, but did not admit responsibility. The post stated that prior to this heightened attention a Mirai botnet of 380,000 devices could be assembled, but that this had become more difficult as awareness

of IoT security improved. In addition to links to .zip files containing the malware source code, the post contained detailed instructions on setting up and configuring the bot, including configuring command and control (C2) servers.

- The post estimated that the set-up process would take approximately one hour for a competent user. However, following this, a large number of posts and threads were added to HackForums (Figure 2) by users who had been unable to independently set up and operate Mirai and were requesting assistance. This likely indicates that setting up Mirai and creating a botnet requires a certain level of technical competence and would likely be beyond very low capability actors. This was also corroborated by the discovery in October 2016 of a listing on the criminal marketplace AlphaBay for a botnet of IoT devices (Figure 3) which, if genuine, may be comprised of devices infected with Mirai.

Figure 2: Post in Hackforums.net from October 11, 2016

Will Pay for Mirai Help!! - ImNostalgia - **Today 08:19 PM**

Im having an insane ammount of trouble with mirai if anyone could assist me (NOT SET IT UP FOR ME, But teach me how to set it up) I will pay but we will have to negotiate a price via skype or my teamspeak server.

Figure 3: Post on Alphabay from November 9, 2016

- On October 21, 2016, DynDNS was subjected to a series of DDoS attacks which third-party analysis later indicated were conducted, at least in part, using a botnet of IoT devices infected with Mirai.[7] The attacks caused major disruption and prevented users based in the U.S. from accessing a large number of high-profile online services hosted on DynDNS infrastructure, including Twitter, Amazon and Spotify. This included major news websites, payment platforms, online games and video on demand (VOD) services. Subsequent analyses of the attacks on DynDNS indicated that they were at least partiallly conducted using a botnet largely comprised of DVRs and web connected cameras that had been infected with Mirai.[8]

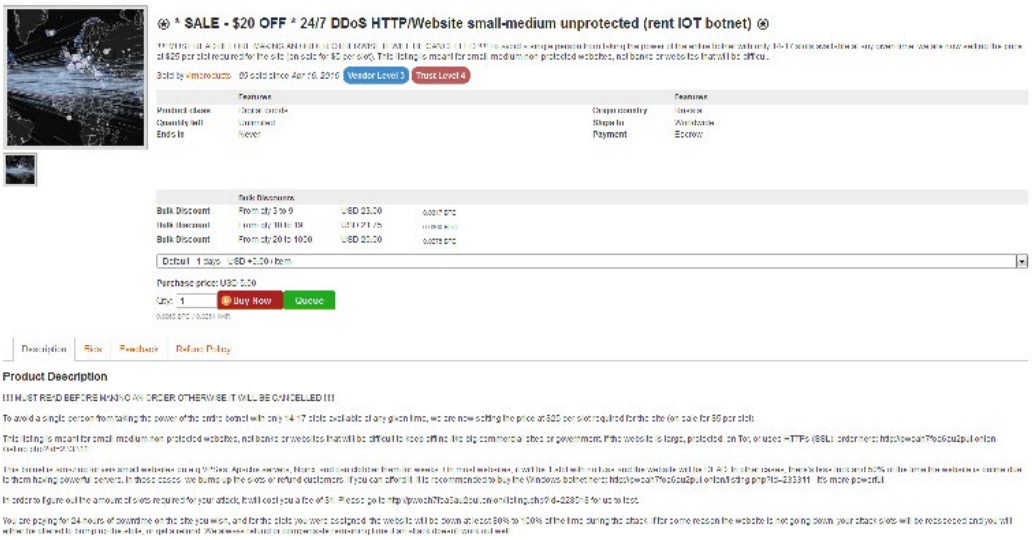
- Although the hacktivist group New World Hackers has claimed responsibility for the attacks (Figure 4), significant uncertainty remains regarding the attribution of this attack. Despite the lack of evidence to suggest this was a targeted attack, the disruption caused by the attack on DynDNS was disproportionate to the resources and level of capability which would have been required to execute the attack. This highlights the inherent vulnerability of infrastructure operated by a single organization to support the operations of multiple prominent services and the potential to enable low capability actors to launch high-impact attacks across multiple targets.

Figure 4: Claim of attack by New World Hackers

- On November 3, 2016, Mirai was observed to have launched a 500Gbps attack on a mobile telecommunications provider in Liberia. While claims that there was a countrywide outage appear to be exaggerated, this incident provides an interesting potential future scenario for us to consider.[9]

• Mirai is making its way into the DDoS-as-a-Service market. One example is Vimproducts, who on November 8, 2016 claimed to have rendered five Russian bank websites offline through a series of DDoS attacks. This actor has multiple botnet-based DDoS-as-a-Service offerings on AlphaBay, one of which they claim is an IoT botnet (Figure 5).

Figure 5: Vimproducts posting on Alphabay, from November 20, 2016



• Prior to this, on November 7, 2016, it was reported that remote code execution could be achieved on some routers using TR-064 commands.[10] A proof of concept exploit for this vulnerability was released shortly thereafter. On November 27, 2016, reports emerged which suggested that a worm using some of Mirai's source code had attempted to infect routers by exploiting a vulnerability in the TR-064 protocol on some router models.[11] At the time of writing it had been reported that 900,000 Deutsche Telekom customers were affected, however it was reported that additional devices were vulnerable.[12] Two previously known threat actors known by their monikers "BestBuy" and "Popopret" claimed responsibility for the German attacks, but no attribution was confirmed at the time of writing.

• In an event that was possibly related to the Deutsche Telekom incident, as many as 100,000 Post Office customers might have been affected, especially users of the Zyxel AMG1302 internet router. TalkTalk admitted that its D-Link DSL-3780 routers were affected, but said only a small percentage of its customers used them. While details about the TalkTalk/Post Office attack are still being developed, the targeting of routers could reflect a competition amongst malware developers to infect and enslave the largest number of devices and maximize the capability of their botnets.

When it comes to DDoS, Mirai isn't the only option

It is important to emphasize that there are many ways to launch DDoS attacks. The use of botnets of IoT devices is not a new development and is not unique to Mirai. In October of 2015 Incapsula reported that several of its clients had been targeted with DoS attacks using botnets comprised of compromised CCTV cameras.[14] In fact, there are at least three botnets known to have used IoT devices to launch attacks.

- **BASHLITE.** Targeting insecure IoT devices, BASHLITE has reportedly succeeded in infecting around one million endpoint devices, the majority of which are IoT devices.[15] While the majority of attacks are TCP and UDP floods, there has also been evidence of HTTP attacks.[16]

- **LizardStresser.** This botnet was originally written by the infamous Lizard Squad DDoS group. The source code was released publicly in early 2015, an act that encouraged aspiring DDoS actors to build their own botnets. A set of threat actors behind LizardStresser have focused on targeting IoT devices using default passwords that are shared among entire device classes.

- **Linux/IRCTelnet.** More recently, researchers discovered another botnet with similarities to Mirai called Linux/IRCTelnet.[17] This botnet also targets the insecurity of IoT devices, specifically the use of weak default passwords. These IoT devices enable this botnet to carry out a host of methods, such as UDP and TCP floods.

Figure 6: BASHlite file on Github, from Oct 29, 2016

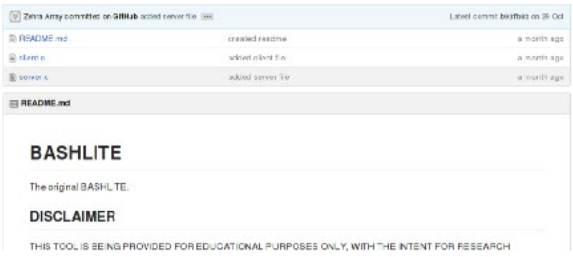
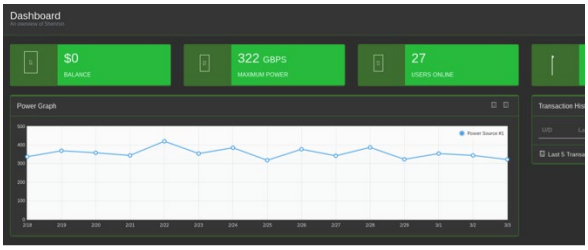


Figure 7: LizardStresser Dashboard



In addition to non-Mirai based IoT botnets, it is critical for defenders to remember that amplification attacks can still be used to conduct large-scale DDoS attacks against their organizations. Amplification attacks against Network Time Protocol (NTP) and open Domain Name System (DNS) resolvers haven't gone away. Far too many DNS servers are misconfigured in a way that can lead to DNS amplification attacks. A Shodan search revealed that 2,104,384 DNS servers have recursion enabled. A Censys search revealed 5,725,817 DNS servers have open recursive resolvers. Misconfigurations like these can lead to attacks like those we saw during the Rio Olympics.[18]

Forecasting The Threat in 2017

The fact that Mirai has been released publicly has substantially lowered the bar for launching large-scale DDoS attacks. The available information has indicated that a certain level of technical capability is required to install and operate Mirai, however it is unlikely that this constitutes a significant obstacle for a determined actor, as guides and advice on this malware are widely available online. Mirai therefore has the potential to act as a force multiplier for a range of actors engaging in DDoS attacks, including hacktivists, extortionists and politically-inspired actors. There are three main motivations behind those who use DDoS as a tactic:

1. Online protest, typically planned, orchestrated and launched by hacktivist groups. These campaigns have targeted specified industries and geographies, both in the private and public sector.
2. Financial profitability, a significant motivation for a number of actors, such as extortion actors who use the threat of DoS or DDoS in return for a ransom payment. This is largely, although not exclusively, the preserve of the cyber criminal. DDoS attacks may also be used as a distraction for network intrusions conducted for profit.
3. Political gain, launched by nation state affiliated actors.

In order to understand what the DDoS threat landscape will look like in 2017, we will leverage the structured analysis technique known as the "cone of plausibility." The method identifies three scenarios for each motivation: a preferable scenario, a probable scenario and a wild card scenario.[19]

Cone of Plausibility Methodology

The cone of plausibility is useful to the analyst and the consumer in that it provides an audit trail of how the scenarios were developed and a structured way of forecasting possible future scenarios. This is because all of the drivers that are assessed to contribute to a given question are listed alongside analyst assumptions of how these drivers will continue. It also allows assumptions to be changed in order for other scenarios, such as wild card or plausible, to be developed.

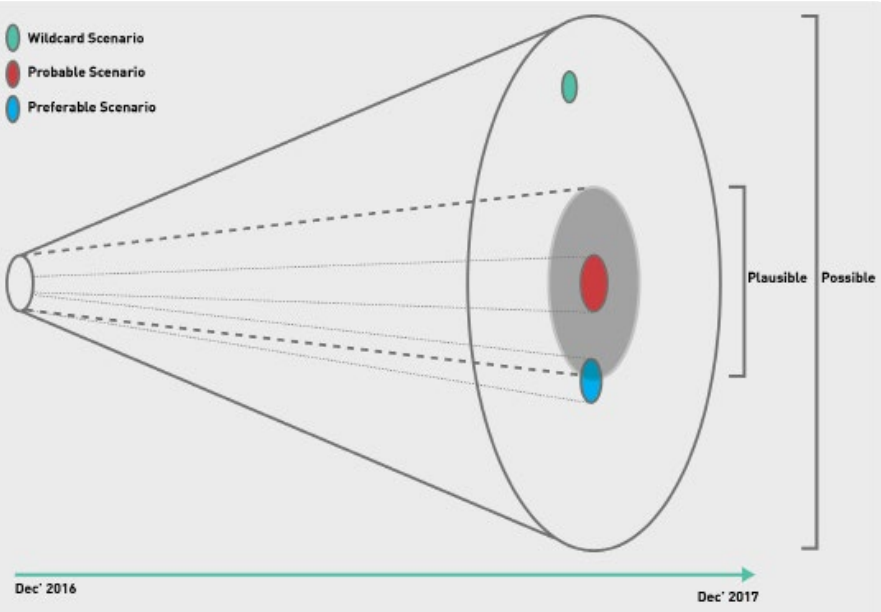
Of course, these are not predictions of the future but provide a framework for assessing scenarios that are based on current drivers and assumptions. This should encourage organizations to look beyond the current noise surrounding IoT botnets and assess the likely threat posed to their organization, sector and geography.

Before creating scenarios, it is first necessary to agree upon the timeframe which, in this case, is one year. The current conditions are then assessed, enabling us to identify the main drivers and trends.

In order to produce scenarios, underlying assumptions are explicitly listed. The most probable or "baseline" scenario is based on a continuation of what we have already observed, coupled with any future influencing events that may change a scenario. Estimating the likelihood of a scenario is largely based on what we have seen already, coupled with an analyst's experience and assumptions.

In order to produce alternative plausible scenarios, one or two assumptions are changed, resulting in a significantly different outcome. Changing yet more assumptions in a radical way will create a vastly different, possible scenario – known as a wild card.

In this way, the cone of plausibility allows for the development of scenarios that are within the bounds of possibility and allows for the thought process behind these scenarios to be more clearly documented.[20] While any number of scenarios can be generated using the cone of plausibility, three provides a solid spectrum for consideration.



The Cone of Plausibility Model for Actors Using DDoS as a Protest Tool

Current conditions

Although some variation in the number of hacktivist DDoS attacks has been observed, Digital Shadows has consistently observed high levels of operational hacktivist activity in 2016. Our reporting record shows notable DDoS activity has been conducted by eight hacktivist actors, with Ghost Squad hackers, New World Hackers and OurMine Team having conducted or claimed the most attacks.[21] It should be noted that hacktivist campaigns normally involve multiple actors with varying levels of involvement and some operations, such as OpIsrael, can involve large numbers of actors. It is possible to identify four broad trends pertaining to hacktivists' use of DDoS in 2016.

1. Most hacktivists aren't financially motivated

Through 2016, the attacks have been conducted in association with a variety of ideological causes, including political ideologies, anti-establishment ideologies and environmental concerns. However, such actors are not primarily motivated by a financial incentive.

The majority of hacktivist activity and the most active campaigns recorded by Digital Shadows have involved the targeting of financial services, governments and technology companies. Seventy-two countries, particularly across North America, Europe and Japan, were targeted by hacktivist actors.

2. Many hacktivists have limited capabilities and rely on off-the-shelf tools

Despite exceptions including campaigns like OpAfrica and actors like Phineas Fisher,[22] the primary tool of hacktivists remains DoS. In some instances however, it has been possible to connect specific TTPs and vectors of attacks with specific actors and operations, if not with specific attacks. The table below shows all of the DDoS TTPs and vectors of attack that have been linked with hacktivist actors or operations in 2016.

Figure 8: An overview of the tactics and tools used by hacktivist actors and operations

Actor/Operation	Tactic Used	Tools Used
Mr Hackintosh		WebHive
Anonymous Saudi	ICMP flood, HTTP flood, SYN flood,	WebHive
OpIcarus	SlowLoris	LOIC, TorsHammer, PyLoris, TorStress, Slowhttptest, Xerxes, and Ufonet, HULK, Saphyra
OpIsrael	HTTP flood	WebHive
OpKillingBay		Bangstresser
OpSaudi	HTTP flood	WebHive
OpSeaworld	HTTP flood, UDP flood	

Aside from New World Hackers' unsubstantiated claims of attacking DynDNS, we have not yet detected hacktivists incorporating Mirai into their toolset. However, as shown below, they are certainly discussing it. The freely available source code of Mirai will act as a force multiplier for hacktivist campaigns that have otherwise demonstrated a low level of sophistication.

Figure 9: IRC Conversation, November 4, 2016

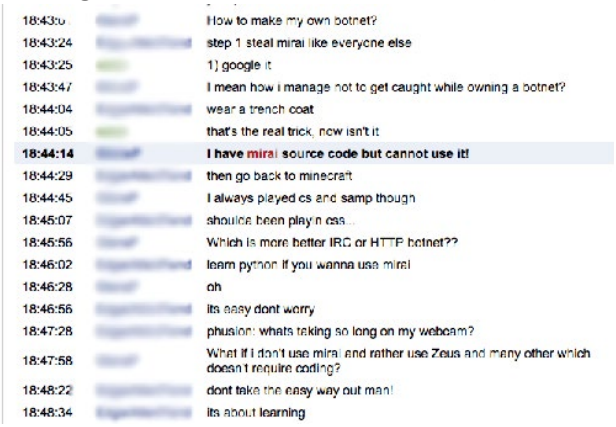


Figure 10: OpIcarus Facebook Post, October 22

3. Media headlines motivate the hacktivist

A large number of hacktivist threat actors have demonstrated the desire to garner media and peer attention as part of their activity. While hacktivists engaging with journalists is not a new phenomenon, a recent trend has been observed of previously unknown actors using the media to self-publicize, speaking to journalists about their attacks in an attempt to garner publicity.[23]

4. Law Enforcement has disrupted hacktivist activities

In 2016, there have been notable successes for law enforcement. In October 2016, several suspected members of Lizard Squad and Poodlecorp were arrested on suspicion of operating DDoS-as-a-Service websites.[24] While such arrests likely act as some sort of deterrent, it should be noted that a great deal of the impetus for the investigation is likely to have been the public sector nature of the targets. Attacks against private organizations are less likely to attract such investigative resources.

Overview of Main Drivers

1. Availability of Tools – The public release of the Mirai source code adds to the availability of tools, however the setup of Mirai is non-trivial for low capability actors and, therefore, the widespread use of Mirai will be dependent on the growth of the DDoS-as-a-Service market. As threat actors continue to incorporate more types of vulnerable devices into their botnets, the availability of tools will increase.

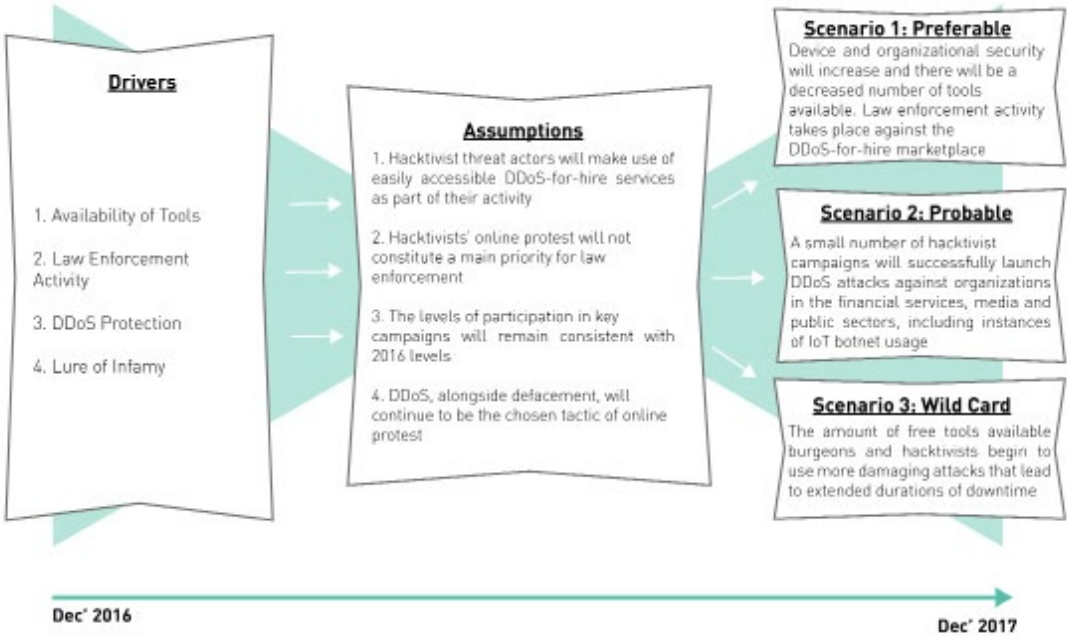
2. Law Enforcement – Law enforcement has had an impact on hacktivists targeting government bodies.

3. DDoS Protection – DDoS protection services have struggled to deal with high-impact attacks, such as Krebs on Security, OVH and DynDNS.

4. Lure of Infamy - A large number of hacktivist threat actors have demonstrated the desire to garner media and peer attention as part of their activity.

Scenarios

Figure 11: The Cone of Plausibility Model for Actors Using DDoS as a Protest Tool



Most Probable

A small number of hacktivist campaigns will successfully launch DDoS attacks against organizations in the financial services, media and public sectors. The increased sophistication of DDoS tools has been achieved through the development of the DDoS-as-a-Service marketplace, which have made use of IoT botnets, allowing hacktivists with low capability to launch high-impact attacks.

Changing our Assumptions

If users and manufacturers improve device security and organizations improve their own security, this will serve to reduce the threat and offer a preferable scenario. The decreased supply of vulnerable devices, alongside an increasing demand from threat actors, will decrease the availability of tools. Although there has been an emergence of DDoS-as-a-Service marketplaces, this will be an area of concern for law enforcement, and it is possible that there will be disruption.

Wild Card Scenario

Alternatively, in a wild card scenario, the availability and amount of free tools, including IoT botnets, greatly increases the accessibility of tools. Hacktivists begin to use more damaging attacks that lead to extended durations of downtime. Hacktivism becomes a real worry for organizations that are named on hacktivist target lists.

The Cone of Plausibility Model for Actors Using DDoS as an Extortion Tool

Current conditions

DDoS extortion has been a real threat to organizations in 2016. The process, shown below, has been relatively standard, wherein threat actors contact a company and threaten to target its infrastructure with DDoS attacks unless a ransom is paid. It is possible to identify several common trends within this area.

1. DDoS Extortion is both profitable and popular

Unlike actors using DDoS as a protest tool, cyber criminals do not tend to publicize their activities – although there are exceptions to this. Additionally, organizations targeted by criminal actors may elect to avoid the negative publicity associated with having been subjected to a cyber attack by not releasing any statements acknowledging that they have been targeted. These reasons likely contributed to fewer criminal actors being identified as active when compared to hacktivists. Nevertheless, there are three main extortion actors that have been active throughout 2016: Kadyrovtsy, Lizard Squad and Armada Collective.

2. A strong reputation is critical for DDoS extortionists

Developing a strong reputation is important for DDoS extortion actors and a good indication of this is the emergence of suspected copycat actors. For example, it is likely that copycat actors not affiliated with the Armada Collective used the group's name to add credibility to spam email campaigns.

Mirai's publicity is likely to result in high volumes of extortion attempts that have no intention of actually launching an attack, but rather seek to reference Mirai to intimidate targets into paying the ransom. Users of the Web Hosting Talk forum recently reported receiving Mirai extortion emails from "annasenpai[at]sigaint[.]org" demanding a ransom of two BTC (approximately $1320 USD). These appear to have been empty threats, with no attacks taking place after expiry of the stated 96 hour window.[25]

Figure 12: Extortion email using the Anna Senpai and Mirai names

3. Limited success from law enforcement.

In January 2016, Europol published a press release stating that an individual suspected of being a "key member" of the extortionist group DD4BC had been arrested, and that a further suspect had been detained in Bosnia and Herzegovina.[26] Although other actors, such as Armada Collective and Kadyrovtsy, filled the void left by DD4BC, it is possible that these arrests helped to change the impression that DDoS extortion could easily profit with relative impunity.

Overview of Main Drivers

1. Availability of tools – The public release of the Mirai source code adds to the availability of tools, however the setup of Mirai is non-trivial for low capability actors. There are early indications of IoT botnets being incorporated into the pre-existing, professionalized DDoS-as-a-Service market, as demonstrated by claimed offerings of vendors such as BestBuy.[27]

2. Target availability – Although instances of cyber extortion are underreported, there are organizations that do pay, succumbing to extortion demands.

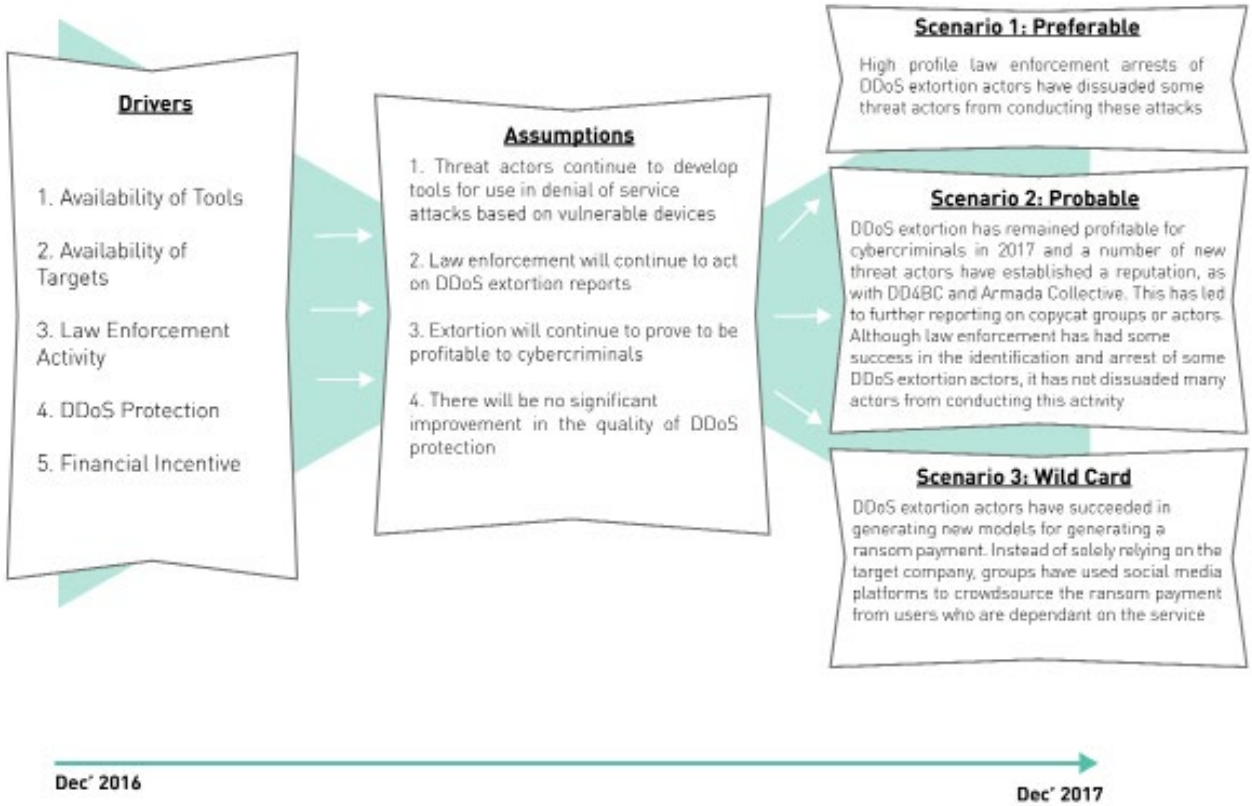
3. DDoS protection - The quality and adoption rate of DDoS protection services, and their ability to thwart large-scale attacks, has a significant impact on the threat posed by DDoS.

4. Financial incentive - Actors continue to be driven by revenue, and extortion will remain a profitable business for cyber criminals.

5. Law enforcement – The arrest of DD4BC in January demonstrated intent by law enforcement to investigate and prosecute DDoS extortion actors.

Scenarios

Figure 13: The Cone of Plausibility Model for Actors Using DDoS as an Extortion Tool



Most Probable

Based on these drivers and underlying assumptions, in December 2017, the most probable scenario is that actors will emerge and build up their reputation, as with Armada Collective and DD4BC. Actors seeking to benefit from this reputation will emerge and conduct copycat attacks. Actors will seek to add to their threat by using the name of high-profile IoT botnets in their extortion email. While high-profile law enforcement arrests of DDoS extortion actors have dissuaded some threat actors from conducting these attacks, the tactic continues to be profitable for threat actors. In particular, as retail organizations prepare for the 2017 holiday season, actors will seek to target these organizations.

Changing our Assumptions

Changing assumptions about the role played by law enforcement in 2017 will have an impact, and a preferable scenario would be the high-profile arrests by law enforcement of DDoS extortion actors. Such arrests succeed in dissuading some threat actors from conducting these attacks and build confidence in organizations' decisions not to pay ransom demands.

Wild Card Scenario

In a wild card scenario, DDoS extortion actors have succeeded in creating new models for generating a ransom payment. Instead of solely relying on the target company, groups use social media platforms to crowdsource the ransom payment from users who are dependent on the service. For example, following an attack against a gaming network, such as Xbox Live or PlayStation Network, attackers would demand ransom payments from users themselves.

The Cone of Plausibility Model for Actors Using DDoS as a Political Tool

Current conditions

It can be tempting to think of DDoS as a tactic limited to hacktivists and extortionists. However, it has been a key tool in nation state arsenals for many years, allowing actors to combine psychological operations, network operations, information gathering and military action to form a cohesive strategic plan.[28] Of course, state actors operate with a high degree of operations security, enabling plausible deniability to avoid the geopolitical consequences of having engaged in the targeting of foreign entities.

Nevertheless, it is possible to identify several politically-motivated attacks. The most famous example occurred with the attacks on Estonia and Georgia in 2007 and 2008 respectively. However, these attacks were not isolated.[29] For example, in the late 1990s, following the bombing of the Chinese Embassy by a U.S. airplane in the former Yugoslavia, NATO computers and U.S. military sites were attacked.[30] More recently, in 2015, the targeting of Github with a prolonged DDoS attack was highly likely to have been carried out by the Chinese state.

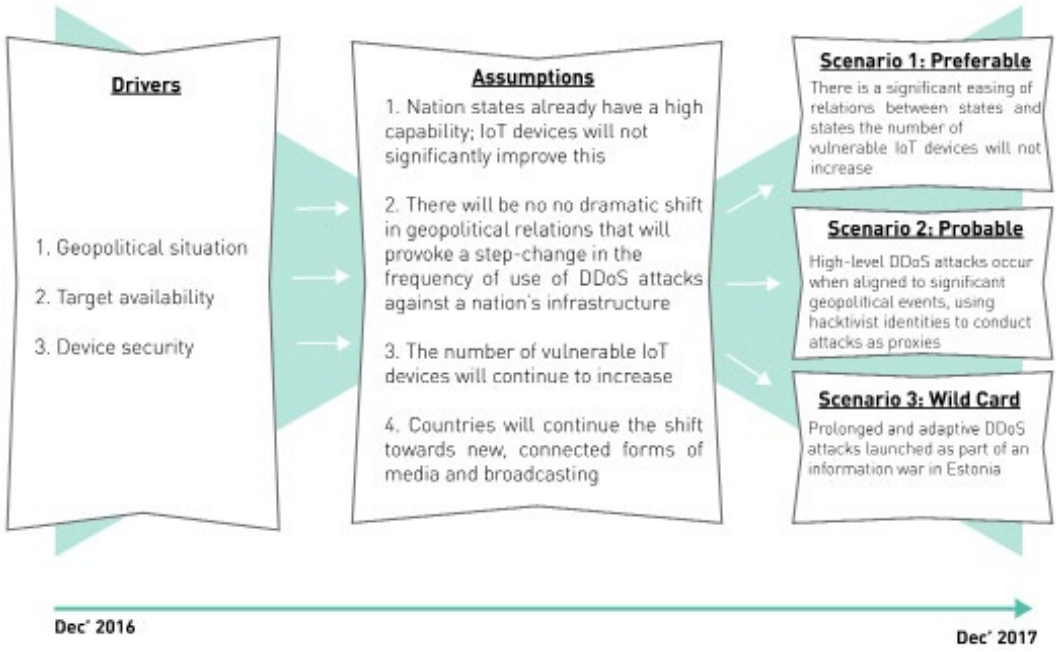
In 2016, only one instance of a DDoS attack has been reported which was suspected to be linked to a state or state proxy actor, although this attribution was never confirmed. In March 2016, a number of Swedish websites were rendered offline by what appeared to be multiple targeted DDoS attacks. Several online sources have claimed that the attacks originated in Russia due to an increase in activity originating from several Russian ISPs. Additionally, some Swedish sources have suggested that the attacks originated in Russia and were carried out by Russian actors. The attacks either partially or totally shut down a number of Swedish news sites.[31]

Overview of Main Drivers

1. **Geopolitical situation** – The geopolitical situation between countries has acted as the main factor for nation state affiliated actors launching DDoS attacks this year.
2. **Targets available** – Countries, even those that are less mature, have adopted new technologies apace and are now more and more connected. Media and broadcasting organizations within target countries are a particularly attractive target, such as the incident in Sweden in March 2016.
3. **Device security** – The extent to which there is a sufficient number of insecure IoT devices to exploit will have an impact on the prevalence on DDoS attacks launched for political reasons. While the scramble to generate large botnets may be considered a zero sum game, the increase in IoT devices may lead to a never-ending pool of vulnerable devices.

Scenarios

Figure 14: The Cone of Plausibility Model for Actors Using DDoS as a Political Tool



Most Probable

Based on the current drivers and the assumptions we have made, it is probable that while there will be no dramatic shift in geopolitical relations that will provoke a step-change in the frequency of use of DDoS attacks against a nation's infrastructure, it is possible that there will be a small number of reactive attacks to previously unforeseen events. High-level DDoS attacks are most likely to occur when aligned to significant geopolitical events, such as the on-going political crisis in South Korea and the disruption likely to be caused by resignation and possible impeachment of Park Geun-Hye. In this instance Government entities, media and broadcasting organizations would be likely targets. The extensive breached data that is publicly available allows states to easily develop convincing hacktivist legends and act with a high degree of plausible deniability.

Changing our Assumptions

Another plausible and preferable scenario would occur if the number of vulnerable IoT devices were to actually decrease, limiting the potential numbers of actors with significant botnet sizes. When combined with a growing realization and awareness of the threats posed to industries like media and broadcasting, this would likely create a more favorable environment. However, the most significant driver is the geopolitical situation between states. A significant easing of relations between major states, such as the United States and Russia, would further create a more favorable environment. Added to this, states have become more cognizant of the threat posed to industries like media and broadcasting, prioritizing security and resilience accordingly.

Wild Card Scenario

In a wild card scenario, Juri Ratas, the Prime Minister of Estonia, loses power, causing the political climate to be split between pro-Russian and pro-European Union candidates. In a move to consolidate their influence in the region, Russia affiliated actors target broadcasting organizations, online newspapers and social media that are anti-Russian with prolonged and adaptive DDoS attacks. The botnets used to conduct these attacks include vulnerable IoT devices and other web services, such as Content Management Systems, and the websites targeted are inadequately prepared to deal with the attacks.

Mirai: The "Future" of DDoS?

As previously stated, the translation of "Mirai" from Japanese is "the future". If claims by actors such as BestBuy and Popopret are true, the total number of IoT devices infected with Mirai has increased since this malware variant was publicly released on September 30, 2016.[32]

The past has shown us that when malware source code is published freely online, the code will inevitably be adapted and new variants will emerge. The reuse of code is a resource saver and can help actors with a lower capability, as well as those with a higher capability, by providing access to well-developed malware code for use in their own variants.

However, not all of the malware variants developed from published source code are successful and not all of them will become prominent. A great example of this evolutionary phase occurred in 2015, when the source code for the "hidden tear" ransomware was published online and made available for anyone who cared to use it. While the code was used in numerous new variants, many contained serious problems, such as "Cryptear" that was discovered in January 2016 and was all but unusable due to the use of an encryption routine which was easily overcome by researchers.

The emergence of successful and dominant malware variants based on released source code is likely to be the result of actors or groups with the capability and resources to improve or develop the malware's code for use in attacks. An example of this was the use of the leaked Gozi banking trojan source code to develop the GozNym banking trojan, whereby developers had taken the web-inject module of Gozi and combined it with that of the Nymaim trojan. As of April 2016, GozNym had reportedly resulted in the theft of $4 million USD.

While published source code does not necessarily constitute an increased threat level overall, it does provide access to the nuts and bolts of functioning malware that can be modified or improved to create new variants. When combined with the appropriate resourcing and capability, it has the potential to lead to the emergence of a handful of prominent malware variants. We have already seen botnets that include more devices, such as home routers, and given the amount of vulnerable devices it is likely that we will see more. For example, we found other esoteric devices, such as Automatic Number Plate Recognition, 3G backups, GPRS modems and cable set-top boxes were also vulnerable. And this is only for IoT devices. It is important to consider the implications of botnets that incorporate far more than IoT devices, as the potential for incorporating vulnerable web servers, such as Content Management Systems, into these botnets is a strong possibility.[33]

The success of these variants, which will inevitably emerge from the release of the Mirai source code, depends upon their adoption by well-resourced groups with profitable business models and the means and motivation to continually develop their "product," take it to market and satisfy their customers with good service.

What Practitioners can do to Prepare for DDoS in 2017

These scenarios demonstrate that there are many factors that must be considered when forecasting the threat posed by DDoS in 2017. These forecasts allow organizations to consider alternative scenarios and look beyond the current noise surrounding IoT botnets to assess the likely threat posed to their organization, sector and geography.

Prepare for the Probable; Consider the Plausible

Protest	A small number of hacktivist campaigns will successfully launch DDoS attacks against organizations in the financial services, media and public sectors. The increased sophistication of DDoS tools has been achieved through the development of the DDoS-as-a-Service marketplace, which have made use of IoT botnets, allowing hacktivist with low capability to launch high-impact attacks.
Extortion	Actors will emerge and build up their reputation, as with Armada Collective and DD4BC. Actors seeking to benefit from this reputation will emerge and conduct copycat attacks. Actors will seek to add to their threat by using the name of high-profile IoT botnets in their extortion email. While high profile law enforcement arrests of DDoS extortion actors have dissuaded some threat actors from conducting these attacks, the continuing discovering of more vulnerable IoT devices means that this tactic continues to be profitable for threat actors. In particular, as retail organizations prepare for the 2017 holiday season, actors will seek to target these organizations.
Political	High-level DDoS attacks are most likely to occur when aligned to significant geopolitical events, such as the on-going political crisis in South Korea and the disruption likely to be caused by resignation and possible impeachment of Park Geun-Hye. In this instance Government entities, media and broadcasting organizations would be likely targets. The extensive breached data that is publicly available allows states to easily develop convincing hacktivist legends and act with a high degree of plausible deniability.

Although the current drivers and our underlying assumptions have identified these three scenarios, it is important to note that any number of these variables could change. For these purposes, we have created the alternative scenarios that allow organizations to understand how they might be protected against evolving threats.

These scenarios enable both the analyst and consumer to consider the multiple possible future outcomes, what they might entail and how they might impact operations, and test them against future policies and strategies. Furthermore, warning indicators can be developed and monitored to show how something is developing, for example, if a scenario is coming true or if factors have emerged that make scenarios less likely.

10 Steps to Protect Against DDoS in 2017

Don't hyper focus on individual threats like Mirai. Mirai will evolve and other DDoS attack vectors will emerge. Instead of focusing on the threat de jour, focus on building resilience into all of your external-facing services. Start with these 10 steps:

1. **Build out your threat model.** Understand the threat actors targeting your industry and geography and monitor which tools they are using. This will allow you to prioritize security spending based on threats specific to you.

2. **Prioritize the services that must be available and confirm executive buy-in for DDoS protection/mitigations.** Gain this buy-in by communicating the losses incurred for downtime. How much will one hour of downtime cost you? How does that line up against the cost of protection?

3. **Don't be part of the problem- A.** Secure your own devices and do not use default or generic passwords. Consider disabling all remote access to devices and perform administrative tasks internally, instead of via Telnet, FTP and HTTP use SSH, SFTP and HTTPS.

4. **Don't be part of the problem - B.** To address DNS reflection, disable recursion on authoritative name servers and limit recursion to authorized clients. To address NTP reflection, update ntpd to the latest version and disable the monitor function for legacy ntpd versions.

5. **Develop a DDoS response playbook.** Developing a DDoS attack response playbook in the midst of a DDoS attack that has taken your critical services offline is a less than ideal situation. Be proactive so that you can fully vet the playbook with all affected stakeholders.

6. **Prepare for a DDoS extortion scenario.** Assume that you will receive a DDoS extortion attempt. Establish internal processes for mitigation, recovery and external communication.

7. **If possible, test out your DDoS mitigation service.** The theoretical swing to a migration service is very different than the actual swing to that service. Fully understand the realities of DNS redirection or Border Gateway Protocol (BGP) routing changes and validate your service provider's migration capabilities

8. **Understand that all DDoS attacks aren't volumetric.** Ask your upstream and on-premises DDoS mitigation providers how they address application level attacks. Deploy countermeasures to "low and slow' attacks that target your services.

9. **Don't lose situational awareness.** When leveraging an upstream mitigation provider, you can lose visibility as the service provider alerts you when an attack is in place. Work with service providers to ensure you get monitoring and logging capabilities that help identify precursors to attacks before it's too late.

10. **Become familiar with the infrastructure and configuration of your external services.** Ensure that the requisite redundancy and failover capabilities are available and working for these services.

End Notes

1. http://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/
2. https://twitter.com/NewWorldHacking/status/795530737407574016
3. Investigation of Linux.Mirai Trojan family, hxxps://st[.]drweb[.]com/static/new-www/news/2016/september/Investigation_of_Linux.Mirai_Trojan_family_en.pdf.
4. KrebsOnSecurity Hit With Record DDoS, hxxps://krebsonsecurity[.]com/2016/09/krebsonsecurity-hit-with-record-ddos.
5. https://content.akamai.com/pg7407-soti-security-report-q3-en.html
6. https://f5.com/about-us/news/articles/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-ddos-attack-on-ovh-21937
7. Dyn Statement on 10/21/2016 DDoS Attack, hxxp://dyn[.]com/blog/dyn-statement-on-10212016-ddos-attack.
8. https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/
9. https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-really-take-liberia-offline/
10. https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/
11 https://packetstormsecurity.com/news/view/27233/Deutsche-Telekom-Says-Fixed-Network-Outage-May-Be-Work-Of-Hackers.html
12. https://isc.sans.edu/forums/diary/Port+7547+SOAP+Remote+Code+Execution+Attack+Against+DSL+Modems/21759/
13. http://www.bbc.co.uk/news/technology-38167453
14. CCTV DDoS Botnet In Our Own Back Yard, hxxps://www[.]incapsula[.]com/blog/cctv-ddos-botnet-back-yard.html.
15. http://blog.level3.com/security/attack-of-things/
16. http://blog.level3.com/security/attack-of-things/
17. http://blog.malwaremustdie.org/2016/10/mmd-0059-2016-linuxirctelnet-new-ddos.html
18. http://www.itworldcanada.com/article/rio-olympics-faced-olympic-sized-ddos-attacks/386207
19. http://webarchive.nationalarchives.gov.uk/20140108140803/www.bis.gov.uk/assets/foresight/docs/horizon-scanning-centre/foresight_scenario_planning.pdf
20. http://webarchive.nationalarchives.gov.uk/20121212135622/http://www.bis.gov.uk/assets/foresight/docs/horizon-scanning-centre/foresight_scenario_planning.pdf
21. Other actors among the eight were Phantom Squad, Anonymous Saudi, DownSec Belgium, K., and Mr Hacktintosh.
22. https://www.reddit.com/r/netsec/comments/4f3e6p/full_english_translation_of_phineas_fishers/
23. https://www.youtube.com/watch?v=BpyCl1Qm6Xs

24. https://www.justice.gov/usao-ndil/pr/american-and-dutch-teenagers-arrested-criminal-charges-allegedly-operating
25. http://www.webhostingtalk.com/showthread.php?t=1606018
26. https://www.europol.europa.eu/newsroom/news/international-action-against-dd4bc-cybercriminal-group
27. http://motherboard.vice.com/read/two-hackers-new-mirai-internet-of-things-botnet-deutsche-telekom
28. https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf
29. https://www.wired.com/2007/08/ff-estonia/
30. ACTIVISM, HACKTIVISM, AND CYBERTERRORISM: THE INTERNET AS A TOOL FOR INFLUENCING, Denning, D.E., in Networks and netwars: The future of terror, crime, and militancy, 2001.
31. Sites included: Dagens Nyheter, Svenska Dagbladet, Expressen, Aftonbladet, Dagens Industri, Sydsvenskan and Helsingborgs Dagblad
32. http://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/
33. https://www.digitalshadows.com/blog-and-research/plumbing-the-depths-the-telnet-protocol/

About Digital Shadows

Digital Shadows provides insight into an organization's external digital risks and the threat actors targeting them. Digital Shadows SearchLight™ service combines scalable data analytics with human analysts to monitor for cyber threats, data leakage, and reputation risks. Digital Shadows continually monitors the Internet across the visible, deep and dark web, as well as other online sources to create an up-to-the minute view of an organization and provide it with tailored threat intelligence. The company is jointly headquartered in London and San Francisco. For more information, visit www.digitalshadows.com.

London +44 (0) 203 393 7001
Level 39, One Canada Square, London, E14 5AB

San Francisco +1 (888) 889 4143
332 Pine Street, Suite 600 San Francisco, CA 94104

info@digitalshadows.com

digital shadows_