Mirai Botnet Continues to Plague IoT Space

blog.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space

Threat Research | September 10, 2019

Blog Author
Josip Milić, Software Engineer at ReversingLabs. Read More...

The concept of devices with a specific purpose, interconnected over the Internet, was introduced in the 1980's when a beverage vending machine reported its inventory and temperature (i.e. data on whether the stored drinks were cold) back to a central server. This was not set up by the machine distributor, but university engineers who were fed up with the fact that they would walk great distances to the vending machine and find it empty, or even worse, filled with warm drinks. Their idea was simple- provide useful information, wirelessly and automatically.

This concept has evolved into what we call the 'Internet of Things (IoT).' And while this term has been with us for over two decades, it took years of computer hardware and software development, especially in the fields of network connectivity and infrastructure, for IoT to become commercially viable and accessible to the mass population. All kinds of monitoring, automation, and accessory devices, ranging from Internet routers, web-based cameras, and remote monitoring sensors, became cheaper and more readily available. It's not a big surprise that since the beginning of the current decade, the number of IoT devices has grown and continues to grow exponentially. Current estimates of IoT devices per person worldwide is around 3.5, and this is projected to grow to 9.4 in 2025 - that is a lot of devices with access to the Internet!

Throughout our digital history lots of regular computer and server vulnerabilities have been exposed, and unfortunately these unpatched systems have been exploited by attackers. Subsequently, hardware and software manufacturers have taken action to minimize attack points, and their customers have invested in additional third-party security solutions in efforts to mitigate their risks from attack. And while security has gained more attention, there has also been increasing interest in finding new security holes to leverage in malicious activities as well. Attackers are innovating as fast as security providers innovate. Knowledge taken from this never-ending battle has helped create better security standards and practices,

however IoT manufactures and their devices are still catching up to them. It doesn't help that some IoT manufacturers rush to bring their products to market for competitive advantage, often overlooking fundamental security in the process. This makes them potentially exposed to different kinds of attacks, including those which were already seen and studied, thus potentially avoidable.

Introducing Mirai

With growing interest in the potential of IoT and connected things, attackers have found opportunities to exploit these devices. New malware and botnets (i.e. a network of interconnected devices or robots which are controlled by an attacker through a Command and Control (C&C) server) are being specifically built to target IoT devices. BASHLITE was one such early malware used to infect IoT devices.

Another malicious software is known as Mirai. Mirai is perhaps the most famous IoT botnet used to create distributed denial of service (DDoS) attacks with record breaking traffic peaks (reported up to 1 Tbits). In September 2016 Mirai was used to create huge botnets which simultaneously attacked high profile web sites and service providers, for example:

- Potent IoT DDoS Attack Leverages Published Source Code
  1 Tbits DDoS attack hits OVH (French web hosting provider)
- DDoS Attack Uses Mirai
  Undisclosed traffic peak DDoS attack hits Dyn (DNS service provider)
- Cyber Criminals Get Jail
  620 Gbits DDoS attack reported by the owner

These events made headlines even on non-security focused websites, and (re)raised questions about security of IoT devices, particularly since most of the infected IoT devices were consumer-centric home security systems. The most concerning part of the story was that Mirai didn’t use something special to infect the IoT devices - it used a simple brute force technique with a predetermined list of default credentials for various IoT devices. TCP SYN probes had been sent to random IPv4 addresses (except private networks and certain subnets) on Telnet TCP ports 23 and 2323. In case of a response from pinged devices it would try to login using the default credentials and if successful, reported the credentials to a C&C server. A scanning file would then be downloaded from the server to find out the underlying architecture and finally - the appropriate Mirai malware would be executed and then wait for attack commands from the server. There is also an interesting fact that any other found malware was removed. The infected devices still worked as intended, with some occasional resource issues making them appear slow, so its users couldn't detect that there was something wrong with their devices.

Once the targets had been chosen, they received attack commands from the C&C server and started the DDoS attacks which were difficult to mitigate since they came from devices with many different IP addresses. There are reports that the number of devices infected by Mirai peaked at 600,000! A simple solution was to reboot the infected IoT device and change

the login credentials, but as noted, most users were unaware of the issue, and many vendors don't bother to patch the devices to make them more secure, or often didn't have the resources or capabilities to update.

Shortly after the attacks (end of September 2016), the source code of Mirai malware was put online making it available for anyone to use the malware or create new variants (Figure 1). There are reports of new variants which have emerged such as Okiru, Masuta, PureMasuta, Satori, OMG and Wicked. They are designed to use various other attack methods, so the malware has advanced beyond just DDoS attacks.

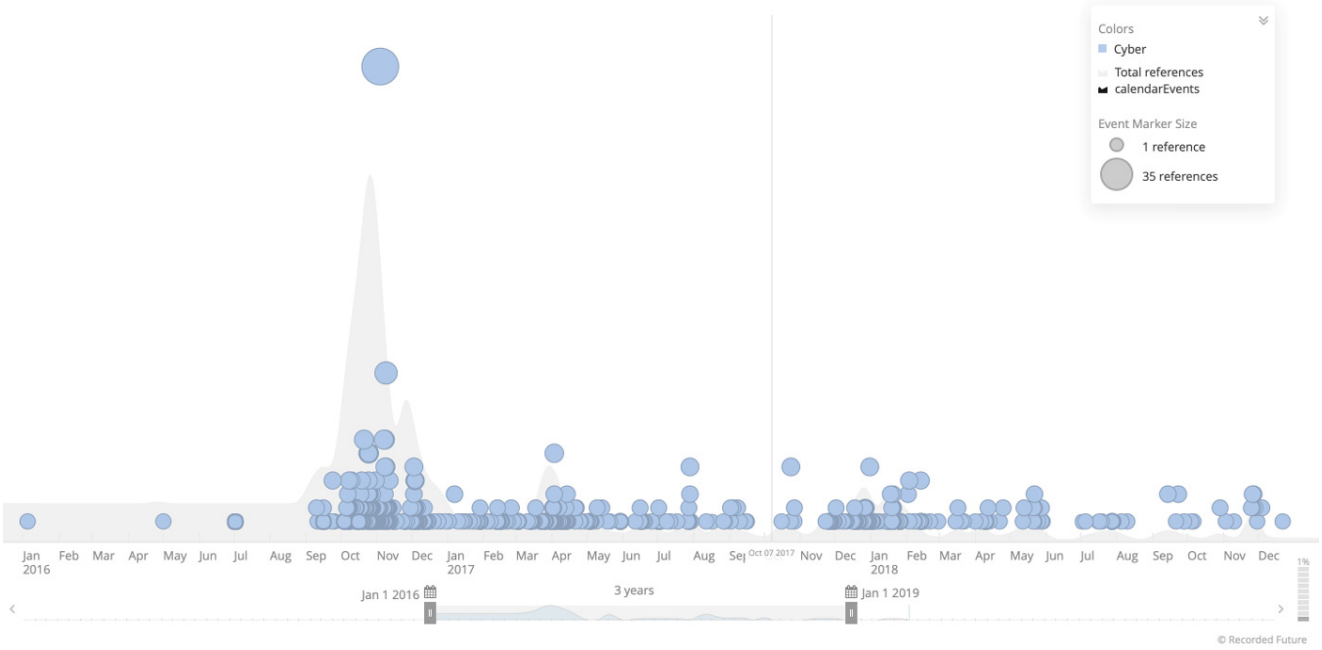

Figure 1: Recorded Future chart illustrating rise of Mirai and variants

Additional Mirai research is highlighted in the 1H 2019 NETSCOUT Threat Intelligence Report

Using ReversingLabs malware analysis repository, which includes insights into over 1.5 billion files, we can track the number of Mirai samples observed and collected from the wild for the first time. Figure 2 shows the increasing trend in the number of Mirai samples collected over time, with an approximate 2x increase in the 2nd half of 2018. Of all the 218K different Mirai files the repository contains, half of them (110K) were first seen since the beginning of the current year (2019).

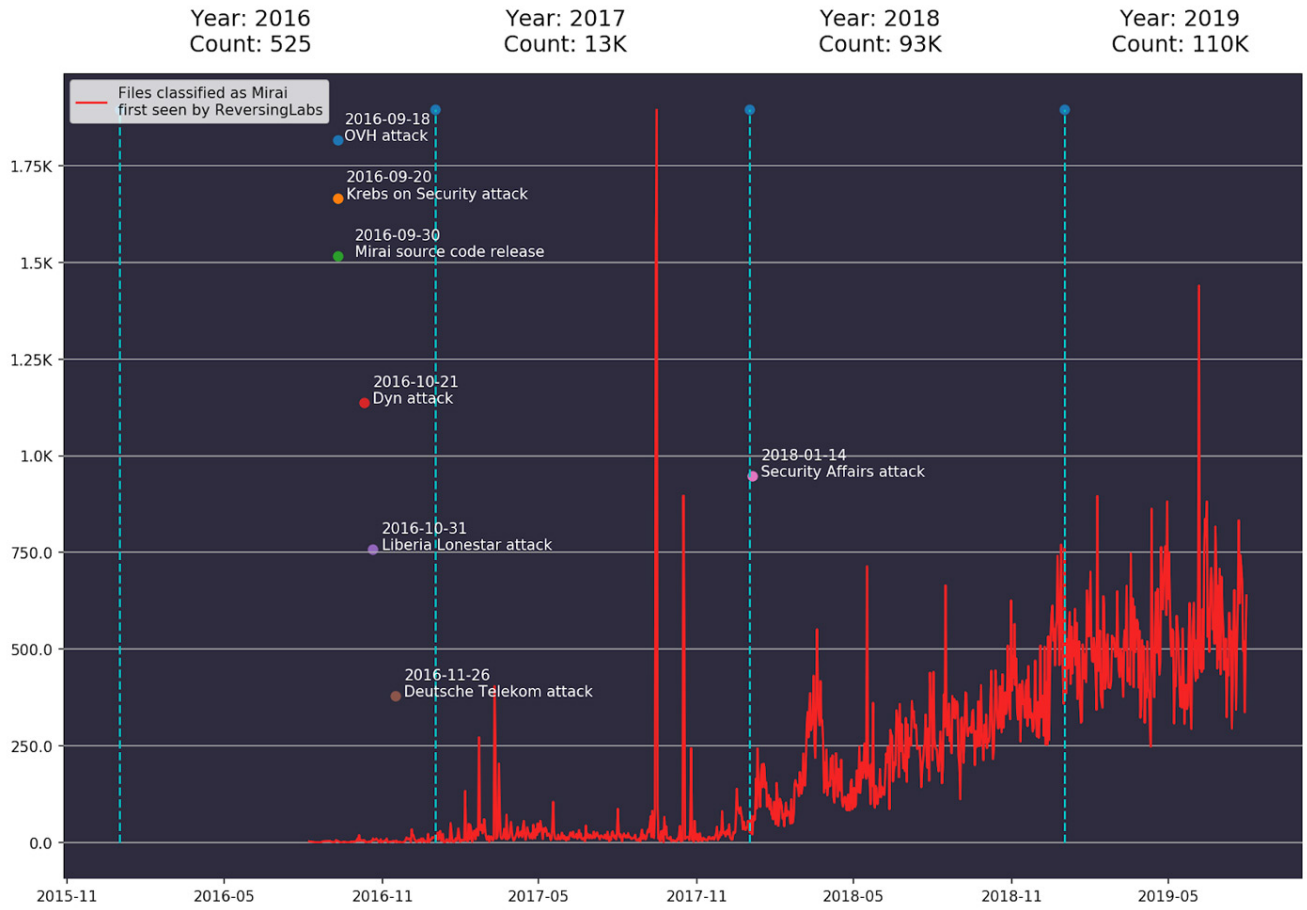

Figure 2: Number of Mirai files first seen by ReversingLabs

Most of the Mirai files first seen in the current year have ELF as their identified file type, which is expected since Mirai targets Linux embedded systems (Figure 3). There are some Text files (mostly shell scripts) and interestingly one image file (a JPEG) which is used as a downloader.

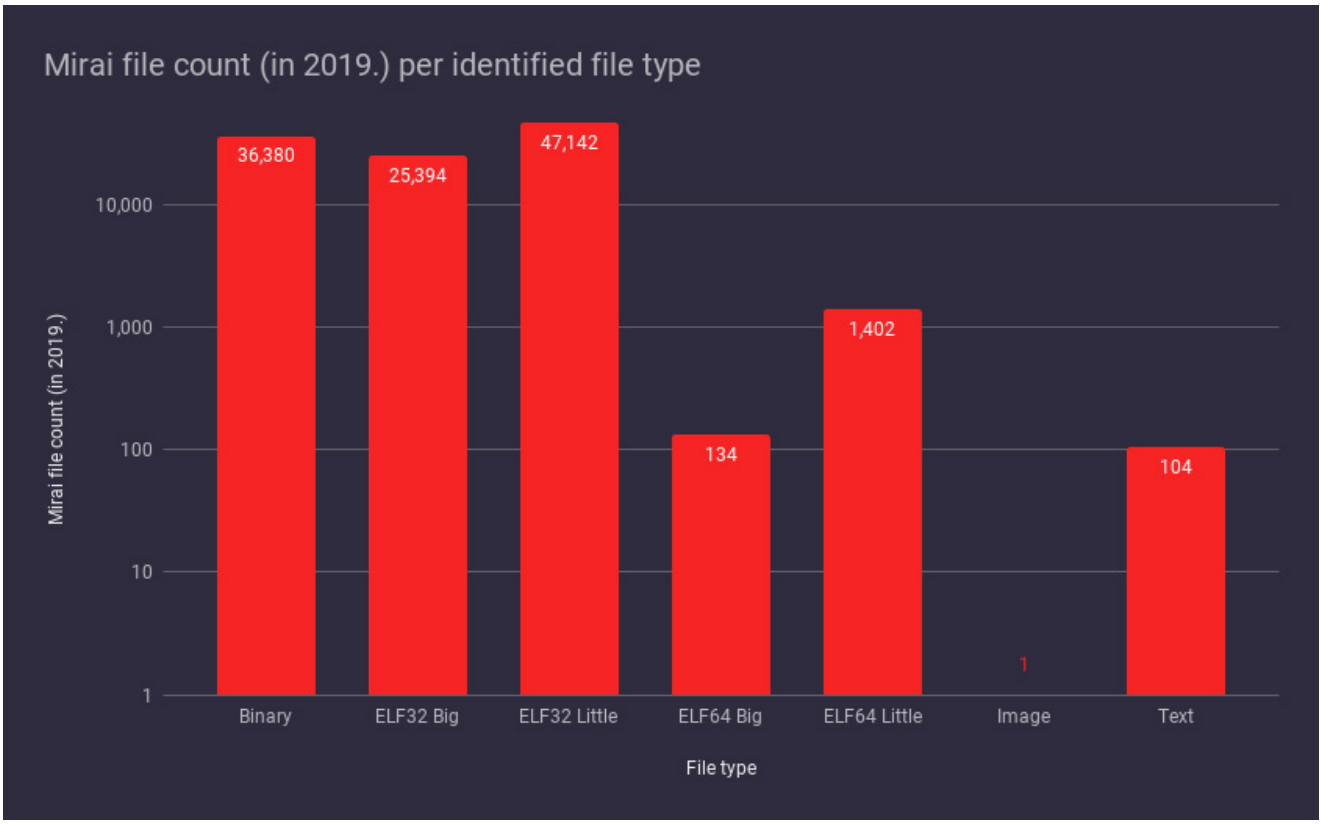

Figure 3: Mirai File count by File Type

In taking a closer look at this JPEG image file in the downloader using the A1000, the malware analysis and investigation component to ReversingLabs Titanium Platform (Figure 4), we can see that it contains 180 files embedded inside of it, and 18 of them have a malicious classification.

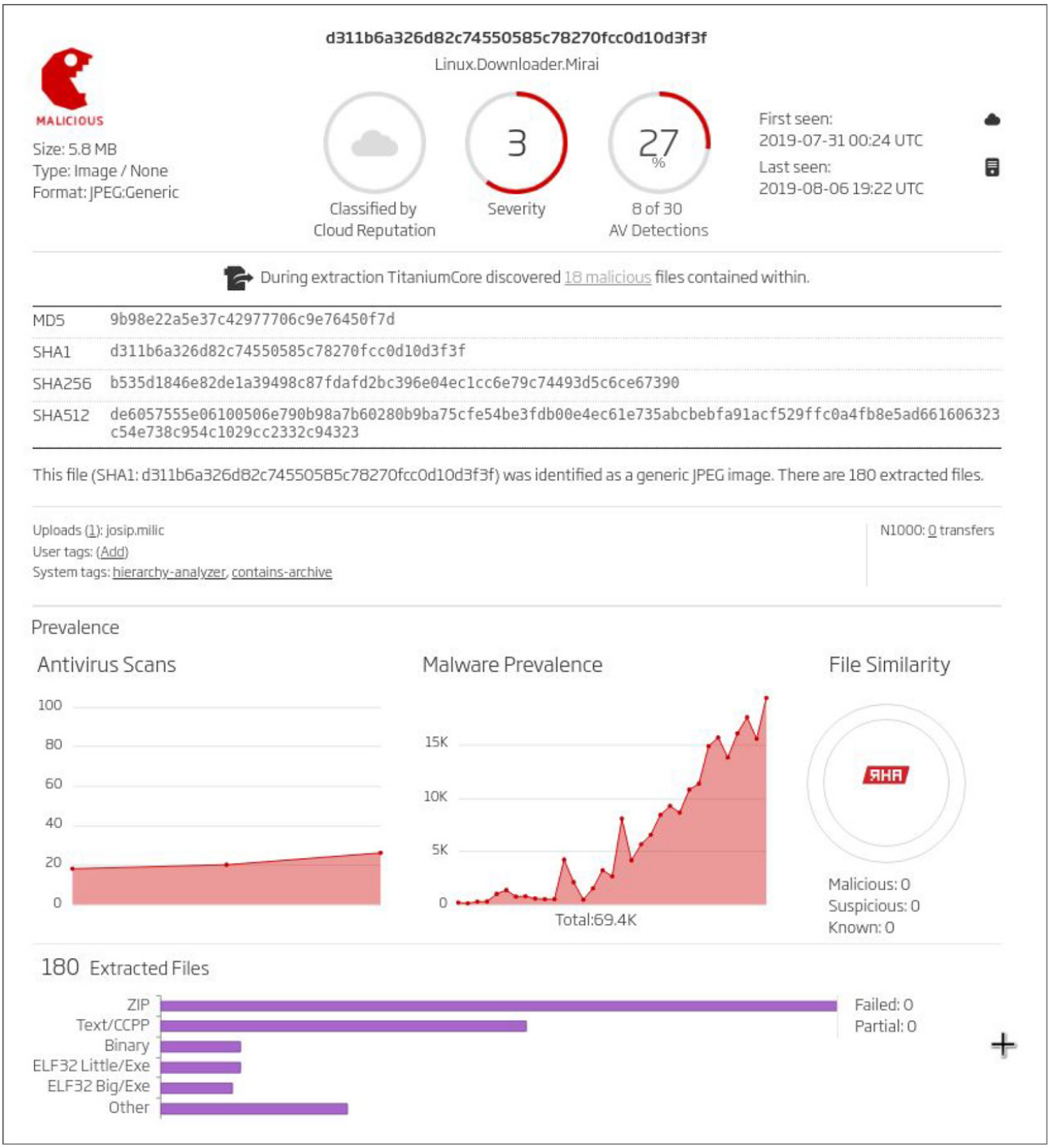

Figure 4: ReversingLabs A1000 Console

The Mirai botnet continues to reign as the king of IoT malware. And its proliferation through cybercriminal and hacker code sharing, increasing efficiencies across the dark web ecosystem, and innovations in payload obfuscation and delivery continue to make Mirai a potent threat. On a positive note, the community is seeing more arrests of botnet operators, as well as new regulations on IoT device security that will drive manufacturers to factor security into their products.

MORE BLOG ARTICLES