SECURITY (HTTPS://WWW.INCAPSULA.COM/BLOG/CATEGORY/SECURITY) · APRIL 10, 2017

How to Identify a Mirai-Style DDoS Attack

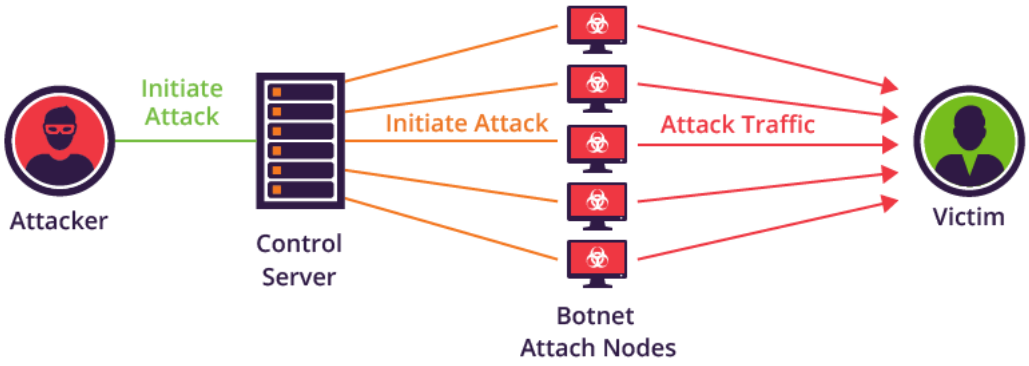
Guest Author Andrew Shoemaker (https://www.incapsula.com/blog/author/andrewshoemaker)

The Mirai internet of things (IoT) botnet is infamous for targeting connected household consumer products. It attaches itself to cameras, alarm systems and personal routers, and spreads quickly. The damage can be quite substantial. People might not realize that their internet-enabled webcam was actually responsible for attacking Netflix.

My company NimbusDDOS (https://www.nimbusddos.com) recently co-hosted a webinar with Incapsula to help ops teams and consumers alike understand Mirai better. You can watch the full broadcast "How to Identify a Mirai-Style DDoS Attack (https://www.brighttalk.com/webcast/14611/249565?utm_campaign=webcasts-search-results-feed&utm_content=How%20to%20Identify%20a%20Mirai-Style%20DDoS%20Attack&utm_source=brighttalk-portal&utm_medium=web)" online.

A DDoS Botnet

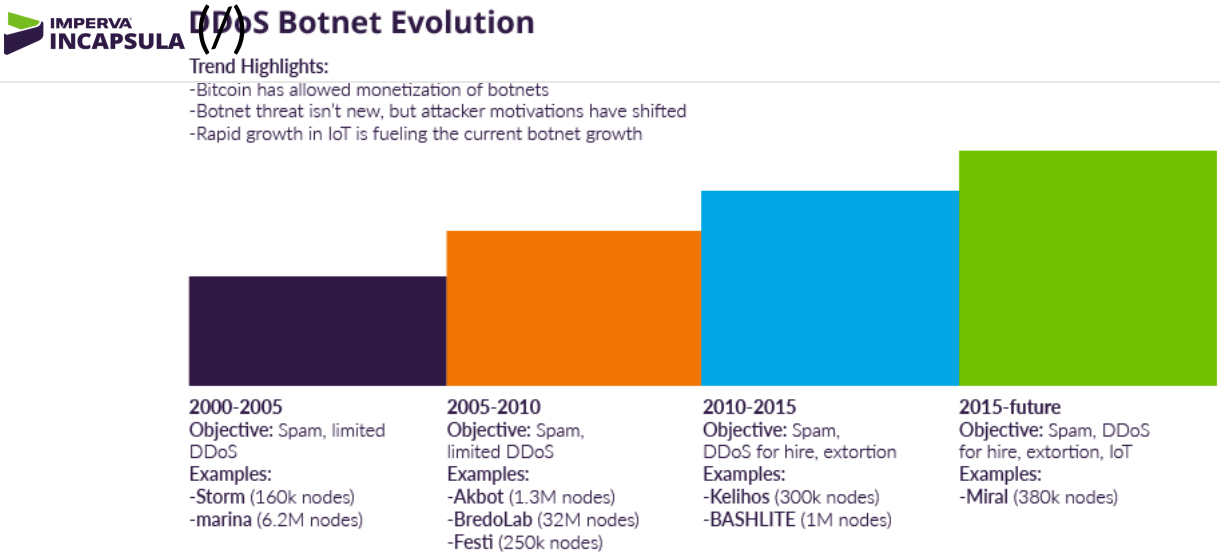
A DDoS botnet attack is pretty straightforward. It gives commands to the control server. And the control server issues attack commands to each of the individual nodes (infected devices) in the botnet. They in turn send the attack traffic to the target.



Not all DDoS attacks (https://www.incapsula.com/ddos/ddos-attacks/) come from botnets, but here's why botnets are effective.

- **Obfuscation** – The attacker is able to conceal themselves from the victim.
- **Amplification** – By using compromised systems, the attacker can launch a larger attack.
- **Geographical Dispersion** – A large botnet can span the globe making for a massively distributed attack that is hard to mitigate.

There's nothing new about botnets. They've been with us for a long time. In fact, some very large ones existed in the early 2000s that involved millions of nodes.

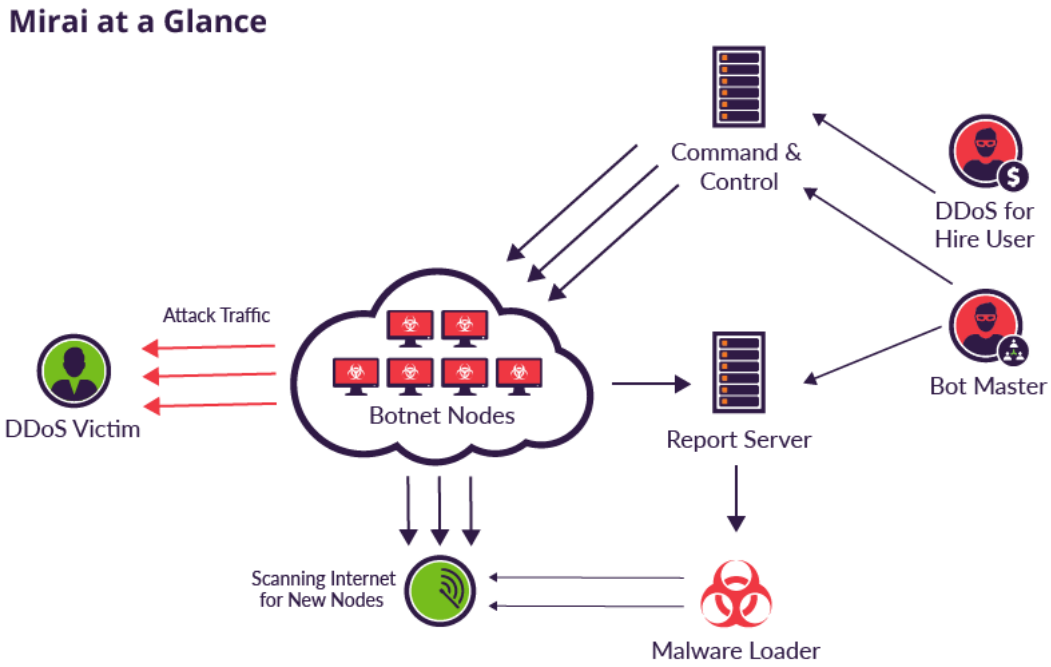


Evolving the DDoS Attack

But there's been a major shift over time in the motivation of the people behind the DDoS attacks. Instead of simply trafficking in spam, botnet operators have figured out a way to monetize their efforts through extortion or by launching a DDoS-for-hire platform like Mirai (https://www.incapsula.com/blog/new-variant-mirai-embeds-talktalk-home-routers.html).

When people talk about Mirai they often talk about the emerging threat caused by household IoT devices. This doesn't account for 100 percent of Mirai activity, but certainly there are some aspects that make these personal devices attractive to attackers.

- Large Numbers of Devices – Most people have a single computer, but they probably also have multiple internet-enabled appliances.
- Vendor Security Is Weak – IoT appliances have historically not been very secure, causing a proliferation of insecure devices.
- Consumers Neglect Security – Consumers are less likely to secure their internet toaster than their personal computer.
- Emerging Market Means Opportunity – With the proliferation of the IoT, the pool of possible botnet nodes is growing. The numbers are in the attacker's favor.
- Homogenous Platforms – Unlike personal computers, IoT platforms are generally identical.



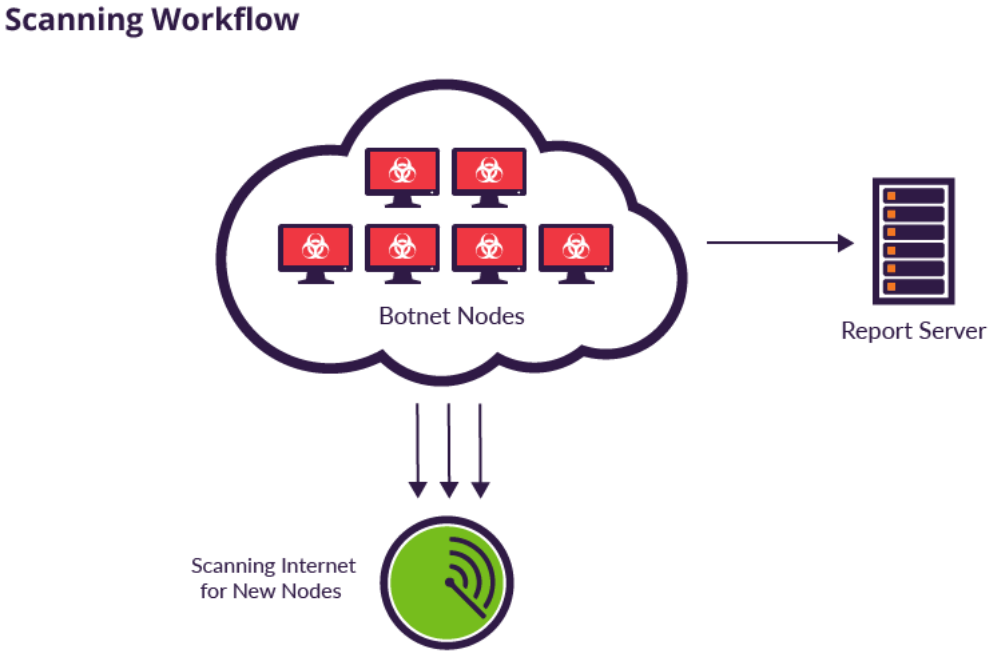
Now let's take a look at the high level topology of Mirai. There are three distinct workflows that are going on: scanning, infection and attack.

Preparing the Attack

The scanning workflow is responsible for identifying potential new members for inclusion in the botnet. They consist of the botnet nodes, a report server, and the random systems on the internet that are being probed.

The Mirai scanning workflow can be broken down into three primary activities.

1. **SYN Port Scan** – probing the internet to identify possible targets
2. **Brute Force Authentication** – performing simple pattern matches
3. **Report Success** – results are sent to a centralized reporting server



As you might imagine, the speed with which the botnet can scan the internet is incredibly fast. In fact, as the botnet grows, it almost becomes an exponential growth.

Deploying the Malware

So how does the Mirai malware actually gets on to IoT devices in the first place? The infection workflow follows this pathway.

- Scan success identified
- Loader receives data
- Loader pushes malware

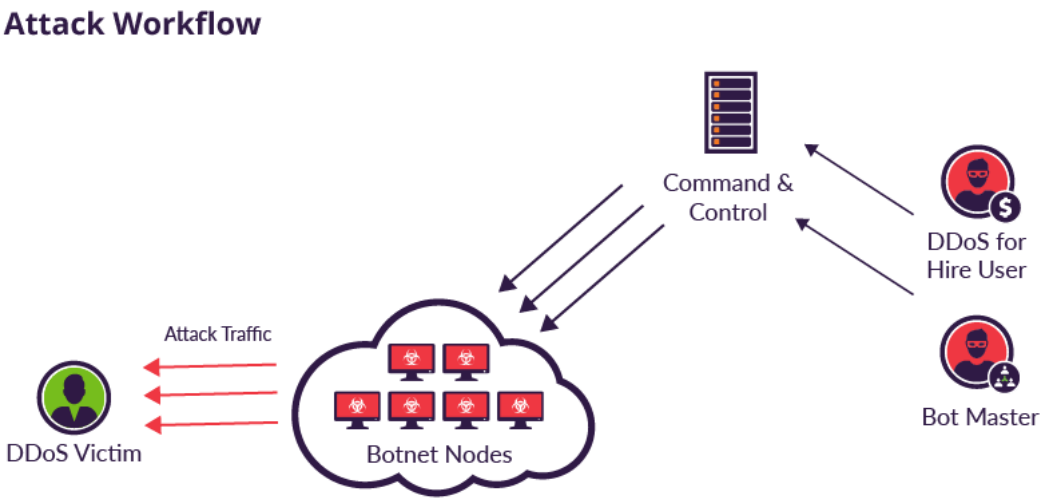
It is worth noting at this point that the malware code is cross-compiled on a variety of architectures. The loader attempts to identify the architecture of the device and load the proper executable. Then with the executable running, the device is now a member of the botnet and begins performing the same scanning and attack activities as any other node in the botnet.

Repeating the Attack

The actual attack workflow is shown in the flowchart below which illustrates the functionality that's responsible for activating the DDoS attacks on the nodes inside the botnet. The process consists of three primary activities.

- The bot master issues an attack command to the command and control server.

- The command and control system tells each node in the botnet to launch an attack with specific details.
- Each node receives a message from the command and control system it immediately executes the desired attack sending packets as quickly as possible with no rate limit.



Keep in mind that during the attack, the node continues all of its usual background scanning activities. Continuously processing, the node never stops looking for new websites and devices to infect.

Covering Tracks and Blocking Competitors

The last thing I should mention is how Mirai can be used to improve the operation of botnets that are embedded in the initial code.

Mirai does a few things to protect itself from discovery. It'll delete itself from the file system once the malware is running. It deletes itself from the running process. And finally, it alters its name to a randomized value.

Another interesting behavior pattern is that the malware attempts to protect itself from competing botnets. As soon as it breaks into the system, it tries to prevent anyone else from breaking in using any other methods.

Once in place, Mirai looks for certain identifiers associated with competing botnets. If it finds any, it'll kill that process and basically take over the system.

That's Mirai in a nutshell. It's a highly complex and nuanced malware program. For further details (including additional questions from the audience), I encourage everyone to watch the webinar (https://www.brighttalk.com/webcast/14611/249565?utm_campaign=webcasts-search-results-feed&utm_content=How%20to%20Identify%20a%20Mirai-Style%20DDoS%20Attack&utm_source=brighttalk-portal&utm_medium=web) presentation.

Leave me a question in the comments below and I'll do my best to answer it.
