FIREDOME

Attack Case: Mirai and Hangzhou Xiongmai Camera Recall

Do you remember the day in 2016 when both Netflix and Twitter went down? That October, millions of IoT devices infected with Mirai malware were part of a coordinated cyber attack. The malicious code, made public that year, scans the web for devices with vulnerable ports to infect and add them to a botnet. Below, we show how Mirai affected manufacturer Hangzhou Xiongmai Technologies (HXT) and how Firedome could mitigate this kind of attack. HXT, while not the target, still had to recall 4.3 million cameras due to the attack, causing a colossal loss to their bottom line.

The First Attack: October 21, 2016

The target of the Mirai attack was Domain Naming Service (DNS) Dyn Inc, servicing sites like Twitter and Netflix. The weeks before the attack, hackers infected millions of IoT devices, including HXT cameras, forming a botnet.

A botnet is a group of commonly infected devices that can be commanded to act in unison for behaviors such as distributed denial of service (DDoS) attacks, stealing data, sending spam, and disabling or bricking the devices themselves en masse. In this case, the hackers used the devices for a massive DDoS attack in order to cause DYN servers to crash, causing very expensive downtime for websites like Twitter and Netflix.

For HXT, the problem was not that they were the target hackers wanted to attack, but that they had many vulnerable devices ripe for infecting. HXT cameras were vulnerable due to default credentials that are easily guessed by Mirai. Despite patching the issue in September 2015 with a password change prompt at installation, millions of already deployed cameras remained online with older, vulnerable firmware.

Ultimately, even though HXT was not the company hackers wanted to damage most, because their devices were vulnerable, they faced devastating consequences. Once security firm Flashpoint revealed to the media that HXT devices were among the most infected, HXT was pressured to recall all 4.3 million cameras sold in the U.S and update millions more, diverting their R&D resources to fix the issue and release new firmware.

"Security vulnerabilities are a common problem for mankind," the company claimed in a public statement responding to the attack and confirming the recall decision. "All industry leaders will experience them." Beyond just the resources and expense needed to execute the recall, HXT would also needed to divert R&D resources from new launches to strengthening password functions and releasing patches for existing stock.

Mirai: How the Malware Works and Has Evolved Over Time

Now we'll take a closer look at what the Mirai malware actually does to devices from a technical perspective.

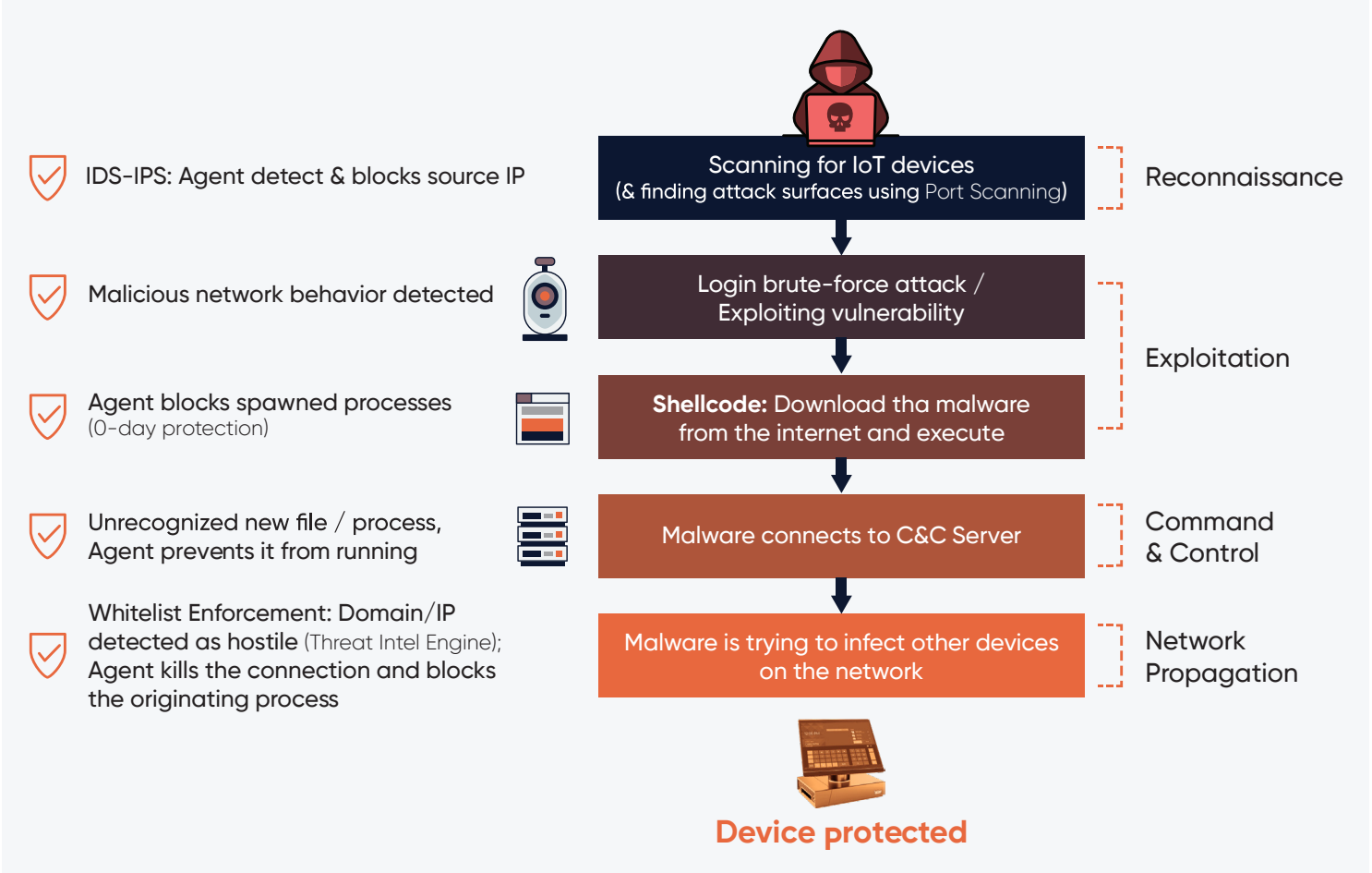
The original version of Mirai was designed to infect a range of IoT devices (with architectures like x86, ARM, MIPS) by scanning for public IP addresses with ports 23 and 2323 open. These ports are mostly used by Telnet, an old unsecured protocol. If a device is listening on these ports, Mirai will try to brute-force its login info using commonly known default user and password pairs (based on known vendor defaults). If it is successful, it then downloads and installs (using a shellcode) the Mirai malware payload to the device, which becomes a new bot, part of the botnet and gains complete control of the device.

With the leak of the source code, hackers have found new ways to evolve the code to better evade detection and penetrate harder to access systems. The malware has adopted significantly, gaining new exploitation capabilities which include a new propagation phase (exploiting vulnerabilities of other IoT devices). This phase involves scanning for them on the same network (LAN) and trying to infect them too.

New variants of Mirai-based IoT malware are discovered almost every day. For example, this latest Mirai variant called AirDropBot was discovered in September 2019 by security researcher 0xrb. In the same week (1st of Oct), a new variant called GUCCI was discovered as well. Although the malware itself, its infrastructure and the attacker behind it were different, the modus-operandi of these variants used common hacking techniques in their cyber kill-chain steps.

Mirai: How Firedome Protects Against Existing and Future Variants of Mirai

Firedome's solution can stop attack vectors which recent Mirai strains like GUCCI use in the different steps of the infection.



At the reconnaissance phase, the Firedome agent will detect port scans these kind of variants conduct. It will also detect and block brute force attempts of services with login prompts. Whether the exploitation phase involves known or unknown (zero-day) exploits, Firedome's smart execution engine will be able to detect and mitigate the threat.

Even if Mirai is installed and running, Firedome's agent will detect the network traffic communication (DNS/TCP/UDP- domains/IP addresses) used by Mirai's Command & Control servers and block its communication within the device, thus making the infection useless. It also detects and shares insight on the Firedome UI about such new attempted network connections by the malware. This allows the AI / SOC to act on the infected device itself or across the fleet, by creating a security alert for malicious activities.

Firedome's machine learning can also detect large scale attacks targeting specific manufacturers, respond to them and block them on the entire fleet automatically, before they can try to spread to other devices.

Learning from HXT: Unique Cyber Risks for IoT Manufacturers

An important lesson for manufacturers from HXT's recall is that IoT companies are uniquely vulnerable in today's increasingly lucrative environment for cyber crime. Whether hackers intend to damage the device maker itself or just use their devices to attack others, the exposure is highly damaging at all levels:

4 Categories of Risk for IoT Device Manufacturers

1) A hacker bricks a manufacturer's entire device base
   - Hacker is paid off by a competitor
   - Hacker wants revenge for a bad customer experience
   - Hacker wants notoriety for taking down a well known brand
2) A hacker disables devices so they are temporarily inoperable / taken hostage
   - Hacker demands ransom
3) A hacker infects or exploits specific targeted device(s)
   - Hacker steals IP: A device with access to a major company's trade secrets on it
   - Hacker steals PII: A consumer's device that ends up being covered in the media
4) A hacker infects devices to use in a botnet
   - Bad PR: The media exposes that specific brand's devices are not secure (like HXT's recall experience)

The scary part is, while HXT was victim to only a lower risk scenario from the above, they still had to recall 4.3 million devices! They were fortunate that the devices they recalled could be updated and resold and were not bricked by the hackers. Don't let your company become the victim or collateral damage of the next attack. Invest now in a proactive cyber-security solution for both known and unknown, evolving threats.