Source Code for IoT Botnet ‘Mirai’ Released

krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

The source code that powers the “Internet of Things” (IoT) botnet responsible for launching the historically large distributed denial-of-service (DDoS) attack against KrebsOnSecurity last month has been publicly released, virtually guaranteeing that the Internet will soon be flooded with attacks from many new botnets powered by insecure routers, IP cameras, digital video recorders and other easily hackable devices.

The leak of the source code was announced Friday on the English-language hacking community **Hackforums**. The malware, dubbed “**Mirai**,” spreads to vulnerable devices by continuously scanning the Internet for IoT systems protected by factory default or hard-coded usernames and passwords.

The Hackforums post that includes links to the Mirai source code.

Vulnerable devices are then seeded with malicious software that turns them into “bots,” forcing them to report to a central control server that can be used as a staging ground for launching powerful DDoS attacks designed to knock Web sites offline.

The Hackforums user who released the code, using the nickname “**Anna-senpai**,” told forum members the source code was being released in response to increased scrutiny from the security industry.

“When I first go in DDoS industry, I wasn’t planning on staying in it long,” Anna-senpai wrote. “I made my money, there’s lots of eyes looking at IOT now, so it’s time to GTFO [link added]. So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb [sic] DDoS, ISPs been slowly shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.”

Sources tell KrebsOnSecurity that Mirai is one of at least two malware families that are currently being used to quickly assemble very large IoT-based DDoS armies. The other dominant strain of IoT malware, dubbed "**Bashlight**," functions similarly to Mirai in that it also infects systems via default usernames and passwords on IoT devices.

According to research from security firm **Level3 Communications**, the Bashlight botnet currently is responsible for enslaving nearly a million IoT devices and is in direct competition with botnets based on Mirai.

"Both [are] going after the same IoT device exposure and, in a lot of cases, the same devices," said **Dale Drew**, Level3's chief security officer.

Infected systems can be cleaned up by simply rebooting them — thus wiping the malicious code from memory. But experts say there is so much constant scanning going on for vulnerable systems that *vulnerable IoT devices can be re-infected within minutes of a reboot*. Only changing the default password protects them from rapidly being reinfected on reboot.

In the days since the record 620 Gbps DDoS on KrebsOnSecurity.com, this author has been able to confirm that the attack was launched by a Mirai botnet. As I wrote last month, preliminary analysis of the attack traffic suggested that perhaps the biggest chunk of the attack came in the form of traffic designed to look like it was generic routing encapsulation (GRE) data packets, a communication protocol used to establish a direct, point-to-point connection between network nodes. GRE lets two peers share data they wouldn't be able to share over the public network itself.

One security expert who asked to remain anonymous said he examined the Mirai source code following its publication online and confirmed that it includes a section responsible for coordinating GRE attacks.

It's an open question why anna-senpai released the source code for Mirai, but it's unlikely to have been an altruistic gesture: Miscreants who develop malicious software often dump their source code publicly when law enforcement investigators and security firms start sniffing around a little too close to home. Publishing the code online for all to see and download ensures that the code's original authors aren't the only ones found possessing it if and when the authorities come knocking with search warrants.

My guess is that (if it's not already happening) there will soon be many Internet users complaining to their ISPs about slow Internet speeds as a result of hacked IoT devices on their network hogging all the bandwidth. On the bright side, if that happens it may help to lessen the number of vulnerable systems.

On the not-so-cheerful side, there are plenty of new, default-insecure IoT devices being plugged into the Internet each day. **Gartner Inc.** forecasts that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020. In 2016, 5.5 million new things will get connected each day, Gartner estimates.

For more on what we can and must do about the dawning IoT nightmare, see the second half of this week's story, The Democratization of Censorship. In the meantime, this post from **Sucuri Inc.** points to some of the hardware makers whose default-insecure products are powering this IoT mess.