REAPER / IOTROOP BOTNET REPORT PRODUCED FOR NORWEGIAN HULL CLUB

26 October 2017

COMMITTED
GLOBAL
EXPERTISE

NORWEGIAN HULL CLUB

IOTROOP / REAPER BOTNET

Reaper (or IOTroop) is the latest Internet of Things (IoT) botnet that has spread at an unprecedented rate, exceeding the reach of the 2016 Mirai botnet. As of 26 October 2017, over one million wireless network devices have been infected. The malware, which was first discovered in September 2017, exploits vulnerabilities in wireless devices that use an Internet Protocol (IP) address such as security cameras and internet routers.

Reaper appears to be an evolution of the Mirai botnet, but can reportedly spread at a faster rate than its predecessor and is more sophisticated. While the Mirai botnet scanned for and exploited hardcoded, administrative, weak or default passwords, Reaper uses more sophisticated software hacking tools. This means that although using a similar source code, the number of potential victims is exponentially greater.

Current threat

Although over one million devices have been infected as of 26 October, only 10,000 are communicating daily with the command-and-control server operated by the unidentified creator of the botnet. Given the large number of devices infected, it is unlikely the botnet has been released in order to steal data or capture video from them (though these outcomes remain possible). Instead, it is highly likely the infected devices will be used to unleash a powerful DDoS attack. The Mirai botnet infected approximately 2.5 million devices in 2016, and their collective power was used to send an incapable amount of connection requests to DNS provider Dyn – which subsequently crashed several major websites including Spotify, Reddit and The New York Times.

According to some reports, millions of infected devices (that are not communicating with the command-and-control server) are “queued” to do so. More alarmingly, the malware reportedly includes a Lua-based platform that allows the command-and-control software to update or change its function. This means that while a large-scale DDoS attack is likely the intended outcome, the botnet is flexible and the criminals’ tactics could change.

Devices targeted at present include GoAhead, D-Link, TP-Link, NETGEAR, AVTECH, MikroTik, Linksys, Synology and Linux.

What is a botnet?

A botnet is a number of internet connected smart devices infected with malware and controlled remotely by a threat actor (command-and-control server). The network of infected systems allows threat actors to execute high-impact cyber attacks by collectively harnessing their capabilities to send connection requests (DDoS), to steal data, to send spam or to crash servers.

Mitigation measures

To check if your IoT device could have been infected, check Check Point's website for a list of affected gadgets (https://research.checkpoint.com/new-iot-botnet-storm-coming/).

Viewing the IP traffic from any IoT device could reveal if the device has been infected (an abnormal spike in activity will be observable). However, this will require specialist software rarely found at consumer level. Additionally, a spike in traffic will only be observable if the device is infected ***and*** communicating with the command-and-control server.

If your device appears on the list above, it is recommended you perform a factory reset on its firmware to remove the malware.

Best Practice steps that can be taken to prevent and / or limit the impact include:

- Segregation of smart devices from critical networks in order to isolate devices that may be infected and prevent further contamination
- Review of access control lists to ensure permissions attached to devices are integral for their processes, ensuring only required permissions are listed and others are disabled to limit the attack surface

For further information on the Reaper botnet, or for guidance on risk mitigation, contact NYA at info@nyarisk.com or visit www.nyarisk.com.

CONTACT US

LONDON

40 Lime Street
London
EC3M 7AW
United Kingdom

NEW YORK

77 Water Street
New York, NY
10005
United States

SINGAPORE

One Raffles Place
Tower 1
1 Raffles Place
Singapore 048616
Singapore

NYA 24

nyarisk.com