Jan 08 2024

NETMANAGEIT

Intelligence Report

Mirai.TBOT Uncovered: Over 100 Groups and 30,000+ Infected Hosts in a big IoT Botnet

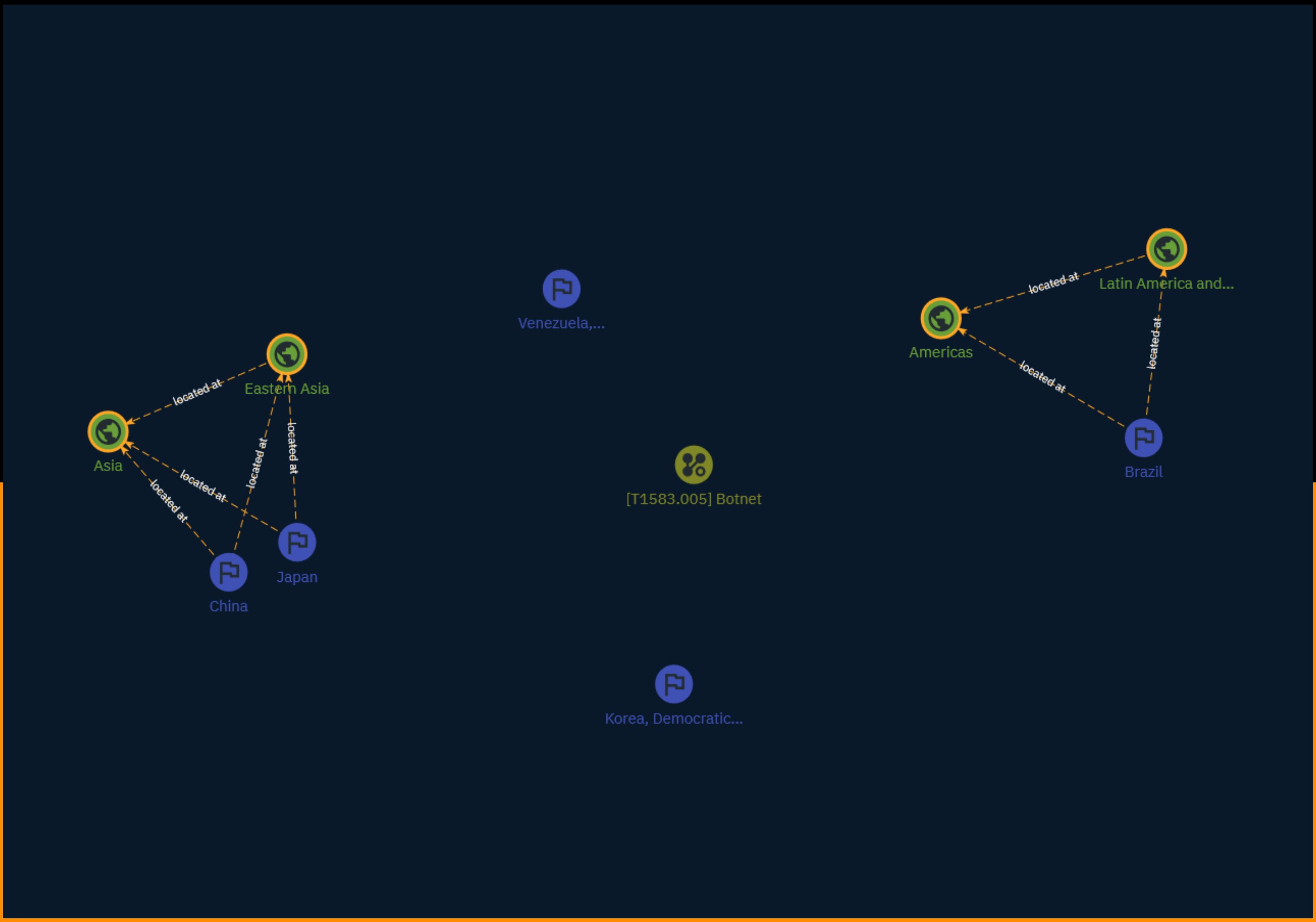

Table of contents

Overview

Entities

External References

Overview

Description

Mirai was first discovered in 2016 and it infects IoT devices by exploiting their weak passwords and vulnerabilities. Once the devices are infected, they become part of a botnet controlled by attackers for large-scale distributed denial-of-service attacks. Mirai botnets usually classify bots into different groups. Recently a discovered Mirai botnet actually had more than 100 Bot groups

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name

Botnet

ID

T1583.005

Description

Adversaries may buy, lease, or rent a network of compromised systems that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Adversaries may purchase a subscription to use an existing botnet from a booter/stresser service. With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing](https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS).(Citation: Imperva DDoS for Hire)(Citation: Krebs-Anna)(Citation: Krebs-Bazaar)(Citation: Krebs-Booter)

Country

Name
Brazil

Name
Venezuela, Bolivarian Republic of

Name
Japan

Name
Korea, Democratic People's Republic of

Name
China

Region

Name
Asia

Name
Americas

Name
Eastern Asia

Name
Latin America and the Caribbean

External References

- https://otx.alienvault.com/pulse/659bcf203d564c6741cf7bf7
- https://blog.xlab.qianxin.com/mirai-tbot-en/