# [INDUSTRY] Threat Digest: Week of [Month, Day, Year]

*Published on:* MM/DD/YYYY

**Distribution**: SHAREABLE — Can be shared with client and prospects

## Executive Summary

Highlights of this week's digest:

- **[CUSTOMER-SPECIFIC]**
  - 10 Domains Found Emulating Company Brand
  - Two Company Accounts Advertised on Underground Marketplace
  - Tech Stack: PoC Exploit Code Published for Operating System Vulnerability
- **[INDUSTRY]**
  - Tick APT Actors' Ongoing Campaign Within East Asia Continues
  - Global IoT Risk Report Finds Widespread Security Issues in Industrial Sector
- **[GENERAL]**
  - Chalubo Botnet Brute-Forces IoT Devices for Targeted DDoS
  - Two of 20 Magento Extensions Vulnerable to Zero-Day Attack, Security Researcher Asks InfoSec Community for Help Discovering Remaining 18

## Prominent Information Security Events

### Chalubo Botnet Brute-Forces IoT Devices for Targeted DDoS

**Source**: *Sophos* | Recorded Future: *Monitor IoT Botnet Activity*
**Intelligence Cards**: *Chalubo Botnet* | *23.247.2.0/24* | *183.131.206.0/24*

On October 22, 2018, researchers from Sophos disclosed findings regarding the Chalubo botnet. The Chalubo family targets Linux-based devices, particularly Internet of Things (IoT) devices with preset administrative credentials, via SSH brute-forcing. Chalubo borrows code from Mirai, but gets its name from its encryption techniques, using a Lua command script and a ChaCha stream cipher to obfuscate its code. The malware has evolved since its first sighting in late August 2018, now targeting additional processor architectures including 32- and 64-bit ARM, x86, x86_64, and more.

Upon dropping a webshell or gaining access to a victim machine via root:admin SSH credentials, Chalubo attackers run commands to access the Chalubo downloader, the main bot components, and the Lua encryption script. The command stops any firewall activity and pulls down a downloader, dubbed "libsdes," from the command and control IP address. The downloader creates an empty file to prevent multiple infections, and attempts persistence by installing its scripts into multiple areas of the disk to avoid detection and survive reboot. The downloader can then install the bot, using the Lua script to decrypt the payload, which contains primary functions for denial of service attacks over UDP, DNS, and SYN. Sophos found SYN flood attacks are commonly ordered over port 10100, and Chalubo makes no effort to mask the source IP. Interestingly, it checks the /24 address of the local IP against 23.247.2[.]0, and if it is in that range, then it will set the source IP to one within the 183.131.206.0/24 range.

**Analyst Comment:** This latest iteration of an IoT botnet continues the trend of focusing on denial-of-service attacks, but uses a more basic SSH brute-forcing infection vector. Interestingly, the attackers seem intent on insulating the 23.247.2.0/24 CIDR range during denial-of-service attacks for unknown reasons. Sophos researchers noted that Chalubo communications occur over TCP port 8852, which can be monitored in the Recorded Future Platform, in customer IDS, IPS, and firewall devices.