

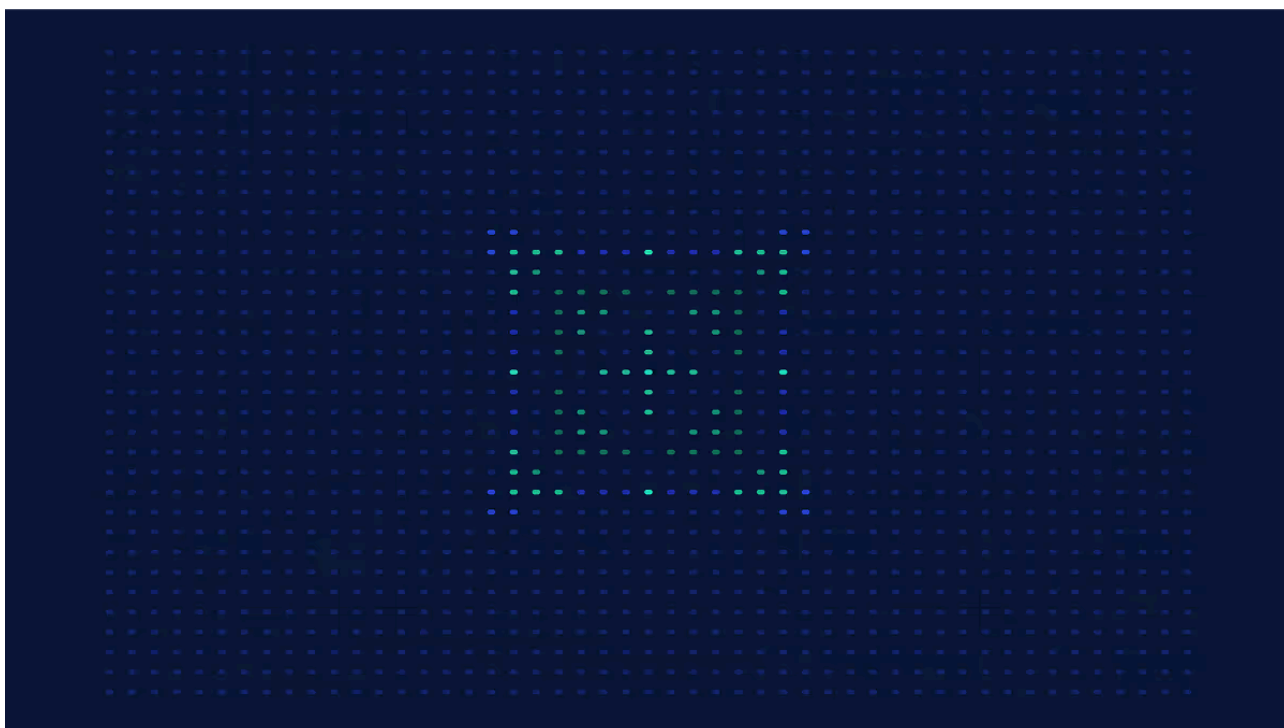
# Pulling Linux Rabbit/Rabbit Malware Out of a Hat

By Anomali Threat Research

Published: 2025-12-31 · Archived: 2026-04-05 16:42:22 UTC

Cyber threat researchers from Anomali Labs have discovered a new malware, called “Linux Rabbit and Rabbit,” that targeted Linux servers and IoT devices.

- [Overview](#)



## Overview

Cyber threat researchers from Anomali Labs have discovered a new malware, called “Linux Rabbit,” that targeted Linux servers and Internet-of-Things (IoT) devices in a campaign that began in August 2018 and continued until October 2018. The campaign targeted devices in Russia, South Korea, the UK, and the US. The campaign utilizes two strains of malware that share the same code base called Linux Rabbit and “Rabbit”. The goal of this campaign is to install cryptocurrency miners onto the targeted servers and devices. The type of Monero cryptominer installed is dependent upon what the machine’s architecture is. The threat bulletins associated with this blog post will thoroughly examine the general campaign and the individual malware processes for both Linux Rabbit and Rabbit.

This campaign was conducted by unknown threat actors and it is currently unclear what the initial infection vector is. The first campaign began in August 2018 and was utilizing the Linux Rabbit malware to infect Linux systems. The Linux Rabbit malware only targeted Linux servers that were located in specific countries: Russia, South Korea, the UK, and the US. This malware has four main functionalities which are:

- Establish a connection to the Command and Control (C2) server using Tor gateways
- Setup persistence
- SSH brute force
- Install the cryptocurrency miner

Additional information discussing the campaign such as infrastructure data and downloaded files can be viewed by ThreatStream users [here](#).

For Linux Rabbit to establish a connection with the C2 server, it utilizes Tor hidden services to act as contact points to access a Tor gateway. The malware will randomly select one of the hidden services and then a Tor gateway to follow in order to establish an active C2 URL. The payload for the malware is then sent from the C2 server as an encoded URL parameter.

The malware's second functionality is to gain persistence on an infected machine. This is completed through "rc.local" files and ".bashrc" files. After obtaining persistence, the next functionality of Linux Rabbit is to brute force SSH passwords which ultimately allows the malware to install the cryptocurrency miner onto the server. The SSH brute forcing begins by the malware first generating a random IPv4 string and checking its geolocation to see where it is located. If the IP is located within a country that is "blacklisted," it will stop and move on until it finds an IP that is located in an allowed geolocation, which for this malware are Russia, South Korea, the UK, and the US. Once an allowed IP location is discovered, Linux Rabbit will check to see if an SSH server is listening on Port 22. The malware will open a socket to see if it receives a response, and if it does, it will attempt to obtain the machine's hostname. Interestingly, this malware will also check the Top-Level Domain (TLD) of a host, and will skip any TLD that is blacklisted. Many of the blacklisted TLDs are government-related sites in a variety of countries. If the TLD is not blacklisted, the malware will run through a process of authentication utilizing a list of hard-coded credentials it has. The first two authentication certifications are to ensure that the malware is not in a "honey pot". This is likely to avoid static analysis of the malware.

After all this, if the malware successfully discovers a viable target and is able to gain access through SSH credential brute forcing, the malware will be able to begin installation of the cryptocurrency miner. Linux Rabbit attempts to install both "CNRig" and "CoinHive" Monero miners onto the machine, but only one will actually successfully install depending on what type of architecture the machine is. If the machine is a x86-bit, it will install CNRig Monero miner and if the machine is an ARM/MISP, it will install CoinHive. If the infected machine is a web server, the malware will inject CoinHive script tags into every HTML file, so that even visitors of the site/server are also infected with the cryptocurrency miner. Linux Rabbit is able to connect to GitHub and receive updates from the threat actors. It also has a killswitch built-in. It is able to detect other miners already on a target machine and delete them from the machine during the installation of its own miner.

A technical breakdown of Linux Rabbit can be viewed by ThreatStream users [here](#).

Following the Linux Rabbit campaign that occurred in August 2018, a new campaign followed it from September 2018 until October 2018 that utilized a different malware strain to infect machines. This new campaign used a self-propagating worm called “Rabbit” that shared the same code base with Linux Rabbit. However, Rabbit is not limited to infecting just Linux servers like Linux Rabbit because it can also target and infect Internet-of-Things (IoT) devices via known vulnerabilities. Most crucially, it is not restricted to only attacking devices in specific geolocations. The known vulnerabilities that Rabbit is capable of exploiting include the following:

- CVE-2018-1149
- CVE-2018-9866
- CVE-2017-6884
- CVE-2016-0792
- CVE-2015-2051
- <https://www.exploit-db.com/exploits/31683/>
- <https://www.exploit-db.com/exploits/27528/>
- <https://www.exploit-db.com/exploits/39596/>
- <https://www.exploit-db.com/exploits/42114/>
- <https://www.exploit-db.com/exploits/40500/>
- <https://www.exploit-db.com/exploits/41499/>
- <https://www.exploit-db.com/exploits/40212/>
- <https://www.exploit-db.com/exploits/43055/>
- <https://www.exploit-db.com/exploits/44760/>
- <https://www.exploit-db.com/exploits/41471/>
- <https://blogs.securiteam.com/index.php/archives/3445>

A technical breakdown of Rabbit can be viewed by ThreatStream users [here](#).

Both malware strains share the same code base which means they function almost exactly the same, except Rabbit will send all its payloads through an open port 80 to the Linux (web)servers, not checking to ensure that the process is successful. Since the malware will install different payloads depending on the architecture of the machine, it, in theory, does not need to check what was successfully installed or not, since one of the two cryptominers is guaranteed to run. Rabbit will also install CoinHive miners into various web pages via the infected web server by searching for “.HTML” files and inserting JavaScript files into the browser.

## IOCs

96bcd95abb6838f4e3e250357e1fcb9  
9dfb99f6357c36b992f589f7a1cedde8  
9ec44ec63c48b7f9ddafc0ed7e197e2d  
05aa20355187ffcd2b6712362c0f7213  
b62b646bc24070afc4a7e0a5325916b8  
8207caf23de638a5d25eb2e6ade657c1  
03e4c44f6812268d95f811cf327d0665  
0e9eedbc6ab395b0b23f43adebe54e58  
c6488b538f45c7acd43b98d50e241c15

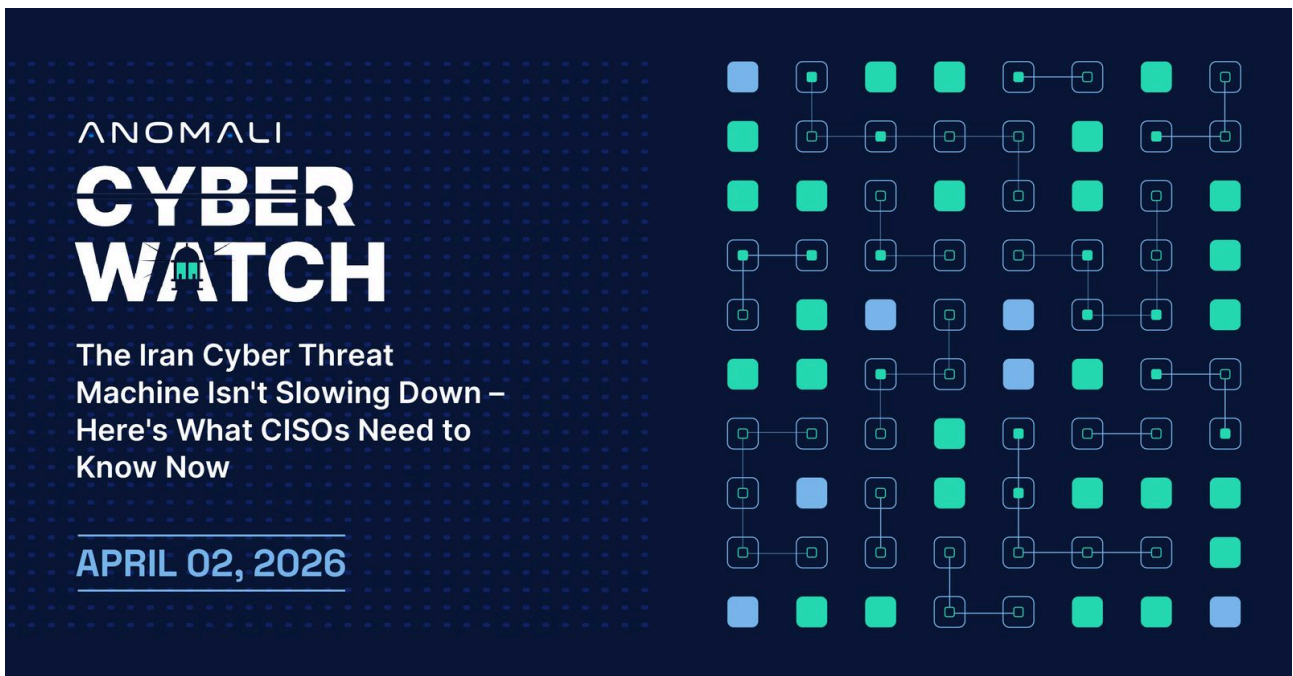
ea692602f556b91f4fa82c77ed746a3d  
58ea13f8cc9af6bd193dd0962818446f  
19238225434d6298524447a8cf976fce  
642636dd8f76384e1e09e3a12829a8e8  
b666100d3d3555dc8ed845d6fe12b3a5  
e236822a8659e6e357e09980594661fb  
20d73873bc862e57c212de88a0316138  
fec12470177b4b34337adb8f86fca126  
6b0169e4cc070f575195901d99a4792e  
f9532eb1b0cd3b2033bb3b626e26fdb6  
3987fee76bc7752b63fd50480d7cbb5f  
e064fa34b2f135f099f4cf39dba3a53d  
e4c15aa25df48b8094b60b219669d749  
310fda74f6726aec0636c9d079461d74  
1d70b9f8661bf3135a38d652dd9aa624  
1ed94aaaf65e51545f90061c76d898a4  
fb6485999580f1ee743ed0bb489dee66  
642630a7857358378fa2ac014a836080  
7b7e3d4984ba280a8dce86ac5344f610  
23292aa6afab8a4dac33ab126d133844  
8ebde43f35d2eb0b0f5f83d7a3f6ed4c  
f565d38c2e0b5bf70dac1b68e055db60  
d4858f464e44c0d694cf9a051fc946a1  
ab19ac58bbc689c65048b0f20e9a3c20  
a695226a7be0c1de4b18fd650ea5c796  
ce2e3b285abae4bdf7f5781e700e013c



## Iran's IRGC Names Western Tech Giants as "Legitimate Targets": What CISOs Must Do Now



## When 766 Systems Fall in 24 Hours: The Threats Bearing Down on State Government Networks



## The Iran Cyber Threat Machine Isn't Slowing Down — Here's What CISOs Need to Know Now