December 6, 2018 - Anomali Threat Research

Pulling Linux Rabbit/Rabbot Malware Out of a Hat

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Manage Preferences

Accept All

Reject All

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 "Rabbot". 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 Rabbot.

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

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

"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.

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

- 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 Rabbot can be viewed by ThreatStream users here.

Both malware strains share the same code base which means they function almost

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

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

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Get the Latest Anomali Updates and Cybersecurity News – Straight To Your Inbox

Become a subscriber to the Anomali Newsletter

Receive a monthly summary of our latest threat intelligence content, research, news, events, and more.

SUBSCRIBE TODAY

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

ANOMALI SECURITY OPERATIONS PLATFORM

COMPLIANCE

CYBER THREAT INTELLIGENCE

ISAC

MALWARE

MODERN HONEY NETWORK

RESEARCH

SIEM

SOAR

STAXX

THREAT INTELLIGENCE

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

808 Winslow Street , Redwood City, CA, 94063, United States

+1 844 4 THREATS (847328)
+44 8000 148096 (International Toll-Free)

Platform and Products

Anomali Platform

Anomali Copilot

Marketplace

Anomali Marketplace

Threat Intelligence Feeds

Partners

Partners Overview

Join the Technology Partner Program

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Support

Press Room

Glossary

Contact Us

Schedule Demo

© Copyright 2024 Anomali®. All rights reserved. ThreatStream® is a registered trademark of Anomali Inc. Anomali Match™ ("Match") and Anomali Lens™ ("Lens") are trademarks of Anomali Inc.

Privacy Policy Terms of Use Cookies Policy Security

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy