



Monero Mining Pool FQDNs

by Florian Roth | Oct 24, 2021

Malware that deploys crypto mining software has become more and more popular and annoying. It's not always possible to scan every device in your network with our free or commercial compromise assessment scanners.

The good news is that the mining pools for the most popular crypto currency Monero (Symbol: XMR) are limited.

Therefore we've decided to compile a list of these mining pools that you can use to monitor your firewall or DNS servers.

For a very generic approach, you could try using the following patterns:

xmr.

*pool.com

*pool.org

pool.*

Our customers can use THOR to scan for scripts, executables, DNS cache, process connections, log entries and other elements for traces of crypto mining activity.



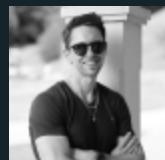
MONERO

Monero Mining Pool Addresses

pool.minexmr.com
fr.minexmr.com
de.minexmr.com
sg.minexmr.com
ca.minexmr.com
us-west.minexmr.com
pool.supportxmr.com
mine.c3pool.com
xmr-eu1.nanopool.org
xmr-eu2.nanopool.org
xmr-us-east1.nanopool.org
xmr-us-west1.nanopool.org
xmr-asia1.nanopool.org
xmr-jp1.nanopool.org
xmr-au1.nanopool.org
xmr.2miners.com
xmr.hashcity.org
xmr.f2pool.com

xmrpool.eu
pool.hashvault.pro
moneroocean.stream
monerocean.stream

About the author:



Florian Roth

Florian Roth serves as the Head of Research and Development at Nextron Systems. With a background in IT security since 2000, he has delved deep into nation-state cyber attacks since 2012.

Florian has developed the THOR Scanner and actively engages with the community via his Twitter handle @cyb3rops. He has contributed to open-source projects, including 'Sigma', a generic SIEM rule format, and 'LOKI', an open-source scanner.

Additionally, he has shared valuable resources like a mapping of APT groups and operations and an Antivirus Event Analysis Cheat Sheet.

**Subscribe to our
Newsletter**

Monthly news, tips and insights.

[SUBSCRIBE](#)

Follow Us



Recent Blog Posts

Introducing
@NextronResearch:
A New Channel for
Threat Intelligence

October 31, 2024



In-Depth Analysis of
Lynx Ransomware

October 11, 2024



Important
Announcement:
Upcoming Migration
of our Update Servers

August 14, 2024



Introducing THOR
Cloud: Next-Level
Automated
Compromise
Assessments

August 2, 2024



Upgrade Your Cyber Defense with THOR

Detect hacker activity with the
advanced APT scanner THOR.

Utilize signature-based detection,
YARA rules, anomaly detection,
and fileless attack analysis to
identify and respond to
sophisticated intrusions.

[LEARN MORE](#)

Antivirus Event Analysis Cheat
Sheet v1.13.0
July 17, 2024

Top Blog Topics

- 📁 THOR
- 📁 THOR Lite
- 📁 YARA
- 📁 Sigma
- 📁 AURORA
- 📁 ASGARD Management Center
- 📁 ASGARD Analysis Cockpit
- 📁 THOR Thunderstorm
- 📁 THOR Cloud
- 📁 Research
- 📁 Security Monitoring
- 📁 Service Notice

Recommended Blog Posts



**Introducing THOR Cloud:
Next-Level Automated
Compromise Assessments**

Florian Roth
Aug 2, 2024

[Read More](#)



**Cybersecurity is Not Just an
IT Security Issue**

Franziska Ploss
Jul 4, 2024

[Read More](#)

• • • •

← Silent Scanning - Compromise
Assessment with THOR Lite on a
Compromised Exchange 2019 Server

THOR 10.6.11 with Support for Apple
M1 Architecture →



Nextron Systems GmbH © 2024

All Rights Reserved

Resources

Manuals

Fact Sheets

Customer Portal

Company

About Us / Contact

Jobs

Newsletter

Monthly news, tips and insights.

SUBSCRIBE

[Imprint](#) [Privacy Policy](#) [Change privacy consent](#) [Privacy consents history](#)

[Revoke privacy consents](#)