LevelBlue - Open Threat Exchange

By trainingstudent

Archived: 2026-04-02 11:59:05 UTC

WanaCrypt0r Ransomworm

FileHash-MD5: 10 | **URL:** 1 | **Domain:** 5 | **Hostname:** 1

Cloned from https://otx.alienvault.com/pulse/591c4a4755434c05f8311424

- 58 Subscribers

- 157 Subscribers

- 128 Subscribers

Thor Lite Windows 11 Enterprise - Scan of impacted AHS Workstation/Sample - 01.31.25 - Not Enriched

CVE: 1 | **FileHash-MD5:** 1135 | **FileHash-SHA1:** 627 | **FileHash-SHA256:** 593 | **SSLCertFingerprint:** 5 | **URL:** 39 | **Domain:** 5 | **Email:** 1 | **Hostname:** 11

Completed a Thor-Lite 64 Scan v. 10.7.18 on AHS Workstation/Sample Device Scan ID: S-5thsJ4jlWSA Signature Database: 2025/01/31-192845 Operators --intense --allfiles --vtkey *** --vtmode full Modules: Filescan 2, LogScan 300, ProcessIntegrity 62 -> Alerts 0, Warnings 18, Notice 350, Info 1423, Errors 0 Updated: 05.12.25

- 128 Subscribers

- 128 Subscribers

Thor Linux Lite Scan - Sample Device & SG2 - 02.07.25 - Unenriched

CVE: 830 | **FileHash-MD5:** 701 | **FileHash-SHA1:** 871 | **FileHash-SHA256:** 897 | **URL:** 2920 | **Domain:** 388 | **Email:** 17 | **Hostname:** 295

Took a few tries but here is the complete thor Linux 64 Lite Scan on: Sample Device & a single drive (one of many) of the 77 TB of: things I have but don't know what to do with --- Old Notes on previous scan attempts for this sample. See Comments on VT MD5 de880994c51d4055c960e2d32db89774 SHA-1 539e7c2eefd7a6aa17db436d83738c117f26798c SHA-256 a6b9deae18604003aa3963d5d83775f5c66bfbe93ea4608fe8a69e6af3722f45 SSDEEP 98304:hpUsCWtdIdOKfb44V0ipGuEwWPKhmMWMCURFfxzRq6R5qJJfrPOOD86U6BDfIokW:BKftFfuDfqAfPPfa4f3 TLSH T10D571AC3C70811188D2373EBE1B4BA59BD06381EDECA9D59F08D642C97946467A2EDCF

- 128 Subscribers

Thor Lite 64 - 10.09.24

CVE: 13 | **FileHash-MD5:** 1136 | **FileHash-SHA1:** 647 | **FileHash-SHA256:** 604 | **URL:** 89 | **Domain:** 25 | **Email:** 2 | **Hostname:** 47

Just a Thor Lite 64 scan of 'things missed' on sample device.

- 128 Subscribers

Thor Lite 64 and Orico Dive - 06.14.24

FileHash-MD5: 932 | **FileHash-SHA1:** 483 | **FileHash-SHA256:** 510 | **URL:** 74 | **Domain:** 4 | **Email:** 1 | **Hostname:** 47

Description SCANID: S-MYo9X22NxW8 Tags: crowdsourced base64-embedded contains-zip

- 128 Subscribers

Thor Lite Scan Kano & SG2 - 06.12.24

CVE: 10 | **FileHash-MD5:** 969 | **FileHash-SHA1:** 541 | **FileHash-SHA256:** 645 | **URL:** 168 | **Domain:** 29 | **Email:** 2 | **Hostname:** 90

Just a Thor-Lite scan of W11 Kano PC sample and SG2 Backup Drive 06.12.24: https://www.virustotal.com/graph/embed/gfe2fba6acfb04c7a95689313b7e20d286b56f9fdf4204834a94080660ff4c752?theme=dark

- 128 Subscribers

Thor-Lite - ASUS, SG1 & 128 USB - 06.12.24

CVE: 8 | **FileHash-MD5:** 1064 | **FileHash-SHA1:** 549 | **FileHash-SHA256:** 567 | **URL:** 105 | **Domain:** 19 | **Email:** 2 | **Hostname:** 77

Just a thor-lite scan of a sample W11 Asus Device, a backup drive, and a 128 GB US -Some false positives (b/c ya know - community edition) 06.12.24: https://www.virustotal.com/graph/embed/g23296a8424204aeda69d32bb307e46820e4f1803c8f54cdd97b5e92a9cb58552?theme=dark

- 128 Subscribers

Thor-Lite Linux 64 (06.11.24) - enriched a bit more but not 'pruned'

CVE: 247 | **FileHash-MD5:** 1183 | **FileHash-SHA1:** 1553 | **FileHash-SHA256:** 1240 | **URL:** 486 | **Domain:** 294 | **Email:** 8 | **Hostname:** 138

Please note: This sample is a tad 'outdated' as I ran both scans kind of by accident lol (i.e. did not update w. the utils utility). I was a bit tired so a happy accident of more data? - but gives a general 'picture' or 'painting' anyways on a rather small set of data. Have some more data to put up (picked up by Huntress Labs) - just have to get that back online. Would love to accommodate for some confounding variables - e.g. filter for false positives, windows logs, networking capabilities (better than what I have now) to better inform the team taking care of me (us). Note: Given it was using some outdated thor modules (lite-version), it was 'good enough' to provide some data worth looking into that 'falls in line' w. what I've come across. Just a combined sample (2 in 1) of a thor-lite scan of a linux instance (06.11.24) I've just listed a few places I have some direct ties to in one way or another (not including the other UAlberta students affected that have been in contact with me or reached out).

- 128 Subscribers

Unix.Trojan.Mirai-6981158-0 | Win32/1ms0rry CoinMiner Botnet affects android user

FileHash-MD5: 1195 | **FileHash-SHA1:** 745 | **FileHash-SHA256:** 1212 | **URL:** 2436 | **Domain:** 1264 | **Email:** 1 | **Hostname:** 1148

Found an IP address in block: http://100.116.0.0/? Found on android device user. Target is being tracked. Uses .ru but tracks back to US based on other studies. Command 'redirect blame' found in association. Active, moved.

- 224 Subscribers

Thor Lite Scan - 10.7.15 - Ubuntu Scan on Archived Files

CVE: 6108 | **FileHash-MD5:** 164 | **FileHash-SHA1:** 625 | **FileHash-SHA256:** 148 | **URL:** 2267 | **Domain:** 426 | **Email:** 9 | **Hostname:** 400

Joe-MBA_thor_2024-05-18_1025 Ubuntu 22.04.4 LTS Scan ID S-I9VvMTB6cZU hmmm...I can't tell if this is 'way too much' or 'probably fairly accurate'

- 128 Subscribers

- 258 Subscribers

- 258 Subscribers

- 181 Subscribers

- 52 Subscribers

- 258 Subscribers

- 181 Subscribers

- 37 Subscribers

Indicators Search

Show expired indicators

We've found 236 indicators

Source: https://otx.alienvault.com/browse/pulses?q=tag:DoublePulsar