

Appendix

May 10, 2024

Tables from 1 to Table 16, show the Yara rule matching with the corresponding malware families and provides a comprehensive exploration of the effectiveness utilizing Coverage, Precision and Recall metrics.

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|------------------------------|-----------------|------------------|---------------|-------------------|
| ransomware_windows_wannacry | 88% | 100% | 89% | Binary Alert |
| cerberus | 0.19% | 0% | 0% | Yara-Rules |
| memory_shylock | 0.19% | 0% | 0% | Yara-Rules |
| ms17_010_wanacry_worm | 100% | 100% | 100% | Yara-Rules |
| spyeye_plugins | 0.19% | 0% | 0% | Yara-Rules |
| wanna_cry_ransomware_generic | 88% | 100% | 88% | Yara-Rules |
| wannacry_ransomware | 100% | 100% | 100% | Yara-Rules |
| wannacry_ransomware | 100% | 100% | 100% | Neo23x0 |
| wannacry_static_ransom | 88% | 100% | 88% | Yara-Rules |
| worm_ms17_010 | 100% | 0% | 0% | Yara-Rules |
| wannadecryptor | 96% | 100% | 96% | Yara-Rules |
| with_sqlite | 0.38% | 0% | 0% | Yara-Rules |

Table 1: Yara Rules Matches for Wannacry

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|--------------------------|-----------------|------------------|---------------|-------------------|
| win_industroyer2_auto | 33% | 100% | 33% | Binary Alert |
| win_industroyer_auto | 17% | 100% | 17% | Yara-Rules |
| industroyer_malware_4 | 33% | 100% | 33% | Yara-Rules |
| industroyer_malware_4 | 33% | 100% | 33% | Yara-Rules |

Table 2: Yara Rules Matches for Industroyer

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|-------------------|----------|-----------|--------|------------|
| rookie | 33% | 0% | 0% | Yara-Rules |
| rookiestrings | 0% | 0% | 0% | Yara-Rules |

Table 3: Yara Rules Matches for Unknown_Trojan

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|----------------------|----------|-----------|--------|------------------|
| linux_trojan_xorddos | 100% | 100% | 100% | Elastic Security |
| xor_ddosv1 | 25% | 100% | 25% | Yara-Rules |

Table 4: Yara Rules Matches for Xor_ddos

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|-------------------------|----------|-----------|--------|------------------|
| windows_ransomware_maui | 100% | 100% | 100% | Elastic Security |
| win_maui_auto | 100% | 100% | 100% | Malpedia |

Table 5: Yara Rules Matches for Maui

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|-----------------------------|-----------------|------------------|---------------|-------------------|
| xmrig_monero_miner | 100% | 100% | 100% | Neo23x0 |
| xmrig_miner | 100% | 100% | 100% | Yara-Rules |
| linux_cryptominer_Camelot | 50% | 0% | 0% | Elastic Security |
| linux_cryptominer_flystudio | 50% | 0% | 0% | Elastic Security |
| linux_cryptominer_xmrminer | 50% | 100% | 50% | Elastic Security |
| linux_trojan_pornoasset | 100% | 0% | 0% | Elastic Security |
| macos_cryptominer_generic | 100% | 0% | 0% | Elastic Security |
| macos_cryptominer_xmrig | 100% | 100% | 100% | Elastic Security |

Table 6: Yara Rules Matches for Xmrig

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|--------------------------|-----------------|------------------|---------------|-------------------|
| linux_trojan_mirai | 52% | 0% | 0% | Elastic Security |

Table 7: Yara Rules Matches for Rapper_bot_mirai_botnet

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|--------------------------|-----------------|------------------|---------------|-------------------|
| linux_trojan_mirai | 15% | 100% | 15% | Elastic Security |
| linux_trojan_gafgyt | 15% | 100% | 15% | Elastic Security |

Table 8: Yara Rules Matches for Unknown_mirai_botnet

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|---------------------|----------|-----------|--------|------------------|
| linux_trojan_mirai | 67% | 0% | 0% | Elastic Security |
| linux_trojan_gafgyt | 67% | 0% | 0% | Elastic Security |
| elf_mirai_auto | 33% | 0% | 0% | Malpedia |
| susp_xored_mozilla | 100% | 0% | 0% | Neo23x0 |

Table 9: Yara Rules Matches for Moobot_mirai_botnet

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|-------------------|----------|-----------|--------|------------|
| rookie | 100% | 0% | 0% | Yara-Rules |
| rookiestrings | 100% | 0% | 0% | Yara-Rules |

Table 10: Yara Rules Matches for Zombieboy_cryptomining_worm

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|---------------------|----------|-----------|--------|------------------|
| linux_trojan_gafgyt | 100% | 100% | 100% | Elastic Security |

Table 11: Yara Rules Matches for Gafgyt_mirai_botnet

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|-------------------|----------|-----------|--------|------------|
| rookie | 100% | 0% | 0% | Yara-Rules |
| rookiestrings | 100% | 0% | 0% | Yara-Rules |

Table 12: Yara Rules Matches for Tiny_banking_trojan

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|--------------------------|-----------------|------------------|---------------|-------------------|
| linux_trojan_mirai | 100% | 0% | 0% | Elastic Security |
| linux.trojan.gafgyt | 100% | 0% | 0% | Elastic Security |

Table 13: Yara Rules Matches for Cult_mirai_botnet

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|--------------------------|-----------------|------------------|---------------|-------------------|
| warp | 100% | 0% | 0% | Yara-Rules |
| warpstrings | 100% | 0% | 0% | Yara-Rules |
| poetrat_python | 100% | 0% | 0% | Yara-Rules |

Table 14: Yara Rules Matches for Panchan_cryptominer

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|--------------------------|-----------------|------------------|---------------|-------------------|
| linux_trojan_kaiji | 100% | 100% | 100% | Elastic Security |

Table 15: Yara Rules Matches for Chaos_botnet

| Matched Yara-Rule | Coverage | Precision | Recall | Repository |
|--------------------------|-----------------|------------------|---------------|-------------------|
| linux.trojan.gafgyt | 100% | 0% | 0% | Elastic Security |
| linux.trojan.gafgyt | 100% | 0% | 0% | Elastic Security |
| susp_xored_mozilla | 100% | 0% | 0% | Neo23x0 |

Table 16: Yara Rules Matches for Infectednight_mirai_botnet