protections-artifacts/yara/rules/Windows_Trojan_GhostEngine.yar at main · elastic/protections-artifacts

By protectionsmachine

Archived: 2026-04-05 17:07:35 UTC

- Linux_Backdoor_Bash.yar
- Linux_Backdoor_Fontonlake.yar
- Linux_Backdoor_Generic.yar
- Linux_Backdoor_Python.yar
- Linux_Backdoor_Tinyshell.yar
- Linux_Cryptominer_Attribute.yar
- Linux_Cryptominer_Bscope.yar
- Linux_Cryptominer_Bulz.yar
- Linux_Cryptominer_Camelot.yar
- Linux_Cryptominer_Casdet.yar
- Linux_Cryptominer_Ccminer.yar
- Linux_Cryptominer_Flystudio.yar
- Linux_Cryptominer_Generic.yar
- Linux_Cryptominer_Ksmdbot.yar
- Linux_Cryptominer_Loudminer.yar
- Linux_Cryptominer_Malxmr.yar
- Linux_Cryptominer_Miancha.yar
- Linux_Cryptominer_Minertr.yar
- Linux_Cryptominer_Pgminer.yar
- Linux_Cryptominer_Presenoker.yar
- Linux_Cryptominer_Roboto.yar

- Linux_Cryptominer_Stak.yar
- Linux_Cryptominer_Ursu.yar
- Linux_Cryptominer_Uwamson.yar
- Linux_Cryptominer_Xmrig.yar
- Linux_Cryptominer_Xmrminer.yar
- Linux_Cryptominer_Xpaj.yar
- Linux_Cryptominer_Zexaf.yar
- Linux_Downloader_Generic.yar
- Linux_Exploit_Abrox.yar
- Linux_Exploit_Alie.yar
- Linux_Exploit_CVE_2009_1897.yar
- Linux_Exploit_CVE_2009_2698.yar
- Linux_Exploit_CVE_2009_2908.yar
- Linux_Exploit_CVE_2010_3301.yar
- Linux_Exploit_CVE_2012_0056.yar
- Linux_Exploit_CVE_2014_3153.yar
- Linux_Exploit_CVE_2016_4557.yar
- Linux_Exploit_CVE_2016_5195.yar
- Linux_Exploit_CVE_2017_100011.yar
- Linux_Exploit_CVE_2017_16995.yar
- Linux_Exploit_CVE_2018_10561.yar
- Linux_Exploit_CVE_2019_13272.yar
- Linux_Exploit_CVE_2021_3156.yar
- Linux_Exploit_CVE_2021_3490.yar
- Linux_Exploit_CVE_2021_4034.yar
- Linux_Exploit_CVE_2022_0847.yar

- Linux_Exploit_Cornelgen.yar
- Linux_Exploit_Courier.yar
- Linux_Exploit_Criscras.yar
- Linux_Exploit_Dirtycow.yar
- Linux_Exploit_Enoket.yar
- Linux_Exploit_Foda.yar
- Linux_Exploit_IOUring.yar
- Linux_Exploit_Intfour.yar
- Linux_Exploit_Local.yar
- Linux_Exploit_Log4j.yar
- Linux_Exploit_Lotoor.yar
- Linux_Exploit_Moogrey.yar
- Linux_Exploit_Openssl.yar
- Linux_Exploit_Perl.yar
- Linux_Exploit_Pulse.yar
- Linux_Exploit_Race.yar
- Linux_Exploit_Ramen.yar
- Linux_Exploit_Sorso.yar
- Linux_Exploit_Vmsplice.yar
- Linux_Exploit_Wuftpd.yar
- Linux_Generic_Threat.yar
- Linux_Hacktool_Aduh.yar
- Linux_Hacktool_Bruteforce.yar
- Linux_Hacktool_Cleanlog.yar
- Linux_Hacktool_Earthworm.yar
- Linux_Hacktool_Exploitscan.yar

- Linux_Hacktool_Flooder.yar
- Linux_Hacktool_Fontonlake.yar
- Linux_Hacktool_Infectionmonkey.yar
- Linux_Hacktool_Lightning.yar
- Linux_Hacktool_LigoloNG.yar
- Linux_Hacktool_Outlaw.yar
- Linux_Hacktool_Portscan.yar
- Linux_Hacktool_Prochide.yar
- Linux_Hacktool_Tcpscan.yar
- Linux_Hacktool_Wipelog.yar
- Linux_Packer_Patched_UPX.yar
- Linux_Proxy_Frp.yar
- Linux_Ransomware_Agenda.yar
- Linux_Ransomware_Akira.yar
- Linux_Ransomware_Babuk.yar
- Linux_Ransomware_BlackBasta.yar
- Linux_Ransomware_BlackSuit.yar
- Linux_Ransomware_Clop.yar
- Linux_Ransomware_Conti.yar
- Linux_Ransomware_EchoRaix.yar
- Linux_Ransomware_Erebus.yar
- Linux_Ransomware_Esxiargs.yar
- Linux_Ransomware_Gonnacry.yar
- Linux_Ransomware_Hellokitty.yar
- Linux_Ransomware_Hive.yar
- Linux_Ransomware_ItsSoEasy.yar

- Linux_Ransomware_LimpDemon.yar
- Linux_Ransomware_Lockbit.yar
- Linux_Ransomware_Monti.yar
- Linux_Ransomware_NoEscape.yar
- Linux_Ransomware_Quantum.yar
- Linux_Ransomware_RagnarLocker.yar
- Linux_Ransomware_RedAlert.yar
- Linux_Ransomware_RoyalPest.yar
- Linux_Ransomware_SFile.yar
- Linux_Ransomware_Sodinokibi.yar
- Linux_Rootkit_Adore.yar
- Linux_Rootkit_Arkd.yar
- Linux_Rootkit_Bedevil.yar
- Linux_Rootkit_BrokePKG.yar
- Linux_Rootkit_Dakkatoni.yar
- Linux_Rootkit_Diamorphine.yar
- Linux_Rootkit_Flipswitch.yar
- Linux_Rootkit_Fontonlake.yar
- Linux_Rootkit_Generic.yar
- Linux_Rootkit_HiddenWasp.yar
- Linux_Rootkit_Jynx.yar
- Linux_Rootkit_Kovid.yar
- Linux_Rootkit_Melofee.yar
- Linux_Rootkit_Mobkit.yar
- Linux_Rootkit_Perfctl.yar
- Linux_Rootkit_Reptile.yar

- Linux_Rootkit_Snapekit.yar
- Linux_Rootkit_Suterusu.yar
- Linux_Shellcode_Generic.yar
- Linux_Trojan_Adlibrary.yar
- Linux_Trojan_Asacub.yar
- Linux_Trojan_Autocolor.yar
- Linux_Trojan_Azeela.yar
- Linux_Trojan_BPFDoor.yar
- Linux_Trojan_Backconnect.yar
- Linux_Trojan_Backegmm.yar
- Linux_Trojan_Badbee.yar
- Linux_Trojan_Banload.yar
- Linux_Trojan_Bedevil.yar
- Linux_Trojan_Bish.yar
- Linux_Trojan_Bluez.yar
- Linux_Trojan_Cerbu.yar
- Linux_Trojan_Chinaz.yar
- Linux_Trojan_Connectback.yar
- Linux_Trojan_Ddostf.yar
- Linux_Trojan_DinodasRAT.yar
- Linux_Trojan_Dnsamp.yar
- Linux_Trojan_Dofloo.yar
- Linux_Trojan_Dropperl.yar
- Linux_Trojan_Ebury.yar
- Linux_Trojan_FinalDraft.yar
- Linux_Trojan_Gafgyt.yar

- Linux_Trojan_Ganiw.yar
- Linux_Trojan_Generic.yar
- Linux_Trojan_Getshell.yar
- Linux_Trojan_Godlua.yar
- Linux_Trojan_Godropper.yar
- Linux_Trojan_Gognt.yar
- Linux_Trojan_Hiddad.yar
- Linux_Trojan_Ipstorm.yar
- Linux_Trojan_Ircbot.yar
- Linux_Trojan_Iroffer.yar
- Linux_Trojan_Kaiji.yar
- Linux_Trojan_Kinsing.yar
- Linux_Trojan_Ladvix.yar
- Linux_Trojan_Lady.yar
- Linux_Trojan_Lala.yar
- Linux_Trojan_Malxmr.yar
- Linux_Trojan_Marut.yar
- Linux_Trojan_Masan.yar
- Linux_Trojan_Mech.yar
- Linux_Trojan_Mechbot.yar
- Linux_Trojan_Melofee.yar
- Linux_Trojan_Merlin.yar
- Linux_Trojan_Metasploit.yar
- Linux_Trojan_Meterpreter.yar
- Linux_Trojan_Mettle.yar
- Linux_Trojan_Mirai.yar

- Linux_Trojan_Mobidash.yar
- Linux_Trojan_Mumblehard.yar
- Linux_Trojan_Ngioweb.yar
- Linux_Trojan_Nuker.yar
- Linux_Trojan_Orbit.yar
- Linux_Trojan_Patpooty.yar
- Linux_Trojan_Pnscan.yar
- Linux_Trojan_Pornoasset.yar
- Linux_Trojan_Psybnc.yar
- Linux_Trojan_Pumakit.yar
- Linux_Trojan_Rbot.yar
- Linux_Trojan_Rekoobe.yar
- Linux_Trojan_Roopre.yar
- Linux_Trojan_Rooter.yar
- Linux_Trojan_Rotajakiro.yar
- Linux_Trojan_Rozena.yar
- Linux_Trojan_Sambashell.yar
- Linux_Trojan_Sckit.yar
- Linux_Trojan_Sdbot.yar
- Linux_Trojan_Setag.yar
- Linux_Trojan_Sfloost.yar
- Linux_Trojan_Shark.yar
- Linux_Trojan_Shellbot.yar
- Linux_Trojan_Skidmap.yar
- Linux_Trojan_Snessik.yar
- Linux_Trojan_Snowlight.yar

- Linux_Trojan_Springtail.yar
- Linux_Trojan_Sqlexp.yar
- Linux_Trojan_Sshdkit.yar
- Linux_Trojan_Sshdoor.yar
- Linux_Trojan_Subsevux.yar
- Linux_Trojan_Swrort.yar
- Linux_Trojan_Sysrv.yar
- Linux_Trojan_Truncpx.yar
- Linux_Trojan_Tsunami.yar
- Linux_Trojan_Winnti.yar
- Linux_Trojan_XZBackdoor.yar
- Linux_Trojan_Xhide.yar
- Linux_Trojan_Xorddos.yar
- Linux_Trojan_Xpmmap.yar
- Linux_Trojan_Zerobot.yar
- Linux_Trojan_Zpevdo.yar
- Linux_Virus_Gmon.yar
- Linux_Virus_Rst.yar
- Linux_Virus_Staffcounter.yar
- Linux_Virus_Thebe.yar
- Linux_Webshell_Generic.yar
- Linux_Worm_Generic.yar
- MacOS_Backdoor_Applejeus.yar
- MacOS_Backdoor_Fakeflashlxk.yar
- MacOS_Backdoor_Kagent.yar
- MacOS_Backdoor_Keyboardrecord.yar

- MacOS_Backdoor_Useragent.yar
- MacOS_Creddump_KeychainAccess.yar
- MacOS_Cryptominer_Generic.yar
- MacOS_Cryptominer_Xmrig.yar
- MacOS_Exploit_Log4j.yar
- MacOS_Hacktool_Bifrost.yar
- MacOS_Hacktool_Swiftbelt.yar
- MacOS_Infostealer_MdQueryPassw.yar
- MacOS_Infostealer_MdQuerySecret.yar
- MacOS_Infostealer_MdQueryTCC.yar
- MacOS_Infostealer_MdQueryToken.yar
- MacOS_Trojan_Adload.yar
- MacOS_Trojan_Amcleaner.yar
- MacOS_Trojan_Aobokeylogger.yar
- MacOS_Trojan_Bundlore.yar
- MacOS_Trojan_Eggshell.yar
- MacOS_Trojan_Electrorat.yar
- MacOS_Trojan_Fplayer.yar
- MacOS_Trojan_Generic.yar
- MacOS_Trojan_Genieo.yar
- MacOS_Trojan_Getshell.yar
- MacOS_Trojan_HLoader.yar
- MacOS_Trojan_KandyKorn.yar
- MacOS_Trojan_Metasploit.yar
- MacOS_Trojan_RustBucket.yar
- MacOS_Trojan_SugarLoader.yar

- MacOS_Trojan_Thiefquest.yar
- MacOS_Virus_Maxofferdeal.yar
- MacOS_Virus_Pirrit.yar
- MacOS_Virus_Vsearch.yar
- Macos_Hacktool_JokerSpy.yar
- Macos_Infostealer_EncodedOsascript.yar
- Macos_Infostealer_Wallets.yar
- Multi_AttackSimulation_Blindspot.yar
- Multi_Cryptominer_Xmrig.yar
- Multi_EICAR.yar
- Multi_Generic_Threat.yar
- Multi_Hacktool_Gsocket.yar
- Multi_Hacktool_Nps.yar
- Multi_Hacktool_Rakshasa.yar
- Multi_Hacktool_Stowaway.yar
- Multi_Hacktool_SuperShell.yar
- Multi_Ransomware_Akira.yar
- Multi_Ransomware_BlackCat.yar
- Multi_Ransomware_Luna.yar
- Multi_Ransomware_RansomHub.yar
- Multi_Trojan_Coreimpact.yar
- Multi_Trojan_EmpirGo.yar
- Multi_Trojan_FinalDraft.yar
- Multi_Trojan_Goffloader.yar
- Multi_Trojan_Gosar.yar
- Multi_Trojan_Merlin.yar

- Multi_Trojan_Mythic.yar
- Multi_Trojan_Sliver.yar
- Multi_Trojan_SparkRat.yar
- Windows_AttackSimulation_Hovercraft.yar
- Windows_Backdoor_DragonCastling.yar
- Windows_Backdoor_Goldbackdoor.yar
- Windows_Backdoor_TeamViewer.yar
- Windows_Clickfraud_LuckySlots.yar
- Windows_Cryptominer_Generic.yar
- Windows_Exploit_CVE_2022_38028.yar
- Windows_Exploit_Dcom.yar
- Windows_Exploit_Eternalblue.yar
- Windows_Exploit_FakePipe.yar
- Windows_Exploit_Generic.yar
- Windows_Exploit_IoRing.yar
- Windows_Exploit_Log4j.yar
- Windows_Exploit_Perfusion.yar
- Windows_Exploit_RpcJunction.yar
- Windows_Generic_MalCert.yar
- Windows_Generic_Threat.yar
- Windows_Hacktool_AskCreds.yar
- Windows_Hacktool_BlackBone.yar
- Windows_Hacktool_COFFLoader.yar
- Windows_Hacktool_Capcom.yar
- Windows_Hacktool_Certify.yar
- Windows_Hacktool_CheatEngine.yar

- Windows_Hacktool_ChromeKatz.yar
- Windows_Hacktool_ClrOxide.yar
- Windows_Hacktool_CpuLocker.yar
- Windows_Hacktool_DarkLoadLibrary.yar
- Windows_Hacktool_Dcsyncer.yar
- Windows_Hacktool_DinvokeRust.yar
- Windows_Hacktool_EDRWFP.yar
- Windows_Hacktool_EDRrecon.yar
- Windows_Hacktool_ExecuteAssembly.yar
- Windows_Hacktool_Gmer.yar
- Windows_Hacktool_GodPotato.yar
- Windows_Hacktool_Iox.yar
- Windows_Hacktool_LeiGod.yar
- Windows_Hacktool_Mimikatz.yar
- Windows_Hacktool_NetFilter.yar
- Windows_Hacktool_Nimhawk.yar
- Windows_Hacktool_Phant0m.yar
- Windows_Hacktool_PhysMem.yar
- Windows_Hacktool_ProcessHacker.yar
- Windows_Hacktool_RingQ.yar
- Windows_Hacktool_Rubeus.yar
- Windows_Hacktool_SafetyKatz.yar
- Windows_Hacktool_Seatbelt.yar
- Windows_Hacktool_SharPersist.yar
- Windows_Hacktool_SharpAppLocker.yar
- Windows_Hacktool_SharpChromium.yar

- Windows_Hacktool_SharpDump.yar
- Windows_Hacktool_SharpGPOAbuse.yar
- Windows_Hacktool_SharpHound.yar
- Windows_Hacktool_SharpLAPS.yar
- Windows_Hacktool_SharpMove.yar
- Windows_Hacktool_SharpRDP.yar
- Windows_Hacktool_SharpSCCM.yar
- Windows_Hacktool_SharpShares.yar
- Windows_Hacktool_SharpStay.yar
- Windows_Hacktool_SharpUp.yar
- Windows_Hacktool_SharpView.yar
- Windows_Hacktool_SharpWMI.yar
- Windows_Hacktool_SleepObfLoader.yar
- Windows_Hacktool_WinPEAS_ng.yar
- Windows_Infostealer_EddieStealer.yar
- Windows_Infostealer_Generic.yar
- Windows_Infostealer_NovaBlight.yar
- Windows_Infostealer_PhemedroneStealer.yar
- Windows_Infostealer_Strela.yar
- Windows_PUP_Generic.yar
- Windows_PUP_MediaArena.yar
- Windows_PUP_Veriato.yar
- Windows_Packer_ScrubCrypt.yar
- Windows_Ransomware_Agenda.yar
- Windows_Ransomware_Akira.yar
- Windows_Ransomware_Avoslocker.yar

- Windows_Ransomware_Azov.yar
- Windows_Ransomware_Bitpaymer.yar
- Windows_Ransomware_BlackBasta.yar
- Windows_Ransomware_BlackHunt.yar
- Windows_Ransomware_Blackmatter.yar
- Windows_Ransomware_Cicada3301.yar
- Windows_Ransomware_Clop.yar
- Windows_Ransomware_Conti.yar
- Windows_Ransomware_Crytox.yar
- Windows_Ransomware_Cuba.yar
- Windows_Ransomware_Darkside.yar
- Windows_Ransomware_Dharma.yar
- Windows_Ransomware_Doppelpaymer.yar
- Windows_Ransomware_DragonForce.yar
- Windows_Ransomware_Egregor.yar
- Windows_Ransomware_GandCrab.yar
- Windows_Ransomware_Generic.yar
- Windows_Ransomware_Grief.yar
- Windows_Ransomware_Haron.yar
- Windows_Ransomware_Hellokitty.yar
- Windows_Ransomware_Helloxd.yar
- Windows_Ransomware_Hive.yar
- Windows_Ransomware_Lockbit.yar
- Windows_Ransomware_Lockfile.yar
- Windows_Ransomware_Magniber.yar
- Windows_Ransomware_Makop.yar

- Windows_Ransomware_Maui.yar
- Windows_Ransomware_Maze.yar
- Windows_Ransomware_Medusa.yar
- Windows_Ransomware_Mespinoza.yar
- Windows_Ransomware_Mountlocker.yar
- Windows_Ransomware_Nightsky.yar
- Windows_Ransomware_Pandora.yar
- Windows_Ransomware_Phobos.yar
- Windows_Ransomware_Ragnarok.yar
- Windows_Ransomware_Ransomexx.yar
- Windows_Ransomware_Rook.yar
- Windows_Ransomware_Royal.yar
- Windows_Ransomware_Ryuk.yar
- Windows_Ransomware_Snake.yar
- Windows_Ransomware_Sodinokibi.yar
- Windows_Ransomware_Stop.yar
- Windows_Ransomware_Thanos.yar
- Windows_Ransomware_Vgod.yar
- Windows_Ransomware_Vhd.yar
- Windows_Ransomware_WannaCry.yar
- Windows_Ransomware_WhisperGate.yar
- Windows_RemoteAdmin_UltraVNC.yar
- Windows_Rootkit_AbyssWorker.yar
- Windows_Rootkit_R77.yar
- Windows_Shellcode_Generic.yar
- Windows_Shellcode_Rdi.yar

- Windows_Trojan_A310logger.yar
- Windows_Trojan_ACRStealer.yar
- Windows_Trojan_Adaptix.yar
- Windows_Trojan_Afdk.yar
- Windows_Trojan_AgentTesla.yar
- Windows_Trojan_Amadey.yar
- Windows_Trojan_Arechclient2.yar
- Windows_Trojan_ArkeiStealer.yar
- Windows_Trojan_Asyncrat.yar
- Windows_Trojan_AveMaria.yar
- Windows_Trojan_Azorult.yar
- Windows_Trojan_BITSloth.yar
- Windows_Trojan_Babble.yar
- Windows_Trojan_Babylonrat.yar
- Windows_Trojan_Backoff.yar
- Windows_Trojan_BadIIS.yar
- Windows_Trojan_Bandook.yar
- Windows_Trojan_Bazar.yar
- Windows_Trojan_Beam.yar
- Windows_Trojan_Behinder.yar
- Windows_Trojan_Bitrat.yar
- Windows_Trojan_BlackShades.yar
- Windows_Trojan_Blackwood.yar
- Windows_Trojan_Blister.yar
- Windows_Trojan_BloodAlchemy.yar
- Windows_Trojan_BruteRatel.yar

- Windows_Trojan_Buerloader.yar
- Windows_Trojan_Bughatch.yar
- Windows_Trojan_Bumblebee.yar
- Windows_Trojan_CaesarKbd.yar
- Windows_Trojan_Carberp.yar
- Windows_Trojan_CastleLoader.yar
- Windows_Trojan_Clipbanker.yar
- Windows_Trojan_CobaltStrike.yar
- Windows_Trojan_Cryptbot.yar
- Windows_Trojan_CyberGate.yar
- Windows_Trojan_DBatLoader.yar
- Windows_Trojan_DCRat.yar
- Windows_Trojan_DTrack.yar
- Windows_Trojan_Danabot.yar
- Windows_Trojan_Dante.yar
- Windows_Trojan_DarkCloud.yar
- Windows_Trojan_DarkGate.yar
- Windows_Trojan_DarkVNC.yar
- Windows_Trojan_Darkcomet.yar
- Windows_Trojan_DeerStealer.yar
- Windows_Trojan_Deimos.yar
- Windows_Trojan_DiamondFox.yar
- Windows_Trojan_Diceloader.yar
- Windows_Trojan_DodgeBox.yar
- Windows_Trojan_Donutloader.yar
- Windows_Trojan_DoorMe.yar

- Windows_Trojan_DoubleBack.yar
- Windows_Trojan_DoubleLoader.yar
- Windows_Trojan_DownTown.yar
- Windows_Trojan_DragonBreath.yar
- Windows_Trojan_DreamJob.yar
- Windows_Trojan_Dridex.yar
- Windows_Trojan_DustyWarehouse.yar
- Windows_Trojan_EagerBee.yar
- Windows_Trojan_Emotet.yar
- Windows_Trojan_Fabookie.yar
- Windows_Trojan_FalseFont.yar
- Windows_Trojan_Farfli.yar
- Windows_Trojan_Fickerstealer.yar
- Windows_Trojan_FinalDraft.yar
- Windows_Trojan_FlawedGrace.yar
- Windows_Trojan_Formbook.yar
- Windows_Trojan_Garble.yar
- Windows_Trojan_Generic.yar
- Windows_Trojan_Gh0st.yar
- Windows_Trojan_GhostEngine.yar
- Windows_Trojan_GhostPulse.yar
- Windows_Trojan_Glupteba.yar
- Windows_Trojan_Gozi.yar
- Windows_Trojan_Grandoreiro.yar
- Windows_Trojan_GuidLoader.yar
- Windows_Trojan_Guloader.yar

- Windows_Trojan_Hancitor.yar
- Windows_Trojan_Havoc.yar
- Windows_Trojan_Hawkeye.yar
- Windows_Trojan_HazelCobra.yar
- Windows_Trojan_HiddenCli.yar
- Windows_Trojan_HiddenDriver.yar
- Windows_Trojan_HijackLoader.yar
- Windows_Trojan_HotPage.yar
- Windows_Trojan_IcedID.yar
- Windows_Trojan_JesterStealer.yar
- Windows_Trojan_Jupyter.yar
- Windows_Trojan_KoiLoader.yar
- Windows_Trojan_Kronos.yar
- Windows_Trojan_Latrodectus.yar
- Windows_Trojan_LegionLoader.yar
- Windows_Trojan_Limerat.yar
- Windows_Trojan_Lobshot.yar
- Windows_Trojan_Lokibot.yar
- Windows_Trojan_Lumma.yar
- Windows_Trojan_Lurker.yar
- Windows_Trojan_M0yv.yar
- Windows_Trojan_MagicRat.yar
- Windows_Trojan_MassLogger.yar
- Windows_Trojan_Mata.yar
- Windows_Trojan_Matanbuchus.yar
- Windows_Trojan_Merlin.yar

- Windows_Trojan_MetaStealer.yar
- Windows_Trojan_Metasploit.yar
- Windows_Trojan_MicroBackdoor.yar
- Windows_Trojan_MimicRat.yar
- Windows_Trojan_ModPipe.yar
- Windows_Trojan_MonsterV2.yar
- Windows_Trojan_MyloBot.yar
- Windows_Trojan_NanoRemote.yar
- Windows_Trojan_Nanocore.yar
- Windows_Trojan_NapListener.yar
- Windows_Trojan_Netwire.yar
- Windows_Trojan_Nighthawk.yar
- Windows_Trojan_NightshadeC2.yar
- Windows_Trojan_Nimplant.yar
- Windows_Trojan_Njrat.yar
- Windows_Trojan_NukeSped.yar
- Windows_Trojan_Octopus.yar
- Windows_Trojan_OnlyLogger.yar
- Windows_Trojan_OskiStealer.yar
- Windows_Trojan_Oyster.yar
- Windows_Trojan_P8Loader.yar
- Windows_Trojan_Pandastealer.yar
- Windows_Trojan_Parallax.yar
- Windows_Trojan_PathLoader.yar
- Windows_Trojan_Phoreal.yar
- Windows_Trojan_PikaBot.yar

- Windows_Trojan_Pingpull.yar
- Windows_Trojan_PipeDance.yar
- Windows_Trojan_PizzaPotion.yar
- Windows_Trojan_PlugX.yar
- Windows_Trojan_Pony.yar
- Windows_Trojan_PoshC2.yar
- Windows_Trojan_PowerSeal.yar
- Windows_Trojan_PrivateLoader.yar
- Windows_Trojan_ProtectS.yar
- Windows_Trojan_Qbot.yar
- Windows_Trojan_Quasarrat.yar
- Windows_Trojan_Raccoon.yar
- Windows_Trojan_RaspberryRobin.yar
- Windows_Trojan_RedLineStealer.yar
- Windows_Trojan_Remcos.yar
- Windows_Trojan_Revcoderat.yar
- Windows_Trojan_Revengerat.yar
- Windows_Trojan_Rhadamanthys.yar
- Windows_Trojan_RoningLoader.yar
- Windows_Trojan_RudeBird.yar
- Windows_Trojan_STRRAT.yar
- Windows_Trojan_SVCReady.yar
- Windows_Trojan_SadBridge.yar
- Windows_Trojan_SalatStealer.yar
- Windows_Trojan_ServHelper.yar
- Windows_Trojan_ShadowPad.yar

- Windows_Trojan_ShelbyC2.yar
- Windows_Trojan_ShelbyLoader.yar
- Windows_Trojan_Shellter.yar
- Windows_Trojan_SiestaGraph.yar
- Windows_Trojan_SilentConnect.yar
- Windows_Trojan_Sliver.yar
- Windows_Trojan_Smokeloader.yar
- Windows_Trojan_SnakeKeylogger.yar
- Windows_Trojan_SolarMarker.yar
- Windows_Trojan_SomniRecord.yar
- Windows_Trojan_SourShark.yar
- Windows_Trojan_SpectralViper.yar
- Windows_Trojan_Squirrelwaffle.yar
- Windows_Trojan_Stealc.yar
- Windows_Trojan_StormKitty.yar
- Windows_Trojan_StumpZarus.yar
- Windows_Trojan_SuddenIcon.yar
- Windows_Trojan_Supper.yar
- Windows_Trojan_SysJoker.yar
- Windows_Trojan_SystemBC.yar
- Windows_Trojan_Sythe.yar
- Windows_Trojan_Tofsee.yar
- Windows_Trojan_Tollbooth.yar
- Windows_Trojan_Trickbot.yar
- Windows_Trojan_Tuoni.yar
- Windows_Trojan_TwistedTinsel.yar

- Windows_Trojan_Vidar.yar
- Windows_Trojan_WMLoader.yar
- Windows_Trojan_WarmCookie.yar
- Windows_Trojan_WhisperGate.yar
- Windows_Trojan_WikiLoader.yar
- Windows_Trojan_WineLoader.yar
- Windows_Trojan_Winos.yar
- Windows_Trojan_XWorm.yar
- Windows_Trojan_Xeno.yar
- Windows_Trojan_Xpertrat.yar
- Windows_Trojan_XtremeRAT.yar
- Windows_Trojan_Zeus.yar
- Windows_Trojan_Zloader.yar
- Windows_Virus_Expiro.yar
- Windows_Virus_Floxif.yar
- Windows_Virus_Neshta.yar
- Windows_VulnDriver_ATSZIO.yar
- Windows_VulnDriver_Agent64.yar
- Windows_VulnDriver_Amifldrv.yar
- Windows_VulnDriver_ArPot.yar
- Windows_VulnDriver_AsIo.yar
- Windows_VulnDriver_Asrock.yar
- Windows_VulnDriver_Atillk.yar
- Windows_VulnDriver_BSMI.yar
- Windows_VulnDriver_Biostar.yar
- Windows_VulnDriver_CCProtect.yar

- Windows_VulnDriver_Cpuz.yar
- Windows_VulnDriver_DBUtil.yar
- Windows_VulnDriver_DirectIo.yar
- Windows_VulnDriver_EchoDrv.yar
- Windows_VulnDriver_ElRawDisk.yar
- Windows_VulnDriver_Elby.yar
- Windows_VulnDriver_EneIo.yar
- Windows_VulnDriver_FidDrv.yar
- Windows_VulnDriver_Fidpci.yar
- Windows_VulnDriver_Fileseclab.yar
- Windows_VulnDriver_GDrv.yar
- Windows_VulnDriver_GlckIo.yar
- Windows_VulnDriver_Gvci.yar
- Windows_VulnDriver_HpPortIo.yar
- Windows_VulnDriver_HrSword.yar
- Windows_VulnDriver_IoBitUnlocker.yar
- Windows_VulnDriver_Iqvw.yar
- Windows_VulnDriver_LLAccess.yar
- Windows_VulnDriver_Lha.yar
- Windows_VulnDriver_MarvinHW.yar
- Windows_VulnDriver_Mhyprot.yar
- Windows_VulnDriver_MicroStar.yar
- Windows_VulnDriver_MsIo.yar
- Windows_VulnDriver_MtcBsv.yar
- Windows_VulnDriver_PowerProfiler.yar
- Windows_VulnDriver_PowerTool.yar

- Windows_VulnDriver_ProcExp.yar
- Windows_VulnDriver_ProcId.yar
- Windows_VulnDriver_RWEverything.yar
- Windows_VulnDriver_RentDrv.yar
- Windows_VulnDriver_RtCore.yar
- Windows_VulnDriver_Rtkio.yar
- Windows_VulnDriver_Ryzen.yar
- Windows_VulnDriver_Sandra.yar
- Windows_VulnDriver_Segwin.yar
- Windows_VulnDriver_Speedfan.yar
- Windows_VulnDriver_ThreatFire.yar
- Windows_VulnDriver_ThrottleStop.yar
- Windows_VulnDriver_TmComm.yar
- Windows_VulnDriver_TopazOFD.yar
- Windows_VulnDriver_ToshibaBios.yar
- Windows_VulnDriver_TrueSight.yar
- Windows_VulnDriver_VBox.yar
- Windows_VulnDriver_Viragt.yar
- Windows_VulnDriver_Vmdrv.yar
- Windows_VulnDriver_WinDivert.yar
- Windows_VulnDriver_WinFlash.yar
- Windows_VulnDriver_WinIo.yar
- Windows_VulnDriver_XTier.yar
- Windows_VulnDriver_Zam.yar
- Windows_Wiper_CaddyWiper.yar
- Windows_Wiper_DoubleZero.yar

- Windows_Wiper_HermeticWiper.yar
- Windows_Wiper_IsaacWiper.yar
