

## **protections- artifacts/yara/rules/Windows\_Trojan\_WarmCookie.yar at main · elastic/protections-artifacts**

By protectionsmachine

Archived: 2026-04-06 00:15:00 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\_Ksmbot.yar
- Linux\_Cryptominer\_Loudminer.yar
- Linux\_Cryptominer\_Malxmr.yar
- Linux\_Cryptominer\_Miancha.yar
- Linux\_Cryptominer\_Minetr.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\_Xpmmmap.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\_Fakeflashlxx.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\_BITSlloth.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\_Diceloder.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\_Latroductus.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\_Quasarat.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\_Amifldr.yar
- Windows\_VulnDriver\_ArPot.yar
- Windows\_VulnDriver\_AsIo.yar
- Windows\_VulnDriver\_Asrock.yar
- Windows\_VulnDriver\_Atillk.yar
- Windows\_VulnDriver\_BSML.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\_Iqyw.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](#)

---

Source: [https://github.com/elastic/protections-artifacts/blob/main/yara/rules/Windows\\_Trojan\\_WarmCookie.yar](https://github.com/elastic/protections-artifacts/blob/main/yara/rules/Windows_Trojan_WarmCookie.yar)