# CVE Detail – CVE-2021-32638

Github's CodeQL action is provided to run CodeQL-based code scanning on non-GitHub CI/CD systems and requires a GitHub access token to connect to a GitHub repository. The runner and its documentation previously suggested passing the GitHub token as a command-line parameter to the process instead of reading it from a file, standard input, or an environment variable. This approach made the token visible to other processes on the same machine, for example in the output of the `ps` command. If the CI system publicly exposes the output of `ps`, for example by logging the output, then the GitHub access token can be exposed beyond the scope intended. Users of the CodeQL runner on 3rd-party systems, who are passing a GitHub token via the `--github-auth` flag, are affected. This applies to both GitHub.com and GitHub Enterprise users. Users of the CodeQL Action on GitHub Actions are not affected. The `--github-auth` flag is now considered insecure and deprecated. The undocumented `--external-repository-token` flag has been removed. To securely provide a GitHub access token to the CodeQL runner, users should \*\*do one of the following instead\*\*: Use the `--github-auth-stdin` flag and pass the token on the command line via standard input OR set the `GITHUB\_TOKEN` environment variable to contain the token, then call the command without passing in the token. The old flag remains present for backwards compatibility with existing workflows. If the user tries to specify an access token using the `--github-auth` flag, there is a deprecation warning printed to the terminal that directs the user to one of the above options. All CodeQL runner releases codeql-bundle-20210304 onwards contain the patches. We recommend updating to a recent version of the CodeQL runner, storing a token in your CI system's secret storage mechanism, and passing the token to the CodeQL runner using `--github-auth-stdin` or the `GITHUB\_TOKEN` environment variable. If still using the old flag, ensure that process output, such as from `ps`, is not persisted in CI logs.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.2275

## CVSS Scoring

CVSS v3.1 Score: 4.4

Severity: MEDIUM

## Mapped CWE(s)

* CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
* CWE-214: Invocation of Process Using Visible Sensitive Information

## CAPEC(s)

* CAPEC-116: Excavation
* CAPEC-13: Subverting Environment Variable Values
* CAPEC-169: Footprinting
* CAPEC-22: Exploiting Trust in Client
* CAPEC-224: Fingerprinting
* CAPEC-285: ICMP Echo Request Ping
* CAPEC-287: TCP SYN Scan
* CAPEC-290: Enumerate Mail Exchange (MX) Records
* CAPEC-291: DNS Zone Transfers
* CAPEC-292: Host Discovery
* CAPEC-293: Traceroute Route Enumeration
* CAPEC-294: ICMP Address Mask Request
* CAPEC-295: Timestamp Request
* CAPEC-296: ICMP Information Request
* CAPEC-297: TCP ACK Ping
* CAPEC-298: UDP Ping
* CAPEC-299: TCP SYN Ping
* CAPEC-300: Port Scanning
* CAPEC-301: TCP Connect Scan
* CAPEC-302: TCP FIN Scan
* CAPEC-303: TCP Xmas Scan
* CAPEC-304: TCP Null Scan
* CAPEC-305: TCP ACK Scan
* CAPEC-306: TCP Window Scan
* CAPEC-307: TCP RPC Scan
* CAPEC-308: UDP Scan
* CAPEC-309: Network Topology Mapping
* CAPEC-310: Scanning for Vulnerable Software
* CAPEC-312: Active OS Fingerprinting
* CAPEC-313: Passive OS Fingerprinting
* CAPEC-317: IP ID Sequencing Probe
* CAPEC-318: IP 'ID' Echoed Byte-Order Probe
* CAPEC-319: IP (DF) 'Don't Fragment Bit' Echoing Probe
* CAPEC-320: TCP Timestamp Probe
* CAPEC-321: TCP Sequence Number Probe
* CAPEC-322: TCP (ISN) Greatest Common Divisor Probe
* CAPEC-323: TCP (ISN) Counter Rate Probe
* CAPEC-324: TCP (ISN) Sequence Predictability Probe
* CAPEC-325: TCP Congestion Control Flag (ECN) Probe
* CAPEC-326: TCP Initial Window Size Probe
* CAPEC-327: TCP Options Probe
* CAPEC-328: TCP 'RST' Flag Checksum Probe
* CAPEC-329: ICMP Error Message Quoting Probe
* CAPEC-330: ICMP Error Message Echoing Integrity Probe
* CAPEC-472: Browser Fingerprinting
* CAPEC-497: File Discovery
* CAPEC-508: Shoulder Surfing
* CAPEC-573: Process Footprinting
* CAPEC-574: Services Footprinting
* CAPEC-575: Account Footprinting
* CAPEC-576: Group Permission Footprinting
* CAPEC-577: Owner Footprinting
* CAPEC-59: Session Credential Falsification through Prediction
* CAPEC-60: Reusing Session IDs (aka Session Replay)
* CAPEC-616: Establish Rogue Location
* CAPEC-643: Identify Shared Files/Directories on System
* CAPEC-646: Peripheral Footprinting
* CAPEC-651: Eavesdropping
* CAPEC-79: Using Slashes in Alternate Encoding

## ATT&CK Techniques

* T1033: System Owner/User Discovery
* T1592: Gather Victim Host Information
* T1574.007: Path Interception by PATH Environment Variable
* T1069: Permission Groups Discovery
* T1615: Group Policy Discovery
* T1036.005: Match Legitimate Resource Name or Location
* T1007: System Service Discovery
* T1135: Network Share Discovery
* T1120: Peripheral Device Discovery
* T1082: System Information Discovery
* T1217: Browser Information Discovery
* T1574.006: Dynamic Linker Hijacking
* T1595: Active Scanning
* T1016: System Network Configuration Discovery
* T1087: Account Discovery
* T1083: File and Directory Discovery
* T1049: System Network Connections Discovery
* T1134.001: Token Impersonation/Theft
* T1057: Process Discovery
* T1562.003: Impair Command History Logging
* T1590: Gather Victim Network Information
* T1550.004: Web Session Cookie
* T1111: Multi-Factor Authentication Interception
* T1018: Remote System Discovery
* T1046: Network Service Discovery
* T1124: System Time Discovery

## Used By (Actors/Tools)

* HDoor (malware)
* TrickBot (malware)
* cd00r (malware)
* PowerDuke (malware)
* EKANS (malware)
* BLINDINGCAN (malware)
* Ninja (malware)
* Pikabot (malware)
* RCSession (malware)
* Spark (malware)
* QuietSieve (malware)
* SynAck (malware)
* Bumblebee (malware)
* MURKYTOP (malware)
* AcidRain (malware)
* GRIFFON (malware)
* Amadey (malware)
* Proxysvc (malware)
* Orz (malware)
* Torisma (malware)
* NOKKI (malware)
* yty (malware)
* Backdoor.Oldrea (malware)
* Stuxnet (malware)
* RotaJakiro (malware)
* AvosLocker (malware)
* Get2 (malware)
* POWRUNER (malware)
* KOPILUWAK (malware)
* Chinoxy (malware)
* SharpStage (malware)
* COATHANGER (malware)
* Sardonic (malware)
* Smoke Loader (malware)
* HALFBAKED (malware)
* WindTail (malware)
* Misdat (malware)
* Linux Rabbit (malware)
* Emissary (malware)
* Exaramel for Linux (malware)
* KEYMARBLE (malware)
* BUBBLEWRAP (malware)
* HAWKBALL (malware)
* Ursnif (malware)
* ThreatNeedle (malware)
* RansomHub (malware)
* ZLib (malware)
* RedLeaves (malware)
* LITTLELAMB.WOOLTEA (malware)
* Felismus (malware)
* Zeus Panda (malware)
* GeminiDuke (malware)
* CARROTBAT (malware)
* FrameworkPOS (malware)
* GravityRAT (malware)
* Prestige (malware)
* Bankshot (malware)
* SharpDisco (malware)
* StrongPity (malware)
* HAPPYWORK (malware)
* xCaon (malware)
* PLAINTEE (malware)
* Pony (malware)
* WinMM (malware)
* Nebulae (malware)
* AuditCred (malware)
* UPSTYLE (malware)
* Kasidet (malware)
* OceanSalt (malware)
* Playcrypt (malware)
* Brave Prince (malware)
* RainyDay (malware)
* AppleSeed (malware)
* macOS.OSAMiner (malware)
* NETWIRE (malware)
* TinyTurla (malware)
* PyDCrypt (malware)
* J-magic (malware)
* iKitten (malware)
* OLDBAIT (malware)
* Bad Rabbit (malware)
* CosmicDuke (malware)
* EnvyScout (malware)
* SslMM (malware)
* IMAPLoader (malware)
* GreyEnergy (malware)
* Gomir (malware)
* Aria-body (malware)
* Emotet (malware)
* Olympic Destroyer (malware)
* BOLDMOVE (malware)
* Crimson (malware)
* TEARDROP (malware)
* DUSTTRAP (malware)
* Turian (malware)
* BADHATCH (malware)
* Machete (malware)
* PowerLess (malware)
* Action RAT (malware)
* Avenger (malware)
* DUSTPAN (malware)
* Prikormka (malware)
* Gootloader (malware)
* PingPull (malware)
* WellMess (malware)
* Dacls (malware)
* DropBook (malware)
* Woody RAT (malware)
* Mafalda (malware)
* KARAE (malware)
* Squirrelwaffle (malware)
* ELMER (malware)
* AuTo Stealer (malware)
* ShrinkLocker (malware)
* Hildegard (malware)
* Agent.btz (malware)
* SLOWDRIFT (malware)
* SHUTTERSPEED (malware)
* SombRAT (malware)
* ODAgent (malware)
* BlackByte 2.0 Ransomware (malware)
* FLASHFLOOD (malware)
* FlawedAmmyy (malware)
* Snip3 (malware)
* FYAnti (malware)
* Rifdoor (malware)
* LoFiSe (malware)
* HOPLIGHT (malware)
* Cuckoo Stealer (malware)
* MobileOrder (malware)
* WastedLocker (malware)
* InvisiMole (malware)
* P.A.S. Webshell (malware)
* QUIETEXIT (malware)
* Naid (malware)
* Apostle (malware)
* Volgmer (malware)
* WINERACK (malware)
* WhisperGate (malware)
* FruitFly (malware)
* ZeroT (malware)
* AcidPour (malware)
* RDAT (malware)
* Skidmap (malware)
* Okrum (malware)
* TRANSLATEXT (malware)
* Bonadan (malware)
* Line Dancer (malware)
* Neoichor (malware)
* Conti (malware)
* Raspberry Robin (malware)
* Mispadu (malware)
* Megazord (malware)
* Diavol (malware)
* Raindrop (malware)
* Doki (malware)
* Siloscape (malware)
* BlackCat (malware)
* Fysbis (malware)
* IcedID (malware)
* VERMIN (malware)
* UBoatRAT (malware)
* Nightdoor (malware)
* MarkiRAT (malware)
* PowerShower (malware)
* Kazuar (malware)
* NavRAT (malware)
* DarkComet (malware)
* NETEAGLE (malware)
* POORAIM (malware)
* CHIMNEYSWEEP (malware)
* Ragnar Locker (malware)
* FatDuke (malware)
* Lucifer (malware)
* BlackEnergy (malware)
* zwShell (malware)
* DCSrv (malware)
* DRATzarus (malware)
* Rising Sun (malware)
* NotPetya (malware)
* ShimRat (malware)
* Chrommme (malware)
* BADFLICK (malware)
* ObliqueRAT (malware)
* SHOTPUT (malware)
* Avaddon (malware)
* Conficker (malware)
* SocGholish (malware)
* Flagpro (malware)
* SpicyOmelette (malware)
* XAgentOSX (malware)
* Green Lambert (malware)
* China Chopper (malware)
* LightSpy (malware)
* PUNCHBUGGY (malware)
* GoldMax (malware)
* HELLOKITTY (malware)
* Cheerscrypt (malware)
* KeyBoy (malware)
* MiniDuke (malware)
* HyperBro (malware)
* Anchor (malware)
* Pteranodon (malware)
* DarkTortilla (malware)
* ROKRAT (malware)
* CORESHELL (malware)
* RunningRAT (malware)
* Babuk (malware)
* Exbyte (malware)
* DarkWatchman (malware)
* Dyre (malware)
* BlackMould (malware)
* Javali (malware)
* PACEMAKER (malware)
* LunarLoader (malware)
* BBSRAT (malware)
* PlugX (malware)
* Reaver (malware)
* Bisonal (malware)
* MultiLayer Wiper (malware)
* S-Type (malware)
* Lumma Stealer (malware)
* DustySky (malware)
* Duqu (malware)
* Remsec (malware)
* Industroyer2 (malware)
* Sykipot (malware)
* Explosive (malware)
* Xbash (malware)
* Rover (malware)
* Epic (malware)
* LightNeuron (malware)
* Peppy (malware)
* KEYPLUG (malware)
* Cuba (malware)
* DEATHRANSOM (malware)
* Clambling (malware)
* Akira (malware)
* DarkGate (malware)
* Mongall (malware)
* NanHaiShu (malware)
* LockBit 3.0 (malware)
* SVCReady (malware)
* ThiefQuest (malware)
* FoggyWeb (malware)
* NGLite (malware)
* Carbanak (malware)
* XTunnel (malware)
* Hydraq (malware)
* SHARPSTATS (malware)
* Ferocious (malware)
* CreepyDrive (malware)
* Caterpillar WebShell (malware)
* Netwalker (malware)
* Elise (malware)
* USBferry (malware)
* WannaCry (malware)
* Gazer (malware)
* TSCookie (malware)
* Latrodectus (malware)
* Saint Bot (malware)
* Pay2Key (malware)
* Chaes (malware)
* CharmPower (malware)
* TYPEFRAME (malware)
* 3PARA RAT (malware)
* Bundlore (malware)
* P8RAT (malware)
* EVILNUM (malware)
* KOMPROGO (malware)
* SMOKEDHAM (malware)
* QUADAGENT (malware)
* Sagerunex (malware)
* TAINTEDSCRIBE (malware)
* Sys10 (malware)
* Royal (malware)
* BendyBear (malware)
* Uroburos (malware)
* Metamorfo (malware)
* Spica (malware)
* Trojan.Karagany (malware)
* Bandook (malware)
* PipeMon (malware)
* MagicRAT (malware)
* TINYTYPHON (malware)
* KONNI (malware)
* T9000 (malware)
* gh0st RAT (malware)
* Shamoon (malware)
* DnsSystem (malware)
* MoleNet (malware)
* CORALDECK (malware)
* JHUHUGIT (malware)
* SPACESHIP (malware)
* BLUELIGHT (malware)
* KGH\_SPY (malware)
* down\_new (malware)
* Ixeshe (malware)
* Micropsia (malware)
* Kerrdown (malware)
* RARSTONE (malware)
* BPFDoor (malware)
* Black Basta (malware)
* ZeroCleare (malware)
* Catchamas (malware)
* StoneDrill (malware)
* OopsIE (malware)
* 4H RAT (malware)
* RogueRobin (malware)
* Attor (malware)
* LitePower (malware)
* MegaCortex (malware)
* StreamEx (malware)
* BoxCaon (malware)
* NightClub (malware)
* Crutch (malware)
* Akira \_v2 (malware)
* SDBbot (malware)
* Mosquito (malware)
* RTM (malware)
* QUIETCANARY (malware)
* Derusbi (malware)
* BlackByte Ransomware (malware)
* SodaMaster (malware)
* StrelaStealer (malware)
* Grandoreiro (malware)
* WellMail (malware)
* LiteDuke (malware)
* Starloader (malware)
* Sibot (malware)
* ZxxZ (malware)
* Tarrask (malware)
* GoBear (malware)
* WINDSHIELD (malware)
* Shark (malware)
* Bazar (malware)
* Kobalos (malware)
* BadPatch (malware)
* MESSAGETAP (malware)
* RATANKBA (malware)
* SUGARDUMP (malware)
* XLoader (malware)
* SOUNDBITE (malware)
* BADCALL (malware)
* MoonWind (malware)
* Ryuk (malware)
* Cryptoistic (malware)
* HermeticWiper (malware)
* Pysa (malware)
* Final1stspy (malware)
* MgBot (malware)
* ccf32 (malware)
* Kapeka (malware)
* LockBit 2.0 (malware)
* Zebrocy (malware)
* Pandora (malware)
* FinFisher (malware)
* SpeakUp (malware)
* LunarMail (malware)
* CrossRAT (malware)
* OwaAuth (malware)
* Cadelspy (malware)
* Cobalt Strike (malware)
* SampleCheck5000 (malware)
* SUNBURST (malware)
* EvilBunny (malware)
* Wingbird (malware)
* HotCroissant (malware)
* ServHelper (malware)
* Unknown Logger (malware)
* REvil (malware)
* Valak (malware)
* Samurai (malware)
* PinchDuke (malware)
* Milan (malware)
* USBStealer (malware)
* OSX\_OCEANLOTUS.D (malware)
* OilBooster (malware)
* Taidoor (malware)
* SUPERNOVA (malware)
* Kivars (malware)
* CaddyWiper (malware)
* Cyclops Blink (malware)
* Seasalt (malware)
* NanoCore (malware)
* TajMahal (malware)
* PLEAD (malware)
* Raccoon Stealer (malware)
* IPsec Helper (malware)
* Daserf (malware)
* Carbon (malware)
* Cardinal RAT (malware)
* DanBot (malware)
* BISCUIT (malware)
* Calisto (malware)
* Solar (malware)
* Pisloader (malware)
* GoldenSpy (malware)
* Gold Dragon (malware)
* RGDoor (malware)
* Ramsay (malware)
* Carberp (malware)
* NKAbuse (malware)
* Pillowmint (malware)
* Revenge RAT (malware)
* MacMa (malware)
* FunnyDream (malware)
* ROADSWEEP (malware)
* SUNSPOT (malware)
* More\_eggs (malware)
* SysUpdate (malware)
* OutSteel (malware)
* BackConfig (malware)
* PowGoop (malware)
* Kwampirs (malware)
* BoomBox (malware)
* DEADEYE (malware)
* Mango (malware)
* InnaputRAT (malware)
* Kessel (malware)
* GrimAgent (malware)
* LookBack (malware)
* Clop (malware)
* YAHOYAH (malware)
* Lokibot (malware)
* Egregor (malware)
* PoetRAT (malware)
* CHOPSTICK (malware)
* StealBit (malware)
* FELIXROOT (malware)
* ZxShell (malware)
* NDiskMonitor (malware)
* DDKONG (malware)
* Penquin (malware)
* BabyShark (malware)
* Cannon (malware)
* CreepySnail (malware)
* build\_downer (malware)
* Winnti for Windows (malware)
* Troll Stealer (malware)
* BLACKCOFFEE (malware)
* Ebury (malware)
* Kinsing (malware)
* Meteor (malware)
* njRAT (malware)
* ZIPLINE (malware)
* Maze (malware)
* ComRAT (malware)
* TURNEDUP (malware)
* ChChes (malware)
* PowerStallion (malware)
* ANDROMEDA (malware)
* Manjusaka (malware)
* IceApple (malware)
* JPIN (malware)
* metaMain (malware)
* SideTwist (malware)
* KOCTOPUS (malware)
* MechaFlounder (malware)
* Psylo (malware)
* Heyoka Backdoor (malware)
* HTTPBrowser (malware)
* Mis-Type (malware)
* LunarWeb (malware)
* XCSSET (malware)
* Octopus (malware)
* KillDisk (malware)
* AppleJeus (malware)
* SoreFang (malware)
* STARWHALE (malware)
* MirageFox (malware)
* Industroyer (malware)
* DownPaper (malware)
* Socksbot (malware)
* Pcexter (malware)
* CozyCar (malware)
* Kevin (malware)
* Agent Tesla (malware)
* Pasam (malware)
* POWERSTATS (malware)
* BADNEWS (malware)
* Linfo (malware)
* Goopy (malware)
* ShadowPad (malware)
* Remexi (malware)
* Astaroth (malware)
* QakBot (malware)
* SYSCON (malware)
* CookieMiner (malware)
* Gelsemium (malware)
* jRAT (malware)
* Helminth (malware)
* Dridex (malware)
* Komplex (malware)
* OSX/Shlayer (malware)
* Denis (malware)
* INC Ransomware (malware)
* DEADWOOD (malware)
* Waterbear (malware)
* FIVEHANDS (malware)
* Comnie (malware)
* AutoIt backdoor (malware)
* OSInfo (malware)
* Lizar (malware)
* Dtrack (malware)
* SLOWPULSE (malware)
* LoudMiner (malware)
* Azorult (malware)
* BitPaymer (malware)
* BACKSPACE (malware)
* Zox (malware)
* UPPERCUT (malware)
* ADVSTORESHELL (malware)
* StrifeWater (malware)
* HiddenWasp (malware)
* WarzoneRAT (malware)
* SLOTHFULMEDIA (malware)
* FALLCHILL (malware)
* Small Sieve (malware)
* HermeticWizard (malware)
* Net (tool)
* RemoteUtilities (tool)
* Covenant (tool)
* BloodHound (tool)
* ShimRatReporter (tool)
* Sliver (tool)
* SILENTTRINITY (tool)
* PowerSploit (tool)
* Pacu (tool)
* ipconfig (tool)
* Tasklist (tool)
* Arp (tool)
* Empire (tool)
* ifconfig (tool)
* FRP (tool)
* dsquery (tool)
* PcShare (tool)
* netstat (tool)
* PoshC2 (tool)
* Rclone (tool)
* AsyncRAT (tool)
* ROADTools (tool)
* Brute Ratel C4 (tool)
* Peirates (tool)
* Remcos (tool)
* Systeminfo (tool)
* Imminent Monitor (tool)
* Forfiles (tool)
* MCMD (tool)
* Nltest (tool)
* Donut (tool)
* IronNetInjector (tool)
* nbtstat (tool)
* NBTscan (tool)
* Ping (tool)
* cmd (tool)
* route (tool)
* CrackMapExec (tool)
* Koadic (tool)
* Pupy (tool)
* QuasarRAT (tool)
* AdFind (tool)
* Indrik Spider (intrusion-set)
* C0027 (campaign)
* LuminousMoth (intrusion-set)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Velvet Ant (intrusion-set)
* WIRTE (intrusion-set)
* FunnyDream (campaign)
* ArcaneDoor (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Equation (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Aquatic Panda (intrusion-set)
* Daggerfly (intrusion-set)
* TA505 (intrusion-set)
* Inception (intrusion-set)
* admin@338 (intrusion-set)
* BlackTech (intrusion-set)
* APT42 (intrusion-set)
* Malteiro (intrusion-set)
* Earth Lusca (intrusion-set)
* Operation CuckooBees (campaign)
* Juicy Mix (campaign)
* Play (intrusion-set)
* Sandworm Team (intrusion-set)
* Turla (intrusion-set)
* Suckfly (intrusion-set)
* Ember Bear (intrusion-set)
* CostaRicto (campaign)
* TeamTNT (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* Patchwork (intrusion-set)
* APT28 (intrusion-set)
* Aoqin Dragon (intrusion-set)
* HEXANE (intrusion-set)
* Darkhotel (intrusion-set)
* Ke3chang (intrusion-set)
* Volt Typhoon (intrusion-set)
* Leafminer (intrusion-set)
* Magic Hound (intrusion-set)
* APT29 (intrusion-set)
* Operation Honeybee (campaign)
* 2016 Ukraine Electric Power Attack (campaign)
* Cobalt Group (intrusion-set)
* Andariel (intrusion-set)
* HAFNIUM (intrusion-set)
* APT39 (intrusion-set)
* MuddyWater (intrusion-set)
* APT38 (intrusion-set)
* Transparent Tribe (intrusion-set)
* APT32 (intrusion-set)
* BRONZE BUTLER (intrusion-set)
* APT5 (intrusion-set)
* BackdoorDiplomacy (intrusion-set)
* Kimsuky (intrusion-set)
* Storm-1811 (intrusion-set)
* Akira (intrusion-set)
* Mustang Panda (intrusion-set)
* LAPSUS$ (intrusion-set)
* RedDelta Modified PlugX Infection Chain Operations (campaign)
* Chimera (intrusion-set)
* TA2541 (intrusion-set)
* ToddyCat (intrusion-set)
* menuPass (intrusion-set)
* Tropic Trooper (intrusion-set)
* Mustard Tempest (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* C0018 (campaign)
* APT19 (intrusion-set)
* Moses Staff (intrusion-set)
* Operation Dream Job (campaign)
* Molerats (intrusion-set)
* Stealth Falcon (intrusion-set)
* DarkVishnya (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* INC Ransom (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* FIN10 (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* FIN8 (intrusion-set)
* Rocke (intrusion-set)
* Scattered Spider (intrusion-set)
* CURIUM (intrusion-set)
* Windigo (intrusion-set)
* Blue Mockingbird (intrusion-set)
* RedCurl (intrusion-set)
* Frankenstein (campaign)
* Sidewinder (intrusion-set)
* Outer Space (campaign)
* Higaisa (intrusion-set)
* Windshift (intrusion-set)
* Confucius (intrusion-set)
* BlackByte (intrusion-set)
* Threat Group-3390 (intrusion-set)
* Tonto Team (intrusion-set)
* Gamaredon Group (intrusion-set)
* Night Dragon (campaign)
* Agrius (intrusion-set)
* Sea Turtle (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* Moonstone Sleet (intrusion-set)
* ShadowRay (campaign)
* Dark Caracal (intrusion-set)
* APT3 (intrusion-set)
* C0032 (campaign)
* ZIRCONIUM (intrusion-set)
* APT1 (intrusion-set)
* Naikon (intrusion-set)
* Sowbug (intrusion-set)
* Machete (intrusion-set)
* HomeLand Justice (campaign)
* C0017 (campaign)
* FIN5 (intrusion-set)
* Winter Vivern (intrusion-set)
* SideCopy (intrusion-set)
* Operation Sharpshooter (campaign)
* Cutting Edge (campaign)
* Lotus Blossom (intrusion-set)
* Whitefly (intrusion-set)
* APT18 (intrusion-set)
* Carbanak (intrusion-set)
* J-magic Campaign (campaign)
* Triton Safety Instrumented System Attack (campaign)
* Deep Panda (intrusion-set)
* KV Botnet Activity (campaign)
* The White Company (intrusion-set)
* Poseidon Group (intrusion-set)
* Star Blizzard (intrusion-set)
* PROMETHIUM (intrusion-set)
* Ferocious Kitten (intrusion-set)

## Affected Products

* cpe:2.3:a:github:codeql\_action:\*:\*:\*:\*:\*:\*:\*:\*