Google Threat Intelligence

ADVANCED SEARCH MODIFIERS CHEAT SHEET

ABOUT ENTITIES

The 'entity' modifier determines the result type (e.g., file, URL, domain, IP address or collection) for intelligence searches. Each entity type has its own specific set of modifiers you can use to refine your query. Full details on the available modifiers for each entity are documented (files, URLs, domains, IP addresses and collections). Here you can find a few examples:

- `entity:file engines:keylogger size:100kb-`
- `entity:domain category:phishing`
- `entity:url port:8080 header_value:"Apache"`
- `entity:ip asn:15169 communicating_files_max_detections:30+`
- `detected_communicating_files_count: 5+`
- `entity:collection tag:Kimsuky`

SUSPICIOUS DOCUMENTS

Malicious documents (according to Google TI verdict) with specific names:

- `type:document name:" My Company Name" gti_verdict:malicious`

PDF Documents in the Russian language submitted from Ukraine, that exhibited behaviors related to QR codes during automated sandbox analysis:

- `type:pdf lang:ru submitter:UA behaviour_tags:qr_code`

Macro-enabled documents with a Google TI score above 30 and first observed in the past month:

- `(type:doc OR type:docx) tag:macros fs:30d+ gti_score:30+`

Malicious DOC files sent as attachments with filenames including 'Payroll Tax Payment':

- `type:doc tag:attachment name:" Payroll Tax Payment" gti_verdict:malicious`

Excel files that can read system environment variables and make registry changes to hide execution or to persist on a system (Using tags or MBC):

- `type:xls mbc:E1112 tag:environ`

Malicious OneNote files that are using macros to execute PowerShell, probably to manipulate Windows Registry settings via WMI:

- `type:onenote tag:macro-powershell tag:calls-wmi`

Powerpoint files executing other files and containing obfuscated code or content:

- `(type:ppt OR type:pptx) tag:run-file tag:obfuscated`

Documents that make use of an specific CVE exploitation:

- `type:document tag:cve-2023-36884 tag:exploit`

SIGNATURES

Leaked or stolen certificates (i.e: Anydesk), using submission timestamp after the leak date:

- `signature:" 0d bf 15 2d ea f0 b9 81 a8 a9 38 d5 3f 76 9d b8" and fs:2024-01-01+`

Malicious recent signed files with valid signatures:

- `gti_verdict:malicious signature:" © Microsoft Corporation. All rights reserved." tag:signed AND NOT (tag:invalid-signature OR tag:revoked-cert) fs:2025-01-01+`

NETWORK AND INFRASTRUCTURE

URLs with known suspicious paths. Useful when searching additional infrastructure:

- `entity:url path:/c2sock`

URLs with the .xyz top-level domain that contain "admin panel" either in their page title or within their metadata:

- `entity:url tld:xyz (title:" admin panel" OR meta:" admin panel")`

URLs with the .ru top-level domain that could be used to distribute Android APK files:

- `entity:url tld:ru url:android tag:downloads-apk`

Undetected URLs (according to Google TI verdict) using a specific tracker identifier:

- `entity:url gti_verdict:undetected tracker:G-KVN8M54JBZ`

URLs related to a parent domain/subdomain with a specific header in the response:

- `entity:url parent_domain:domain.org header_value:" SimpleHTTPServer"`

IPs belonging to an ASN, that have been identified by GCP abuse or Safe browsing as cryptocurrency mining:

- `entity:ip asn:48287 (gcp_abuse_intelligence:miner OR google_safebrowsing:miner)`

Suspicious IPs within a specified subnet (updated in the last week in Google TI) potentially involved in malicious activity.

- `entity:ip ip:" 172.31.0.0/16" last_modification_date:7d+ (urls_max_detections:5+ OR communicating_files_max_detections:10+ OR downloaded_files_max_detections:10+ OR referring_files_max_detections:10+)`

BEHAVIOR (During sandbox detonation)

Search by any file system operations (open, write, read, remove). Useful in different cases such as dropping malware payloads with specific name and path:

- `behaviour_files:" %TEMP%\\is-OOGKQ.tmp\\tsetup-x64.tmp"`

Files executing PowerShell and creating a process to run 'rundll32.exe'*:

- `behaviour_command_executions:" powershell.exe" AND behaviour_created_processes:" rundll32.exe"`

(*) It's possible to combine various behaviour modifiers to refine your search.

Files contacting a specific endpoint or with a given network-related behaviour. Useful when searching additional samples contacting the same infrastructure:

- `behaviour_network:" https://api.telegram.org/"`
- `behaviour_network:" :3389"`

Files using specific services or daemons:

- `behaviour_services:itsbjssks`

Files using a specific Mitre attack technique or malware behaviour catalog:

- `(attack_technique:T1547.001 AND attack_technique:T1053) OR mbc:OB0012`

Download our latest cheat sheet version here

Google Threat Intelligence

ADVANCED SEARCH MODIFIERS CHEAT SHEET

IN THE WILD MALWARE

Malicious unsigned DMG files downloaded from a given URL or IP:

- **type:dmg gti_verdict:malicious (itw:mediafire.com OR itw:196.251.*.*) AND NOT tag:signed**

Potential exploits related to a specific vuln (or group) with ITW distribution details available:

- **tag:exploit have:in_the_wild tag:cve-2025***

Malware contacting (during sandbox detonation) a given IP address or subnet:

- **contacted_ip:194.36.189.179**
- **contacted_ip:194.36.189.0/15**

Files which seem to communicate with DGA C&C domains, exhibit P2P C&C communication or use already inactive C&C infrastructure:

- **tag:suspicious-dns**
- **tag:suspicious-udp**
- **tag:nxdomain**

Find the full list of tags here.

NON-WINDOW SAMPLES

Linux files that potentially attempt to establish persistence or modify system settings:

- **type:elf behaviour_files:"/etc/profile.d/" behaviour_files:".sh/"**

MAC OS files with activity in the bash_sessions folder:

- **type:macho behaviour_files:"/.bash_sessions/"**

Search for APK files with specific package name and permissions:

- **type:apk androguard_package:com.metasploit.stage AND androguard:android.permission.SEND_SMS**

Search for APK files containing a specific resource file path or using a specific favicon:

- **type:apk "res/wNe.png" OR main_icon_dhash:0d0e334707330e0c**

EMAILS

Emails with a specific mail server detected by at least 5 AVs:

- **type:email content: "@domain." p:5+**

Emails tagged as relating to or utilizing an exploit for the vulnerability CVE-2024-38213

- **type:email tag:exploit tag:cve-2024-38213**

Suspicious emails containing your domain that contain attachments:

- **type:email have:email_attachment content:@yourdomain.com**

GOOGLE THREAT INTELLIGENCE SCORING SYSTEM

Provides a numeric score from 0 to 100, to prioritize potential security threats among entities. For instance:

- **entity:file name:" invoice" gti_score:30+**

The Google Threat Intelligence Score is calculated by combining the verdict and severity, with adjustments based on other factors:

Verdict: Determines the likelihood that the entity is malicious. Possible verdicts include: 'Malicious', 'Suspicious', 'Undetected', or 'Benign'. For example:

- **entity:domain category:"command and control" gti_verdict: suspicious**

Severity: evaluates the potential impact, assigning levels such as 'High', 'Medium', 'Low', or 'None' depending on the threat type. For example:

- **entity:ip asn:27831 gti_severity:high**

For more details and examples check the documentation.

ANTI-PHISHING, ANTI-FRAUD AND BRAND MONITORING

Documents mentioning your brand used as the first stage in the Cyber kill chain:

- **type:document (have:behavior_network OR have:itw) (name:"Your Brand" OR metadata:"Your Brand")**

URLs redirecting to your domain:

- **entity:url redirects_to:"yourdomain.com" AND NOT parent_domain:yourdomain.com**

Similar domains to your domain:

- **entity:domain fuzzy_domain:yourdomain.com AND NOT parent_domain:yourdomain.com**

Domains using a similar favicon* than your domain:

- **entity:domain main_icon_dhash:youricondhash AND NOT parent_domain:yourdomain.com**

(*) To obtain your dhash value, search your domain in Google TI and click on the favicon located on the top right corner.

You can also use broad searches that aren't specific to your company. Here are some examples:

Domains categorized as phishing within certain Top Level Domain (TLD), registrant and SSL certificate issuer:

- **entity:domain category:phishing tld:top registrar:GoDaddy ssl_issuer:"Let's Encrypt"**

Potential Phishing URLs used for Credential Harvesting:

- **entity:url title:"login" AND content:"username" AND content:"password"**

SEARCH MODIFIERS OFFICIAL DOCUMENTATION

Each entity type works in combination with specific modifiers as you can check below:

File modifiers, URL modifiers, IP address modifiers, Domain modifiers and Collection modifiers

Download our latest cheat sheet version here

Google Threat Intelligence

ADVANCED SEARCH MODIFIERS CHEAT SHEET

APT DETECTION & TRACKING

Track files related to UNC5448 that show evidence of suspicious PowerShell commands that have been encoded using a Sigma rule (Find the full list here):

- `sigma_rule:12273189dbbd1ed526c045fb9a7d5e45682ba4e0a13e2e94d65376962a0bfc2e AND threat_actor:UNC5448`

Identify potential domains linked to Lazarus through comments:

- `entity:domain comment:"Lazarus" OR comment:"Hidden Cobra" OR comment:"APT38"`

Track new malware samples based on the malware config extraction:

- `(engines:vidar OR malware_config:vidar) fs:2d+`

Identify malicious files based on the unique characteristics of their TLS client communications (JA4 fingerprint):

- `behaviour_network:t10d070600_c50f5591e341_1a3805c3aa63`

Detect potential LNK files used by APT44 using a specific crowdsourced yara:

- `crowdsourced_yara_rule:00032bfe82|SUSP_LNK_Suspicious Commands`

COLLECTIONS

Google TI allows you to perform advanced searches over the different sets of collections (Threat Actor, Malware Family, Software Toolkit, Campaign and IOC collection).

Search for threat actors who target European companies and use HAVOCDEMON malware:

- `entity:collection collection_type:threat-actor targeted_region:europe malware_family:HAVOCDEMON`

Find malware families that delete Windows Volume Shadow Copies:

- `entity:collection collection_type:malware-family capability:"Deletes Volume Shadow Copy files" operating_system:"Windows"`

Search for espionage campaigns against energy companies:

- `entity:collection collection_type:campaign motivation:espionage targeted_industry:oil&gas`

Find campaigns associated to 'AZCOPY' tool usage:

- `entity:collection collection_type:campaign software_toolkit:AZCOPY`

Find IOC collections containing "akira" in the name or description, created in the last 30 days:

- `entity:collection collection_type:collection (name:"akira" OR description:"akira") creation_date:30d+`

CODE INSIGHT

Detect .bat files identified as keyloggers by CodeInsights:

- `type:bat and codeinsight:keylogger`

Search for undetected Powershell files that attempt to disable antivirus:

- `type:powershell codeinsight:"disable antivirus" gti_verdict:undetected`

CONTENT FILTERING

Files containing hardcoded content (string/hex values) related to Lumma:

- `content:{c70000000000 85c9 7406 c70100000000 c7466cfeffffff}`
- `content:"rundll32.exe shell32.dll,Control_RunDLL MMSys.cpl"`

Suspicious combinations of hardcoded strings in the sample (EDR killer):

- `type:peexe content:"QualysAgent.exe" AND content:"SentinelAgent.exe" AND content:"CylanceSvc.exe"`

SIMILARITIES

Finding other Beacon malware files through the imphash value:

- `imphash:c782987849999c5ae345a5deafbd73fb`

Using ssdeep to find similar documents:

- `ssdeep:12288:US5dQhIQSCoEAt8CSROwGeqUcmFGhPKD6tD:US5uhIQhA091cm0dD`

Pivoting to other similar files, structurally similar to the one provided using similar-to and SHA256 file value:

- `similar-to:7a86c0f44dd01271fef8a38c8859a7ee0e907fe8899aa79cc3f1e42522a2e85b`

Pivoting to other similar files, based on the exhibit behaviour:

- `behash:6517a3151ed7acebdc9d3b66ec7647d2`

VULNERABILITIES

Identify vulnerabilities with a 'High' risk rating and 'confirmed' exploitation state, created in the last 30 days:

- `entity:collection collection_type:vulnerability risk_rating:high exploitation_state:confirmed creation_date:30d+`

Find zero-day vulnerabilities observed in the wild:

- `entity:collection collection_type:vulnerability vulnerability_filter:"Observed In The Wild" vulnerability_filter:"Zero Day"`

Find vulnerabilities related to Kubernetes Ingress NGINX Controller with a CVSS 3.1 base score above 9.0:

- `entity:collection collection_type:vulnerability vulnerable_product:Ingress-nginx vulnerable_vendor:Kubernetes cvss_3x_base_score:9.0+`

Download our latest cheat sheet version here