VirusTotal Hunting Cheat Sheet

WebGUI field guide | Intelligence search + report pivots + Graph | 2026-07

GRAMMAR **AND** is implicit; use **OR**, **NOT**, **(...)**, and quotes. **5+** larger/after; **5-** smaller/before; exact has no suffix. **entity:url|domain|ip** selects non-file corpora. Raw MD5/SHA1/SHA256 lookup stands alone. Wildcards are field-specific; the filter assistant cannot build complex Boolean expressions.

FILE - CORE FILTERS

type: Magic/type tag. Common: peexe, pedll, elf, macho, apk, pdf, doc/docx, xls/xlsx, ppt/pptx, rtf, js, ps1, lnk, zip, rar, iso, email, pcap.
size: Bytes by default; KB/MB allowed. Example: size:120KB+ size:2MB-.
p: / positives: AV detection count. Range: p:1+ p:6- means 1-5.
cp: Maximum detections among child files (archives/bundles).
fs: / ls: / la: First submitted / last submitted / last analyzed. ISO datetime or relative, e.g. fs:7d+.
s: / submissions: Times submitted; sources: counts distinct submission sources.
name: / filename: Submitted filename contains literal; quotes preserve phrases.
tag: VT tags: signed, trusted, nsrl, corrupt, 64bits, assembly, exploit, email-spam, powershell, obfuscated, upx...
submitter: Country code or interface (web/api); first_submitter: for first source country.
itw: In-the-wild download URL contains literal.
have: Require indexed data/relationship, e.g. have:behaviour have:embedded_urls.

FILE - STATIC, CONTENT & CONTEXT

metadata: Exif/tool metadata; sigcheck: or signature: searches code-signing fields.
creation_date: Compile/build timestamp (also gen:, pets:, petimestamp:); subspan: compares submit vs compile time.
imports: / exports: Imported library or exported symbol. section: / sectionmd5: / segment: for structure.
peresource: SHA-256 of contained PE resource; detectiteasy:, trid:, magika: identify tool/type.
content: VTGrep literal or bytes: content:"Hello" or content:{CAFEBABE}. Results cannot be sorted.
malware_config: Extracted config value. androguard_package: targets Android package name.
engines: Family/label from any engine; vendor field targets one engine, e.g. microsoft:trojan.
min_engines_[label]: Minimum engines returning normalized label, e.g. min_engines_emotet:5.
comment: Community comment text; comment_author: filters commenter.
threat_actor: Related actor (related_actor: alias). codeinsight:, crowdsourced_ai_analysis:, and crowdsourced_ai_verdict: search AI fields.

FILE - BEHAVIOR & DETECTION

behaviour: Any dynamic report literal (behavior: US alias).
behaviour_files: Filesystem; _processes:, _created_processes:, _injected_processes: process activity.
behaviour_registry: Registry; _services: services/daemons; _network: network observations; _tags: sandbox tags.
behaviour_signature: Sandbox signature name/description; sandbox_name: limits provider.
attack_technique: MITRE ATT&CK ID (T1055); attack_tactic: tactic ID (TA0003); mbc: MBC ID.
capability_tag: Capability label; sigma_rule: rule hash; sigma_critical/high/medium/low: match count.
traffic: Domain/URL/IP observed inside a PCAP; contacted_ip: supports CIDR.

FILE - SIMILARITY KEYS

similar-to:[HASH] structural similarity. Exact-feature pivots: **imphash:** imports; **vhash:** VT structure; **ssdeep:** fuzzy bytes; **tlsh:** locality; **telfhash:** symbols; **authentihash:** signed PE content; **permhash:** APK/CRX permissions; **behash:** behavior; **main_icon_dhash:** visual icon; **main_icon_md5:** exact icon.

URL CORPUS - PREFIX WITH ENTITY:URL

url: / hostname: URL text or host; path: subword, exact_path: exact path, extension: parsed file extension.
query_field/value: Query key/value. username: URI user; scheme: protocol; port: server port.
title: / meta: HTML title / META text; password: password-field text; tracker: shared ad/analytics ID.
header/value: HTTP response header key/value; cookie/value: response cookie name/value.
response_code: HTTP status; response_size: bytes; response_positives: detections for delivered content.
redirects_to: Destination URL; outgoing_link: links in response. parent_domain: registrable parent.
ip: / asn: / aso: Serving IP/CIDR, AS number, AS owner. tld: top-level domain.
main_icon_dhash: Visually similar favicon. Best phishing pivot; exclude legitimate hosts with NOT.
tag: Useful: downloads-pe/apk/elf/dmg/zip/pdf/doc, opendir, contains-pe/zip/msi/apk/dmg, ip, non-ascii.
p: / engines: Detections / any label; [engine]:[label] for one scanner; max_url_positives: historical peak.
fs/ls/la/lm: First/last seen, last analyzed, last modified. Also s:, submitter:, first_submitter:.
category/reputation: Domain content category / community score. have:, comment:, threat_actor: also apply.

DOMAIN CORPUS - PREFIX WITH ENTITY:DOMAIN

domain: Contains/full-text with wildcard; domain_regex: regex; fuzzy_domain: typo-similarity pivot.
parent_domain: Registrable parent; tld: suffix; depth: label count.
a/aaaa: IPv4/IPv6 record (prefer Relations for one IP; use this for ranges).
cname/dname/mx/ns/soa/txt: DNS record content. Add _record form if desired.
ttl / [record]_ttl: Any/specific record TTL; tight low-TTL ranges can expose fast flux.
creation_date: WHOIS creation; last_update_date: registration update; lm: VT object update.
registrar: / whois: Registrar only / any redacted WHOIS text.
ssl_issuer/subject: Certificate text; ssl_serial/thumbprint: exact certificate keys; ssl_not_before/after: dates.
jarm: TLS server fingerprint; main_icon_dhash: favicon similarity.
category/popularity_rank: Content class / aggregated popularity rank (1 is most popular).
p/engines/reputation/tag: Detections, engine labels, votes, and tags (dga, dynamic-dns, nxdomain, hex, non-ascii...).
have/comment/actor: have:[field], comment:, comment_author:, threat_actor:/related_actor:.

IP CORPUS - PREFIX WITH ENTITY:IP

ip: IP/CIDR range; asn: number; aso: owner; country:/continent: ISO code.
p/engines/reputation/tag: Detections, labels, vote score; tag: reserved/private/loopback/link-local/multicast.
domain_resolutions_count: Number of hosted domains (saturates at documented cap).
ssl_* / jarm: Issuer, subject, serial, thumbprint, validity dates, or JARM TLS fingerprint.
whois/lm/have: Registration text, last VT update, required field. comment: and threat_actor: also apply.

DOMAIN/IP RELATIONSHIP COUNTERS

Use on **entity:domain** or **entity:ip**: **detected_communicating_files_count:** + **communicating_files_max_detections:**; **detected_downloaded_files_count:** + **downloaded_files_max_detections:**; **detected_referring_files_count:** + **referring_files_max_detections:**; **detected_urls_count:** + **urls_max_detections:**.

REPORT / RELATIONS PIVOT MAP

FILE -> INFRASTRUCTURE
contacted domains / IPs / URLs (runtime) -> inspect detections, first/last seen, resolutions, then communicating files. **embedded domains / IPs / URLs** (static) -> validate whether reached. **ITW domains / IPs / URLs** -> delivery origin.
FILE -> FILE
dropped / bundled files; compressed/ciphered/email/execution parents; overlay, PCAP, and PE-resource children/parents; similar files; screenshots; sandbox behaviours. Parent links often reveal the delivery chain; child links reveal payloads.
DOMAIN / IP -> INFRASTRUCTURE
Resolutions (historical passive DNS) domain <-> IP; domain parent/subdomains/siblings and URLs; IP URLs. Pivot on shared **SSL certificate, JARM, WHOIS, NS/MX/CNAME**, favicon, AS owner, and time window.
DOMAIN / IP / URL -> FILES
communicating = sandbox contacted; **downloaded** = hosted/delivered; **referrer** = value embedded/referenced. URL additionally exposes redirects, redirecting/referrer URLs, last serving IP, contacted infra, embedded JS, and URLs related by tracker ID.
GRAPH ACTIONS
Open in Graph -> expand selected relationships -> multi-select -> **Commonalities** -> launch VT search/add results -> calculate commonalities again. Use full expansion sparingly; pin time-bounded, independently corroborated nodes. Save useful clusters to a Graph or Collection.

HIGH-SIGNAL PIVOT ORDER

1. **Exact:** SHA-256/SHA-1/MD5, URL, domain, IP.
2. **Stable:** signer/authentihash, imphash, resources, package ID, JARM/cert, tracker, favicon.
3. **Structural:** vhash, similar-to, TLSH/ssdeep, sections/imports/exports, metadata.
4. **Behavioral:** contacted infra, process/registry/files, behash, ATT&CK/MBC, Sigma.
5. **Context:** parents/children, pDNS, first/last seen, WHOIS, submissions, actor/reference.

Promotion rule: widen only after 2+ independent features agree; re-check dates and exclusions at every hop.

READY-TO-PASTE HUNTS

```
type:peexe fs:3d+ p:1+ p:6- NOT tag:trusted
(imphash:[IMPHASH] OR vhash:[VHASH]) fs:30d+ NOT tag:trusted
attack_technique:T1055 behaviour_network:"*[DOMAIN]*" fs:30d+
type:peexe content:"powershell -enc" NOT tag:nsrl
entity:url title:"Microsoft 365" p:1+ NOT hostname:microsoft.com
entity:url main_icon_dhash:[DHASH] NOT hostname:[LEGIT_DOMAIN]
entity:domain tag:dynamic-dns creation_date:14d+ p:1+
entity:domain a_record_ttl:1+ a_record_ttl:301- p:1+
entity:ip jarm:[JARM] p:1+ NOT asn:[KNOWN_GOOD_ASN]
```

WEBGUI OPERATING LOOP

Seed report -> review Details / Relations / Behavior -> click/copy a feature -> search with a tight time window -> sort/inspect outliers -> exclude known good -> pivot once -> compare commonalities -> save search/Graph/Collection -> operationalize strong patterns with YARA Livehunt (future submissions/reanalysis) or Retrohunt (historical corpus).
Safety: do not upload confidential samples to the public service. Plan entitlements, visibility, downloads, Hunting, and some relations vary.