VIRUSTOTAL

VT INTELLIGENCE CHEAT SHEET

ABOUT ENTITIES

This modifier simply determines the output (ip, domain, url, file or collection) for a VTIntelligence search. Please note that depending on the entity we select, there are some specific modifiers we can or we cannot use (here you have full details for files, URLs, domains and IPs). Here you can find a few examples:

- **entity:ip asn:15169 communicating_files_max_detections:30+ detected_communicating_files_count: 5+**
- **entity:domain downloaded_files_max_detections:20+**
- **entity:url p:3+ have:tracker**
- **entity:file tag:signed p:10+**
- **entity:collection (name:apt OR tag:apt)**

SUSPICIOUS DOCUMENTS

Recently created documents with macros embedded, detected at least by 5 AVs:
- **(type:doc OR type: docx) tag:macros p:5+ generated:30d+**

Excel files bundled with powershell scripts and uploaded to VT for the last 10 days:
- **(type:xls OR type:xlsx) tag:powershell fs:10d+**

Documents with obfuscated VBA code executing other files.
- **(type:doc OR type: docx) tag:exe-pattern tag:run-file tag:obfuscated**

Suspicious documents (according to AV verdicts) with specific names:
- **type:document name:"My Company Name" p:5+**

Or documents used as email attachments:
- **type:document name:"My Company Name" tag:attachment**

Follina-like exploit payloads:
- **entity:file magic:"HTML document text" tag:powershell have:itw_url**

Or any observable exploiting any vulnerability published since 2022:
- **tag:cve-2022-***

NETWORK AND INFRASTRUCTURE

Search for URLs with known suspicious endpoints. Useful when searching additional infrastructure:
- **entity:url path:logpost.php**

URLs within certain Top Level Domain (tld) and specific meta content in the HTML response:
- **entity:url tld:xyz meta:"admin panel"**

URLs with specific cookie names (“cookie” modifier) or specific cookie values (“cookie_value” modifier):
- **entity:url cookie:njnmsdkfsdfbiuonsdkfnsdfl**
- **entity:url cookie_value:1433a6c2ee8a92a887d7bfcc90b0c171**

URLs related to specified parent domain/subdomain with a specific header in the response:
- **entity:url header_value:"Apache/2.4.41 (Ubuntu)" parent_domain:domain.org**

Suspicious (recently updated on VirusTotal) IPs within a specified ASN/subnet:
- **entity:ip asn:15169 (urls_max_detections:5+ OR reputation:-20- OR p:5+ OR communicating_files_max_detections:10+ OR downloaded_files_max_detections:10+ OR referring_files_max_detections:10+) last_modification_date:3d+**
- **entity:ip ip:"172.31.0.0/16" (urls_max_detections:5+ OR reputation:-20- OR p:5+ OR downloaded_files_max_detections:5+ OR referring_files_max_detections:10+ OR (detected_communicating_files_count:2+ AND communicating_files_max_detections:5+)) last_modification_date:7d+**

BEHAVIOR (DURING SANDBOX DETONATION)

Find samples with a given network-related sandbox output (ip, domain, USER_AGENT and any other PCAP content):
- **behavior_network:bumblebee (type:peexe OR type:pedll)**

Samples contacting a specific endpoint. This helps discovering additional samples deploying the same backend in different infrastructure:
- **behaviour_network:"/vpnchecker.php"**

Search by any file system operations (open, write, read, remove). Useful in different cases such as dropping malware payloads with specific names:
- **behaviour_files:"<SYSTEM32>\\windowspowershell\\v1.0\\powershell.exe" AND behaviour_files:"%TEMP%\\4.ps1"**
- **behaviour_files:"/80C.dat" AND behaviour_files:"/7FC.dat"**

Samples attempting execution of Powershell with Execution Policy bypass:
- **behaviour_processes:"powershell.exe -ep bypass -File"**

Samples abusing VSSAdmin tool to remove shadow volume copies (can be used to detect all sorts of ransomware/cryptolocker malware):
- **behaviour_processes:"\\vssadmin.exe delete shadows /all /quiet"**

NON-WINDOWS SAMPLES

Signed iOS app packages detected by at least 5 AVs:
- **tag:iphone tag:signed p:5+**

Use any entity (like hardcoded URL, resource string or any other statically determined object) to match with Androguard output. For instance, part of SpyMaster’s stalkerware URL:
- **androguard:"spyMobile/"**

APKs that mimic a legitimate app by using the same icon*, but having a different signature:
- **main_icon_dhash:c0c0c0c0fcc8e4e4 type:apk AND NOT androguard:"O:BBVA" AND NOT androguard:"OU:BBVA"**

**Note: main_icon_dhash is the hash used for visual similarity. To find the hash you are looking for, the best way is finding the legit resource (file or domain) in VirusTotal and clicking on visual similarity.*

APK files with specific package name (note: its new, so it works only for newly indexed files since March 2022):
- **androguard_package:org.xmlpush.v3**

Searching for the APKs contained a certain files in assets directory:
- **("assets/s.bin" AND "assets/l.bin") OR ("assets/s.bin" AND "assets/m.bin") OR ("assets/m.bin" AND "assets/c.bin")**

IN THE WILD MALWARE

Suspicious malware (according to AV verdicts) downloaded from a given URL:
- **itw:cdn.domain.com p:5+**

Any iOS/macOS malware with ITW distribution details available:
- **(type:apple OR type:mac) have:in_the_wild p:5+**

iOS/macOS files served from a given URL:
- **(type:apple OR type:mac) itw:cdn.domain.com**

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 seems to communicate with DGA C&C domains, exhibit P2P C&C communication or uses already inactive C&C infrastructure
- **entity:file tag:suspicious-dns**
- **entity:file tag:suspicious-udp**
- **entity:file tag:nxdomain**

Download here: virustotal.com/go/vti-cheatsheet

virustotal.com

V.1.1

VIRUSTOTAL

VT INTELLIGENCE CHEAT SHEET

SIGNATURES

Searching for leaked or stolen certificates, using submission timestamp after the leak date. This example uses Nvidia leaked certificates:
- fs:"2022-03-01T00:00:00+" (signature:"43 bb 43 7d 60 98 66 28 6d d8 39 e1 d0 03 09 f5" OR signature:"14 78 1b c8 62 e8 dc 50 3a 55 93 46 f5 dc c5 18")

Suspicious (according to AV verdicts) recent signed files with valid signatures:
- signature:"© Microsoft Corporation. All rights reserved." tag:signed p:5+ not (tag:invalid-signature or tag:revoked-cert) fs:2022-01-01+

COLLECTIONS

Searching for collections containing specific names or tags:
- entity:collection (name:Sofacy OR tag:Sofacy OR name:apt28 OR tag:apt28)

Extracting specific type of IOCs (file, ip, domain, url) from a certain collection*:
- collection:alienvault_60eff240c7c9cb4f24907049 entity:file type:pedll p:10+

**Note: To obtain the ID for a given collection, you can find it in the browser's URL when visiting it.*

ANTI-PHISHING, ANTI-FRAUD AND BRAND MONITORING

Searching for URLs using the same title and favicon as a given company detected by at least 5 AVs:
- entity:url main_icon_dhash:0e969e969306710f title:"Company" NOT parent_domain:" CompanyDomain." p:5+

Detect domains similar to a legitimate one:
- entity:domain fuzzy_domain:"domain.com"
- entity:domain fuzzy_domain:"domain.com" urls_max_detections:1+ AND (NOT parent_domain:domain.com)

URL with suspicious phishing content:
- entity:url content:"Enter password" content:"Microsoft" fs:1d+

Suspicious URLs with a specific HTML title:
- entity:url (title:"XY Company" or title:"X.Y. Company" or title:"XYCompany") p:5+

If we don't want to rely on AVs detection, we can replace "p:" with specific suspicious content:
- entity:url (title:"XY Company" or title:"X.Y. Company" or title:"XYCompany") content:"email"

EMAILS

Emails with a specific mail server detected at least by 5 AVs:
- type:email content: "@domain." p:5+

Suspicious emails with attachments:
- type:email have:email_attachment p:5+

Suspicious email attachments allegedly using an exploit:
- tag:attachment tag:exploit

APT DETECTION

Using AV verdicts (all of them, or certain vendors only):
- engines:wellmess
- kaspersky:wellmess OR eset:wellmess

Looking for domains related to a specified APT based on users' comments:
- entity:domain (comment:APT29 OR comment:CozyBear OR comment:NobleBaron OR comment:UNC2452 OR comment:YTTRIUM)

Getting all recent files detected by crowdsourced rules (Yara, IDS, Sigma) related to a specific actor:
- crowdsourced_yara_rule:APT29 OR crowdsourced_ids:APT29 OR sigma_rule: 976e44f1eafa22eaa455580b185aaa44b66676f51fe2219d84736dc8b997d3e OR crowdsourced_yara_rule:CozyBear OR crowdsourced_ids:CozyBear OR sigma_rule: 34f4cff056f24abe91bb29dc04a37ee746a4255101a21724b9ff28d79785247a

**Note: You can find IDs for sigma_rule by clicking on "Other files" when exploring a particular rule, or you can check all crowdsourced rules here.*

List all recent collections related to an specific actor:
- entity:collection (name:APT29 OR tag:APT29 OR name:CozyBear OR tag:CozyBear) creation_date:2021-01-01+

CONTENT FILTERING (VT GREP)*

**Note: A regular search in VTIntelligence will check all content provided in the sample report. VTGrep focuses on the content of the samples, including the option of binary searches.*

Samples containing hardcoded malicious address (string and hex search are allowed):
- content:"maliciousdomain.com"
- content:{6d 61 6c 69 63 69 6f 75 73 64 6f 6d 61 69 6e 2e 63 6f 6d}

Searching for Android FinSpy malware using wildcards in the content we are looking for ("assets/Configurations/*[1-15]183.dat"):
- content:{6173736574732f436f6e666967757261746f6e732f [1-15] 3138332e646174}

Suspicious combinations of hardcoded strings in the sample (AV product evasion most likely):
- content:"nod32.exe" AND content:"avp.exe" AND content:"qserver.exe"

Documents containing suspicious information, usually used for phishing:
- content:xxx.com type:document
- content:"bitcoin" content:"elon musk" type:document

Download here: virustotal.com/go/vti-cheatsheet

virustotal.com

V.1.1

VIRUSTOTAL

VT INTELLIGENCE CHEAT SHEET

File search modifiers

AV PRODUCTS

- **positives:/p:** number of AV detections (**positives:20+ positives:31**)
- **children_positives:/cp:** - number of detections of children files for a given sample, i.e. bundles, ROMs, etc
- **engines:** - any AV verdict name (**engines:"Android.Zbot.1"**)

FILE METADATA

- **size:** - (**size:500+, size:120KB+, size:15MB-**)
- **type:** - full list here1 (**type:pdf**)
- **name:** - (**name:"winshell.ocx"**)
- **content:** string/binary (**content:"Hello World!", content:{CAFEBABE}**)
- **creation_date:** - (**creation_date:2018-08-21T18:18:38**)
- **lang:** - for PE and office files mainly (**lang:farsi, lang:"portuguese brazilian", lang:"es-ar"**)
- **metadata:** - any other1 indexed metadata (**metadata:"Ubuntu Developers"**)

SUBMISSION

- **fs:** - first submission (**fs:2012-08-2116:00:00+ fs:2012-08-2116:59:22-, fs:3d+**)
- **ls:** - last submission
- **la:** - last analysis
- **submissions:/s:** - number of times file was submitted (**submissions:10+ submissions:20-**)
- **sources:** - number of distinct sources
- **submitter:** - country code and web/api (**submitter:web submitter:BR**)

VT ANALYSIS

- **tag:** - tags assigned by VT [1]
- **similar-to:** - structure similarity (**similar-to:19b86fe81df05de2b4207e8eb0c3aa40**)
- **ssdeep:** - ssdeep hash sim (**ssdeep:"24576:KrKqlGCPcJKwybUDwEZZODYmR9G..."**)
- **imphash:** - import hash sim [2] (**imphash:7fa974366048f9c551ef45714595665e**)
- **have:** - report contain selected fields (**have:embedded_urls have:behaviour**)
- **clue_rule:** - VT Clue rule hash (**clue_rule:1bd7d049d5d2d9b6a9ba92814d5e59f6e...**)
- **comment:** - strings from comment section (**comment:"#math_entropy_close_8"**)
- **comment_author:** - (**comment_author:javilinux**)

EXECUTABLES

- **sigcheck:/signature:** - sigcheck output (**sigcheck:"Google Update Setup"**)
- **section:/sectionmd5:** - name/md5 of the section (**section:".xxx", /sectionmd5:d41...**)
- **imports:** - (**imports:"crypt32.dll"**)
- **exports:** - name of exported function (**exports:"_FormMain"**)
- **exports:** - [PE] dif in sec between first submission time and compilation (**exports:100-**)
- **resource:** - [PE] resource type/file type/sha256 (**resource:"RTF_FILE"**)
- **segment:** - [MACHO] segment with the name provided (**segment:"__LINKEDIT"**)
- **androguard:** - [Android] any indexed Androguard output (**androguard:" Time Out Bistro"**)

SANDBOX

- **behavior:/behaviour:** [3] - any entity from SB reports (**behavior:"explorer.exe"**)
- **behavior_files:** - file system changes (**behavior_files:Crack**)
- **behavior_processes:** - executed process (**behavior_processes:"calc.exe")**
- **behavior_registry:** - Windows registry modifications (**behavior_registry: dc971ee5-44eb**)
- **behavior_services:** - services and daemons (**behavior_services:TheServiceName**)
- **behavior_tags:** - tags generated by sandboxes [4] (**behavior_tags:mysql_ communication**)
- **sandbox_name:** - only specific [5] SB report (**sandbox_name:VirusTotal**)

TTPs

- **attack_technique:** - samples matching techniques based on MITRE ATT&CK when detonated in sandbox (**attack_technique:T1055**)
- **attack_tactic:** - samples matching tactics based on MITRE ATT&CK when detonated in sandbox (**attack_tactic:TA0003**)

SIGNATURES

- **crowdsourced_yara_rule:** -rule/ruleset(**crowdsourced_yara_rule:Follina**)
- **crowdsourced_ids:** - IDS rule/ruleset
- **sigma_[critical|high|medium|low]:** - number of matched rules (**sigma_high:1+**)

WEB

- **itw:** - files that have been downloaded by given URL/part of it (**itw:"&abc=", itw:"ya.ru"**)
- **traffic:** - any URL/domain/IP (**traffic:"google.com"**)

1. https://support.virustotal.com/hc/en-us/articles/360001385897
2. https://www.mandiant.com/blog/tracking-malware-import-hashing/
3. “behaviour” = “behavior” here and below
4. https://support.virustotal.com/hc/en-us/articles/360017236198
5. https://support.virustotal.com/hc/en-us/articles/360001385897-File-search-modifiers

Download here: virustotal.com/go/vti-cheatsheet

virustotal.com

V.1.1