

VirusTotal Domain Intelligence Feed

Elevate your network defense solutions and/or data lake with timely, rich and actionable intelligence on domains

VirusTotal feeds allow organizations to ingest unrivaled crowdsourced intelligence locally. The domain intelligence feed provides reputation and context related to any domain that VirusTotal analyzes, live, as the scans conclude. This real-time stream includes botnet C&Cs, ransomware & exploit kit infrastructure, domains delivering malware, phishing domains, etc. Add a second opinion to your multi-layered defense-in-depth strategy and find threats before they find you.

Breach prevention & improved detection

Use data analytics to automatically digest the feed into hunting and preventative IoCs. Feed these into your existing tech stack (IDS, firewalls, secure web proxy, etc.) and take your security investments to the next level by proactively blocking threats before they hit you.

Attacker dwell time reduction

Perform automated, continuous, retroactive enrichment of domains logged in your SIEM, flag suspicious historical patterns as soon as new findings are uncovered by the community. Uncover silent breaches earlier and radically reduce recovery costs.

Regulatory & secops policy compliance

Leverage VirusTotal's unmatched threat landscape visibility in your own investigative warehouse, ensuring compliance with legal regulations or security operations best practices for sensitive investigations.

Fraud risk reduction & brand protection

Take down/neutralize phishing threats and other types of scams before they cause harm to your users or employees. Mitigate reputational damage.

In a nutshell >>>

Pubsub-like live stream of all analysis reports & metadata generated by VirusTotal for domains.



Massive >> 10M - 20M domain analyses per day, 340K+ detected by 1+ vendors



Diverse >> Contributions by 3M+ monthly users from 232 countries



Rich >> Industry threat reputation, server-side response, web components, DNS info, submission and in-the-wild metadata, etc.



Real-time >> Ingest new threat details on-the-fly as the community discovers and submits them to VirusTotal









Actionable >> Machine readable JSON and threat graph interlinking

[Read API docs](#)

Any threat

Unlike other feeds, VirusTotal's domain intelligence stream is not fragmented by kind.

License a single feed and receive timely updates on any kind of nefarious activity leveraging domains. **Consolidate & lower costs.**

 <p>Botnet Command & Control</p>	 <p>Malware distribution domains</p>	 <p>Dropzones and exfiltration domains</p>
 <p>Exploit kits</p>	 <p>Phishing & Scams</p>	 <p>Spam</p>



Industry threat reputation
85+ blocklists, AVs, network solutions, community votes...



Threat/Content category
E.g. Phishing, Search engine portal, Newspaper, etc.



Popularity rank
Domains prevalence among Internet users



Whois lookup
Registrar, Registrant and other domain setup information



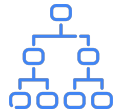
SSL Certificate
Subject, Issuer, Serial No, Thumbprint, Alternative Names



Last DNS records
A, AAA, MX, NS, SOA, TXT, etc. TTL values to spot fast flux



Historical passive DNS
Last 20 resolutions for each domain published



Subdomains & Siblings
mal.evl.com is a sub of evl.com and a sibling of bad.evl.com



Related IoCs
Files communicating, files downloaded, URLs, etc.

Every detail

Unparalleled visibility into threats. **No more missed threats due to lack of context.**

VirusTotal's multi-angular analysis provides superior context to power faster, more accurate and more confident security operations.

Anywhere

Boost the ROI of your security investments, radically accelerate incident response through automation and **hunt for unknown threats flying under the industry's radar.**



Data lake



TIP



Email GW



SIEM / XDR



Firewall / IDS / NDR / Proxy



SOAR

On-premise

In-the-cloud

In your hosting

In your corporate network

Anywhere, everywhere

Diverse and differentiated threat sources

Random users world-wide

3M+ users/month, 230+ countries

Academic researchers

Running honeypots, crawlers, etc.

Security professionals

1M+ registered users dissecting malware

Corporate security workflows

SOAR playbooks, alert triage, etc.

Participating security vendors

Domain/URL blocklists, fresh malware, etc.

Data exchange partnerships

E.g. DNS service providing 30B+ pDNS/day

VirusTotal browser extensions

ITW files, URLs, browser DNS resolutions

VirusTotal feedback loops

E.g. Scan URLs seen in file detonations

Newly registered domain feeds

Main TLDs daily, before attack launch

Google crawler cookbooks

EXE downloads, open directories, etc.

Real-time sightings

Example: Thousands of companies world-wide connect their SOAR platforms to VirusTotal for phishing triage. This acts as a massive distributed set of sensors allowing us to see real-time new attacker campaigns as they traverse email gateways.



2M+ files/day
4M+ URLs/day
18M+ domains+IPs/day
30B+ pDNS records/day
3M+ monthly users
230+ countries

Known good & known bad

Network location analysis engine

Consistently scanning 10M - 20M domains / day

Not only parent domains, subdomains and unindexed infrastructure

340K+ domains / day detected by 1+ vendors

150K+ detected by 5 security vendors or more

150K+ domains / day downloading detected files

Trojans, ransomware, mobile malware, IoT threats, etc.

Use cases



Local dataset replica

Merge with other feeds. Create a private investigative instance. Address secops/regulatory needs.



Discovery of unknown threats

Threat commonality identification. Advanced hunting rules (YARA on domain metadata).



Continuous enrichment

Live matching of locs. Automatic historical log searches to perform retroactive hunting.



IoC and IDS rule generation

Remediation. Hunting. Prevention by flagging pre-operational malicious infrastructure.



Machine learning

Threat categorization. Campaign / toolkit clustering. Flag repetitive contextual patterns.



Anti-fraud & Brand monitoring

Phishing takedowns. Brand impersonation. Corporate infrastructure abuse.



What Makes Us Different?

Many domain intelligence vendors just identify anomalous patterns in newly registered domain feeds. Malicious infrastructure often leverages subdomains, these rarely get indexed in the open web. **Only crowdsourcing gives you superior visibility into unindexed nefarious Internet infrastructure.**

Moreover, VirusTotal detonates received files in **15+ home-grown and 3rd-party sandboxes, recording any network communications generated by malware.** This results in an unrivaled stream of command-and-control servers, second stage delivery vectors, dropzones, data exfiltration points, etc. None of these would ever be spotted through crawling or through new domain registration monitoring.

Most importantly, domains get analyzed by **90+ blocklists/vendors** and reports incorporate high signal information such as whois lookups, DNS resolutions, related IoCs, etc.



Global and open user community

Guarantees diversity, timeliness and visibility into cloaked resources or those requiring human intervention to be triggered.



Security industry crowdsourcing

Strategic partnerships contributing unprecedented volumes to VirusTotal's threat corpus, e.g. 30B+ passive DNS records per day.



Multi-kind analysis

VirusTotal scans and interlinks files, domains, IPs and URLs. We go above and beyond simple typosquatted or look-alike domains.



Planet-scale sandboxing

15+ dynamic analysis systems detonating 1M+ files per day and recording network traffic. Unrivaled source of malware comms and high-signal pDNS.



High signal & relevant

We do not rely solely on random crawling and underground monitoring, but rather on a community of users vetting and dissecting suspicious content.



Superior context & analysis

Graph interlinking with other IoCs in the VirusTotal threat corpus to understand badness. Files downloaded from a given domain, related malware families, etc.



Google internet visibility

Google crawler cookbooks surfacing suspicious / anomalous domains. Best-in-class coverage of the indexed and unindexed web.



Disruptive economics

Predictable flat cost. Single feed including all domain threat categories - no need to license a phishing feed, CnC feed, malware feed, etc.