

VirusTotal Alerts

Lower risk through automatic identification of violations at and beyond your network perimeter

The average cost of a data breach was \$3.86M as of 2020, with an average of 280 days to identify and contain. Companies that contained a breach in less than 30 days saved more than \$1M. Through community backing and security industry crowdsourcing, VirusTotal has become the world's largest threat observatory. VT Alerts applies Google planet-scale capabilities to VirusTotal's unrivaled and differentiated threat stream so as to radically reduce dwell time post-compromise and prevent fraud & account takeovers.



Protect your brand and mitigate reputational damage.

Automatically identify brand impersonation attempts, phishing & counterfeiting. Radically increase your visibility into external threats beyond your network perimeter.



Monitor internet-exposed attack surface, identify hijacks.

Reduce cyber dwell time through early identification of corporate infrastructure abuse & compromise, prevent lateral movement and reduce your remediation costs.



Neutralize threats against your customers & employees.

Take down phishing campaigns targeting your users, customers or employees. Prevent account takeover and eradicate fraud.



Mitigate regulatory fines coming from breaches and asset abuse.

Prevent 3rd-party damage and liability coming from attacks leveraging your network infrastructure. React before increased regulatory ramifications related to rogue internet-exposed assets.

Key Benefits



Early breach detection & dwell time reduction



Phishing and trojan fraud prevention



External threat visibility augmentation

Unique visibility into threats



2M+ files analysed per day



4M+ URLs analysed per day



18M+ domains/IP addresses analysed per day



30B+ passive DNS records per day



Contributions by 3M+ monthly users coming from 230+ countries


See it in action

Your security stack and corporate telemetry only takes you so far, gain close to real-time visibility into external threats

Deep and dark web monitoring is not the answer to external threats either, shedding light into unindexed threats and reverse engineering their targets often requires human intervention. VirusTotal leverages a community of 3M+ users from over 230 countries submitting 2M+ files a day and 4M+ URLs a day in order to see what others can't.

Get notified when VirusTotal sees >>>>

VirusTotal Alerts hooks into the unrivaled and high-signal threat stream processed by VirusTotal, classifying and prioritizing detected violations for...

 <p>Brand impersonation</p>	<p>Fake smartphone apps making use of your logo to phish your users or deceive them into installing malware.</p> <p>Malicious documents/emails containing your logo or mentioning your brand and used as a first stage malware delivery vector.</p>
 <p>Phishing & Counterfeiting</p>	<p>New domains typosquatting your legit domain.</p> <p>Look-alike subdomains.</p> <p>Detected URLs containing your brand in their path.</p> <p>URLs reusing your legit website's favicon.</p> <p>URLs reusing your legit website's title or relevant content text.</p>
 <p>Corporate infrastructure abuse & compromise</p>	<p>Malware being downloaded from your URLs, domains or IP address ranges.</p> <p>Malware communicating with your URLs, domains or IP address ranges.</p> <p>Your URLs, domains or IP addresses inside the raw binary body of malware scanned by VirusTotal.</p> <p>Your URLs, domains or IP addresses detected by at least one security vendor.</p>
 <p>Mistaken industry detections</p>	<p>One of your URLs detected by a single security vendor.</p> <p>One of your domains detected by a single security vendor.</p> <p>One of your IP addresses detected by a single security vendor.</p>
 <p>Shadow & Orphaned IT infrastructure</p>	<p>Open directories in your domains/IP address ranges.</p> <p>{Whois, SSL, DNS} changes for your domains.</p> <p>Expiring SSL certificates and domains.</p>

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.

Unmatched visibility

Thousands of companies world-wide connect their SOAR platforms to VirusTotal for phishing triage. This acts as a massive distributed set of sensors allowing VirusTotal to see real-time new phishing 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

VT ALERTS analysis engine



URL content retrieval



Lexical analysis



Levenshtein distance



OCR on docs/PDFs



Image recognition



Memory dumping



Mobile app unpacking



Pattern matching

Domain, IP address ranges,
logo/favicon, website title and
representative brand strings
watchlists

Early identification of...

Phishing

Trojan-based fraud

Misconfigurations

Counterfeiting

Hacked servers

Rogue setups

Scams

C2s on your network

Impersonation

Fake apps

Detected assets

Mistaken blocks

Managed takedowns

Short on resources? Our advanced partners will take care of malicious infrastructure takedowns on your behalf. Skilled analysts that can augment your team and keep exposure time to a minimum.



Google Cloud



VIRUSTOTAL

What Makes Us Different?

Most anti-phishing vendors just identify typosquatting in newly registered domain feeds. Phishing sites often leverage subdomains of other domains that do not look alike the original domain, or rather deep navigation URL paths. Typosquatting is just one phishing technique. **Only crowdsourcing gives you superior visibility into unindexed nefarious Internet infrastructure.**

Similarly, many vendors will use dark & deep web monitoring as their battle horse. Dark web monitoring will only allow you to identify phishing/malware kit underground sales, not the actual operationalization of these against your organization, i.e. specific sites and trojan variants generated with those kits and configured to target your company.

Dark web monitoring is useful to identify attackers selling stolen company information and user accounts, but, **wouldn't you prefer to prevent the account / information theft from happening in the first place?**



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. Unrivalled 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

Detailed static and dynamic analysis reports for IoCs found in alerts, including interlinking with other IoCs in the VirusTotal threat corpus to understand badness.



Google internet visibility

Google crawler cookbooks surfacing suspicious / anomalous URLs, orphaned infrastructure and misconfigurations.



Disruptive economics

Fixed, predictable, flat cost. Independent of number of assets, alerts, watchlists, seats, lookup volumes, etc. Monitor all your assets.

VT ALERTS

In the last month

Category	Severity	Count
0 Brand Impersonation alerts	Low	-
	Medium	-
	High	-
103 Corporate Infrastructure Abuse alerts	Low	-
	Medium	79
	High	24
157 Phishing & Counterfeiting alerts	Low	-
	Medium	153
	High	4
17 Potential False Positives	Low	-
	Medium	17
	High	-

Notifications from all watchlists

Date	Severity	Alert
2021-09-29 03:44:07	High	http://financeae.com/ , potentially typosquatting : binance.com
2021-09-28 22:37:58	High	http://binance.me/ , reusing one of your brand's favicons
2021-09-28 04:23:38	High	https://binance.com/ flagged as malicious by 2 security vendors, found in the raw binary body of file c2e7...22fb, of type pe_exe, name orck.exe and flagged as malicious by 23 security vendors
2021-09-28 04:23:20	High	binance.com, found in the raw binary body of file c2e7...22fb, of type pe_exe, name orck.exe and flagged as malicious by 23 security vendors
2021-09-28 00:02:55	High	http://financezy.co/wp-admin flagged as malicious by 6 security vendors, reusing one of your brand's favicons
2021-09-27 22:57:42	High	http://steeliedesign.ca/ , reusing one of your brand's favicons
2021-09-27 22:05:26	High	www.binance.com, found in the raw binary body of file e4a7...db9d, of type html and flagged as malicious by 2 security vendors
2021-09-27 15:46:53	High	http://financeae.com/ , potentially typosquatting : binance.com
2021-09-27 11:59:48	High	www.binance.com, found in the raw binary body of file 96a5...5588, of type html and flagged as malicious by 1 security vendor
2021-09-27 01:25:24	High	https://accounts.binance.me/en/re... flagged as malicious by 1 security vendor, reusing one of your brand's favicons
2021-09-26 22:32:31	High	http://binance.com/ flagged as malicious by 2 security vendors
2021-09-26 19:26:23	High	binance.com, found in the raw binary body of file 2576...bc93, of type html and flagged as malicious by 14 security vendors
2021-09-26 03:45:15	High	http://financeae.com/ , potentially typosquatting : binance.com
2021-09-25 22:36:08	High	http://binance.com/ flagged as malicious by 2 security vendors, found in the raw binary body of file fa56...9065, of type javascript
2021-09-25 19:22:04	High	binance.com, found in the raw binary body of file 83e4...1f82, of type html and flagged as malicious by 3 security vendors
2021-09-25 17:07:36	High	www.binance.com, found in the raw binary body of file 6ade...49c8, of type html and flagged as malicious by 14 security vendors
2021-09-25 07:18:15	High	dapi.binance.com, found in the raw binary body of file 76f7...a0f1, of type pe_exe, name hfbot_312.exe and flagged as malicious by 1 security vendor
2021-09-25 06:29:51	High	https://ortbin.info/ , reusing one of your brand's favicons
2021-09-25 04:18:02	High	fapi.binance.com, found in the raw binary body of file e444...865e, of type pe_exe, name CryptoScreener.exe and flagged as malicious by 1 security vendor
2021-09-25 03:47:32	High	http://binancezh.sh/en/my/securit... flagged as malicious by 5 security vendors, reusing one of your brand's favicons

VirusTotal Alerts, we see what others can't