VIRUSTOTAL

PREMIUM SERVICES

Illuminate your data, unearth compromises, protect your business

Knowledge is power. Learn how adversaries operate to defend yourself against them.

The largest historical and live threat observatory

15 years of malicious sightings enriching and providing context around your organization's observations. The rising tide of network threats has created an arms race in security tool accumulation, this in turn has led to alarm fatigue in terms of noisy alerts and false positives. VirusTotal allows you to automatically triage your data and focus on what really matters, complete visibility into any type of artifact: files, domains, IP addresses, URLs, SSL certificates, etc.

WHY VIRUSTOTAL?

Use Cases

- Enrich and triage alerts to make better and faster decisions.
- Generate IoCs that you can use to power-up your security defenses.
- Leverage VirusTotal in your corporate workflows via API
- Track the evolution of malware families and threat actors with YARA.
- Download malware for advanced dissection offline.
- Map out attacker campaigns in collaborative node graphs.
- Seamlessly surface global threat data into your SIEM, SOAR, IDS, etc.
- Radically improve the performance of your SOC analysts.

15 YEARS
OBSERVATIONS GOING BACK TO 2004

2.4B FILES
50B+ considering compressed bundles

2M
analyses per day

600 M+
sandbox reports

232
countries
submitting files

1.9
M users
per month

4.6B URLS
6M+ URL analyses per day

1.6B
DOMAINS

2.5B
pDNS
RESOLUTIONS

45/71
70+ Antivirus vendors
70+ URL blacklists
10+ Sandbox partners

Contact us for more information on service offerings and pricing.

TILT THE PLAYING FIELD TO YOUR ADVANTAGE

VirusTotal was launched back in 2004 under the umbrella of a small security company in Spain, as a simple antivirus aggregator. Since then we have tirelessly pursued the mission of **securing billions of users world-wide by empowering the antivirus industry and global security teams**, acting as a lever to radically improve understanding of attackers and adversarial patterns. These days we do not only focus on files and static analysis, but **cover campaigns from every single angle**, both in terms of kinds of analysis and types of artifacts. More than 15 years of sightings make us the largest historical threat observatory. Our data is so comprehensive and unique that Google decided to acquire VirusTotal back in 2012, so as to secure its mission and neutrality, and make sure that **world leading malware fighting would meet planet-scale technology**, scaling seamlessly to provide unprecedented insights into threats and outsmart attackers.

3 Great reasons to leverage VirusTotal Professional Services

Community first

We see things others can't

VirusTotal is more than a business, it is an ecosystem. Unlike other services, VirusTotal runs a free public website to which any random user can submit threat observables (files, URLs, domains, IP addresses) and have them scanned with a myriad of security solutions.

This means that VirusTotal does not rely on your own internal data or third-party feeds. We have **immediate and word-wide visibility into attacker campaigns**. Our observations are not confined to a specific industry or geographical area. As a consequence, the dataset is diverse, fresh and unique: from malware targeting Tibet activists to advanced tooling used in Fortune 500 state-sponsored compromises.

Holistic threat profiling

We think in petabytes

Similar services focus exclusively on files and hashes, VirusTotal takes a 360º characterization approach for attacker campaigns. We process and understand files, URLs, domains, IPs, etc. You are not simply buying a hash checker, but rather a telescope and a microscope into any kind of threat observable.

Moreover, other services will simply focus on static analysis or sandboxing. We unearth badness by following a **multi-layered approach to analysis and characterization**: static properties, file reputation, dynamic execution, code analysis, relationships surfacing, community scoring, provenance details, etc.

Security industry nexus

We give good the advantage

We align, coordinate and empower different security solutions and threat analyst teams in order to give good the advantage. **Thanks to these partnerships we also get to see things that others can't**, for instance, by collecting unparalleled whitelisting information or by enriching our data with in-the-wild sightings coming from Microsoft Sysinternals tools suite.

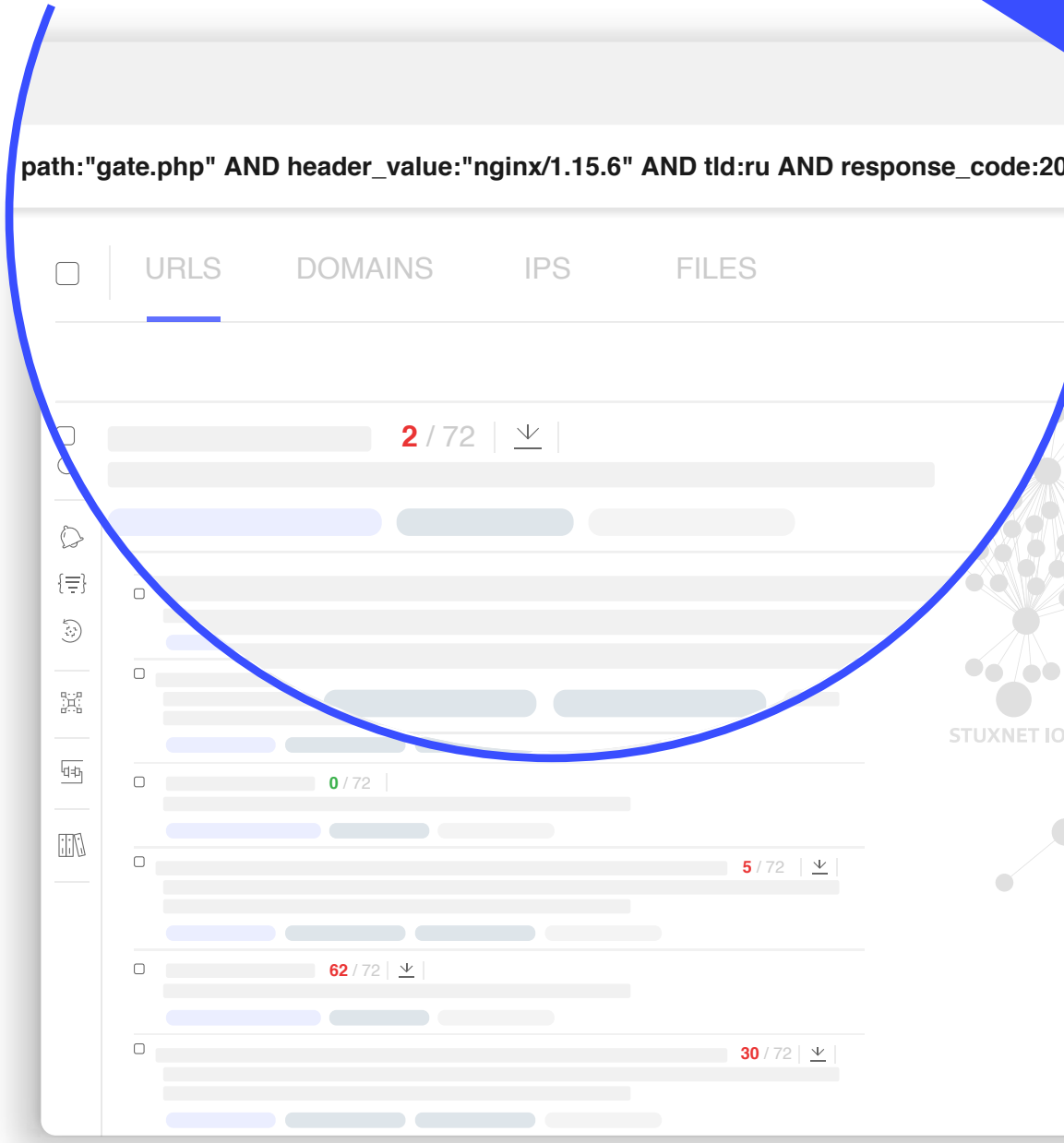
We are the world-largest threat data sharing platform, with unique partnerships where any team can collaborate, not only antivirus vendors providing verdicts. Dozens of companies collaborate with Passive DNS information, sandbox reports, provenance details, static analysis tools, etc.

Contact us for more information on service offerings and pricing.

COMPONENTS OF VIRUSTOTAL PROFESSIONAL SERVICES

VT INTELLIGENCE

- Search for files matching static, structural, dynamic, binary and in-the-wild metadata criteria.
- Download files for further study and dissection offline.
- Discover known and unknown network infrastructure (domains, IPs, URLs, SSL certificates) used by adversaries.
- Pivot over attacker campaign observables based on common properties, reveal IoCs for threats flying under the radar.



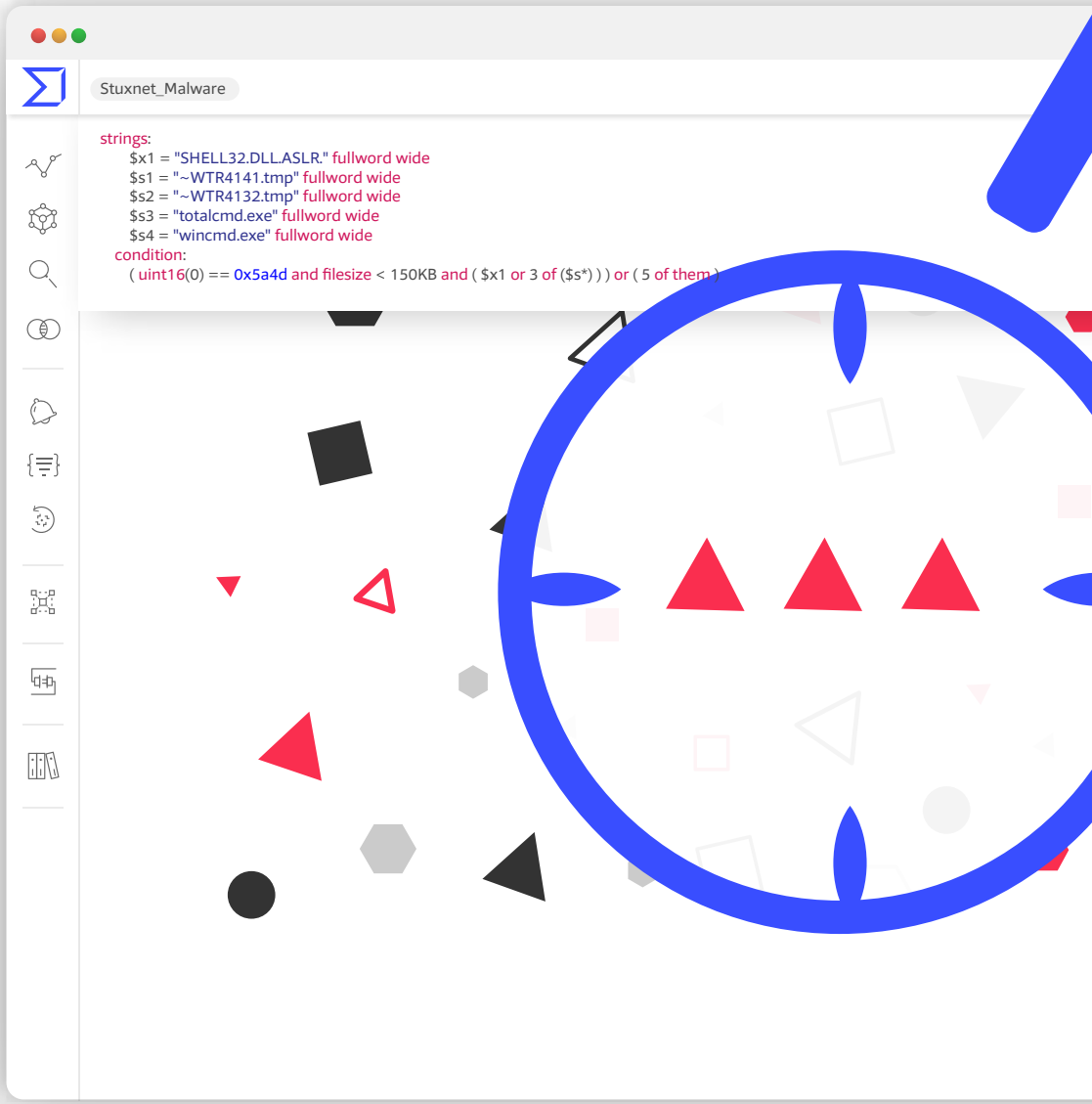
VT Intelligence **extracts and indexes file, URL, domain and IP address actionable properties** and metadata from a security and threat intelligence point of view. The indexed data includes, but is not limited to: sandbox behaviors, network information, office macros, PE imports/exports, authenticode signatures, whois lookups, DNS resolutions, SSL certificates, provenance, popularity rankings, antivirus labels, etc.

Multi-property searches can be performed via advanced modifiers and threat actor campaigns can be fully mapped through pivoting and similarity searching.

Lightning-fast binary n-gram searches complement file similarity searches to find other unknown variants of an attack and different malware pertaining to a same threat actor. Any file uploaded to VirusTotal is downloadable in order to study it further offline, this includes disassembly and debugging, running files in specialised analysis infrastructure such as sandboxes resembling your environment, etc.

VT HUNTING

- Apply YARA to VirusTotal's live file uploads, get notified about any new file matching your rules.
- Run YARA rules back in time against VirusTotal's historical collection to understand the evolution of a given malware family or threat actor.
- Use the API to build workflows to automatically generate IoCs for files that match your criteria.
- Select a group of files and automatically generate optimal detection rules.



VT Hunting is made up of two major components: Livehunt and Retrohunt. Livehunt allows you to create YARA rules and store them in VirusTotal in order to apply them on every single file uploaded to the service, **generating notifications for every new variant of a malware family** that you are tracking.

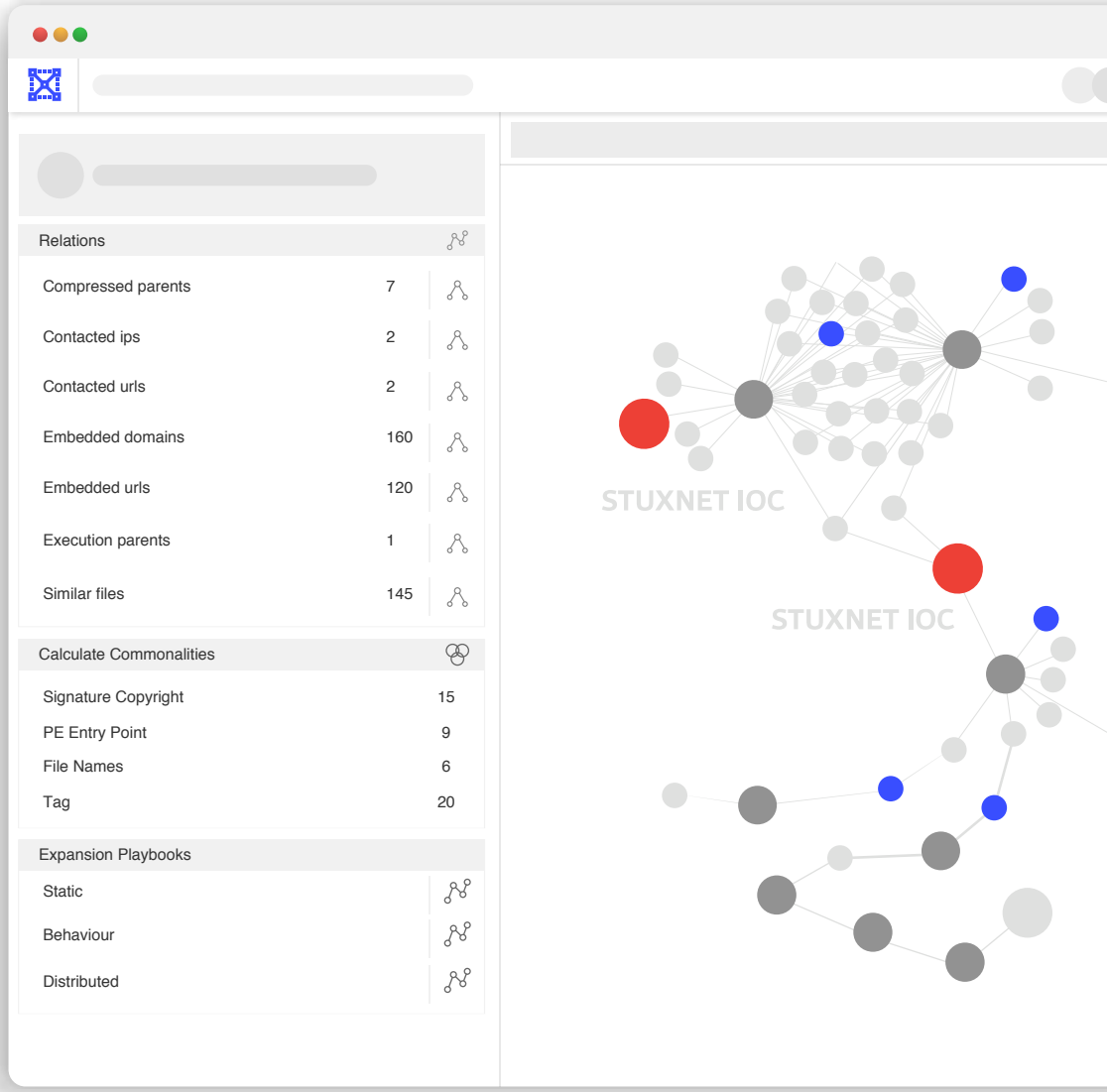
Retrohunt runs **YARA rules back in time against the historical collection** of files, allowing you to track the evolution of a given malware family or threat actor. Retrohunt jobs can be launched against a collection of goodware in order to prevent false positives before using them in production, inside VirusTotal or elsewhere.

Notifications can be **retrieved programmatically via API**, meaning that by combining this capability with other VT Enterprise features such as sandboxing or static analysis, a feed of indicators of compromise can be easily built in order to power-up your security defenses.

Contact us for more information on service offerings and pricing.

VT GRAPH

- Explore VirusTotal's dataset visually in a node-based graph to reveal multiple order connections between threat artifacts.
- Keep your investigations synced real-time with VirusTotal's latest findings.
- Gather input of multiple team members, collaborate in an online workbench and share your investigations with fine-grained access controls.
- Automatically discover commonalities and patterns shared across observables found in an attacker campaign, generate IoCs that you can feed into your security toolset.



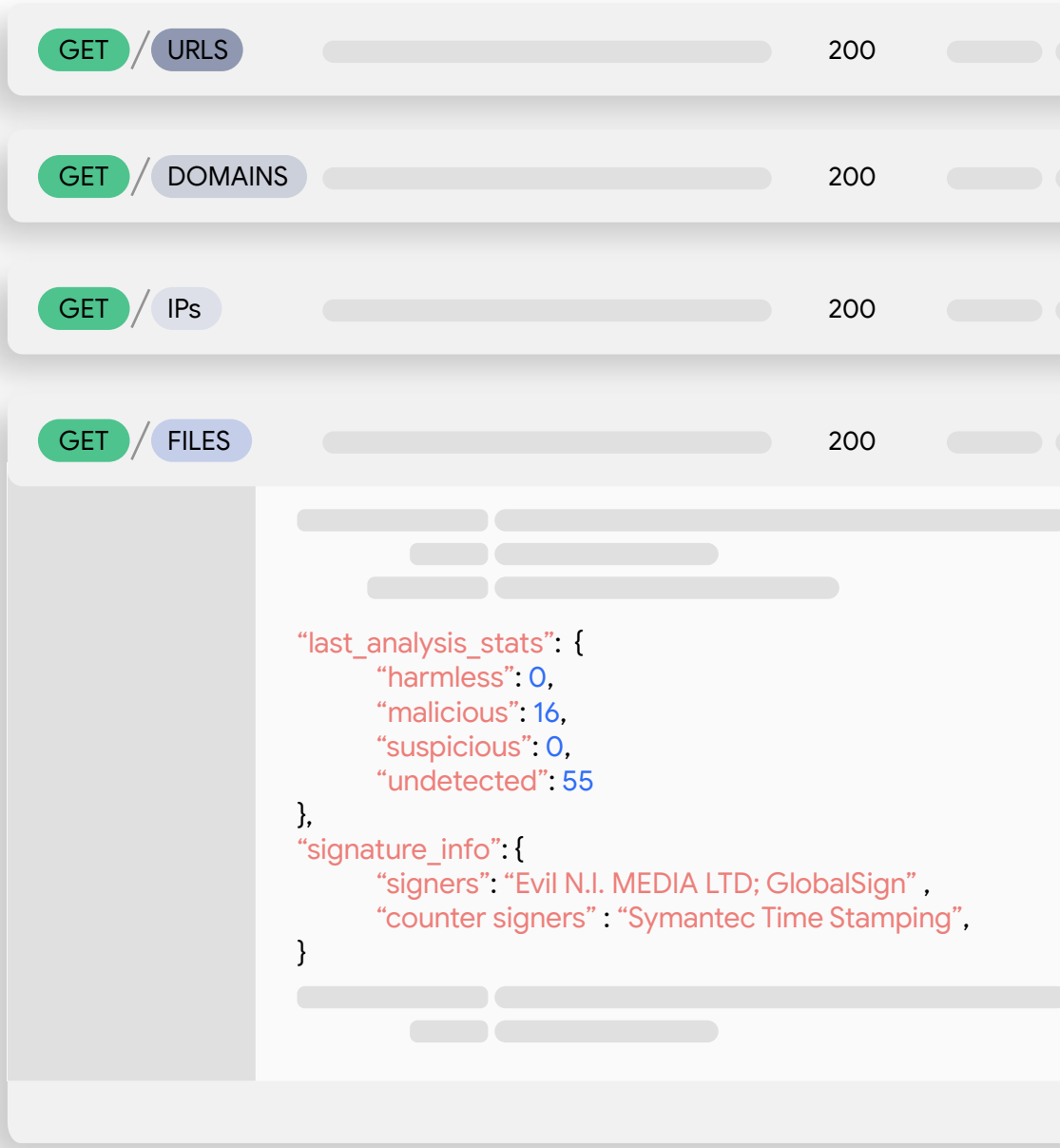
VT Graph allows you to understand the relationships between files, URLs, domains, IP addresses and other observables encountered in an ongoing investigation in order to **visually map out an attacker campaign on a node-based graph** allowing link analysis.

Groups of threat artifacts can be selected in order to automatically **generate commonalities that can be used as IoCs** in defensive security solutions. At the same time, graphs can be shared with fine-grained access controls in order to collaborate on investigations with other team members or industry peers.

VT Graph also expedites research by guiding discovery via **expansion playbooks**, via integrations with threat intelligence platforms such as MISP and by allowing advanced faceted searches over all the investigations conducted by your team.

VT API

- Automate workflows with VirusTotal's dataset, including programmatic enrichment of alerts.
- Integrate VirusTotal with your SIEM, SOAR, EDR or AV.
- Download files for further study and dissection offline.
- Fully characterize any kind of threat campaign observable: files, URLs, domains, IPs, SSL Certificates, etc.



VT API is a RESTful interface to VirusTotal's dataset, allowing you to **programmatically connect your corporate systems and workflows** with our knowledge about threats going back to 2004. All of the capabilities described for the aforementioned components are exposed via API, hence, this solution allows you to enrich any kind of observable: files, URLs, IPs, Domains, etc.

The retrievable data points include, but are not limited to: verdicts, sandbox behaviors, network information, office macros, PE imports/exports, authenticode signatures, whois lookups, DNS resolutions, SSL certificates, provenance, popularity rankings, etc. Many third-party security defenses have VT API integration, meaning that threat enrichment is sometimes as easy as pasting your API key into a simple settings form.

Any file uploaded to VirusTotal is downloadable for further study offline.

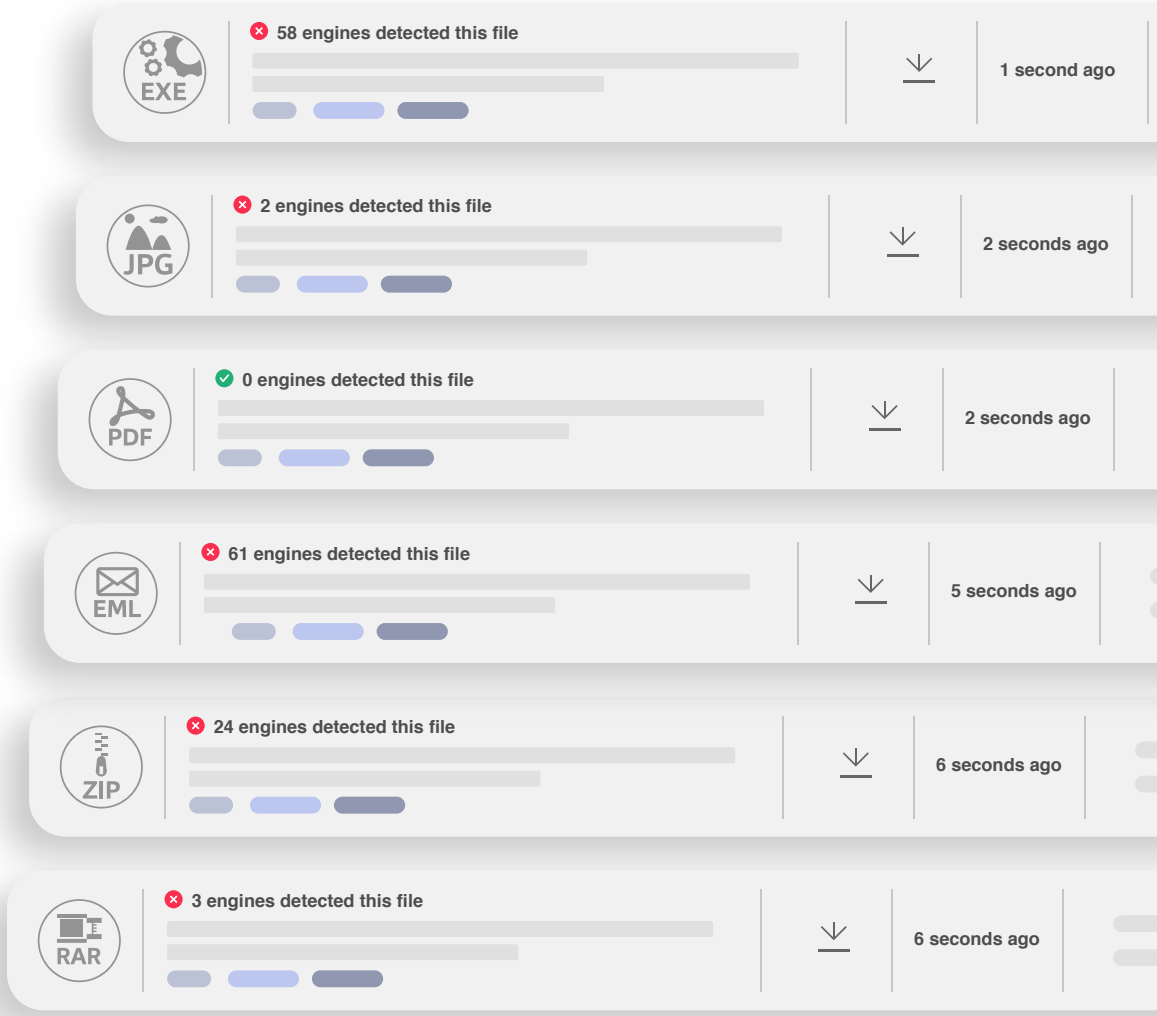
FILE FEED

- Download every single file uploaded to VirusTotal, along with its analysis.
- Programmatically consume all the details generated for every single file: verdicts, static characterization, dynamic analysis, relationships, provenance, submission metadata, etc.
- Build a cache of VirusTotal's dataset to look up items in air-gapped environments or real-time sync your historical logs with new threat observations.
- Implement complex filtering logic to focus exclusively on files of your interest and datamine the stream to generate IoCs to feed into your security solutions.

Time-scoped packages of metadata generated for every file submitted to VirusTotal, along with a link to download each file, 2M files a day on average.

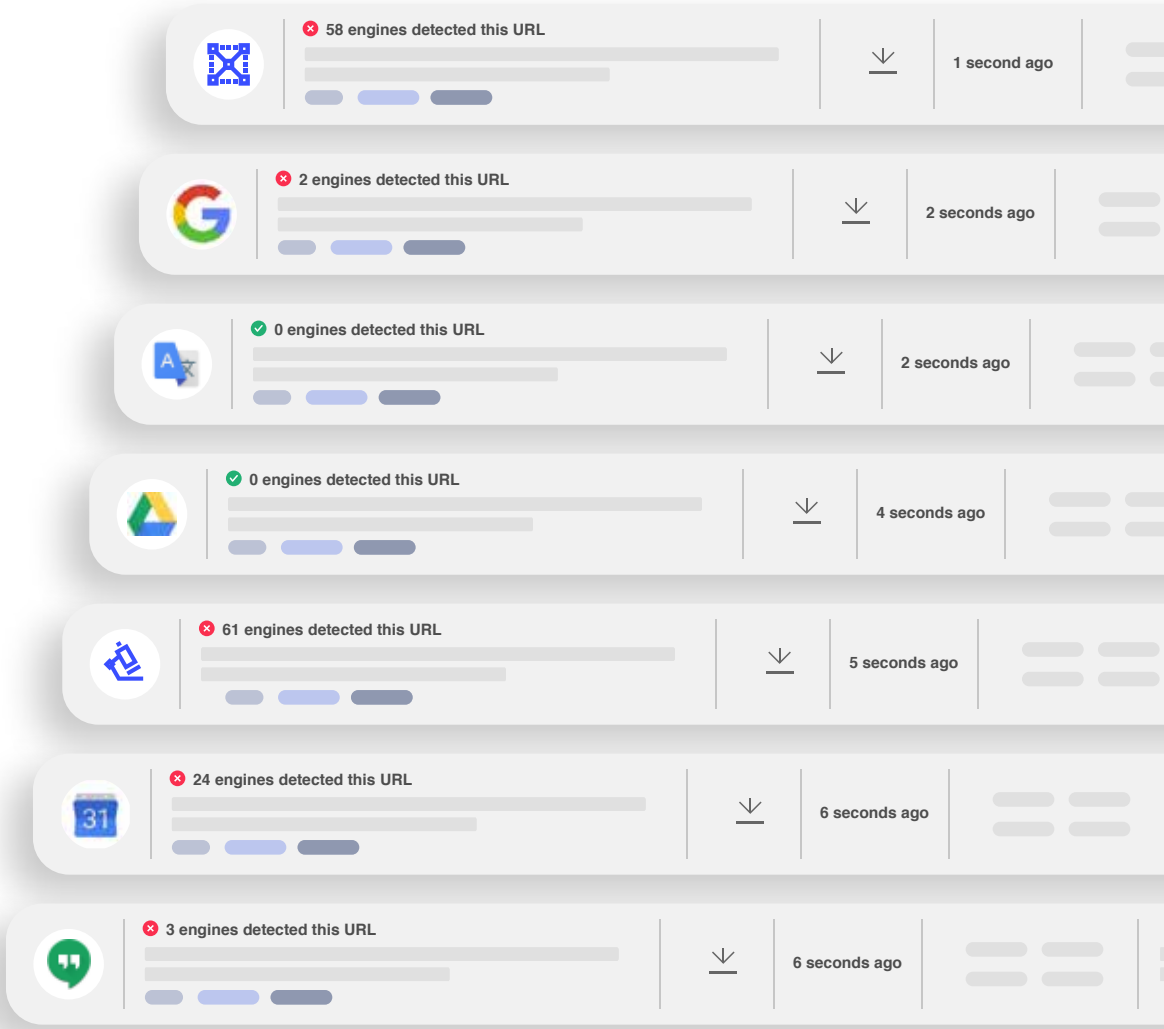
The metadata includes all the information presented on file reports, from detections to advanced static attributes. Additionally, privacy-preserving ciphered submitter identifiers are tied to every item found in the feed, this is a key piece of information that security analysts are using to track threat actors.

This data stream enables you to **build client-side data mining and filtering logic in order to generate indicators of compromise** that can power-up your security defenses.



URL FEED

- Ingest every single URL submitted to VirusTotal along with its analysis.
- Programmatically consume all the details generated for every single URL: verdicts, content categorization, DNS resolution, relationships, submission metadata, etc.
- Datamine the feed and generate IoCs to power-up your network perimeter defenses.
- Build a cache of VirusTotal's dataset to look up items in air-gapped environments or real-time sync your historical logs with new threat observations.

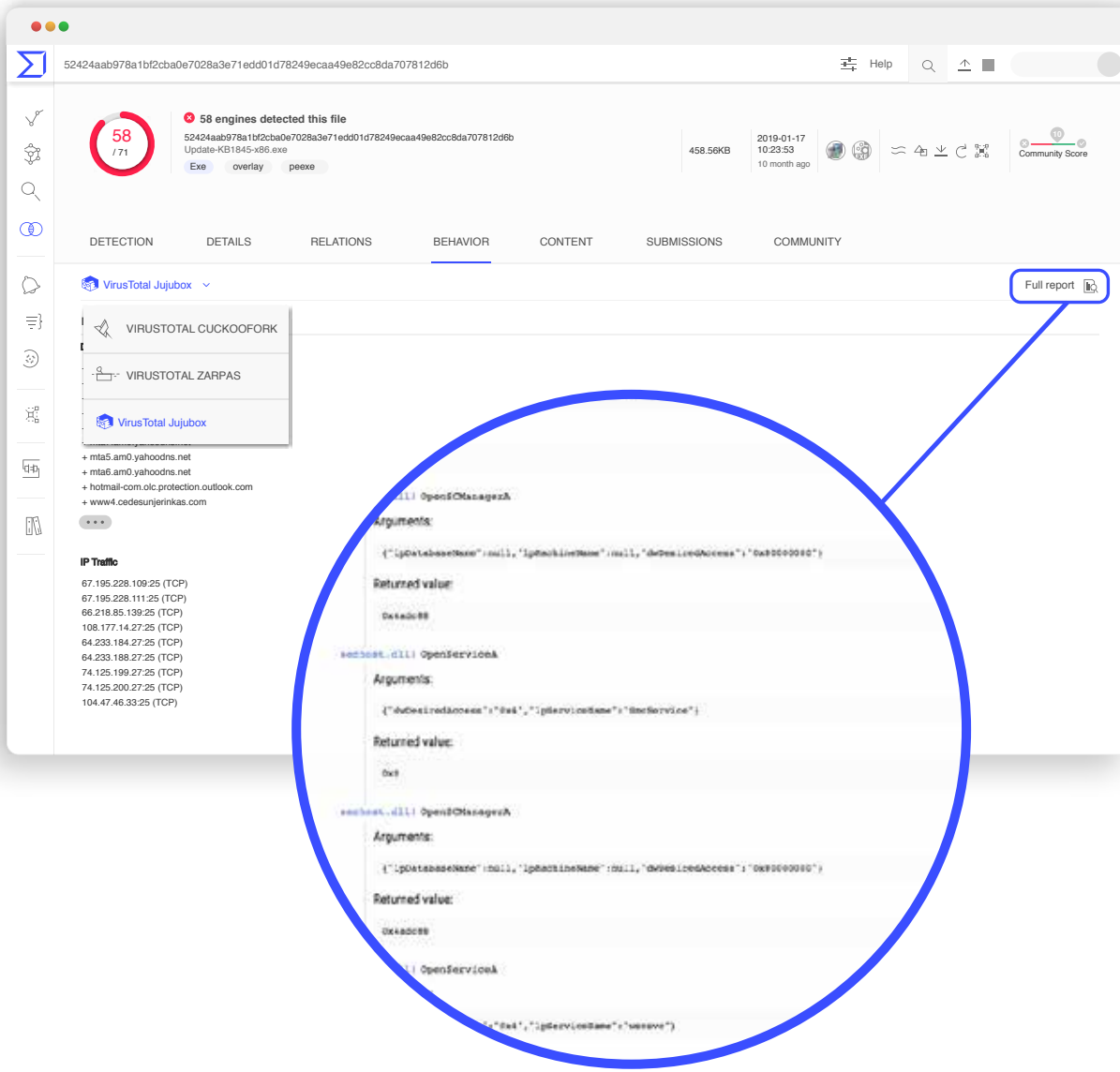


Time-scoped packages of metadata generated for every single URL submitted to VirusTotal, over 6M URLs a day. The metadata includes all the information presented on URL reports, including verdicts, content categorization, DNS resolution, relationships, submission metadata, etc.

This stream of data allows you to identify common C&C, phishing kit, exploit kit patterns (path structure, parameters, server headers etc.) in order to generate detection rules that can prevent future attacks on your organization.

SANDBOX FEED

- Ingest every single sandbox dynamic analysis report generated for all files uploaded to VirusTotal.
- Datamine the feed and identify domains, IP addresses, URLs, mutexes, registry keys, etc. that may be used as indicators of compromise to power-up your security toolset.
- Discover unknown malware flying under the radar of antivirus solutions by studying behavioral patterns.
- Implement complex behavior detection rules.



Time-scoped packages with all the dynamic analysis file execution behavior reports produced by sandboxes on every single file uploaded to VirusTotal (EXEs, DOCs, APKs, DMGs, MACH-Os, etc.).

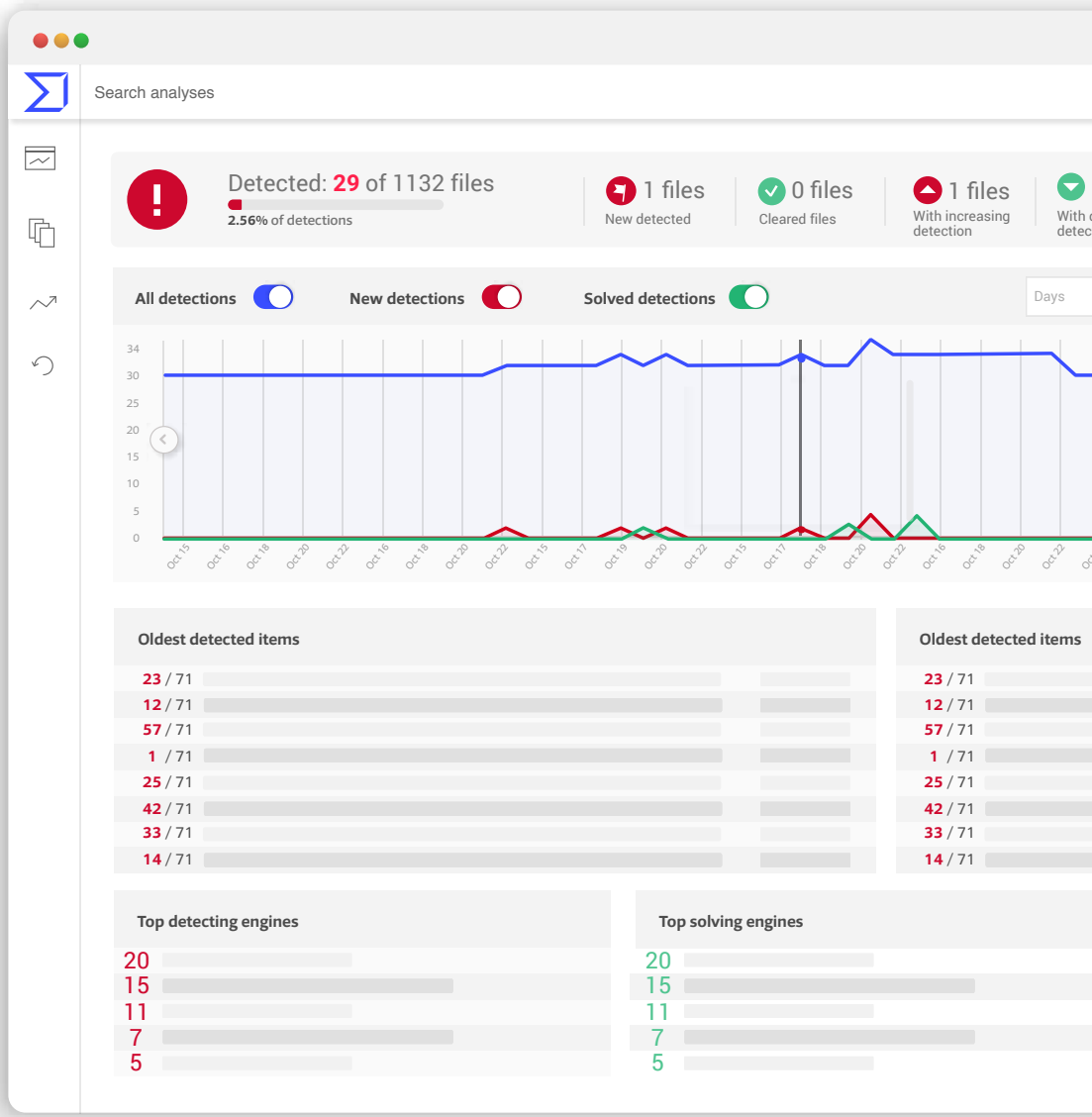
As the **world-largest dynamic analysis deployment**, advanced analytics can be conducted on the feed in order to identify attack commonalities and generate domains, IPs, URLs, mutexes, registry keys, etc. that can be fed into your defensive security solutions so as to protect your organization malware that might be flying under the radar that happens to reuse infrastructure and TTPs observed in past campaigns.

VT MONITOR

- Mitigate the risk of false positive antivirus detections on the software that you develop, prevent business impact and reputation damage.
- Scan your software pre-release and periodically after publishing and be the first one to know about mistaken detections.
- Generate a VirusTotal Trust Seal for any of your files so that your users can download them directly from VirusTotal servers with confidence.
- Notify antivirus vendors directly, without intermediaries.

A **service for the software industry**, allows publishers to upload the software that they develop to a private repository where it gets scanned periodically with the latest antivirus signature sets, notifying both the developer and the antivirus firm upon mistaken detections.

Software publishers use it both to perform pre-release scanning and subsequent QA testing once generally available, **preventing business loss due to antiviruses blocking the pertinent software and reputation damage due to users believing that your company has trojanized the software**. VirusTotal's public site will clearly acknowledge file provenance if the pertinent file happens to be uploaded to the public service, meaning that random users world-wide will not be confused by antivirus false positives.



KEY CAPABILITIES

Powerful search tools

Lightning-fast binary content searches.

5 petabyte n-gram index allowing you to search for files containing random binary subsequences within seconds. Identify variants of an attack or other tools used by a given attacker.

Instant YARA retro-hunting.

Build YARA rules that can be expressed as n-gram searches and seamlessly enjoy instantaneous back-in-time YARA hunts in order to track the evolution of a given adversary or malware family.

Multi-property elastic searching.

Over 40 search modifiers can be used to hunt down malware samples of interest based on static, dynamic and relational properties. Example: type:dmg AND signature: "T8RS3R6DT4" AND metadata:"adharma" AND behaviour:"pkill -9 -i Flash Update 13.6 Installer" AND (behaviour:"rp.wacadacaw.com" OR behaviour:"os.wacadacaw.com")

Any threat campaign observable.

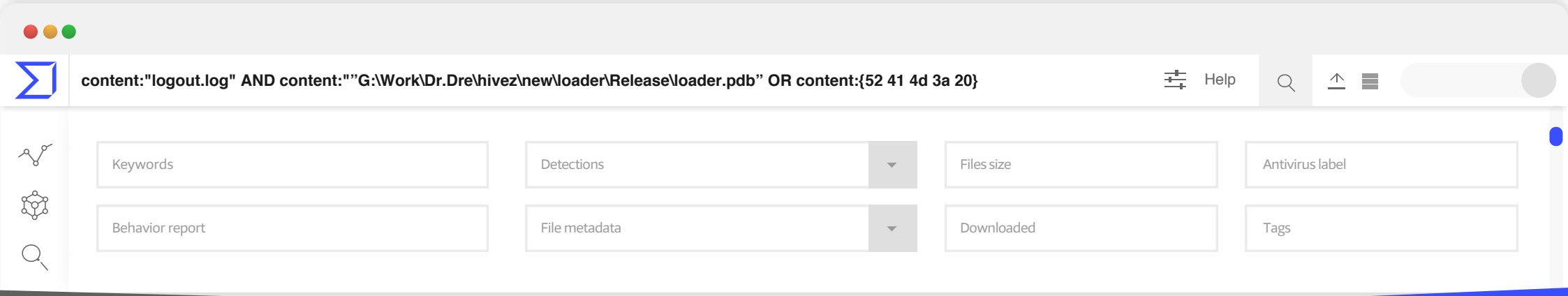
Perform full-text searches over file, URL, domain or IP address properties. For example, discover currently undetected or unused network infrastructure tied to a given attacker by pivoting over Whois fields.

Combine any number of modifiers.

Threat parameters can be combined in order to identify files, URLs, domains or IPs that match rich search criteria, filtering noise and focusing on threats that are relevant to your investigations.

Clustering and similarity search.

Search for similar files using several hashes/algorithms: ssdeep, imphash, icon visual similarity and our own in-house structural feature hash.



Contact us for more information on service offerings and pricing.

Comprehensive details

Submission metadata.

First seen and last seen dates, number of submissions, submission file names, upload countries, submission dates, ciphered submitter identifier, submission interface, etc.

Static information.

Antivirus verdicts, file signature, packer information, PE structure, Exif attributes, ELF structure, package contents, OLE VBA Macro code stream, etc.

Dynamic information.

Behavior characterization through sandbox execution for major operating systems, including multi-partner environments, increasing robustness against cloaking and evasion techniques.

Complete scanning information.

All reports on a given observable, not only the latest snapshot. Understand how threat detections evolve over time.

Telemetry metadata.

Partner tools contribute rich end-user PC metadata to our dataset, e.g. Windows registry keys in which an executable is registered for autolaunch upon reboot, creation date on end-user machine, full name and path of the file.

Goodware and whitelisting information.

Goodware score, VirusTotal Community collective intelligence, aggregation of publicly available goodware databases as well as legitimate software whitelisting details shared by top partners and our VT Monitor service.

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

Submissions

Date	Name	Source	Country
2011-12-10 15:52:37	633027DD00A306AF60950717FB037E00D3E3BEA1.exe	b4973965 - email	DE
2011-12-10 16:01:36	file-3249966_exe	32e81222 - web	ES
2011-12-11 10:56:10	putty.exe	efa433f6 - web	CN
2011-12-13 10:51:35	putty 0.62.exe	cd8869bb - web	DE

Diverse sources

Global origins.

Files submitted from 232 unique ISO country codes, which includes almost 3M distinct sources in the last year. 1.9M users per month. Real-time visibility into world-wide threats, understand prevalence and scope.

Structural clustering of polymorphic variants.

198,000 clusters generated per day during an average month. About 35% of all files with a feature hash are clustered in the top 200 collections.

File types.

Over 100 identified file types seen per day, on average. Examples: Win32 DLL, Win32, EXE, HTML, Java Bytecode, Android, PDF, Text, Mach-O, ZIP, PNG, XML, MS Word, JPEG, ELF, RAR, Office Open XML, C++, C, GZIP, JAR, DOS, EXE, MS Excel, MP3, Python, 7ZIP, Windows, GIF, Email.

ITW file origin.

More than 300M files with origin information; more than 200M portable executables from distinct URLs; over 100M files with rich telemetry data; millions of emails for rich contextual information.

Multiple submission interfaces.

Interact with VirusTotal via API, web platform, email, browser extensions, Android app, etc. Each of these interfaces add rich submission and prevalence metadata. E.g. Browser extensions contribute to passive DNS data generation.

Data sharing partnerships.

Organizations are entitled to a discount in exchange for sharing data that can contribute back to the community and increase visibility into threats. Dozens of companies world-wide share sandbox reports, verdicts, passive DNS data, in-the-wild download URLs for malware, telemetry, etc.

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

ITW Urls

Scanned	Detections	URL
2019-08-30	5 / 71	http://app.2345.cn/appsoft/a155457.apk
2019-05-31	0 / 71	http://azdown.veryhuo.com:8021/soft/0910/app2sd_veryhuo.com.apk
2018-09-22	4 / 71	http://d4.buylequ.com/5577.com.droidsail.dsapp2sd.apk
2018-01-22	3 / 71	http://shouji.360tpcdn.com/140708/261a6e4b95754c7403578b9c0084a0f7/com.droidsail.dsapp2sd_750.apk


VIRUSTOTAL
The path to stronger, more affordable cybersecurity starts here.
www.virustotal.com/contact