COMODO
CYBERSECURITY

The Antivirus Industry and its VirusTotal Deception

VirusTotal (www.virustotal.com) is a crowd-sourced virus scanning project sponsored by Google. VirusTotal solicits suspect files and URLs from users, subscribers and other site visitors and scans them with solutions from over 70 anti-virus (AV) tools suppliers. Basic results are shared with submitters and among participating commercial partners who, in theory, use results to improve their anti-virus software, collectively contributing to the improvement of global IT security.

Key to VirusTotal's ability to attract commercial participants is the project's *Terms of Service*, wherein participants agree not to:

> *…"use the Service in any way which could infringe the rights or interests of VirusTotal, the Community or any third party, including for example, to prove or disprove a concept or discredit, or bait any actor in the anti-malware space."*

These innocuous terms, however, help AV vendors hide a multitude of inadequacies and downright deceptive practices. Participating AV suppliers often:

1. lack actual competence in virus detection, depending instead upon the detection capability of others, and without acknowledging that dependence;
2. overstate and distort the effectiveness of detection, hide misidentification and false positives, trumpet their embrace of AI as a bluff, and engage in tests with repacked viruses and fake malware; and,
3. abuse VirusTotal and other community resources for reporting the supposed efficacy of detection, leveraging a well-intentioned service to support deceptive practices.

Parasitic Virus Detection

Many AV companies have ridden piggyback on VirusTotal and other shared AV services as a means to improve their virus signature libraries. However, some AV vendors have been caught integrating VirusTotal wholesale into their offerings, effectively re-using their competitors' detection engines for free. While VirusTotal actually banished such free-riding back in 2016, the practice continues via other shared services and direct use of competing detection solutions.

The Anti-Virus Bluff

Anti-virus vendors provide a highly optimistic and frankly misleading impression of the state of the art in anti-virus technology. Individual vendors make claims of 99% or greater detection rates (between blacklisting known malware and identifying new samples), and one would expect that the combined detection abilities of 70+ vendors comprising VirusTotal would top that seemingly impressive figure. But these impressions are undermined by the fact that:

- AV solutions miss a significant number of known viruses – overlooking even 1% of the millions of viruses in daily circulation allows tens of thousands of threats onto customer networks and into endpoints **undetected**
- Multiple solutions **fail to detect** the very same viruses, **misidentify** benign files and yield voluminous **false positives** on a regular basis, and exhibit unbounded **detection latency** in recognizing malware
- Even augmenting traditional detection with AI and ML, AV solutions still regularly fail to detect new (zero-day) threats, and 300,000+ unique unknown malware samples appear daily[1]

The Detection Deception

While Google's VirusTotal performs a valuable service to its vendor-members, those members use VirusTotal to perpetrate a great *disservice* upon IT end-users: using the reputation of VirusTotal, AV vendors co-opt Google's service and promote the myth that *detection* constitutes *protection*. When users and third-parties

[1] https://www.av-test.org/en/statistics/malware/

discover that Carbon Black, Crowdstrike, Cylance, McAfee, Symantec et al. do not disclose their failure to identify known malware, it becomes obvious that those vendors are hiding behind the Terms of Service.

A Better Path to Virus-Free Operation

Detection is Not Protection

Since the appearance of the first computer viruses in the 1980s, anti-virus technology has involved two steps: **detect** and **remediate**. Detection has always been an unwinnable paper chase: AV utilities scan incoming emails, local media, memory and other potential hiding places for telltale signs of viruses (signatures) and when known viruses are detected, remediation involves quarantine of infected documents and executables, and removal of virus code from systems already infected. But detection and remediation depend on knowledge gleaned from prior encounters with a virus. New ones, a.k.a. zero-day threats, slip right by blacklist-based AV tech. And thousands of new threats appear every day.

Protection > Detection

Actual *protection* involves much more than mere *detection*. Protection is preemptive and comprehensive, stopping all unknown files *before* they can damage system resources and user assets. Protection isolates and contains both already catalogued and as-yet unknown malware.

Default-Deny, Auto-Containment and Instant Usability

The Detect-Remediate paradigm is inherently flawed. Effective detection requires vendors to keep virus registries 100% current – an impossible task – and further stymied by the fact that AI-powered algorithms simply cannot reliably distinguish between malicious and benign code 100% of the time, even if AV vendors want you to think so.

To meet today's malware onslaught, a change of paradigm is required.

With Advanced Endpoint Protection (AEP), Comodo Cybersecurity combined three best practices – default-deny, auto-containment and instant usability. Comodo Cybersecurity AEP automatically isolates and contains incoming unknown files while letting users remain productive; AEP rapidly identifies and classifies unknown files and delivers rapid verdicting, supported by AI and on-call human analysts, while letting users open unknown documents and execute unknown scripts in isolation, removed from access to system and user resources.

The Comodo Zero-Day Challenge

Put Comodo Cybersecurity to the test: submit a sample of your chosen malware to the Valkyrie Verdict engine (https://verdict.valkyrie.comodo.com/). If you can show that Comodo fails to detect actual malware (not bogus benign bait), we'll publicize your submission – you'll be famous! (And we'll add your submission to our verdicting blacklist.) If we correctly identify your submission as malware, we still publicize your submission, along with your name and photo, as proof of our technology.

We also dare other AV vendors to accept the same challenge, to serve the AV user community through transparency and to help everyone be more secure and virus-free.

Comodo Cybertechnology. We don't hide behind terms of service. We proudly stand in front of our malware prevention.