

URL Sandboxing With Bitdefender

Bitdefender's sandbox operates a separate environment for URL detonations. Files are detonated in virtual machines that simulate real endpoints, complete with user files, applications and settings.

URLs are sent to a purpose-built environment, with its own heuristics, machine learning detection engines, and other filters. These can detect malicious web resources, and extract Threat Intelligence.

Purpose-built heuristics

URL detonations usually follow these steps from submission to result:

- ↳ Ensure full loading of the page, for example by getting past captchas
- ↳ Follow links to other URLs with malicious potential
- ↳ Extract anything we can from the page, like the favicon and Document Object Model (DOM)
- ↳ Apply detection rules specific for URLs

Machine Learning detections

Bitdefender's machine learning models are built to detect malicious activity in very specific scenarios. For example, we have a purpose-built model to analyze favicon, and another to analyze the DOM.

These are trained on large datasets pulled from Bitdefender's telemetry, with over 50 billion threat queries processed by our analysts every day.

Automatic downloads

If a URL points to a file, or if we find a download link on a page while detonating the URL, these files are also downloaded and run through dedicated engines to detect malicious samples.

Powered by Bitdefender Threat Intelligence

The URL sandbox integrates with all Bitdefender sources of Threat Intelligence, including the data pulled from anti-spam engines, our AV, and detections from all over the globe that feed into our URL Status Service, and other TI services.