Recorded Future®

DATA SHEET

Key Feature: Sandbox

Quickly Analyze Malware in a Safe, Customizable Environment

Challenge

Rapidly responding to cyber incidents is critical and deriving how they happened is even more important to prevent them. Yet, traditional defense mechanisms may not be able to detect all malware. Many threat actors, particularly advanced persistent threats (APTs), modify their malware in order to evade detection. Often, actors use malware that includes built-in functionality designed to detect and evade code analyzers and virtual machines (VMs). We need safe environments where we can detonate malware quickly, with fully customizable options to determine technical nuances and built mitigations, while also enriching the data with threat intelligence to determine trends. Ultimately, we need to build an incident response to include malware analysis and understand how and where to block malware of the future.

Solution

Recorded Future's revolutionary sandboxing solution is built with speed and scalability in mind from the ground up, with the capability scale to over 500,000 analyses per day providing analysts with a safe, customizable environment to detonate malware. The sandbox allows users to have live control of the detonation straight from a browser and include powerful countermeasures to known anti-sandbox and anti-analysis techniques. By looking at a malware's actions instead of more traditional AV methods, our sandbox can boost detection of 0-day threats and provide early warning for new and upcoming malware families. Coupled with direct integration with the Recorded Future Intelligence Graph, malware will automatically link to over 300+ billion entities, correlating the malware to the MITRE ATT&CK framework, threat actors, and many other data points to ensure your team can take action against current and future threats.

OVERVIEW

- File, URL, and code analysis for Windows, Linux, Android, and macOS
- Support for large file and archives analysis
- Network simulation options
- API access to automate submissions at scale

TECHNICAL FEATURES

- Family classification for over 350 common families
- Custom x86 static emulation
- TLS/SSL decryption
- Access to PCAPs, dropped files, and memory dumps
- Support for user-submitted YARA rules
- Live VM interaction