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 to evade detection. Often, actors use malware with built-in functionality engineered to detect and evade code analyzers and virtual machines (VMs). We need safe environments where we can quickly detonate malware, with fully customizable options to determine technical nuances and built mitigations while enriching the data with threat intelligence to determine trends. Ultimately, we need to develop an incident response that includes malware analysis that proactively informs how and where to block malware in the future.

Solution

Recorded Future's revolutionary sandboxing solution is built with speed and scalability in mind from the ground up, with the capability to scale to over 500,000 analyses per day, providing analysts with a safe, customizable environment to detonate malware. The sandbox gives users live control of the detonation directly from their browser window and includes robust countermeasures to anti-sandbox and anti-analysis evasion techniques. By looking at a malware's actions, instead of solely relying on more traditional antivirus methods, our sandbox can boost the detection of 0-day threats and provide early warning for new and upcoming malware families. Directly integrated with the Recorded Future Intelligence Graph, the sandbox automatically analyzes malware and compares it across 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

Recorded Future Sandbox or Enterprise Sandbox

Options based on analyses needed and privacy for threat intelligence curation

Recorded Future Sandbox

The sandbox included with the Threat Intelligence and SecOps modules provides up to 1,000 analyses per day per enterprise. Samples submitted are anonymized, with no identifying information shared. Submissions are curated with the Intelligence Graph, providing you insight and pivot points so you can take action on malicious files.

ADDITIONAL DETAILS

- 1,000 analyses/day
- Features listed above

Enterprise Sandbox

Our Enterprise Sandbox allows you to increase the number of analyses your team needs daily, starting at an additional 500 analyses per day per enterprise with options to include an additional 10,000+ analyses per day. Samples submitted are anonymized, with no identifying information shared. And further, with enhanced privacy, the enterprise sandbox only curates information with the Intelligence Graph when a submission is deemed malicious; and then only uses the specific data required to compare the malicious file sample against known malware families and trends. The restricted sharing of information and the detonation results further protect privacy and focus this threat intelligence specific to your organization.

ADDITIONAL DETAILS

- From 1,000 analyses/day to 11,000+ analyses/day
- Add additional analysis starting at 500 analyses/day
- Features listed above
- Additional privacy offered, curating information only when a submission is deemed malicious

How do we deem a file malicious?

Using a range of detection methods across both static and dynamic analysis our sandbox investigates uploaded files and assesses them for malicious content. The analysis includes comparing the submitted sample across a catalog of known threats, network interceptions, investigations using proprietary and open source rules, code analyses, and the inspection analysis of the file's actions and behaviors when executed on the virtual machine. All the different data points contribute to an overall score assessment, which is weighted based on the severity of the action and the possibility that it is malicious.

Best Practices

- Utilize the scoring system to prioritize malicious file investigations
  - Use Recorded Future enrichment to view enhanced contexts for the identified IOCs (Domains, IPs, and URLs) produced from sandbox detonations — to help analysts understand the types of threats assessed from the sandbox samples
  - Use Threat Intelligence to follow through with the investigation, pivoting to other relevant IOCs, hashes, or utilize hunting packages with YARA and/or Sigma rules
- Use XSOAR Playbooks for automatic malware detonation with IOC enrichment from Recorded Future, saving analysts time through automation and playbook actions

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries. Learn more at recordedfuture.com.

www.recordedfuture.com @RecordedFuture

© Recorded Future®, Inc. All rights reserved. All trademarks remain property of their respective owners.