VMRAY

Decoding Malicious Intent:
ENHANCING THREAT HUNTING WITH DYNAMIC ANALYSIS

Step-by-step Approach

As a security analyst practicing threat hunting, you can use dynamic analysis in combination with SIEM (Security Information and Event Management) and EDR (Endpoint Detection and Response) tools to enhance your threat detection capabilities and proactively identify potential threats in your environment.

Here's a step-by-step approach on how to utilize these tools and techniques:

1 Collect samples

Gather suspicious files, emails, or URLs from various sources, such as endpoint alerts, SIEM events, or third-party threat intelligence feeds. Use your EDR and SIEM tools to identify any anomalies that might suggest potential threats.

2 Dynamic analysis in a sandbox

Submit the collected samples to a sandbox environment, which is an isolated and controlled system that allows you to safely execute and analyze potentially malicious files. The sandbox will monitor the sample's behavior, network traffic, and system changes. This can help identify any behavioral patterns, payloads, or techniques that are specific to your organization's infrastructure.

3 Extract IOCs and artifacts

Analyze the results from sandboxing and dynamic analysis to extract IOCs and artifacts, such as IP addresses, domain names, file hashes, registry changes, or malicious function strings.

4 Hunt for threats

Use the collected IOCs, artifacts, and newly created rules to proactively search for signs of compromise in your environment. This can involve querying your SIEM for relevant events, scanning endpoint logs for IOCs, or monitoring network traffic for malicious patterns.

5 Investigate incidents

On top of Incident Response, sandboxing can significantly improve threat hunting and detection engineering practices. By analyzing malicious sample and extracting actionable behavior data, sandboxing can enable security teams to proactively identify and mitigate emerging threats. This proactive approach, in turn, helps strengthen the organization's overall security posture.

6 Update SIEM and EDR rules

If possible, create new detection rules based on the extracted IOCs and artifacts, and add them to your SIEM and EDR systems. This will improve your organization's ability to detect similar threats in the future.

7 Continuous improvement

Regularly review and update your threat hunting process, including your dynamic analysis configurations, to ensure they remain effective and relevant to your organization's evolving threat landscape.

By using sandboxing, SIEM, and EDR tools together, you can enhance your threat hunting capabilities and proactively identify and respond to potential threats in your environment. This comprehensive approach helps improve your organization's overall security posture and reduces the risk of breaches or compromises.

Extending Threat Hunting to the Cloud: The Value of Analyzing Linux Samples

In recent years, the cloud has become an integral part of our digital landscape, reshaping how businesses operate and how security professionals approach threat detection and mitigation. As our reliance on cloud infrastructures grows, it becomes paramount to understand that threat hunting isn't limited to just on-premises environments.

Linux, as the backbone of many cloud services, is a crucial aspect to consider. It powers a majority of the world's servers, making it a prime target for malicious actors. With the increase in Linux-driven services, especially in cloud environments, analyzing Linux malware samples has become more critical than ever for threat hunters.

Here's why:

1 Diverse Threat Landscape

Linux has its unique set of vulnerabilities and threats, such as IoT botnets, crypto-mining malware, and specific ransomware types. Analyzing Linux samples helps in understanding these threats better and preparing for them.

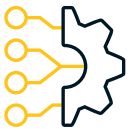
2 Understanding Cloud-specific Behaviors

Malware operating in the cloud often behaves differently from those in traditional on-prem environments. By sandboxing and analyzing Linux malware, threat hunters can discern patterns and indicators specific to cloud infrastructures.

3 Pivot Points for Broader Campaigns

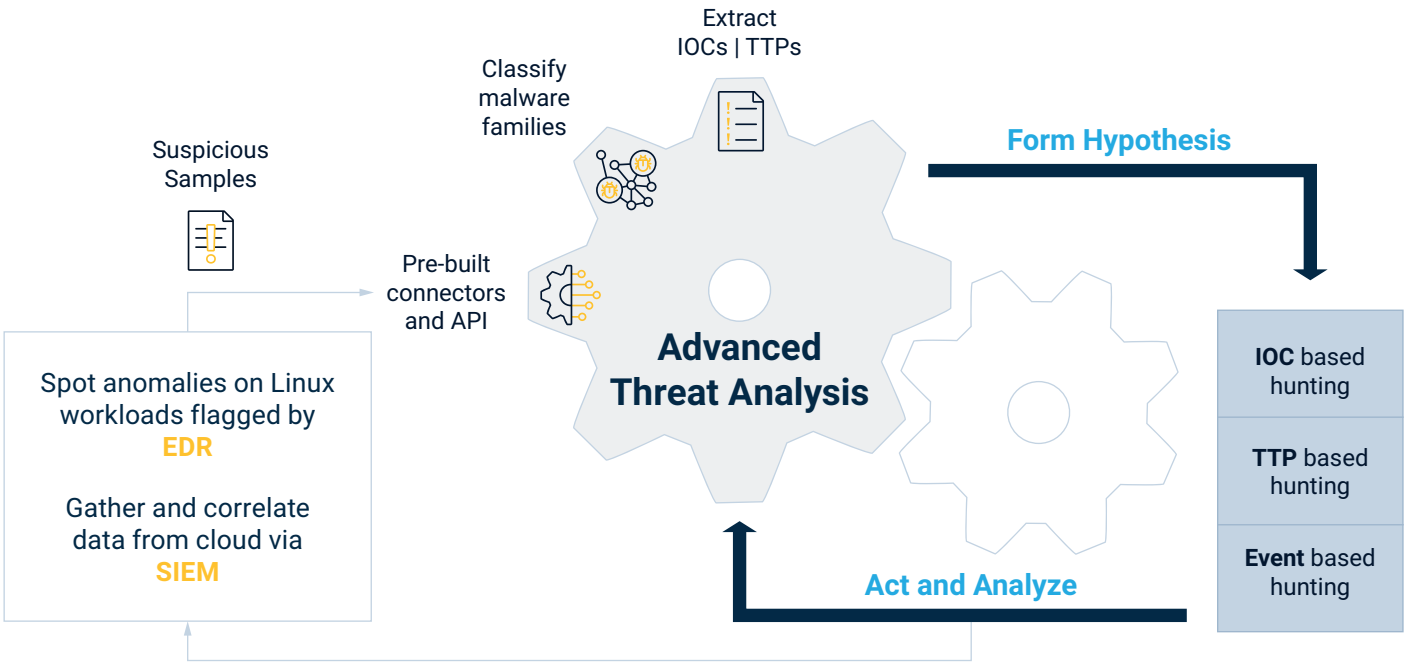
Linux systems in the cloud can act as stepping stones for more extensive campaigns. Identifying malware samples early can provide insights into larger, more complex attack strategies that encompass multiple platforms and environments.

4 Ongoing Evolution



As cloud services evolve, so does malware. Regular analysis of Linux samples allows threat hunting professionals to stay updated with the latest tactics, techniques, and procedures (TTPs) used by adversaries.

How can VMRay Improve Threat Hunting



The reliability of verdicts, MITRE ATT&CK TTPs, IOCs (Indicators of Compromise), and artifacts extracted from VMRay is crucial from a threat hunter perspective **for several reasons:**

1 Accurate threat identification

Accurate sandbox verdicts and IOCs ensure that threat hunters correctly identify and classify malware or other threats, reducing the risk of false positives or misidentifying the threat, which could lead to improper response and wasted resources.

2 Effective detection rules

VMRay allow threat hunters to create precise detection rules for SIEM and EDR systems. Reliable data ensures that these rules effectively detect and alert on relevant threats, minimizing false alarms and improving the overall security posture.

3 Efficient threat hunting

Reliable malware analysis reports enable threat hunters to focus their efforts on the most relevant threats and indicators, saving time and resources. Accurate data allows them to prioritize their investigations and remediation efforts, ensuring a more efficient threat hunting process.

4 Enhanced incident response

With reliable information from VMRay, threat hunters can better understand the nature of the threat, its capabilities, and its potential impact on the organization. This knowledge is critical in informing the incident response process, ensuring the appropriate containment, eradication, and recovery strategies are employed.

At VMRay, our purpose is to liberate the world from **undetectable digital threats**.

Based on the world's most advanced malware and phishing analysis platform, we enable enterprises, government organizations, and MSSPs to automate **security operations**, accelerate **analysis and response**, and build reliable **threat intelligence**.

In times of uncertainty and complexity, we create room for clarity and productivity to help security teams thrive.

Contact Us

Email: sales@vmray.com
Phone: +1 888 958-5801

VMRay GmbH

Suttner-Nobel-Allee 7
44803 Bochum • Germany

VMRay Inc.

75 State Street, Ste 100
Boston, MA 02109 • USA