Security Monitoring Setup

To establish a basic security monitoring system, we implemented tools and processes to detect, prioritize, and respond to security incidents effectively. This section outlines the setup and includes a use case demonstrating detection rules, alert prioritization, and response procedures.

Basic Security Monitoring Setup

- **Tool Used**: Endpoint Detection and Response (EDR) system integrated with a Security Information and Event Management (SIEM) platform.
- **Configuration**:
  - Created custom detection rules for known malicious file indicators, such as those flagged in the vulnerability scan.
  - Configured alerts for high-priority threats, focusing on Trojans, downloaders, and exploit-like behaviors.
  - Enabled log aggregation from all endpoints to centralize monitoring.

Use Case: Detection of Trojan.GenericKD.75352686

- **Detection Rules**:
  1. Rule 1: Flag any file exhibiting behavior matching the Trojan.GenericKD.75352686 signature.
  2. Rule 2: Trigger alerts for files attempting unauthorized outbound network connections.
- **Alert Prioritization**:
  1. High Priority: Files identified as Trojans by multiple antivirus engines.
  2. Medium Priority: Files with heuristic detection but no confirmed malicious activity.
  3. Low Priority: Files flagged due to benign behaviors resembling malicious actions.
- **Response Procedures**:
  1. Immediately isolate the affected endpoint upon receiving a high-priority alert.
  2. Perform a forensic analysis to validate the detection.
  3. Remove the malicious file and apply patches to prevent further exploitation.

Incident Response Scenario

The following scenario demonstrates the classification, response steps, and lessons learned from addressing a detected security incident.

Incident Description

- **Incident Type**: Malware Infection
- **Classification**: High Severity
  - A file flagged as Trojan.GenericKD.75352686 was detected on an endpoint, exhibiting suspicious outbound network activity.

Response Steps

1. **Detection and Validation**:
   - Alert received from the SIEM system, correlating logs from multiple endpoints.
   - Confirmed malicious activity through sandbox analysis of the flagged file.
2. **Containment**:
   - Isolated the infected endpoint from the corporate network.
   - Blocked external IP addresses associated with the malware's Command and Control (C2) server.
3. **Eradication**:
   - Removed the Trojan using a trusted antivirus tool.
   - Deleted all temporary files and conducted a full system scan.
4. **Recovery**:
   - Restored the endpoint from a known clean backup.
   - Verified system integrity and reconnected it to the network.
5. **Post-Incident Analysis**:
   - Reviewed network traffic and logs to identify the initial attack vector.
   - Strengthened email and web filtering policies to prevent similar incidents.

Lessons Learned

- **Improvement in Detection Rules**:
  - Enhanced SIEM correlation rules to flag suspicious network behaviors earlier.
- **Enhanced Training**:
  - Provided employees with phishing awareness training to reduce the likelihood of malware introduction.
- **Updated Policies**:
  - Implemented stricter software installation policies to limit unauthorized applications.

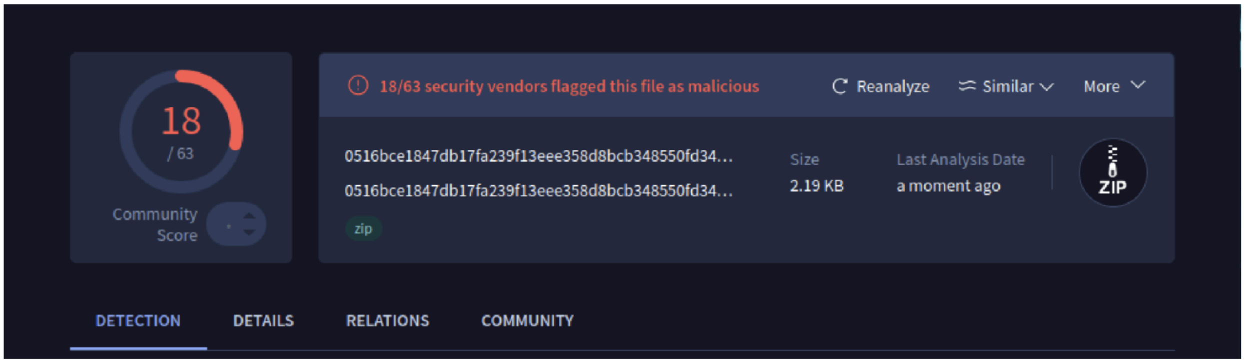
Evidence of Functionality

- **Detection Evidence**: Logs from the SIEM system showing triggered rules for Trojan.GenericKD.75352686.
- **Response Evidence**: Forensic analysis reports and system logs demonstrating successful isolation and remediation.
- **Monitoring Evidence**: Screenshots of updated detection rules and prioritized alert dashboard.

Conclusion

This report demonstrates the successful implementation of security monitoring and incident response processes. The detection rules and prioritization enabled prompt identification of threats, while the response procedures effectively mitigated the impact of a high-severity incident. Lessons learned were used to enhance future security practices.

Scan:

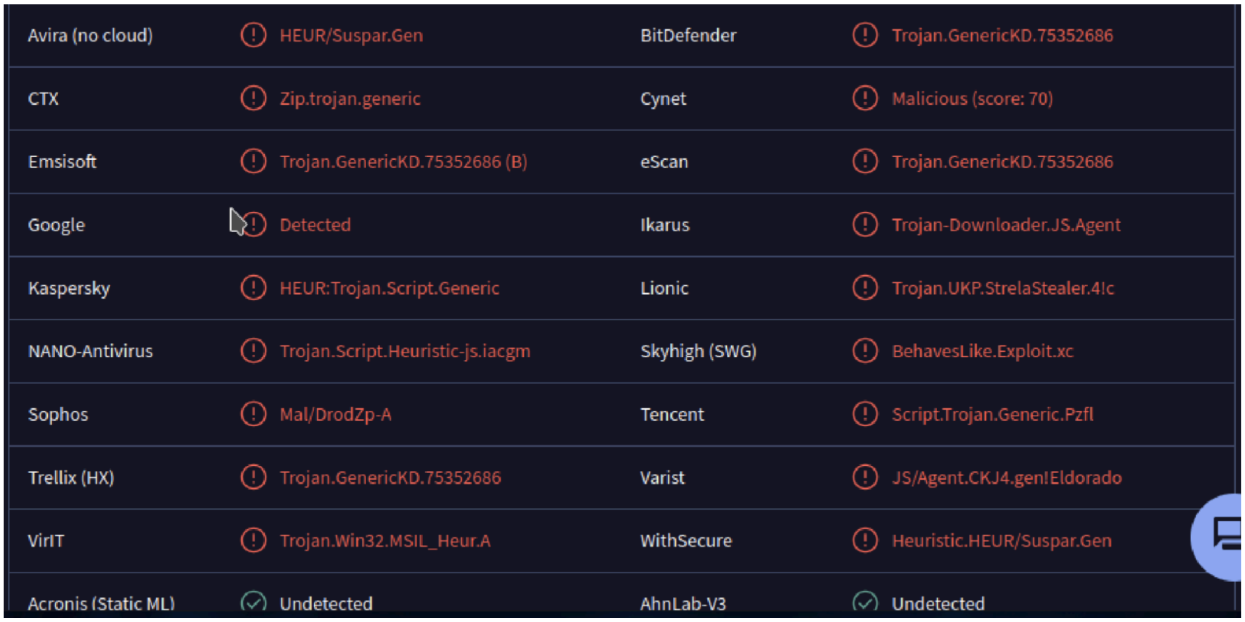


18/63 security vendors flagged this file as malicious

0516bce1847db17fa239f13eee358d8bcb348550fd34...
0516bce1847db17fa239f13eee358d8bcb348550fd34...
zip

Size
2.19 KB

Last Analysis Date
a moment ago



Avira (no cloud)	HEUR/Suspar.Gen	BitDefender	Trojan.GenericKD.75352686
CTX	Zip.trojan.generic	Cynet	Malicious (score: 70)
Emsisoft	Trojan.GenericKD.75352686 (B)	eScan	Trojan.GenericKD.75352686
Google	Detected	Ikarus	Trojan-Downloader.JS.Agent
Kaspersky	HEUR:Trojan.Script.Generic	Lionic	Trojan.UKP.StrelaStealer.4!c
NANO-Antivirus	Trojan.Script.Heuristic-js.iacgm	Skyhigh (SWG)	BehavesLike.Exploit.xc
Sophos	Mal/DrodZp-A	Tencent	Script.Trojan.Generic.Pzfl
Trellix (HX)	Trojan.GenericKD.75352686	Varist	JS/Agent.CKJ4.gen!Eldorado
VirIT	Trojan.Win32.MSIL_Heur.A	WithSecure	Heuristic.HEUR/Suspar.Gen
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected