CHECK POINT THREAT FORENSICS

THREAT FORENSICS

Intelligent threat containment and remediation

Product Benefits

- Identify and mitigate threats before significant damage is done
- Enhance threat prevention visibility
- Improve zero-day protection
- Add Indicators of Compromise (IoC) to the Check Point ThreatCloud

Product Features

- Complete forensic coverage, even for zero day threats
- Event storage independence
- Reduces network congestion
- Central management for queries
- Endpoint and gateway forensic reports

INSIGHTS

Every endpoint in the enterprise, remote or on premise, is a potential entry point for a security threat. Cyber-criminals know that if they can control an endpoint, then they can move laterally within an organization and access critical systems and data. If they are careful, then their activity may go undiscovered for months.

In an average enterprise[1]…

- every 60 seconds a host accesses a malicious website
- every 10 minutes known malware is downloaded
- every 24 hours a host is infected with a bot

Finding and analyzing this activity is difficult. Corporate security departments see thousands of alerts on a daily basis and must sift through volumes of data from different sources. Once they find an infected endpoint, the real detective work begins:

- How was the device compromised?
- Which files and processes are affected?
- Who else has the same files?
- What else was compromised?
- What should I do next?

Security teams need rock-solid forensic tools to contain and remediate these threats when they occur. Dissecting each step provides an understanding of the attack, the actor, and how to contain and remediate the threat.

SOLUTION

Our Check Point Threat Forensics solution identifies and mitigates threats before significant damage happens. A Threat Forensics agent monitors files, processes, and network activity on managed endpoints. When our threat prevention technologies detect an attack, either on the endpoint or on the network, then the agent automatically begins an analysis of the attack. It then uploads details of the event to the security management server. Here, endpoint and network security events are correlated to understand what, when, and how an event happened. This knowledge prevents similar breaches from occurring in the future.

[1] Source: Check Point 2014 Security Report

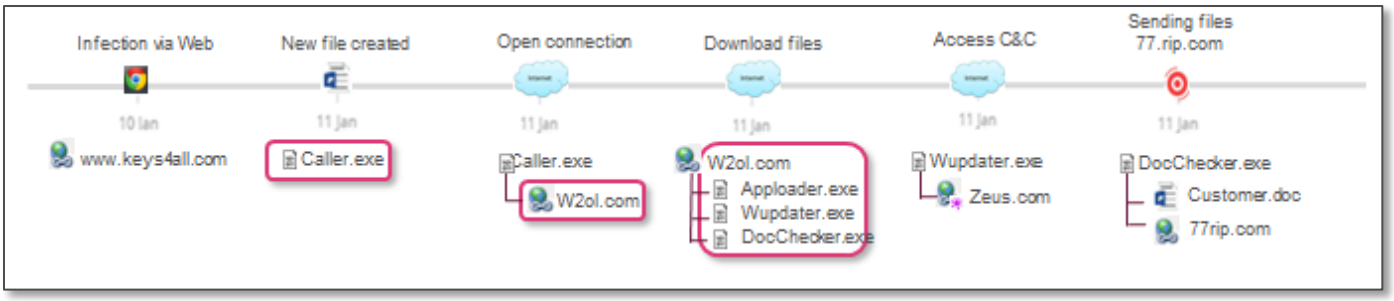


Figure 1: Attack Timeline

HOW IT WORKS

Endpoint Security Threat Forensics adds detailed intelligence to show the entire story of the attack - from the time of bot detection to the spear-phishing mail that was the entry point for the initial compromise:

1. Monitors and records all endpoint events
2. Collects attack details and analyzes the incident
3. Sends incident report and logs to management
4. Follows the attack timeline, containing the threat

ENDPOINT INTELLLIGENCE

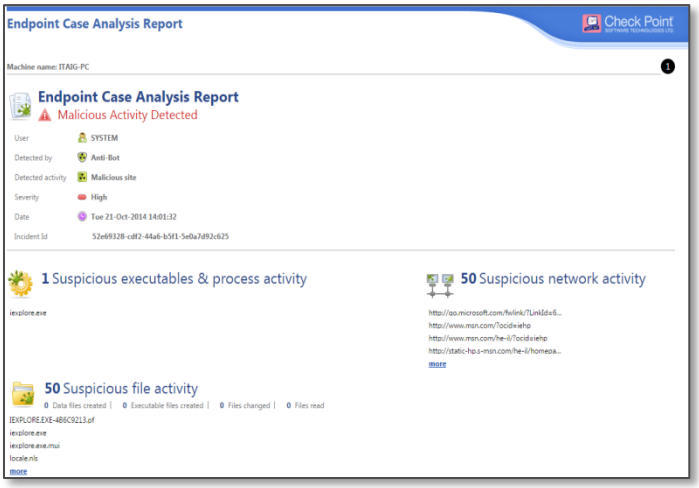
By monitoring and recording all endpoint events (including files affected, processes launched, system registry changes and network activity), we are able to trace and report on the steps taken by any malware, including zero-day threats.

All of the endpoint sensor data is efficiently stored on the endpoint itself, erasing the need for additional appliances. Even with thousands of endpoints, this distributed storage of endpoint events keeps traffic down and does not overload the network.

Our kernel level-sensors are secure and cannot be disabled by malicious processes.

INCIDENT REPORTS

Our Threat Forensics Solution allows you to view event reports from a central location like the endpoint security management server. Events that trigger the Incident Report creation may come from the endpoint itself or the gateway. Users can also generate reports for known malicious events, providing a detailed cyber kill chain analysis.



PRIORITIZED EVENTS

The sheer number of security events can be overwhelming. Our Check Point SmartEvent helps security teams by prioritizing events, letting them focus on the most important events.

SmartEvent aggregates and correlates network and endpoint events from our Next Generation Threat Prevention Appliances and Endpoint Security Suite. With the additional intel from Endpoint Threat Forensics, security teams have a better understanding of the attack and are able to mitigate security incidents more efficiently.

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com