Rapid7 UserInsight and FireEye TAP and Network NX

Detect and Investigate Compromised Credentials and Malware

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

- FireEye NX detects malware and FireEye TAP detects threats.
- Rapid7 UserInsight detects compromised credentials and sends alerts to FireEye TAP.
- Rapid7 UserInsight provides user context to FireEye NX malware alerts for investigations.
- Seamless integration between FireEye and Rapid7 through a lightweight collector.

OVERVIEW

For today's IT and security operations teams, the need for a clear vision from initial infection via malware or compromised credentials to incident detection and investigation is paramount.

While network security defenders focus on advanced malware, attackers are using compromised credentials to impersonate regular users to fly under the radar undetected. Most security programs can't detect this behavior, so an intruder's lateral movement goes unnoticed. Instead of focusing solely on the perimeter, organizations need detection in depth, covering endpoints, cloud services, and mobile devices.

THE CHALLENGE

Most security monitoring solutions report findings by IP address and flag those that are suspicious. But intruders often hide behind legitimate user accounts on the network. The challenge to overcome this approach is to understand normal user account activity and to identify when a user account is behaving outside of the norm and generate an alert for further investigation. Knowing the user context of an alert is often critical to understanding the impact of an attack and responding to the incident. Without contextual information about users identified in potential threats, all alerts must be investigated. This inquiry can quickly overwhelm most IT staffs.

Advanced attack groups take advantage of siloed security solutions and their inability to correlate the different pieces of a complex breach attempt.

When an attacker threatens a customer network, incident response teams face some tough challenges. Investigating incidents requires specialized expertise that few team members possess. What's worse, incident investigation tools are not optimized to provide answers quickly, wasting valuable time that could be used to mitigate a threat and prevent further damage.

THE INTEGRATED SOLUTION

The integrated solution from FireEye and Rapid7 adds user and account analysis to the FireEye Threat Analysis Platform (TAP). It augments the detection of advanced attacks and insider threats. This joint solution is designed to provide the deepest levels of context to detect, contain, resolve, and prevent threats.

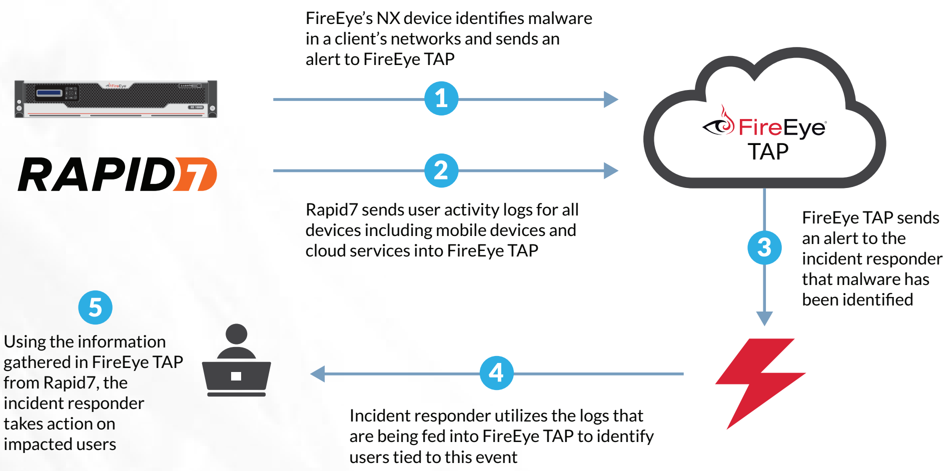
By adding additional data from Rapid7, TAP can aggregate and analyze disparate sets of data from across the network along with user behavior to produce actionable intelligence. This helps security teams and incident responders identify events that matter and prioritize their responses.

FIREEYE PRODUCT AND VERSION

Threat Analytics Platform (TAP) 12.01 and later versions are supported

RAPID7 PRODUCT

UserInsight



1 FireEye's NX device identifies malware in a client's networks and sends an alert to FireEye TAP

2 Rapid7 sends user activity logs for all devices including mobile devices and cloud services into FireEye TAP

3 FireEye TAP sends an alert to the incident responder that malware has been identified

4 Incident responder utilizes the logs that are being fed into FireEye TAP to identify users tied to this event

5 Using the information gathered in FireEye TAP from Rapid7, the incident responder takes action on impacted users

HOW THE JOINT SOLUTION WORKS TOGETHER

When deployed and configured to work together, the Rapid7 UserInsight collector consumes malware identification data from FireEye NX Network Security.

Rapid7 feeds activity logs into the FireEye Threat Analytics Platform (TAP) to provide a user context for suspected compromised credentials and threat analysis.

When suspected malware is detected, FireEye NX sends an alert to the FireEye TAP. The FireEye TAP applies threat intelligence, expert rules, and advanced security data analytics to noisy event data streams and generates an alert to the incident responder. By revealing suspicious behavior patterns and generating alerts that matter, security teams can prioritize and optimize their response efforts.

Using the Rapid7 UserInsight events fed to TAP, the incident responder investigates the suspected malware to identify the users tied to the event.

Using the integrated solution from FireEye and Rapid7, the incident responder can get the alert from FireEye NX in a matter of minutes and correlate that information with the logs that are being fed into FireEye TAP. This alert identifies the host and impacted user so that the responder can quickly get someone on the case to investigate further.

THE VALUE OF THIS PARTNERSHIP

Event data that may or may not represent a threat to network and data security inundates security teams. The partnership between FireEye and Rapid7 enables the integration of multiple products that can reduce the "noise" of superfluous and irrelevant data. Together they provide insight into authorized users and their activities. With UserInsight, the FireEye TAP correlates events in the context of typical and authorized user activity. This partnership supports fast decision making by the customer incident responder to determine which mitigation or remediation steps to take next to resolve the potential credentials compromise.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes 3,400 customers across 67 countries, including over 250 of the Fortune 500.

ABOUT RAPID7

Rapid7's IT security data and analytics solutions collect, contextualize, and analyze the security data needed to fight an increasingly deceptive and pervasive adversary. Unlike traditional vulnerability assessment or incident management, Rapid7 solutions uniquely provide insight into the security state of assets and users across virtual, mobile, private and public cloud networks.

For more information contact CSC@fireeye.com.