Integration Brief

Detect and Investigate Compromised Credentials and Malware with Rapid7 and FireEye

INTEGRATION BENEFITS

- Detect malware and compromised credentials
- Add user context to FireEye alerts
- Investigate FireEye findings in UserInsight
- Seamless integration through a lightweight collector

Solution Overview

Most monitoring solutions report findings by IP address but intruders often hide behind user accounts on the network. Knowing the user context of an alert is often critical to understanding the impact of an attack and responding to the incident – and it's often a lot harder than it sounds.

The joint solution enables security analysts to map findings from FireEye NX Network Security and FireEye Threat Analytics Platform to the user context provided by Rapid7 UserInsight. This enables you to easily correlate this information, even as users are assigned changing IP addresses, use various on-premise and cloud service accounts, and access email on mobile devices.

FireEye NX Network Security

FireEye NX Network Security helps enterprises detect and block attacks from the web. It protects the entire spectrum of attacks from relative unsophisticated drive by malware to highly targeted zero-day exploits. Its capabilities provide an extremely low false positive rate by leveraging the FireEye Multi-vector Virtual Execution (MVX) engine to confirm when malware calls out to C&C servers.

FireEye Threat Analytics Platform

The FireEye Threat Analytics Platform applies threat intelligence, expert rules, and advanced security data analytics to noisy event data streams. By revealing suspicious behavior patterns and generating alerts that matter, security teams can prioritize and optimize their response efforts.

Rapid7 UserInsight

Rapid7's UserInsight detects compromised credentials and enables you to view events, alerts, and incidents in a user context and to easily investigate them. UserInsight consumes data from FireEye NX Network Security and FireEye Threat Analytics Platform to investigate alerts in the user context. This gives you the ability to monitor the attack and identify which users are impacted and whose credentials were compromised.

How it Works

Once you have set up FireEye NX Network Security and Rapid7 UserInsight, the process is as follows:

1. Configure the Rapid7 UserInsight collector to consume data from FireEye NX Network Security

2. Data is automatically imported into Rapid7 UserInsight to enable investigations in the user context

3. UserInsight provides detection of compromised credentials in addition to the malware alerts provided by FireEye NX Network Security, giving you all-round incident detection

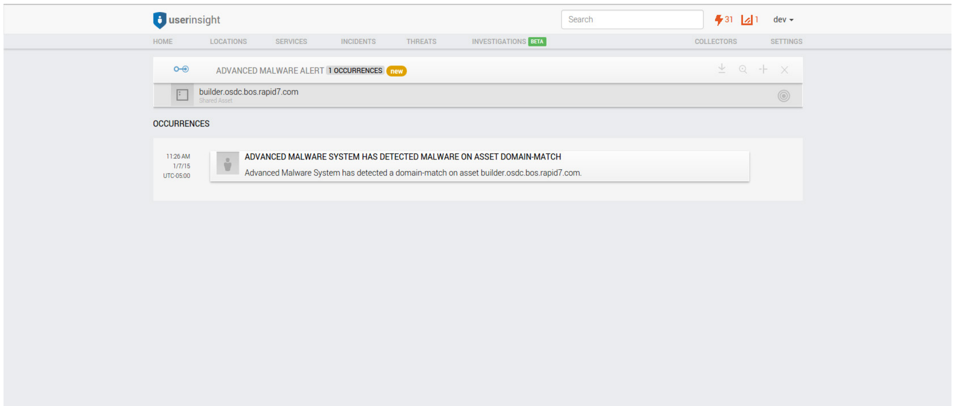
HOW IT WORKS

Configure FireEye NX Network Security to forward data to the lightweight Rapid7 UserInsight collector to see attacks in the user context.

WHAT YOU NEED:

- Rapid7 UserInsight
- FireEye NX Network Security
- FireEye Threat Analytics Platform

Combining powerful attack intelligence with fast and easy incident investigation



ADVANCED MALWARE ALERT 1 OCCURRENCES

builder.osdc.bos.rapid7.com
Shared Asset

OCCURRENCES

11:26 AM
1/7/15
UTC-05:00

ADVANCED MALWARE SYSTEM HAS DETECTED MALWARE ON ASSET DOMAIN-MATCH

Advanced Malware System has detected a domain-match on asset builder.osdc.bos.rapid7.com.

Figure 1: A user-attributed alert using combined information from UserInsight and FireEye

About FireEye, Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber-attacks. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber-attacks in real time. FireEye has over 2,200 customers across more than 60 countries, including over 130 of the Fortune 500.

About Rapid7

Rapid7's IT security data and analytics solutions collect, contextualize and analyze the security data you need 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 your assets and users across virtual, mobile, private and public cloud networks. They enable you to fully manage your risk, simplify compliance, and identify, investigate and stop threats faster. Our threat intelligence, informed by members of the Metasploit open source community and the industry-leading Rapid7 Labs, provides relevant context, real-time updates and prioritized risk. Our solutions are used by more than 25% of the Fortune 1000 and nearly 3,000 enterprise, government and small business organizations across 78 countries. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.