FIREEYE ANALYTICS

EXPERTISE-INFORMED DETECTION

ATTACKERS ARE USING YOUR TOOLS AND CREDENTIALS

The world doesn't stand still, not even for a moment. Not surprisingly, attackers don't stand still either. There is a fundamental shift in attacker behavior underway that the information security profession needs to understand and adapt to.

Advanced attackers are moving away from using malware and more towards using legitimate tools, often in tandem with stolen credentials to infiltrate and compromise organizations. Detecting these attackers in a timely manner is critical to minimizing both the information they steal and the damage they cause.

Originally, detection was performed using signatures. Of course, signatures were limited in that they only detected known knowns — that which was known to be malicious. To bolster the signature-based approach, we added the detonation layer. Adding the detonation layer gave us the advantage of being able to detect malicious binary files that were not yet known.

But how can we continue to ensure timely and accurate detection given the current shift in attacker behavior? This is where analytics becomes so important and specifically, adding a reliable, high-fidelity analytics layer to our detection capabilities.

Adaptive Detection Evolves as Quickly as the Attackers

There is no shortage of vendors marketing their analytics capabilities, but analytics at FireEye is different. Many vendors develop a bunch of algorithms and then go looking for a problem to solve. Unfortunately, analytics conceived without a fundamental understanding of the attacker only adds to the barrage of false positives facing practitioners.

At FireEye, we flip the analytics challenge on its head. Combining industry-defining incident response expertise with extensive adversarial, machine and victim threat intelligence gives FireEye a deep understanding of attacker behavior and methods. We leverage this unique vantage point to design algorithms that identify specific attacker behaviors — without the irrelevant noise.

HIGHLIGHTS

- **Investigative skills** - Technical & investigative skills developed over the course of hundreds of investigations.
- **Threat intelligence** - Profiles of key attack groups including their tools, practices and objectives along with corresponding Indicators of Compromise.
- **Technology** - Advanced tools that automate investigative tasks and enable network traffic and host-based artifacts to be rapidly evaluated — even across networks that contain hundreds of thousands of systems.
- **Management experience** - Experience providing guidance and advice on the business impact of computer security decisions.
- **Dedicated malware team** - A team focused solely on reverse engineering malicious software and researching the latest exploits.
- **Dedicated security research team** - Have studied hundreds of investigations to develop an intuitive understanding of attacker behavior.

FireEye

Analytics that Detect the Undetectable

Security leaders look to analytics as that third layer of detection to identify suspicious and malicious behaviors. Several use cases continually present themselves as a natural fit for an analytics solution:

- Insider Threat
- Lateral Movement
- Stolen Credentials
- Ransomware
- Theft of sensitive, confidential and proprietary data
- Persistent compromises
- Low-and-slow attacks

With global visibility, intensive knowledge of attacker behavior and our use-case based approach to detection, FireEye is ideally positioned in the analytics space. For you as a FireEye customer, that means easier deployment, actionable and high fidelity events and low noise.

All the makings of the analytics solution you've been waiting for.

Sample Analytics Detection Capabilities:

DNS Fast Flux

- Identifies domains that change IP address frequently, which is a common technique employed by malware for command and control purposes
- Provides an analyst with hunting leads to investigate potential malicious code infections
- Detects infections that may fly under the radar of many other detection techniques

Geofeasibility

- Identifies stolen or shared user accounts by examining whether the distance between two physical login locations is feasibly traveled within the specific time window
- Correlated with FireEye intelligence to increase confidence
- Correlated with credential misuse analytic to further increase confidence

Unacknowledged Connections

- Identifies potential command and control activity by looking for connection attempts that receive little to no response
- Detects command and control channels that may not yet be up or that may have already been taken down
- Allows an organization to proactively hunt down infections and data exfiltration risks before they result in data loss and exposure

Credential Misuse

- Identifies user accounts behaving like service accounts, which can often indicate credential theft or policy violation (credential sharing)
- Helps organizations that do not have a reliable list of service accounts identify service accounts
- Enables proactive hunting and analysis of activities indicating poor security hygiene that can expose an organization to significant risk

For more information on FireEye, visit:
www.FireEye.com

ABOUT FIREEYE, INC.

FireEye is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye