Cobalt Strikeout

F I R E E Y E M A N A G E D D E F E N S E I N A C T I O N

Sometimes, malicious activity can be hiding in plain sight, masquerading as legitimate activity that turns out to be more than what it appears.

In a recent instance, FireEye Managed Defense analysts began investigating an alert that showed suspicious activity occurring on a host in a customer’s environment.

Upon interacting, FireEye discovered that the customer was undergoing a legitimate penetration test at the same time this activity was taking place, to which this activity was initially attributed to.

Behind the scenes, Managed Defense analysts continued probing, leveraging resources within the FireEye Intel and TORE-Adversary Pursuit teams. Through collaborative efforts, analysts were able to determine this activity was indeed malicious and connected it to an intrusion that occurred previously at another customer within the same industry.

After reporting the findings, the customer decided to leverage their existing Mandiant Incident Response retainer, and the activity was quickly contained. If not for the front line experience and resources available to Managed Defense analysts and the customer, the outcome could have been worse.

PROBLEM:
Alert generated initially attributed as legitimate customer penetration test.

HOW WE DID IT:
Leveraged internal FireEye resources to investigate and confirm true attacker activity.

HOW WE DID IT BETTER:
Front line experience enabled Managed Defense analysts, Intel resources and the TORE-Adversary Pursuit team to connect the attacker activity occurring in this customers environment, to an intrusion that occurred previously at another customer within the same industry.

RESULT:
In under 4 hours, the FireEye team was able to discover, attribute and contain an aggressive threat actor that had disguised themselves to deeply infiltrate a customers environment.
Cobalt Strikeout

The Managed Defense team routinely collaborates with internal resources across all of FireEye to ensure the protection of our customers.

In this case, analysts were able to leverage Intel resources and the TORE-Adversary Pursuit team to connect live attacker activity found in this environment to an intrusion seen previously at another customer within the same industry.

It would be difficult to find another MDR service or Cyber Security Vendor that can collaborate and leverage all of its resources to discover, attribute and contain an aggressive threat actor that touched over 30 systems in under 4 hours.

**Business Impact**

- HX Alerts for Cobalt Strike
- Threat Assessment Manager Engages customer.
- Customer believes it is a red team exercise. Managed Defense thinks otherwise and continues investigation
- MD collaborates with internal Intel and TORE resources and attributes activity to true evil
- Mandiant Consulting Engaged
- Mandiant reviews activity and recommends containment
- Most recent attacker activity observed

- **101 Days**
  - Average days before a breach is detected*
- **$3.62 M**
  - Average cost of a breach**

*2018 Mirthness Report **2017 Ponemon Report
About Cobalt Strike

Cobalt Strike is a commercially available penetration testing platform with features and functionality that can cover the various stages of the attack lifecycle.