eSENTIRE®

INCIDENT REPORT

# Malicious Insider - A Laid Off Employee Takes a Parting Gift

**Attack Types:**
Malicious Insider

**Industry:**
Investment Banking

**The Threat:**

Malicious Insiders are employees, former employees, contractors or business associates who misuse access to sensitive information or privileged accounts within the network of an organization. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property or the sabotage of computer systems.

This was the case for one eSentire customer, an investment banking firm who were unaware that a recently laid off employee had used his access to exfiltrate sensitive intellectual property before his departure from the organization. Fortunately, eSentire's Security Operation Center (SOC) leveraging esINSIDER, along with data collected via esLOG, esENDPOINT and esNETWORK, discovered the malicious activity.

## THE PROBLEM

Insiders who use their computer access to steal proprietary data or intellectual property can cause significant business losses. Unfortunately, despite the potential negative impact, their malicious activity is often harder to detect and prevent. Because they use legitimate credentials to access data and information on company networks, their activity does not usually trigger an alert via most information security technologies in place at organizations.  To detect malicious insider activity, organizations must have behavior-based detectors in place in order to recognize routine network behavior, and flag abnormal activity.

## NORMALIZING NETWORK BEHAVIOR

This investment banking firm is a long time customer of eSentire, utilizing esENDPOINT, esNetwork and esLOG to protect their network. The customer added eSentire's esINSIDER to their portfolio of protection.

esINSIDER uses industry-leading machine learning algorithms to automatically map network behavior and continuously redefine situational awareness of the network. It looks to normalize network activity by learning behaviors. What looks strange one day may prove to be normal activity over time.  esINSIDER looks for three types of usually normal network activity which when performed together, may represent malicious activity - collection, reconnaissance and exfiltration of data. When at least two out of three of these activities are detected, an alert is triggered.

The customer was onboarded to the service and esINSIDER began collecting data and mapping normal network behavior. Within two weeks, esINSIDER learned enough to detect suspicious activity that had occurred.

## THE EXFIL-TRAITOR

The eSentire Security Operations Center (SOC) was alerted through esINSIDER to some unusual activity on the customer's network and a case was generated. Collection of data, followed by exfiltration to an unusual source was occuring. An employee who was informed of an impending layoff, had taken code that he had written for the company and uploaded it to a personal drive online before his time was up. The information taken was not personally identifiable information (PII) or data with malicious intent, however it did constitute theft of intellectual property (IP).

## THE INVESTIGATION

Once the case was generated by the eSentire SOC, the investigation began. An eSentire analyst performed an IP look-up and saw that the code was uploaded to a code repository online. The analyst pivoted to esENDPOINT to start digging on where the activity originated, which led directly to the employee's machine where they found evidence of the commands used to move the code. This was a legitimate process performed by a legitimate user, so it was not triggered as an attack by the company's endpoint security. The esINSIDER service allowed for the detection because it involved exfiltration of data from the company network to an unusual, or not normalized, host.

## OUTCOME

The nature of the security incident did not warrant immediate escalation procedures because it was a single incident that had already occurred while the user still had legitimate access. Since the user was no longer employed and their access had already been terminated, this was not an ongoing security threat. The customer was alerted and provided with details of eSentire's investigation to use as evidence, including logs of the user's activity and details of the intellectual property that was exfiltrated.