CASE STUDY:

Request for Information

COMPANY DESCRIPTION

A leading North American IT analytics company focused on providing data analytics and information technology software solutions and services for industries ranging from financial, insurance, real-estate, and government. This company employed the use of a third-party vendor to conduct continuous monitoring of their perimeter cybersecurity infrastructure.

ISSUE

This company received an assessment and several reports from the third-party vendor warning of possible cybersecurity issues (malware). The third-party vendor indicated that the internal systems were possibly:

- Communicating with known malicious systems and beaconing to an external command and control server; OR
- Being used to conduct data exfiltration.

The CISO and other leaders within the IT security department sought a means to validate the third-party vendor reports. The company also wanted to gain greater insight into the nature and scope of the threats to help them decide on an appropriate course of mitigation.

Challenge

The immediate challenge was to quickly research all of the intelligence data, which included a large data set associated with the third party vendor (complicated by a lack of specificity and context). The analyzed data would then need to be transformed into useful threat intelligence information that would:

- Identify meaningful trends;
- Narrow the focus of the research (areas of concern) to the most relevant contextual information that helps determine the potential risk, including any 2nd level indicators of compromise (indicators or IOCs) or patterns of behavior (e.g. Techniques);
- Help prove or disprove the veracity of the assessment and reports;
- If possible, uncover any previously unknown threats (e.g. tactical indicators or techniques); and
- Determine how best to address these threats in a timely and effective manner.

Solution

The company leveraged the Anomali Request for Information (RFI) Service to submit an RFI to the Anomali Threat Researcher team. The service was completed within a 48 hour window by experienced cybersecurity threat researchers and intelligence analysts.

Results

The RFI services were able to expedite the review of data by leveraging the research team's expertise and tools from Anomali. The team conducted general

analysis of the data, which pointed to a malware threat and:

- Provided trends concerning the threat, which indicated that it was:
  - A long standing piece of malware that is known within the industry (e.g. several years old);
  - Continuing to propagate globally (based on patterns found within the ThreatStream platform); and
  - Largely identified and reported by trusted groups and vendors that showed that it was concentrated in Western Europe
- Narrowed the focus to those threats that had the highest confidence of being malicious. This information was then used to create a curated list of indicators (~est. 200). This list contained predominantly Domain Names that could be used by the company to identify/block previously unknown outbound C2 and helped provide a view into the types of techniques potentially in use.

Further investigation into the *two primary indicators* (Domain Names associated with the malware) provided by the client's third-party SOC vendor helped to validate the maliciousness of the IOCs. Research and analysis of the first indicator revealed the following:

- The first indicator was associated with numerous Passive DNS records, which indicated that it was likely to be associated with a hosting environment. Through IOC expansion, the team identified associated Domain Names/URLs that a trusted sharing partner specified as being malicious. Further analysis of the data revealed that:
  - Several of the domains, including newly identified Passive DNS domains from the first indicator and others from the trusted partner, shared the same registration email.
  - The first indicator was also associated with another IP address. Ten different premium and open source intelligence providers and numerous sharing partners reported this IP address to be a Malware IP.

As a result, Anomali was able to assess with a high-level of confidence that the *Domain Name in question was malicious*. Research and analysis of the second IOC revealed the following:

- The Domain Name was associated with a group of other Domain Names. Of those, several were identified with a high-level of confidence to be malicious due to the domain appearing on a well-known and vetted Blackhole list. Additional analysis revealed that:
  - Several of the Domain Names shared the same registrant email as the first indicator, which linked the malicious nature of these IOCs.
  - The second Domain Name that was provided had a different IP address than was initially reported by the client. It should be noted that this was not something previously reported by the third party SOC vendor. Therefore, Anomali was able to provide a *new IP address* associated with the malicious activity.

Based on the above analysis, Anomali was able to provide the client with:

- A means to make better tactical decisions about the indicators.
- Additional information and context that could be used to:
  - Better understand the previously known and unknown tactical IOCs that should be monitored by the organization to limit malicious outbound activity; and
  - Search for any additional malicious patterns of behavior (e.g. C2 techniques) within the infrastructure.

FROM THE CUSTOMER

The Anomali/ ThreatStream team provided me an in-depth information with malicious IPs, Domains, compromised email address, and websites including hash files. The turnaround from time of request to time received was a couple of hours. The results were tremendous and information was more than expected. I am not surprised about what type of information Anomali/ ThreatStream provided since I have worked with the product. I am more impressed with the turnaround from the team. Anomali/ ThreatStream team was able to deliver a time sensitive information request without hesitation. This is a product I recommend to all my peers and organizations I come across.