CCS 2000

Threat Intelligence Report - Sample

Client details omitted
## Client Specific Threat Areas

The Cyber Intelligence collected and analyzed for Client 1, suggests there is a number of issues to be resolved. Overall, the threat posture assessed as **Elevated**.

## Threats Identified Summary

Over the period 5th January – 29th January a number of alerts identified; these are classified into **HIGH**, **MEDIUM** and **LOW** categories:

<table>
<thead>
<tr>
<th>Category</th>
<th>HIGH</th>
<th>MEDIUM</th>
<th>LOW</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>

These alerts are further broken down into Attack Intention, Data Leakage, Phishing, Brand Security, VIP and Exploitable Data categories:

<table>
<thead>
<tr>
<th>Category</th>
<th>1</th>
<th>3</th>
<th>3</th>
<th>0</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ATTACK INTENTION</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DATA LEAKAGE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PHISHING</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BRAND SECURITY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VIP</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EXPLOITABLE DATA</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Areas for Attention

This section will provide a summary of the areas of attention that Client 1 should consider, which for this sample report are not fully populated, as we would need to establish the key Business impact areas that Client 1 would like the report to focus upon, but as an example:

**Phishing - Potential fake domains**

We have detected several instances of registered domain names which may have been created with the intention of being used maliciously towards the company. The domain names detected are similar in nature to domain names owned by Client 1 which could mean that they have the ability to be used in phishing attacks.

Several of the domains have been registered using anonymity services in an attempt to keep the owner’s identity anonymous. A few of the domains are owned by known domain parkers and squatters with reports of spam attacks originating from them.

---

1 Cyber Threat Intelligence Overall Client Threat Assessment will range from LOW, ELEVATED and HIGH. These will be based on the monthly threat intelligence alerts received and the overall risk and impact on Client 1.
Data Leakage – Leaked Documents & Emails

A number of instances of leaked documents and emails have been detected. At least one of the emails has been posted without consent through the site WikiLeaks, known for leaking classified information. The other documents appear to have been posted legitimately, albeit potentially without Client 1 being aware. The documents could contain exploitable information which could aid a social engineering attack. The email found on WikiLeaks, originating from the Stratfor breach, contains recipients whose user credentials have also been leaked through the database dump.

VIP – Critical Credentials Leaked

As stated in a previous advisory we have detected an instance of data-leakage which contains critical information on a VIP member of Client 1. The information was detected from the infamous Stratfor leak and has since been posted on a number of different websites. If the issue has not been resolved, it is suggested that you return to the advisory for additional information.

Exploitable Data – Weak SSL Certificate

We have detected a potential weakness one of Client 1’s public facing domains. Some of the certificates used by the website hosted on these domains have been identified to be outdated/insecure. This is a potential security threat as weak certificates are often open to attack. While most Client 1’s websites do not require personal information to be parsed a few domains with login portals have been detected to use weak signatures.

Attack Intention – Potential Spam Campaign

We have detected a number of email addresses used by Client 1 which have been uploaded to the public email dump site Skymem. They are usually obtained after parsing other information through the site such as documents and news articles of which it will then select and display the addresses. Skymem is known to be used maliciously as the emails uploaded are often subject to spam as attackers target these public addresses in phishing campaigns etc.