HITRUST is currently monitoring Petya Ransomware’s Comeback, the latest outbreak which has targeted businesses in the Ukraine, India, France, Russia, and Spain. HITRUST will continue to monitor and update this Threat Bulletin.

The attacks utilize a new variant of the Petya ransomware and uses a fake Microsoft digital signature in the process.

UPDATE #1: This ransomware is using NSA’s EternalBlue code (image below).
UPDATE #2: This variant is using the same exploits as WannaCry, targeting SMB v.1 with the EternalBlue exploit and as such, the mitigation measures that were implemented for WannaCry v2.0 should cover this attack surface.

UPDATE #3: SHA256 IOCs include: 027cc450ef5f8c5f65329641ec1fed91f694e0d229928963b30f6b0d7d3a745 (sample file name: petwrap.exe)

f8dbadbafa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5 (sample file name: dllhost.dat)

Import Session

Session 221110 (0)

No Indicators for this import session.

Comments

T_Boardman (Licking Memorial Health Systems) on 2017-06-27 15:21:53 +0000

Breakdown of this particular strain of Petya


History

<table>
<thead>
<tr>
<th>Commenter</th>
<th>Action</th>
<th>Date</th>
<th>Time</th>
<th>Timezone</th>
</tr>
</thead>
<tbody>
<tr>
<td>elie.nasrallah (hitrustalliance.net)</td>
<td>Updated Report</td>
<td>2017-06-27 15:29:02</td>
<td>+0000</td>
<td></td>
</tr>
<tr>
<td>Trevor Boardman (Licking Memorial Health Systems)</td>
<td>Created Comment</td>
<td>2017-06-27 15:21:53</td>
<td>+0000</td>
<td></td>
</tr>
<tr>
<td>elie.nasrallah (hitrustalliance.net)</td>
<td>Created Report</td>
<td>2017-06-27 15:08:25</td>
<td>+0000</td>
<td></td>
</tr>
</tbody>
</table>