nuix
Homebrew: Developing your own threat intel

Chris Brewer, Chris Woods
About Us

Chris Brewer
Senior Forensic Investigator

Chris Woods
Director of Audit & Compliance
What? Where? How?
A service was installed in the system.
Service Name: PAExec-33636
Service File Name: %SystemRoot%\PAExec-33636\PA Exec.exe -service
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem
What data is valuable…
Where does it come from…
What are the use cases…
What do you use the data for…
What prevents you from using the data…
What does the intel “look like”?

- IOCs
- EDR rules
- Yara rules
## Latest Submissions

There are 10 submission(s) pending.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Input</th>
<th>Threat level</th>
<th>Analysis Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 10, 2018, 19:37 (CEST)</td>
<td>458f2e857a29e5d84e6383134d5a079325c9.xls.tar.gz.renamed cec1a48999baee85abcbabf4a7e03c2bb3b57f4e1f3274b569373b6774</td>
<td>suspicious</td>
<td>Threat Score: 35/100 AV Detection: 1% virus.office.qe2vmc Matched 9 Indicators</td>
</tr>
<tr>
<td>September 10, 2018, 19:36 (CEST)</td>
<td><a href="http://space3design.net/wp-content/uploads/XMMFZaM">http://space3design.net/wp-content/uploads/XMMFZaM</a> PE32 executable (GUI) Intel 80386, for MS Windows d8f6657b2601e59797e44f0f706ed5e8322f6b2878884df8f8e946f7a164c</td>
<td>malicious</td>
<td>Threat Score: 100/100 AV Detection: 23% Kryptik.FGN Matched 3 Indicators</td>
</tr>
<tr>
<td>September 10, 2018, 19:36 (CEST)</td>
<td>BlackGm.exe PE32 executable (GUI) Intel 80386 Mono/Net assembly, for MS Windows 3753cae6db841a59f9b3f2e9916f4e85a8a929a935947f29c137c</td>
<td>ambiguous</td>
<td>Threat Score: 35/100 AV Detection: Unknown Matched 14 Indicators</td>
</tr>
<tr>
<td>September 10, 2018, 19:35 (CEST)</td>
<td>AmericanEquipment.pdf PDF document, version 1.4 d2d5e953977d68982c95f9b574c203222636e6b24b76d6f7c21678ac56c4</td>
<td>no specific threat</td>
<td>AV Detection: Marked as clean Matched 8 Indicators</td>
</tr>
<tr>
<td>September 10, 2018, 19:35 (CEST)</td>
<td>allocate-653de4e666d004b0a951eefc97c19aa-signed.apk Zip archive data, at least v2.0 to extract 3a431f907b241b2c23a746b920d33959cf5dcd4c64f9d373c3a5c42b079</td>
<td>ambiguous</td>
<td>Threat Score: 35/100 AV Detection: 1% Suspicious.GEN/9470V727 Matched 5 Indicators</td>
</tr>
<tr>
<td>September 10, 2018, 19:34 (CEST)</td>
<td><a href="http://saidloitzamuda.com/J2YU0IMGZ/PAYROLL/Smallbusiness/Composite">http://saidloitzamuda.com/J2YU0IMGZ/PAYROLL/Smallbusiness/Composite</a> Document File V2 Document, Little Endian, Os: Windows, Version 6.1, C o _ 8e04c47475bc354092570dd77f7fadd658db7c9b6b2206b59d0e9a9b3c32a</td>
<td>malicious</td>
<td>Threat Score: 100/100 AV Detection: 67% Valxria Matched 26 Indicators</td>
</tr>
<tr>
<td>September 10, 2018, 19:33 (CEST)</td>
<td>honda09102018.pdf</td>
<td>no specific threat</td>
<td>AV Detection: Unknown</td>
</tr>
</tbody>
</table>

© 2017 Nuix
Company Background:
Construction and Engineering firm with offices worldwide

What they did:
Correlating single source IP's logging in to domain controllers using multiple user accounts. ~10 failed attempts within an hour

In their own words:
“… actually didn't give us nearly as bad of a FP count as we thought it would. This alert has caught nation states and pentesters a total of 4 times over the past year attempting to password spray while either internal or external”
Company Background:

Large power company in the Southwestern United States

What they did:

Count of unique ports scanned by a single source bucketed by day averaged by a total amount over 7 days to create a % chance that it is a "new" port scan or if it's a continued automated scan.

In their own words:

“…caught multiple pentesters who either got in or tried to hit our external networks just watching this alert”
Company Background:
   Large financial company in the United States

How it started:
   Office 365 brute force

How it escalated:
   Statistical analysis of connections to Office 365 revealed abnormal connection from 3rd party IT contract company
Questions?
FIND OUT MORE:

- www.nuix.com
- nuix.com/blog
- twitter.com/nuix
- facebook.com/nuixsoftware
- linkedin.com/company/nuix
- youtube.com/nuixsoftware