NETSCOUT Omnis IDS in Action Use Case – Exporting Events to Security Ecosystem to Troubleshoot Ursnif Malware

A new breed of cybersecurity threats has garnered extensive media coverage, with some industry reports citing a 900% increase in malware instances in calendar year 2020. However, as described in this Use Case, a malware attack need not be part of this new breed of cybersecurity threats in order to impair business service performance. Lastly, we know that it’s not if, but when the events happen, and whether organizations are truly prepared to address those events rapidly, succinctly, and with repeatable processes.

For the Security Operations (SecOps) team profiled in this Use Case, the NETSCOUT Omnis Intrusion Detection System (Omnis IDS) improved the efficiency of their malware identification and response processes. Omnis IDS also enabled SecOps analysts to use established workflows in their Splunk Enterprise security information event management (SIEM) remediation tool by enabling the universal forwarder to export events to Splunk for complete visibility and correlation with other security systems.

**Issue**

As part of their daily network monitoring activities, the company’s SecOps team identified a potential security event, which prompted issuance of associated service ticket.

In response, a front-line Tier 1 Security Analyst used the NETSCOUT Omnis IDS to conduct preliminary investigation into this event, recognizing that solution allows for effective and timely event response as incidents occur, which is critically important to SecOps teams everywhere.

**Impact**

Given the location of security event across data center operations and the user’s information regarding the impact on host server performance, transaction delays associated with this issue could result in lost productivity or, in a worst-case scenario, service downtime.

**Troubleshooting**

Accessing network events data aggregated by Omnis™ IDS Sensors deployed across the company’s network, the Tier 1 Analyst commenced the investigation workflow by using the Omnis™ IDS Manager Explorer Timeline, Filter and Search, and Total Events Counter features.

As part of this initial investigation, the Tier 1 Analyst contacted the internal user identified as potentially being impacted by this event. While this user reported issues with a host server running sluggishly (even confirming or affirming the host’s IP address address), the employee could not identify any recent actions or configuration changes that could be linked to potential root cause.

Even at this initial stage of the investigation workflow, using Omnis IDS, the Tier 1 Analyst could see there was a high number of events in the general report timeframe identified in the service ticket – nearly 200,000 of them, to be exact. As exhibited in Figure 2, however, a high volume of them were associated with two IP addresses, with Omnis IDS immediately easing the workflow for the Tier 1 analyst as a result.

Narrowing the IDS Explorer event timeline to correspond to the user-reported service issue enabled the Security Analyst to see relevant details associated with the host server IP address (10.1.21.101) initially shared by the user and recorded in the service ticket.
Figure 1: The front-line Tier 1 Analyst used Omnis IDS to commence the initial investigation workflow, with IDS Explorer providing a Timeline of Events and Bytes (upper panel), a Filter and Attribute window (for quick access to events and threats), and a Total Events Counter (for a given timeframe).

Figure 2: While the number of events displayed by the IDS Explorer’s Event Counter was high, the IP Initiator widget on the lower right panel showed high volumes of them were associated with IP addresses 10.1.21.101 and 10.0.2.103.
Figure 3: The IDS Explorer Event List reflected the entire kill chain of techniques used to accomplish their tactic. This composite view of malicious traffic for techniques was presented in chronological order, including the Ursnif malware highlighted in the IDS Message panel on the right.

<table>
<thead>
<tr>
<th>Event Timestamp</th>
<th>IP Initiator</th>
<th>IP Responder</th>
<th>Port Initiator</th>
<th>Port Responder</th>
<th>Application</th>
<th>Bytes</th>
<th>IDS Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021-03-18 04:43:56 AM</td>
<td>10.1.21.101</td>
<td>162.0.224.165</td>
<td>49775</td>
<td>80</td>
<td>dns</td>
<td>607 bytes</td>
<td>ET INFO - Dotted Quad Host RAR Request</td>
</tr>
<tr>
<td>2021-03-18 04:43:56 AM</td>
<td>10.1.21.101</td>
<td>208.61.222.222</td>
<td>52729</td>
<td>53</td>
<td>dns</td>
<td>76.6 bytes</td>
<td>ET POLICY - External IP Lookup Domain [myya.apprimo.com] in DNS Lookup</td>
</tr>
<tr>
<td>2021-03-18 04:43:56 AM</td>
<td>10.1.21.101</td>
<td>208.61.222.222</td>
<td>52729</td>
<td>53</td>
<td>dns</td>
<td>76.6 bytes</td>
<td>ET POLICY - External IP Lookup Domain [myya.apprimo.com] in DNS Lookup</td>
</tr>
</tbody>
</table>

Figure 4: The list exported list of events from IDS Explorer included highlighted IDS Message details on the Ursnif malware threat associated with the host server.
Figure 5: The Splunk SIEM interface includes integrated Omnis IDS event details in the lower right panel of this example screen.

Figure 6: The IDS Explorer provided event context to the Tier 2 Analyst to confirm a malicious binary download had occurred, including the highlighted details regarding emerging threats signature (upper left panel), source and destination IP (lower left panel), and conclusive event evidence (center panel).
Figure 7: Omnis Cyber Investigator provided the Tier 3 Analyst with an expanded view of all hosts, including listing the containment field, good vs. threat traffic, and a GeoIP list of Top 10.

Figure 8: Cyber Investigator confirmed presence of the Ursnif malware and evidence that many of the security ecosystem’s cybersecurity tools had not detected it.
By entering an IDS Filter attribute using that IP address, the Tier 1 Analyst updated all the displayed events down to those only related to that specific IP address, with the workflow then involving reducing the time period to minutes to generate a smaller data set with which to work. As exhibited in Figure 3, the end result of this workflow involved IDS Explorer sequentially listing various events for the IP address, including details on threats and exploits.

Using Omnis IDS in this manner, the Tier 1 Analyst was able to access IDS classifications related to malicious traffic and quickly visualized in the IDS Message Details that this was an Ursnif malware instance associated with the host server.

Ursnif is a network trojan that exploits users’ systems as part of re-purposed malware. Ursnif is of relevance to any SecOps team, with this malware surfacing in numerous attacks on Japanese banking institutions in 2018, as reported by the NETSCOUT® ATLAS® Security Engineering and Response Team (ASERT). At this stage of the investigation workflow, the Tier 1 Analyst provided an Omnis IDS Threat Summary for handoff to the Tier 2 Analyst managing incident response. As part of that Threat Summary, the Tier 1 Analyst forwarded list of events surrounding that threat (as exhibited in Figure 4).

At this point, the Tier 2 Security Analyst used the NETSCOUT Omnis Application for Splunk to leverage the company’s long-established SecOps workflows for event aggregation, analysis, and reporting in their Splunk Enterprise SIEM solution. With this application, the Tier 2 Security Analyst could access all exported Omnis IDS event data in Splunk. With the export of Omnis IDS event data into the Security Operations ecosystem, the Tier 2 Analyst used existing user interface workflows, as well as trends and timelines, with the ability to pivot to the Omnis IDS solution. Of particular relevance, the Tier 2 Analyst had access to integrated Omnis IDS event details, including alert signatures (as exhibited in Figure 5.)

The Tier 2 Analyst then used Splunk to validate that the event details provided by Omnis IDS corresponded to related events within Splunk (including use of the same destination IP and Source IP), with the workflow subsequently transitioning from Splunk to Omnis IDS.

At this point, the Tier 2 Analyst used IDS Explorer to access the event details and validated that the internal host had in fact downloaded the malware (as exhibited in Figure 6).

Remediation
At this point in the workflow, the service ticketed was transitioned to a Tier 3 Security Analyst to commence remediation activities. Event details were forwarded to the company’s NETSCOUT Omnis™ Cyber Investigator solution, an enterprise-wide network threat and risk investigation platform, which enabled the Tier 3 Analyst to examine the Ursnif malware instance in the context of the company’s cybersecurity policies and take necessary actions for containment and prevention of future occurrences.

The Tier 3 Analyst used the Cyber Investigator host investigation interface to identify the cyber threat, confirm a threat on the external host, and identify a compromised internal host. By contextually drilling down from the internal host icon displayed on the Cyber Investigator interface, the Tier 3 Analyst expands the view to all hosts communicating with the internal host. This remediation workflow process enabled the Tier 3 Analyst to determine that the possible containment field needed to be expanded to factor collateral hosts.

In providing additional verification to the Tier 3 Analyst, the workflow then transitioned to include the Omnis Cyber Investigator packet decode functionality, which confirmed the Ursnif-related file had been downloaded by the internal host. Using Omnis Cyber Investigator, the Tier 3 Analyst forwarded a corresponding packet capture export to the Forensic Security team. In integrating across this additional layer of the security ecosystem, SecOps not only had executive-level visual confirmation of a current and active Ursnif malware, but evidence that only half of the company’s cybersecurity solutions had detected that threat.

In this instance, SecOps revised the company’s perimeter security policy, including updating their NETSCOUT Arbor Edge Defense® (AED) threat detection and DDoS mitigation solution configured at the perimeter edge with a threat filter to mitigate all subsequent traffic and mitigation policy.

Additionally, SecOps was presented with the option to configure their Cyber Investigator solution to use a block command to enable a “blocking host” change.

With these adjustments, the SecOps team had secured the company’s perimeter policy to protection organizational resources.

Summary
In this case, the SecOps team was able to take advantage of Omnis IDS functionality and forward rich event data to Splunk, which enabled use of monitors, workflows, and dashboards familiar to them, while also helping to expedite the evaluation. In taking advantage of the company’s investment in NETSCOUT’s Omnis Cyber Investigator and AED solutions, SecOps made necessary adjustments to organizational security policies to negate the impact of this malware threat and protect the company from future occurrences.

In this manner, Omnis IDS enabled the SecOps team to remediate this malware instance before it could possibly have resulted in taking business services offline.