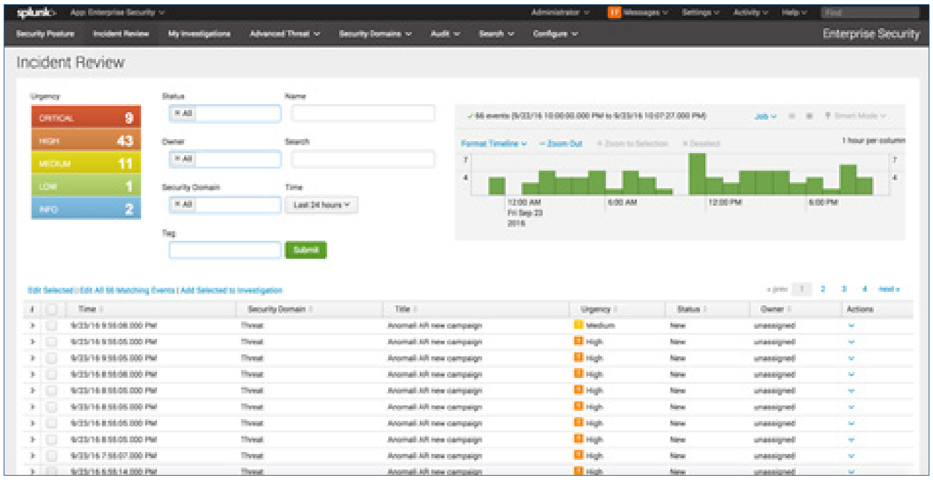
Anomali Adaptive Response App for Splunk

Anomali supports the Splunk Adaptive Response Initiative, delivering rich context regarding IOCs, actors and campaigns seamlessly within the Splunk interface.

- Anomali integrates threat intelligence from the following:
  - Anomali Labs
  - 3rd party sources
  - Open source intelligence
  - Anomali community
- Anomali delivers IOC feeds to Splunk to identify matches against customer log events.
- Splunk displays the matches in the Incident Report view.
- An individual match indicates a single IOC was detected.



Incident Review

Urgency

CRITICAL	9
HIGH	43
MEDIUM	11
LOW	1
INFO	2

Status: × All

Name:

Owner: × All

Search:

Security Domain: × All

Time: Last 24 hours

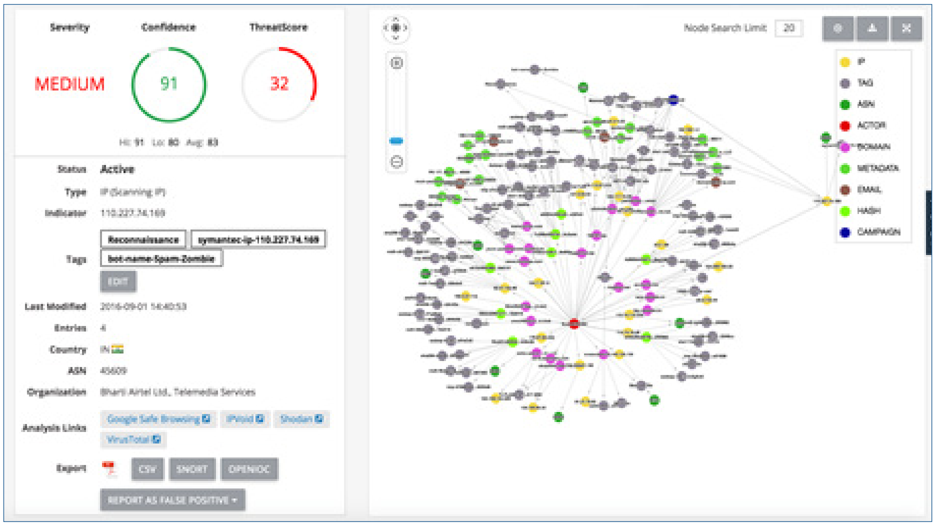
Tag:

✓ 56 events (9/22/16 10:00:00.000 PM to 9/23/16 10:07:27.000 PM)

i	□	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	□	9/23/16 9:55:08.000 PM	Threat	Anomali: AR new campaign	Medium	New	unassigned	⌄
>	□	9/23/16 9:55:05.000 PM	Threat	Anomali: AR new campaign	High	New	unassigned	⌄
>	□	9/23/16 9:55:05.000 PM	Threat	Anomali: AR new campaign	High	New	unassigned	⌄
>	□	9/23/16 8:55:08.000 PM	Threat	Anomali: AR new campaign	High	New	unassigned	⌄
>	□	9/23/16 8:55:05.000 PM	Threat	Anomali: AR new campaign	High	New	unassigned	⌄
>	□	9/23/16 8:55:05.000 PM	Threat	Anomali: AR new campaign	High	New	unassigned	⌄
>	□	9/23/16 8:55:05.000 PM	Threat	Anomali: AR new campaign	High	New	unassigned	⌄
>	□	9/23/16 8:55:05.000 PM	Threat	Anomali: AR new campaign	High	New	unassigned	⌄
>	□	9/23/16 7:55:07.000 PM	Threat	Anomali: AR new campaign	High	New	unassigned	⌄
>	□	9/23/16 6:55:14.000 PM	Threat	Anomali: AR new campaign	High	New	unassigned	⌄

However, that specific IOC is likely associated with an actor and campaign, for which hundreds of other IOCs may be related.

- Anomali maintains this relationship information
- We see the IOC is a single datapoint in a much larger security threat
- To get full context of the potential breach we need to search for all related IOCs



Severity	Confidence	ThreatScore
MEDIUM	91	32

Hi: 91 Lo: 80 Avg: 83

Status: Active

Type: IP (Scanning IP)

Indicator: 110.227.74.169

Tags: Reconnaissance, symantec-ip-110.227.74.169, bot-name-Spam-Zombie

Last Modified: 2016-09-01 14:40:53

Entries: 4

Country: IN

ASN: 45609

Organization: Bharti Airtel Ltd., Telemedia Services

Analysis Links: Google Safe Browsing, IPVoid, Shodan, VirusTotal

Export

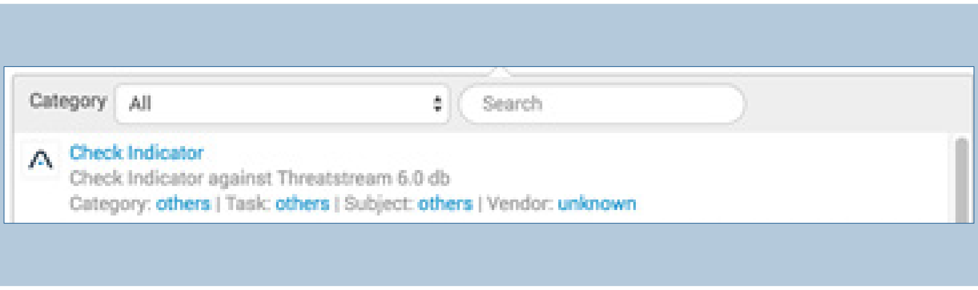
With the Anomali integration and Splunk Adaptive Response, users can perform this analysis with a single click, without ever leaving the Splunk console. Simply select Anomali Check Indicator.

The Anomali App for Splunk then presents all associated IOCs, in the timeline, with categorization for each step of the Kill Chain model. In one single view, organizations can see the extent of a potential breach that started with a single IOC detection.

2317 Broadway, 3rd Floor, Redwood City, CA 94063 USA
1-408-800-4050 | info@anomali.com | www.anomali.com

Anomali Adaptive Response App for Splunk

With the Anomali integration with Splunk Adaptive Response users can perform this analysis with a single click, and without ever leaving the Splunk console. Simply select Anomali Check Indicator



Category: All

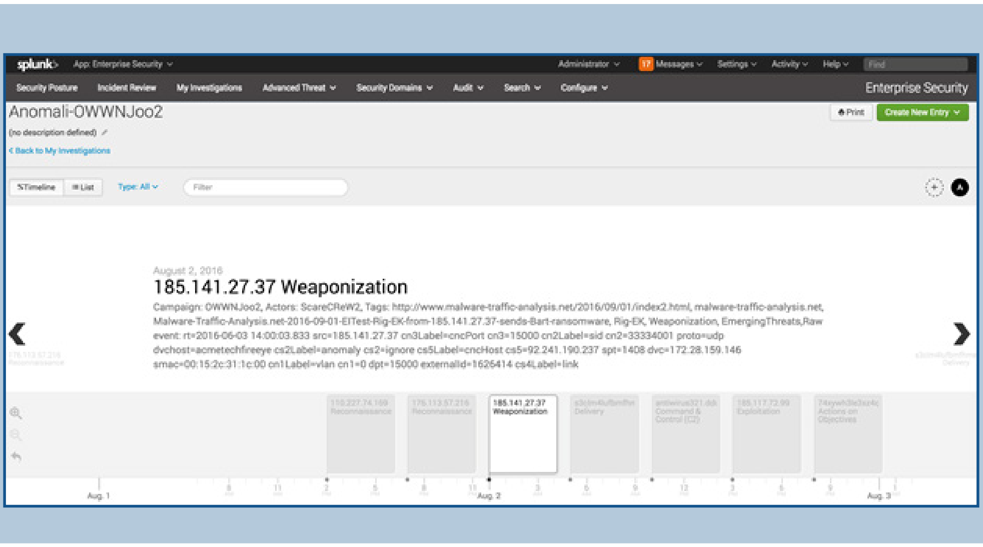
Search

Check Indicator

Check Indicator against Threatstream 6.0 db

Category: others | Task: others | Subject: others | Vendor: unknown

The Anomali app for Splunk then presents all associated IOCs, in the timeline, with categorization for each step of the Kill Chain model. In one single view organizations can see the extent of a potential breach that started with a single IOC detection.



Anomali-OWWNJoo2

(no description defined)

< Back to My Investigations

August 2, 2016

185.141.27.37 Weaponization

Campaign: OWWNJoo2, Actors: ScareCReW2, Tags: http://www.malware-traffic-analysis.net/2016/09/01/index2.html, malware-traffic-analysis.net, Malware-Traffic-Analysis.net-2016-09-01-EITest-Rig-EK-from-185.141.27.37-sends-Bart-ransomware, Rig-EK, Weaponization, EmergingThreats,Raw event: rt=2016-06-03 14:00:03.833 src=185.141.27.37 cn3Label=cncPort cn3=15000 cn2Label=sid cn2=33334001 proto=udp dvchost=acmetechfireeye cs2Label=anomaly cs2=ignore cs5Label=cncHost cs5=92.241.190.237 spt=1408 dvc=172.28.159.146 smac=00:15:2c:31:1c:00 cn1Label=vlan cn1=0 dpt=15000 externalId=1626414 cs4Label=link

110.227.74.169 Reconnaissance

176.113.57.216 Reconnaissance

185.141.27.37 Weaponization

Delivery

Command & Control (C2)

185.117.72.90 Exploitation

Actions on Objectives

About Anomali

Anomali^{TM} is the pioneer of an enterprise class threat intelligence platform, combining comprehensive threat data collection, prioritization, and analytics with secure collaboration in a vetted community. Offering the broadest enterprise security infrastructure integration available, the ThreatStream platform enables organizations to proactively identify and combat cyber threats targeting their operations.

2317 Broadway, 3rd Floor, Redwood City, CA 94063 USA
1-408-800-4050 | info@anomali.com | www.anomali.com