## Finding a Leaking Device from the Portal

This 14-second video steps illustrates one way to investigate a leaking device from the Lumeta 3.3 Portal. A larger, higher-resolution view of the same is available here.



## The step-by-step procedure is here:

1. Let's assume you notice the Command Center on your Lumeta Portal beaconing a warning.



2. You open the notifications window to see what warnings have been issued. Several leaks have been found. You open the link for the first leaking IP address.

SOECTRE <sup>0</sup> Series						Lateria	
Command Center Map							
	(Annual State						
Search reditorities	Name		▼	Device IF Address	Nessan	Www	
alex co-327 cap-33	Less Discovered	1048N	GAMMETERMENT	6538,244.00	Device 65,318,214,80/32 is found 1	3/13/18 3.32.06 PM	I.
alex-cc-327-up-33	Leek Discovered	1048N	GAtestZane001	10.8.0.62	Device 13.9.3.62/32 is found to be	5/15/18 2:02:06 PM	
ates cc-327 cp-33	Device Discovered	NFO	Zanet	10.8-0.62	Device 12.9.3.62/32 cmiled.	3/13/18 3.17.12 PM	
alex-ec-527-up-33	Leek Discovered	1048N	GAtestZane001	65,248,244,92	Device 65.246.244.82/02 is found t	5/15/18.2111-42.PM	
ates cc-327 cp-33	Device Discovered	NFO	QANNED Invedice	65.218.214.92	Device 65.218.214 XU22 created.	3/13/18 3.11.33 PM	
alex-ec-327-up-33	QAtestilication001	NPD	GAtest/2srell()	65,248,244,92	Device 65.246.244.82/92 created.	5/15/18 2:11:03 PM	
atex co-327 up-33	GAMENO/BUILDINGD4	NFO	GAMMETERMENT	65218214.02	Device 65.318.214 83/32 cristed.	3/13/18 3.11.33 PM	
alex-ec-327-up-33	Leok Discovered	1048N	GAtest2ane001	10.8-0.62	Device 13.9.3.62/32 is found to be	5/15/18 2:10:41 PM	
abox co-327 cap-33	Ewolee Eliscowerd	NFO	GAMMETane001	13.8.0.62	Device 13.9-3.62/32 cmilled.	3/13/18 3 10:33 PM	

3. By following that link, you navigate to the device's location in its zone map and can also see that the device is active.



4. Right-click on the device to look more closely at its details.

🖬 🖉 🗷 🗮 Group + Mangangar - 🔍 Seasca -	2. ALERT Q+	B NO D
	65.246.242.14(0.201.0.8 Lagest	Highlighting
2 9	65.246.244,10 <sup>(1)</sup> .100.10.210.201.0.17	Activn 2
	65.286.244.35 <sup>3,240,241,1</sup>	
	10.201.0.965 246 246 151	
	65 246 246.53 10.2011.0.46 +	
	A See Mr With Manager A See Mr With Manager 10.359 10.5	
	65.246.244 232 65.246.244 232 65.246.244 233 65.246.244 233 65.246.244 236 246.24	

5. On the Leak Response tab, we learn that device 65.246.244.92 has both an inbound and an outbound leak path over Port 80.

SPECTRE	a -	1 Plead Doly User -
alex-os-327-up-33 - Device Details		
Enter IP, MAC, or System Name. GAtestZaretter • Beach		
65.545.944.92 (c)		
Device Info Device Profile Attributes Interfaces Connected Hosts - Laper 3	Open TCP Ports Cleased TCP Ports Lank Desparant Medilications Alternate D	Cisco prühid
Discovery Type	Pretocol	Pot
Leek - Inbound	ionp.	
Leak - Dulbound	king .	
Least - Maximal	sp.	80
Leak - Dulbound	Np.	80
Contraction and Constant		

6. On the Notifications tab, we learn the time and date of when the device was found to be leaking.

vice in	b Device Profile	Atributes Int	reference Connected Hosts - Lape	er 3 Open TCP Per	ta Closed 10P Ports Les	uk Response - Notices	Alternate Pa Ci	sce pelitid		
ww	Type	Time	Message		Azknowledged		Acknowledged By		Acknowledged Time	
κ.	LERK, DISCOVERED	091300181533	Device 65.316.214.83/02 is found to	be teaking inbound	tano					
	LEAK, DISCOVERED	0013201815:11	Device 68.246.244.82/32 is found to	be looking eufbound	Miter					
۰.	DEVICE_DISCOVERED	031320181511	Device 65.316.244.82/32 predict.		Salao					