Incident IN00000017

Export Time: 2025-10-13T10:42:51-07:00

Incident ID	IN00000017	Incident Name	Storage Threat Detection against user name demouser@adcto1.test from host 172.31.1.45, Alert ID 3124
Severity	Critical	Incident Category	Malicious Code
Status	New	Assigned To	
Incident Source		Incident Reporter	Superna Data Security Edition
Affected Endpoint	demouser@adcto1.test	Affected Endpoint IP	
Tactics	Impact	Technique	T1486
Incident Detect Time	2025-10-13 09:38:14 PDT	Last Update Time	2025-10-13 10:41:03 PDT
Description	User: demouser@adcto1.test Client IP: 172.31.1.45 Alert ID: 3124 SMB Shares: - marketing (DR:/ifs/data/marketing) - igls-dfs-dfsprod (DR:/ifs/data/dr/dfs) - dfsprod (production:/ifs/data/dfs) - marketing (production:/ifs/data/marketing) Files: - \\production\data\ifs\data\dfs\my data - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy (2) - Copy - Copy.locky - \\production\data\ifs\data\dfs\my data - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy (11) - Copy.locky - \\production\data\ifs\data\dfs\my data - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy (5).locky - \\production\data\ifs\data\dfs\my data - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy (6) - Copy - Copy - Copy.locky - \\production\data\ifs\data\dfs\my data - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy - Copy (3) - Copy - Copy - Copy.locky - ...5 more	Last Comment	

Events

No Data

Comments

No Data

Endpoints

No Data