CTD Alert Report

Produced by CTD on Thursday, Mar 28, 2024

SuspiciousFileTransferAlert

Suspicious file transfer found! File 'program 3' was transferred via 'TRISTATION' and matched the following Yara rules: ['MALWARE_(Claroty_ICS_Triton).yar/triton_download_payload'], Transferred from 10.10.7.43
Alert Score: 100

Status: Unresolved

Alert Details

10.10.7.43

IP	MAC	Network
10.10.7.43	14:B1:C8:00:A8:91	Default

Vendor	Asset Type	Host Name
InfiniWing	Engineering Station	-

Name	Firmware version	Risk Level
10.10.7.43	-	Low

Site	Parsed Asset	Virtual Zone
CyberX	No	Engineering Station: Tristation

10.10.6.81

IP	MAC	Network
10.10.6.81	40:00:00:5D:3F:22	Default

Vendor	Asset Type	Host Name
Triconex	PLC	-

Name	Firmware version	Risk Level
10.10.6.81	TSX: 6271	High

Site	Parsed Asset	Virtual Zone
CyberX	No	PLC: Tristation

Events Details

ID	DESCRIPTION	TYPE	TIME
801	Suspicious file transfer found! File 'program 3' was transferred via 'TRISTATION' and matched the following Yara rules: ['MALWARE_(Claroty_ICS_Triton).yar/triton_download_payload']	Suspicious File Transfer	16/03/2024 08:10:30 UTC
807	Suspicious file transfer found! File 'program 3' was transferred via 'TRISTATION' and matched the following Yara rules: ['MALWARE_(Claroty_ICS_Triton).yar/triton_download_payload']	Suspicious File Transfer	16/03/2024 08:10:30 UTC