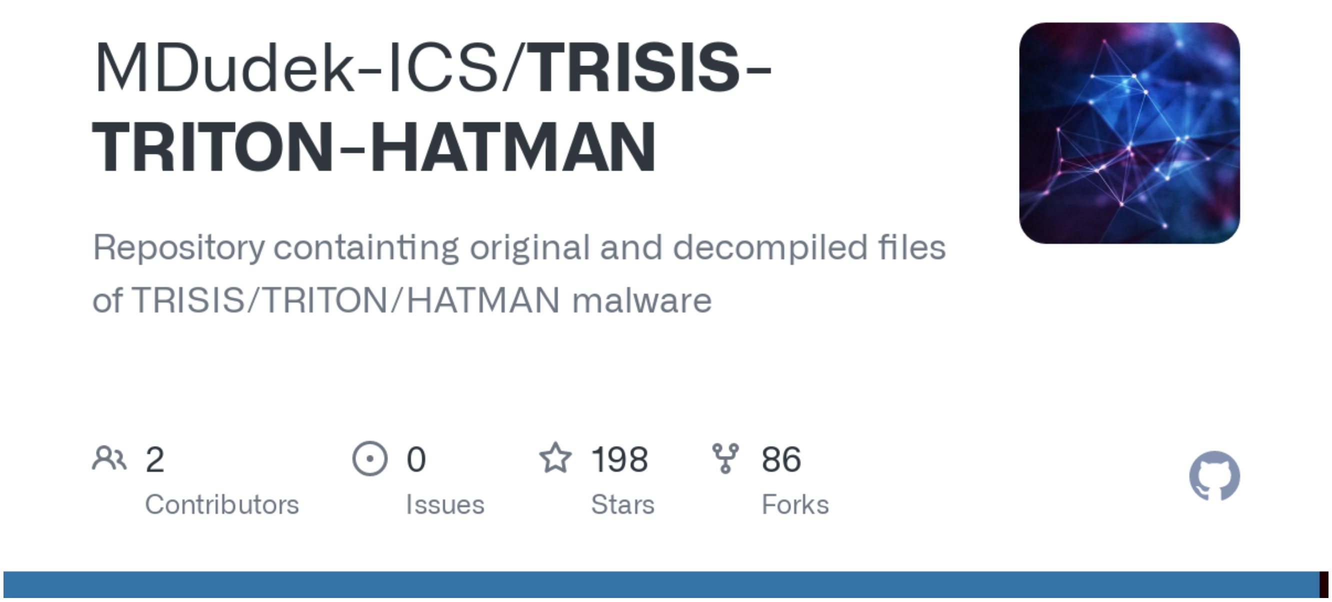
MDudek-ICS/TRISIS-TRITON-HATMAN: Repository containting original and decompiled files of TRISIS/TRITON/HATMAN malware

github.com/ICSrepo/TRISIS-TRITON-HATMAN

MDudek-ICS



MDudek-ICS/**TRISIS-TRITON-HATMAN**

Repository containting original and decompiled files of TRISIS/TRITON/HATMAN malware

2	0	198	86
Contributors	Issues	Stars	Forks

TRISIS / TRITON / HatMan Malware Repository

Description

This repository contains original samples and decompiled sources of malware attacking commonly used in Industrial Control Systems (ICS) *Triconex* Safety Instrumented System (SIS) controllers. For more information scroll to "*Learn More*".

Each organization describing this malware in reports used a different name (TRISIS/TRITON/HatMan). For that reason, there is no one, common name for it.

Folder *original_samples* contains original files used by the malware that could be found in the wild:

Name	MD5	Contains	MD5
trilog.7z	0b4e76e84fa4d6a9716d89107626da9b	trilog.exe	6c39c3f4a08d3d78f2eb973a94bd7718
library.7z	76f84d3aee53b2856575c9f55a9487e7	library.zip	0face841f7b2953e7c29c064d6886523
imain.7z	d173e8016e73f0f2c17b5217a31153be	imain.bin	437f135ba179959a580412e564d3107f
inject.7z	80fdda5ea7eec98bfdd07fec8f644c2d	inject.bin	0544d425c7555dc4e9d76b571f31f500

Name	MD5	Contains	MD5
all.7z	c382f242f62a3c5f4aab2093f6e0fb2f	All files above	-

All archives are secured with password: *infected*

Folder *decompiled_code* contains decompiled python files, originating from *trilog.exe* file and *library.zip* archive described above:

Origin	Result	Method
trilog.exe	script_test.py	unpy2exe + uncompyle6
library.zip	Files in folder library	uncompyle6

Folder *yara_rules* contains yara rules (that I am aware of) detecting this malware:

File	Author
mandiant.yara	@itsreallynick (Mandiant)
ics-cert.yara	DHS/NCCIC/ICS-CERT
ics-cert-v2.yara	DHS/NCCIC/ICS-CERT (from update B report)

Folder *symbolic_execution* contains script for running imain.bin with ANGR symbolic execution engine – credits to @bl4ckic3

Why Publishing? Isn't it dangerous?

Some people in the community were raising the issue that publishing the samples and decompiled sources might be dangerous. I agreed until these were not public. I have found the included files in at least two publicly available sources, that means anyone can download it if know where to search. What is more, I believe that organizations/people who could be able to reuse it and have the capability to deploy it in a real attack have already accessed it long time ago. This repository makes it more accessible for community and academia who might work on improving defense solutions and saves some time on looking for decompilers.

Learn more

Technical Analysis:

Attribution

News Publications:

Others:

Detection:

Any updates to the repository are warmly welcome

Contact:

- @dudekmar
- contact(at)marcindudek.com