Triton (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:38:12 UTC

Triton

aka: Trisis, HatMan

Actor(s): XENOTIME

Malware attacking commonly used in Industrial Control Systems (ICS) Triconex Safety Instrumented System (SIS) controllers.

References

2022-07-26 · Mandiant · Daniel Kapellmann Zafra, Jay Christiansen, Keith Lunden, Ken Proska, Thibault van Geluwe de Berlaere
Mandiant Red Team Emulates FIN11 Tactics To Control Operational Technology Servers
Clop Industroyer MimiKatz Triton

2022-04-20 · CISA · CISA
Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader Killnet

2022-04-20 · CISA · Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), CISA, FBI, Government Communications Security Bureau, National Crime Agency (NCA), NCSC UK, NSA
AA22-110A Joint CSA: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader

2022-03-24 · FBI · FBI
PIN Number 20220324-001 TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems (ICS)
Triton

2022-03-24 · CISA · US-CERT
Alert (AA22-083A) Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
Havex RAT Triton

2021-02-11 · DomainTools · Joe Slowik
Visibility, Monitoring, and Critical Infrastructure Security

Industroyer Stuxnet Triton

2020-12-21 · IronNet · Adam Hlavek, Kimberly Ortiz

Russian cyber attack campaigns and actors

WellMail elf.wellmess Agent.BTZ BlackEnergy EternalPetya Havex RAT Industroyer Ryuk Triton WellMess

2020-10-23 · U.S. Department of the Treasury · U.S. Department of the Treasury

Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware

Triton

2019-08-01 · Kaspersky Labs · GReAT

APT trends report Q2 2019

ZooPark magecart POWERSTATS Chaperone COMpfun EternalPetya FinFisher RAT HawkEye Keylogger HOPLIGHT Microcin NjRAT Olympic Destroyer PLEAD RokRAT Triton Zebrocy

2019-04-10 · Github (ICSrepo) · Marcin Dudek

TRISIS / TRITON / HatMan Malware Repository

Triton

2019-03-07 · E&E News · Blake Sobczak

The inside story of the world's most dangerous malware

Triton

2018-10-23 · FireEye · FireEye Intelligence

TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers

Triton

2018-10-01 · SANS Cyber Summit · Andrea Carcano

TRITON: How it Disrupted Safety Systems and Changed the Threat Landscape of Industrial Control Systems, Forever

Triton

2018-08-08 · Nozomi Networks · Alessandro Di Pinto, Andrea Carcano, Younes Dragoni

TRITON: The First ICS Cyber Attack on Safety Instrument Systems

Triton

2018-04-10 · NCCIC · NCCIC

MAR-17-352-01 HatMan - Safety System Targeted Malware (Update A)

Triton

2018-01-16 · Midnight Blue Labs · Carlo Meijer, Jos Wetzels

Analyzing the TRITON industrial malware

Triton

2017-12-18 · NCCIC · NCCIC

Malware Analysis Report on Hatman

Triton

2017-12-14 · FireEye · Blake Johnson, Christopher Glyer, Dan Caban, Dan Scali, Marina Krotofil, Nathan Brubaker

Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure

Triton TEMP.Veles

2017-12-13 · Dragos · Dragos

TRISIS Malware: Analysis of Safety System Targeted Malware

Triton

Yara Rules

▶ [TLP:WHITE] win_triton_w0 (20180123 | TRITON framework recovered during Mandiant ICS incident response)

▶ [TLP:WHITE] win_triton_w1 (20210727 | Matches the known samples of the HatMan malware.)

Download all Yara Rules
