Pretty-print ☐

{"type":"bundle","id":"bundle--d3fca991-63f4-44f1-ad58-f167c0b3974d","objects":[{"spec_version":"2.1","type":"attack-pattern","id":"attack-pattern--1c145ebc-2b90-4881-a729-a16fc9916166","created":"2025-02-04T12:14:47.100Z","modified":"2026-04-01T15:16:18.225Z","name":"Inhibit Response Function / Data Destruction [T0809] (ICS)","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},{"spec_version":"2.1","type":"attack-pattern","id":"attack-pattern--233061da-54fd-4981-a913-199fff22a1a2","created":"2019-05-16T18:27:40.302Z","modified":"2025-02-10T17:31:20.319Z","name":"Initial Access [TA0001] (ENT)","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},{"spec_version":"2.1","type":"attack-pattern","id":"attack-pattern--3c7f9877-76a6-47da-b3d1-44260b01be01","created":"2020-01-21T14:37:50.234Z","modified":"2026-04-01T15:16:18.221Z","name":"Impact / Data Manipulation: Stored Data Manipulation [T1565.001] (ENT)","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},{"spec_version":"2.1","type":"attack-pattern","id":"attack-pattern--4041a495-a338-463e-8bc1-817996ca0c2b","created":"2019-05-16T18:32:00.508Z","modified":"2025-02-06T19:52:22.744Z","name":"Command and Control [TA0011] (ENT)","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},
{"spec_version":"2.1","type":"attack-pattern","id":"attack-pattern--60ebf64b-2844-4d73-bdf3-1298a383f5f5","created":"2025-02-04T12:14:47.100Z","modified":"2025-03-14T17:00:34.710Z","name":"Command and Control / Commonly Used Port [T0885] (ICS)","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},{"spec_version":"2.1","type":"attack-pattern","id":"attack-pattern--785d61b3-eb56-4a80-9a4f-fdaa694aaeab","created":"2019-05-16T18:33:04.378Z","modified":"2025-02-06T19:25:57.209Z","name":"Impact [TA0040] (ENT)","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},{"spec_version":"2.1","type":"attack-pattern","id":"attack-pattern--9e71363e-f68a-46f3-abe3-0b542f706eea","created":"2025-02-04T12:14:47.100Z","modified":"2026-04-01T15:16:18.220Z","name":"Initial Access / Internet Accessible Device [T0883] (ICS)","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},
{"spec_version":"2.1","type":"attack-pattern","id":"attack-pattern--efcac14c-38cc-42bf-ba59-7bbd3dad429e","created":"2021-04-24T02:19:19.588Z","modified":"2025-05-19T13:18:44.890Z","name":"Impact / Defacement: Internal Defacement [T1491.001] (ENT)","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},
{"spec_version":"2.1","type":"indicator","id":"indicator--2818c180-291d-414f-82ea-08dbbf4aaa47","created":"2026-03-06T02:23:00.536Z","modified":"2026-04-07T16:02:23.037Z","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"],"pattern":"[ipv4-addr:value = '185.82.73.162']","valid_from":"2026-03-06T02:23:00.536Z","pattern_type":"stix","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01"},{"spec_version":"2.1","type":"indicator","id":"indicator--56b12439-ff27-471c-8116-117c408ff6a1","created":"2026-03-06T02:23:00.486Z","modified":"2026-04-07T16:02:23.038Z","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"],"pattern":"[ipv4-addr:value = '185.82.73.167']","valid_from":"2026-03-06T02:23:00.486Z","pattern_type":"stix","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01"},{"spec_version":"2.1","type":"indicator","id":"indicator--9cbb4532-403a-4884-9a11-5a92f98b029b","created":"2026-04-01T14:14:46.530Z","modified":"2026-04-07T16:02:23.038Z","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"],"pattern":"[ipv4-addr:value = '185.82.73.168']","valid_from":"2026-04-01T14:14:46.530Z","pattern_type":"stix","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01"},{"spec_version":"2.1","type":"indicator","id":"indicator--9da4d819-f8f0-4f17-9949-0c0521c9c4eb","created":"2026-03-06T02:23:00.471Z","modified":"2026-04-07T16:02:23.039Z","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"],"pattern":"[ipv4-addr:value = '185.82.73.171']","valid_from":"2026-03-06T02:23:00.471Z","pattern_type":"stix","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01"},{"spec_version":"2.1","type":"indicator","id":"indicator--a06c4b02-eb0b-4bf6-a960-1d313a0950a7","created":"2026-03-06T02:23:00.446Z","modified":"2026-04-07T16:02:23.040Z","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"],"pattern":"[ipv4-addr:value = '185.82.73.165']","valid_from":"2026-03-06T02:23:00.446Z","pattern_type":"stix","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01"},{"spec_version":"2.1","type":"indicator","id":"indicator--bfc273e8-b1ff-4e1d-a148-081672cb1cfd","created":"2026-03-06T02:23:00.520Z","modified":"2026-04-07T16:02:23.041Z","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"],"pattern":"[ipv4-addr:value = '185.82.73.170']","valid_from":"2026-03-06T02:23:00.520Z","pattern_type":"stix","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01"},{"spec_version":"2.1","type":"indicator","id":"indicator--ee43b310-314d-4617-aa04-6347487f8aa1","created":"2026-03-06T02:23:00.425Z","modified":"2026-04-07T16:02:23.041Z","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"],"pattern":"[ipv4-addr:value = '185.82.73.164']","valid_from":"2026-03-06T02:23:00.425Z","pattern_type":"stix","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01"},{"spec_version":"2.1","type":"indicator","id":"indicator--ff491c85-02ba-46c3-90e0-176295b255ba","created":"2026-04-01T14:14:46.323Z","modified":"2026-04-07T16:02:23.042Z","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"],"pattern":"[ipv4-addr:value = '135.136.1.133']","valid_from":"2026-04-01T14:14:46.323Z","pattern_type":"stix","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01"},{"spec_version":"2.1","type":"malware","id":"malware--85b0fbcb-7ca2-4d1b-9f5a-809002ddb6d3","created":"2018-08-14T13:27:29.282Z","modified":"2026-04-01T15:16:18.278Z","name":"Dropbear","is_family":true,"object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},
{"spec_version":"2.1","type":"report","id":"report--0a82b4a1-3063-4039-b3cd-416b0865a181","created":"2026-04-01T14:13:42.001Z","modified":"2026-04-07T13:22:32.209Z","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"],"name":"AA26-097A Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure to Cause Disruption","description":"Iran-affiliated advanced persistent threat (APT) actors are conducting exploitation activity targeting internet-facing operational technology (OT) devices, including programmable logic controllers (PLCs) manufactured by Rockwell Automation/Allen-Bradley. This activity has led to PLC disruptions across several U.S. critical infrastructure sectors through malicious interactions with the project file and manipulation of data on human machine interface (HMI) and supervisory control and data acquisition (SCADA) displays, resulting in operational disruption and financial loss.","published":"2026-04-01T00:00:00.000Z","object_refs":["attack-pattern--1c145ebc-2b90-4881-a729-a16fc9916166","attack-pattern--233061da-54fd-4981-a913-199fff22a1a2","attack-pattern--3c7f9877-76a6-47da-b3d1-44260b01be01","attack-pattern--4041a495-a338-463e-8bc1-817996ca0c2b","attack-pattern--60ebf64b-2844-4d73-bdf3-1298a383f5f5","attack-pattern--785d61b3-eb56-4a80-9a4f-fdaa694aaeab","attack-pattern--9e71363e-f68a-46f3-abe3-0b542f706eea","attack-pattern--efcac14c-38cc-42bf-ba59-7bbd3dad429e","indicator--2818c180-291d-414f-82ea-08dbbf4aaa47","indicator--56b12439-ff27-471c-8116-117c408ff6a1","indicator--9cbb4532-403a-4884-9a11-5a92f98b029b","indicator--9da4d819-f8f0-4f17-9949-0c0521c9c4eb","indicator--a06c4b02-eb0b-4bf6-a960-1d313a0950a7","indicator--bfc273e8-b1ff-4e1d-a148-081672cb1cfd","indicator--ee43b310-314d-4617-aa04-6347487f8aa1","indicator--ff491c85-02ba-46c3-90e0-176295b255ba","malware--85b0fbcb-7ca2-4d1b-9f5a-809002ddb6d3","marking-definition-

Pretty-print

78e480a54c69"],"created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01"},{"type":"marking-definition","spec_version":"2.1","id":"marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","created":"2026-04-07T16:02:48.819Z","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","extensions":{"extension-definition--3a65884d-005a-4290-8335-cb2d778a83ce":{"extension_type":"property-extension","identifier":"isa:guide.19001.DFTA-a9bdb603-7f4f-44c6-acb0-d47f614e64b2","create_date_time":"2026-04-07T16:02:48.819Z","responsible_entity_custodian":"USA.DHS.CISA.CSD.TH","responsible_entity_originator":"USA.DHS.CISA.CSD.TH","policy_reference":"urn:isa:policy:acs:ns:v3.0?privdefault=permit&sharedefault=permit","control_set":{"classification":"U","formal_determination":["INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT","PUBREL"]},"authority_reference":["urn:isa:authority:ais"],"access_privilege":[{"privilege_action":"ANONYMOUSACCESS","rule_effect":"permit","privilege_scope":{"entity":["ALL"],"permitted_nationalities":["ALL"],"permitted_organizations":["ALL"]}}]}}},{"administrative_area":"US-DC","country":"US","created":"2021-03-13T20:09:21.286293Z","created_by_ref":"identity--8ce3f695-d5a4-4dc8-9e93-a65af453a31a","id":"location--78a7f0f3-ea60-4ca2-894e-9e825b94b592","modified":"2021-12-01T16:19:51.601791Z","name":"District of Columbia","spec_version":"2.1","type":"location","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]},{"type":"relationship","spec_version":"2.1","id":"relationship--b6fe158f-fa95-4a40-ac68-78e480a54c69","created_by_ref":"identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01","created":"2024-08-07T16:30:26.628Z","modified":"2024-08-07T16:30:26.628Z","source_ref":"identity--b1160532-b8f3-4cfa-9b7d-423e253fbc59","relationship_type":"located-at","target_ref":"location--78a7f0f3-ea60-4ca2-894e-9e825b94b592","object_marking_refs":["marking-definition--cb110db4-1f54-4455-a261-94f5d9f2f815","marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487"]}]}