This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<stix:STIX_Package xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:marking="http://data-marking.mitre.org/Marking-1" xmlns:ttp="http://stix.mitre.org/TTP-1"
xmlns:threat_actor="http://stix.mitre.org/ThreatActor-1" xmlns:indicator="http://stix.mitre.org/Indicator-2"
xmlns:AddressObj="http://cybox.mitre.org/objects#AddressObject-2" xmlns:MutexObj="http://cybox.mitre.org/objects#MutexObject-2"
xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2" xmlns:HTTPSessionObj="http://cybox.mitre.org/objects#HTTPSessionObject-
2" xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2" xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
xmlns:tlpMarking="http://data-marking.mitre.org/extensions/MarkingStructure#TLP-1" xmlns:simpleMarking="http://data-
marking.mitre.org/extensions/MarkingStructure#Simple-1" xmlns:et="http://stix.mitre.org/ExploitTarget-1"
xmlns:edh2="urn:edm:edh:cyber:v3" xmlns:edh2cyberMarking="http://www.us-
cert.gov/sites/default/files/STIX_Namespace/ISAMarkingsType.v2.xsd" xmlns:edh2cyberMarkingAssert="http://www.us-
cert.gov/sites/default/files/STIX_Namespace/ISAMarkingsAssertionsType.v2.xsd" xmlns:analyst1="gov.dhs.cisa.moe"
xsi:schemaLocation="http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.1.1/stix_core.xsd
http://stix.mitre.org/common-1 http://stix.mitre.org/XMLSchema/common/1.1.1/stix_common.xsd
http://stix.mitre.org/default_vocabularies-1
http://stix.mitre.org/XMLSchema/default_vocabularies/1.1.1/stix_default_vocabularies.xsd http://data-marking.mitre.org/Marking-1
http://stix.mitre.org/XMLSchema/data_marking/1.1.1/data_marking.xsd http://stix.mitre.org/TTP-1
http://stix.mitre.org/XMLSchema/ttp/1.1.1/ttp.xsd http://stix.mitre.org/ThreatActor-1
http://stix.mitre.org/XMLSchema/threat_actor/1.1.1/threat_actor.xsd http://stix.mitre.org/Indicator-2
http://stix.mitre.org/XMLSchema/indicator/2.1.1/indicator.xsd http://cybox.mitre.org/objects#AddressObject-2
http://cybox.mitre.org/XMLSchema/objects/Address/2.1/Address_Object.xsd http://cybox.mitre.org/objects#MutexObject-2
http://cybox.mitre.org/XMLSchema/objects/Mutex/2.1/Mutex_Object.xsd http://cybox.mitre.org/objects#URIObject-2
http://cybox.mitre.org/XMLSchema/objects/URI/2.1/URI_Object.xsd http://cybox.mitre.org/objects#HTTPSessionObject-2
http://cybox.mitre.org/XMLSchema/objects/HTTP_Session/2.1/HTTP_Session_Object.xsd http://cybox.mitre.org/cybox-2
http://cybox.mitre.org/XMLSchema/core/2.1/cybox_core.xsd http://cybox.mitre.org/common-2
http://cybox.mitre.org/XMLSchema/common/2.1/cybox_common.xsd http://cybox.mitre.org/default_vocabularies-2
http://cybox.mitre.org/XMLSchema/default_vocabularies/2.1/cybox_default_vocabularies.xsd
http://cybox.mitre.org/objects#FileObject-2 http://cybox.mitre.org/XMLSchema/objects/File/2.1/File_Object.xsd http://data-
marking.mitre.org/extensions/MarkingStructure#TLP-1 http://stix.mitre.org/XMLSchema/extensions/marking/tlp/1.1.1/tlp_marking.xsd
http://data-marking.mitre.org/extensions/MarkingStructure#Simple-1
http://stix.mitre.org/XMLSchema/extensions/marking/simple/1.1.1/simple_marking.xsd http://stix.mitre.org/ExploitTarget-1
http://stix.mitre.org/XMLSchema/exploit_target/1.1.1/exploit_target.xsd urn:edm:edh:cyber:v3 http://www.us-
cert.gov/sites/default/files/STIX_Namespace/local_SD-EDH_Profile_Cyber.v3.xsd http://www.us-
cert.gov/sites/default/files/STIX_Namespace/ISAMarkingsType.v2.xsd http://www.us-
cert.gov/sites/default/files/STIX_Namespace/local_ISAMarkingsType.v2.xsd http://www.us-
cert.gov/sites/default/files/STIX_Namespace/ISAMarkingsAssertionsType.v2.xsd http://www.us-
cert.gov/sites/default/files/STIX_Namespace/local_ISAMarkingsAssertionsType.v2.xsd" id="analyst1:evidencePackage-17345648"
timestamp="2026-04-07T16:19:27.544Z" version="1.1.1">
  <stix:STIX_Header>
    <stix:Title>AA26-097A Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure
    to Cause Disruption</stix:Title>
    <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Collective Threat Intelligence</stix:Package_Intent>
    <stix: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.</stix:Description>
    <stix:Handling>
      <marking:Marking>
        <marking:Controlled_Structure>/node() | /*/node()[not(self::stix:Indicators)] | /*/*[not(self::stix:Indicators)]//node() |
        /@* | /*/@*[not(self::stix:Indicators)] | /*/*[not(self::stix:Indicators)]//@*</marking:Controlled_Structure>
        <marking:Marking_Structure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
      </marking:Marking>
      <marking:Marking id="analyst1:evidenceTitleMarking-17345648">
        <marking:Controlled_Structure>../../../stix:Title/descendant-or-self::node() | ../../../stix:Title/descendant-or-
        self::node()/@*</marking:Controlled_Structure>
        <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
        id="analyst1:evidenceTitleMarkingStructure-17345648">
          <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
          <edh2:AccessPrivilege>
            <edh2:privilegeAction>ALL</edh2:privilegeAction>
            <edh2:privilegeScope>ALL</edh2:privilegeScope>
            <edh2:ruleEffect>permit</edh2:ruleEffect>
          </edh2:AccessPrivilege>
          <edh2:ControlSet>CLS:U</edh2:ControlSet>
        </marking:Marking_Structure>
      </marking:Marking>
      <marking:Marking id="analyst1:evidenceDescriptionMarking-17345648">
        <marking:Controlled_Structure>../../../stix:Description/descendant-or-self::node() | ../../../stix:Description/descendant-
        or-self::node()/@*</marking:Controlled_Structure>
        <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
        id="analyst1:evidenceDescriptionMarkingStructure-17345648">
          <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
          <edh2:AccessPrivilege>
            <edh2:privilegeAction>ALL</edh2:privilegeAction>
            <edh2:privilegeScope>ALL</edh2:privilegeScope>
            <edh2:ruleEffect>permit</edh2:ruleEffect>
          </edh2:AccessPrivilege>
```

```
      <edh2:ControlSet>CLS:U</edh2:ControlSet>
    </marking:Marking_Structure>
  </marking:Marking>
  <marking:Marking id="analyst1:evidenceReferenceMarking-17345648">
    <marking:Controlled_Structure>../../..//stixCommon:Reference/descendant-or-self::node() |
    ../../..//stixCommon:Reference/descendant-or-self::node()/@*</marking:Controlled_Structure>
    <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
    id="analyst1:evidenceReferenceMarkingStructure-17345648">
      <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
      <edh2:AccessPrivilege>
        <edh2:privilegeAction>ALL</edh2:privilegeAction>
        <edh2:privilegeScope>ALL</edh2:privilegeScope>
        <edh2:ruleEffect>permit</edh2:ruleEffect>
      </edh2:AccessPrivilege>
      <edh2:ControlSet>CLS:U</edh2:ControlSet>
    </marking:Marking_Structure>
  </marking:Marking>
  <marking:Marking>
    <marking:Controlled_Structure>//node() | //@*</marking:Controlled_Structure>
    <marking:Marking_Structure xsi:type="edh2cyberMarking:ISAMarkingsType" isam_version="2.0" id="analyst1:evidencePackage-
    EDH2-17345648">
      <edh2:Identifier>analyst1:evidencePackage-EDH2-17345648</edh2:Identifier>
      <edh2:CreateDateTime>2026-04-07T16:19:27.750Z</edh2:CreateDateTime>
      <edh2:ResponsibleEntity>UNCLASSIFIED//FOUO</edh2:ResponsibleEntity>
    </marking:Marking_Structure>
  </marking:Marking>
 </stix:Handling>
</stix:STIX_Header>
<stix:Indicators>
 <stix:Indicator xsi:type="indicator:IndicatorType" id="analyst1:indicator-111443171" timestamp="2026-04-07T16:19:27.800Z">
  <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
  <indicator:Description/>
  <indicator:Observable id="analyst1:indicatorObs-111443171">
   <cybox:Object id="analyst1:indicatorObsObj-111443171">
    <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
     <AddressObj:Address_Value condition="Equals" apply_condition="ANY">185.82.73.165</AddressObj:Address_Value>
    </cybox:Properties>
   </cybox:Object>
  </indicator:Observable>
  <indicator:Handling>
   <marking:Marking id="analyst1:indicatorMarking-111443171">
    <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
    </marking:Controlled_Structure>
    <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
    id="analyst1:indicatorMarkingStructure-111443171">
     <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
     <edh2:AccessPrivilege>
      <edh2:privilegeAction>ALL</edh2:privilegeAction>
      <edh2:privilegeScope>ALL</edh2:privilegeScope>
      <edh2:ruleEffect>permit</edh2:ruleEffect>
     </edh2:AccessPrivilege>
     <edh2:ControlSet>CLS:U</edh2:ControlSet>
    </marking:Marking_Structure>
   </marking:Marking>
   <marking:Marking>
    <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
    </marking:Controlled_Structure>
    <marking:Marking_Structure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
   </marking:Marking>
  </indicator:Handling>
  <indicator:Confidence timestamp="2026-04-07T16:19:27.800Z">
   <stixCommon:Value vocab_name="HighMediumLowVocab-1.0">Unknown</stixCommon:Value>
  </indicator:Confidence>
 </stix:Indicator>
 <stix:Indicator xsi:type="indicator:IndicatorType" id="analyst1:indicator-119480062" timestamp="2026-04-07T16:19:27.800Z">
  <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
  <indicator:Description/>
  <indicator:Observable id="analyst1:indicatorObs-119480062">
   <cybox:Object id="analyst1:indicatorObsObj-119480062">
    <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
     <AddressObj:Address_Value condition="Equals" apply_condition="ANY">135.136.1.133</AddressObj:Address_Value>
    </cybox:Properties>
   </cybox:Object>
  </indicator:Observable>
  <indicator:Handling>
   <marking:Marking id="analyst1:indicatorMarking-119480062">
    <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
    </marking:Controlled_Structure>
    <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
    id="analyst1:indicatorMarkingStructure-119480062">
     <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
     <edh2:AccessPrivilege>
```

```
        <edh2:privilegeAction>ALL</edh2:privilegeAction>
        <edh2:privilegeScope>ALL</edh2:privilegeScope>
        <edh2:ruleEffect>permit</edh2:ruleEffect>
      </edh2:AccessPrivilege>
      <edh2:ControlSet>CLS:U</edh2:ControlSet>
    </marking:Marking_Structure>
  </marking:Marking>
  <marking:Marking>
    <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
    </marking:Controlled_Structure>
    <marking:Marking_Structure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
  </marking:Marking>
</indicator:Handling>
<indicator:Confidence timestamp="2026-04-07T16:19:27.800Z">
  <stixCommon:Value vocab_name="HighMediumLowVocab-1.0">Unknown</stixCommon:Value>
</indicator:Confidence>
</stix:Indicator>
<stix:Indicator xsi:type="indicator:IndicatorType" id="analyst1:indicator-111443173" timestamp="2026-04-07T16:19:27.800Z">
  <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
  <indicator:Description/>
  <indicator:Observable id="analyst1:indicatorObs-111443173">
    <cybox:Object id="analyst1:indicatorObsObj-111443173">
      <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
        <AddressObj:Address_Value condition="Equals" apply_condition="ANY">185.82.73.167</AddressObj:Address_Value>
      </cybox:Properties>
    </cybox:Object>
  </indicator:Observable>
  <indicator:Handling>
    <marking:Marking id="analyst1:indicatorMarking-111443173">
      <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
      </marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:indicatorMarkingStructure-111443173">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
    <marking:Marking>
      <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
      </marking:Controlled_Structure>
      <marking:Marking_Structure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
    </marking:Marking>
  </indicator:Handling>
  <indicator:Confidence timestamp="2026-04-07T16:19:27.801Z">
    <stixCommon:Value vocab_name="HighMediumLowVocab-1.0">Unknown</stixCommon:Value>
  </indicator:Confidence>
</stix:Indicator>
<stix:Indicator xsi:type="indicator:IndicatorType" id="analyst1:indicator-119480063" timestamp="2026-04-07T16:19:27.801Z">
  <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
  <indicator:Description/>
  <indicator:Observable id="analyst1:indicatorObs-119480063">
    <cybox:Object id="analyst1:indicatorObsObj-119480063">
      <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
        <AddressObj:Address_Value condition="Equals" apply_condition="ANY">185.82.73.168</AddressObj:Address_Value>
      </cybox:Properties>
    </cybox:Object>
  </indicator:Observable>
  <indicator:Handling>
    <marking:Marking id="analyst1:indicatorMarking-119480063">
      <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
      </marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:indicatorMarkingStructure-119480063">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
    <marking:Marking>
      <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
      </marking:Controlled_Structure>
```

```
      <marking:Marking_Structure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
    </marking:Marking>
  </indicator:Handling>
  <indicator:Confidence timestamp="2026-04-07T16:19:27.801Z">
    <stixCommon:Value vocab_name="HighMediumLowVocab-1.0">Unknown</stixCommon:Value>
  </indicator:Confidence>
</stix:Indicator>
<stix:Indicator xsi:type="indicator:IndicatorType" id="analyst1:indicator-111443177" timestamp="2026-04-07T16:19:27.801Z">
  <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
  <indicator:Description/>
  <indicator:Observable id="analyst1:indicatorObs-111443177">
    <cybox:Object id="analyst1:indicatorObsObj-111443177">
      <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
        <AddressObj:Address_Value condition="Equals" apply_condition="ANY">185.82.73.170</AddressObj:Address_Value>
      </cybox:Properties>
    </cybox:Object>
  </indicator:Observable>
  <indicator:Handling>
    <marking:Marking id="analyst1:indicatorMarking-111443177">
      <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
      </marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:indicatorMarkingStructure-111443177">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
    <marking:Marking>
      <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
      </marking:Controlled_Structure>
      <marking:Marking_Structure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
    </marking:Marking>
  </indicator:Handling>
  <indicator:Confidence timestamp="2026-04-07T16:19:27.801Z">
    <stixCommon:Value vocab_name="HighMediumLowVocab-1.0">Unknown</stixCommon:Value>
  </indicator:Confidence>
</stix:Indicator>
<stix:Indicator xsi:type="indicator:IndicatorType" id="analyst1:indicator-111443170" timestamp="2026-04-07T16:19:27.801Z">
  <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
  <indicator:Description/>
  <indicator:Observable id="analyst1:indicatorObs-111443170">
    <cybox:Object id="analyst1:indicatorObsObj-111443170">
      <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
        <AddressObj:Address_Value condition="Equals" apply_condition="ANY">185.82.73.164</AddressObj:Address_Value>
      </cybox:Properties>
    </cybox:Object>
  </indicator:Observable>
  <indicator:Handling>
    <marking:Marking id="analyst1:indicatorMarking-111443170">
      <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
      </marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:indicatorMarkingStructure-111443170">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
    <marking:Marking>
      <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
      </marking:Controlled_Structure>
      <marking:Marking_Structure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
    </marking:Marking>
  </indicator:Handling>
  <indicator:Confidence timestamp="2026-04-07T16:19:27.802Z">
    <stixCommon:Value vocab_name="HighMediumLowVocab-1.0">Unknown</stixCommon:Value>
  </indicator:Confidence>
</stix:Indicator>
<stix:Indicator xsi:type="indicator:IndicatorType" id="analyst1:indicator-111443178" timestamp="2026-04-07T16:19:27.802Z">
  <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
  <indicator:Description/>
```

```
    <indicator:Observable id="analyst1:indicatorObs-111443178">
      <cybox:Object id="analyst1:indicatorObsObj-111443178">
        <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
          <AddressObj:Address_Value condition="Equals" apply_condition="ANY">185.82.73.162</AddressObj:Address_Value>
        </cybox:Properties>
      </cybox:Object>
    </indicator:Observable>
    <indicator:Handling>
      <marking:Marking id="analyst1:indicatorMarking-111443178">
        <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
        </marking:Controlled_Structure>
        <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
        id="analyst1:indicatorMarkingStructure-111443178">
          <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
          <edh2:AccessPrivilege>
            <edh2:privilegeAction>ALL</edh2:privilegeAction>
            <edh2:privilegeScope>ALL</edh2:privilegeScope>
            <edh2:ruleEffect>permit</edh2:ruleEffect>
          </edh2:AccessPrivilege>
          <edh2:ControlSet>CLS:U</edh2:ControlSet>
        </marking:Marking_Structure>
      </marking:Marking>
      <marking:Marking>
        <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
        </marking:Controlled_Structure>
        <marking:Marking_Structure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
      </marking:Marking>
    </indicator:Handling>
    <indicator:Confidence timestamp="2026-04-07T16:19:27.802Z">
      <stixCommon:Value vocab_name="HighMediumLowVocab-1.0">Unknown</stixCommon:Value>
    </indicator:Confidence>
  </stix:Indicator>
  <stix:Indicator xsi:type="indicator:IndicatorType" id="analyst1:indicator-111443172" timestamp="2026-04-07T16:19:27.802Z">
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
    <indicator:Description/>
    <indicator:Observable id="analyst1:indicatorObs-111443172">
      <cybox:Object id="analyst1:indicatorObsObj-111443172">
        <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
          <AddressObj:Address_Value condition="Equals" apply_condition="ANY">185.82.73.171</AddressObj:Address_Value>
        </cybox:Properties>
      </cybox:Object>
    </indicator:Observable>
    <indicator:Handling>
      <marking:Marking id="analyst1:indicatorMarking-111443172">
        <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
        </marking:Controlled_Structure>
        <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
        id="analyst1:indicatorMarkingStructure-111443172">
          <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
          <edh2:AccessPrivilege>
            <edh2:privilegeAction>ALL</edh2:privilegeAction>
            <edh2:privilegeScope>ALL</edh2:privilegeScope>
            <edh2:ruleEffect>permit</edh2:ruleEffect>
          </edh2:AccessPrivilege>
          <edh2:ControlSet>CLS:U</edh2:ControlSet>
        </marking:Marking_Structure>
      </marking:Marking>
      <marking:Marking>
        <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
        </marking:Controlled_Structure>
        <marking:Marking_Structure xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="tlpMarking:TLPMarkingStructureType" color="WHITE"/>
      </marking:Marking>
    </indicator:Handling>
    <indicator:Confidence timestamp="2026-04-07T16:19:27.802Z">
      <stixCommon:Value vocab_name="HighMediumLowVocab-1.0">Unknown</stixCommon:Value>
    </indicator:Confidence>
  </stix:Indicator>
</stix:Indicators>
<stix:TTPs>
  <stix:TTP xsi:type="ttp:TTPType" id="analyst1:ttpAttackPattern-100012" timestamp="2026-04-07T16:19:27.774Z">
    <ttp:Behavior>
      <ttp:Attack_Patterns>
        <ttp:Attack_Pattern id="analyst1:attackPattern-100012">
          <ttp:Title>Initial Access [TA0001] (ENT)</ttp:Title>
        </ttp:Attack_Pattern>
        <ttp:Attack_Pattern id="analyst1:attackPattern-100021">
          <ttp:Title>Command and Control [TA0011] (ENT)</ttp:Title>
        </ttp:Attack_Pattern>
        <ttp:Attack_Pattern id="analyst1:attackPattern-100023">
          <ttp:Title>Impact [TA0040] (ENT)</ttp:Title>
        </ttp:Attack_Pattern>
```

```
      <ttp:Attack_Pattern id="analyst1:attackPattern-100047">
        <ttp:Title>Impact / Data Manipulation: Stored Data Manipulation [T1565.001] (ENT)</ttp:Title>
      </ttp:Attack_Pattern>
      <ttp:Attack_Pattern id="analyst1:attackPattern-101127">
        <ttp:Title>Command and Control / Commonly Used Port [T0885] (ICS)</ttp:Title>
      </ttp:Attack_Pattern>
      <ttp:Attack_Pattern id="analyst1:attackPattern-101057">
        <ttp:Title>Inhibit Response Function / Data Destruction [T0809] (ICS)</ttp:Title>
      </ttp:Attack_Pattern>
      <ttp:Attack_Pattern id="analyst1:attackPattern-101126">
        <ttp:Title>Initial Access / Internet Accessible Device [T0883] (ICS)</ttp:Title>
      </ttp:Attack_Pattern>
      <ttp:Attack_Pattern id="analyst1:attackPattern-100567">
        <ttp:Title>Impact / Defacement: Internal Defacement [T1491.001] (ENT)</ttp:Title>
      </ttp:Attack_Pattern>
    </ttp:Attack_Patterns>
  </ttp:Behavior>
  <ttp:Handling>
    <marking:Marking id="analyst1:evidenceAttackPatternMarking-17345648">
      <marking:Controlled_Structure>../../../ttp:Behavior/ttp:Attack_Patterns/descendant-or-self::node() |
      ../../../ttp:Behavior/ttp:Attack_Patterns/descendant-or-self::node()/@*</marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:evidenceAttackPatternMarkingStructure-17345648">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
  </ttp:Handling>
</stix:TTP>
<stix:TTP xsi:type="ttp:TTPType" id="analyst1:ttpTarget-100042" timestamp="2026-04-07T16:19:27.775Z">
  <ttp:Victim_Targeting>
    <ttp:Identity id="analyst1:target-100042">
      <stixCommon:Name>Industrial Control System(s)</stixCommon:Name>
    </ttp:Identity>
  </ttp:Victim_Targeting>
  <ttp:Handling>
    <marking:Marking id="analyst1:evidenceTargetsMarking-17345648-1">
      <marking:Controlled_Structure>../../../ttp:Victim_Targeting/descendant-or-self::node() |
      ../../../ttp:Victim_Targeting/descendant-or-self::node()/@*</marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:evidenceTargetsMarkingStructure-17345648-1">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
  </ttp:Handling>
</stix:TTP>
<stix:TTP xsi:type="ttp:TTPType" id="analyst1:ttpTarget-100224" timestamp="2026-04-07T16:19:27.775Z">
  <ttp:Victim_Targeting>
    <ttp:Identity id="analyst1:target-100224">
      <stixCommon:Name>US Critical Infrastructure</stixCommon:Name>
    </ttp:Identity>
  </ttp:Victim_Targeting>
  <ttp:Handling>
    <marking:Marking id="analyst1:evidenceTargetsMarking-17345648-2">
      <marking:Controlled_Structure>../../../ttp:Victim_Targeting/descendant-or-self::node() |
      ../../../ttp:Victim_Targeting/descendant-or-self::node()/@*</marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:evidenceTargetsMarkingStructure-17345648-2">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
  </ttp:Handling>
</stix:TTP>
<stix:TTP xsi:type="ttp:TTPType" id="analyst1:ttpTarget-100020" timestamp="2026-04-07T16:19:27.775Z">
  <ttp:Victim_Targeting>
    <ttp:Identity id="analyst1:target-100020">
```

```
      <stixCommon:Name>Water and Wastewater Systems Sector</stixCommon:Name>
    </ttp:Identity>
  </ttp:Victim_Targeting>
  <ttp:Handling>
    <marking:Marking id="analyst1:evidenceTargetsMarking-17345648-3">
      <marking:Controlled_Structure>../../../ttp:Victim_Targeting/descendant-or-self::node() |
      ../../../ttp:Victim_Targeting/descendant-or-self::node()/@*</marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:evidenceTargetsMarkingStructure-17345648-3">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
  </ttp:Handling>
</stix:TTP>
<stix:TTP xsi:type="ttp:TTPType" id="analyst1:ttpTarget-100011" timestamp="2026-04-07T16:19:27.775Z">
  <ttp:Victim_Targeting>
    <ttp:Identity id="analyst1:target-100011">
      <stixCommon:Name>Energy Sector</stixCommon:Name>
    </ttp:Identity>
  </ttp:Victim_Targeting>
  <ttp:Handling>
    <marking:Marking id="analyst1:evidenceTargetsMarking-17345648-4">
      <marking:Controlled_Structure>../../../ttp:Victim_Targeting/descendant-or-self::node() |
      ../../../ttp:Victim_Targeting/descendant-or-self::node()/@*</marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:evidenceTargetsMarkingStructure-17345648-4">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
  </ttp:Handling>
</stix:TTP>
<stix:TTP xsi:type="ttp:TTPType" id="analyst1:ttpMalware-1314" timestamp="2026-04-07T16:19:27.777Z">
  <ttp:Behavior>
    <ttp:Malware>
      <ttp:Malware_Instance id="analyst1:malware-1314">
        <ttp:Name>Dropbear</ttp:Name>
      </ttp:Malware_Instance>
    </ttp:Malware>
  </ttp:Behavior>
  <ttp:Handling>
    <marking:Marking id="analyst1:evidenceMalwareMarking-17345648-1">
      <marking:Controlled_Structure>../../../ttp:Behavior/ttp:Malware/descendant-or-self::node() |
      ../../../ttp:Behavior/ttp:Malware/descendant-or-self::node()/@*</marking:Controlled_Structure>
      <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
      id="analyst1:evidenceMalwareMarkingStructure-17345648-1">
        <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
        <edh2:AccessPrivilege>
          <edh2:privilegeAction>ALL</edh2:privilegeAction>
          <edh2:privilegeScope>ALL</edh2:privilegeScope>
          <edh2:ruleEffect>permit</edh2:ruleEffect>
        </edh2:AccessPrivilege>
        <edh2:ControlSet>CLS:U</edh2:ControlSet>
      </marking:Marking_Structure>
    </marking:Marking>
  </ttp:Handling>
</stix:TTP>
</stix:TTPs>
<stix:Threat_Actors>
  <stix:Threat_Actor id="analyst1:actor-3872" xsi:type="threat_actor:ThreatActorType">
    <threat_actor:Identity>
      <stixCommon:Name>Islamic Revolutionary Guard Corps</stixCommon:Name>
    </threat_actor:Identity>
    <threat_actor:Handling>
      <marking:Marking id="analyst1:evidenceActorMarking-17345648-1">
        <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
        </marking:Controlled_Structure>
        <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
        id="analyst1:evidenceActorMarkingStructure-17345648-1">
          <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
          <edh2:AccessPrivilege>
            <edh2:privilegeAction>ALL</edh2:privilegeAction>
```

```
            <edh2:privilegeScope>ALL</edh2:privilegeScope>
            <edh2:ruleEffect>permit</edh2:ruleEffect>
          </edh2:AccessPrivilege>
          <edh2:ControlSet>CLS:U</edh2:ControlSet>
        </marking:Marking_Structure>
      </marking:Marking>
    </threat_actor:Handling>
  </stix:Threat_Actor>
  <stix:Threat_Actor id="analyst1:actor-4867" xsi:type="threat_actor:ThreatActorType">
    <threat_actor:Identity>
      <stixCommon:Name>CYBER AVENG3RS</stixCommon:Name>
    </threat_actor:Identity>
    <threat_actor:Handling>
      <marking:Marking id="analyst1:evidenceActorMarking-17345648-2">
        <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
        </marking:Controlled_Structure>
        <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
        id="analyst1:evidenceActorMarkingStructure-17345648-2">
          <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
          <edh2:AccessPrivilege>
            <edh2:privilegeAction>ALL</edh2:privilegeAction>
            <edh2:privilegeScope>ALL</edh2:privilegeScope>
            <edh2:ruleEffect>permit</edh2:ruleEffect>
          </edh2:AccessPrivilege>
          <edh2:ControlSet>CLS:U</edh2:ControlSet>
        </marking:Marking_Structure>
      </marking:Marking>
    </threat_actor:Handling>
  </stix:Threat_Actor>
  <stix:Threat_Actor id="analyst1:actor-8264" xsi:type="threat_actor:ThreatActorType">
    <threat_actor:Identity>
      <stixCommon:Name>BAUXITE</stixCommon:Name>
    </threat_actor:Identity>
    <threat_actor:Handling>
      <marking:Marking id="analyst1:evidenceActorMarking-17345648-3">
        <marking:Controlled_Structure>../../../descendant-or-self::node() | ../../../descendant-or-self::node()/@*
        </marking:Controlled_Structure>
        <marking:Marking_Structure xsi:type="edh2cyberMarkingAssert:ISAMarkingsAssertionType" isam_version="2.0"
        id="analyst1:evidenceActorMarkingStructure-17345648-3">
          <edh2:PolicyRef>urn:isa:policy:acs:ns:3.0?privdefault=permit&sharedefault=permit</edh2:PolicyRef>
          <edh2:AccessPrivilege>
            <edh2:privilegeAction>ALL</edh2:privilegeAction>
            <edh2:privilegeScope>ALL</edh2:privilegeScope>
            <edh2:ruleEffect>permit</edh2:ruleEffect>
          </edh2:AccessPrivilege>
          <edh2:ControlSet>CLS:U</edh2:ControlSet>
        </marking:Marking_Structure>
      </marking:Marking>
    </threat_actor:Handling>
  </stix:Threat_Actor>
 </stix:Threat_Actors>
</stix:STIX_Package>
```