PACKETVIPER™

Defending Against Pipedream in ICS & OT Environments

Threat Guidance

A tactical guide to address the Pipedream malware

In a recently published Wired article distributed on April 13, 2021, a new malware toolkit referenced as Pipedream has been identified which could potentially affect every ICS environment around the world. The PacketViper Engineering team has reviewed the details of this new threat vector and determined that when fully deployed, the PacketViper Operational Technology Remote (OTR) would counteract this threat. PacketViper OTR denies access by the threat vector to protected trusted environments, preventing propagation by instantly identifying, alerting and replicating security policies between connected environments. These wire-speed, preventive defensive measures stop any attempts to deploy the malware and employ these tools within protected critical infrastructure segments.

Should any of these malware toolkit components be introduced within an unprotected critical distributed environment - regardless of the delivery system, the attacker would have the capability to disrupt and destroy critical and essential services, including those directly related to human health and safety. Because most devices within ICS environments are poorly protected and generally reside on a flat production network environment, the Pipedream threat should be considered a top priority event and immediately addressed as such.

This threat could permit Windows-related components to facilitate host reconnaissance, command and control, lateral tool transfer, as well as the deployment of unsigned rootkits. These events allow an attacker to leverage access to multiple components to perform rapid reconnaissance of ICS networks by using a variety of mechanisms including:

- Identifying known MAC Addresses
- Port numbers
- HTTP banners
- Omron's proprietary Factory Interface Network Service Protocol (FINS)
- Modbus
- Schneider's custom Discovery broadcast protocol (NetManage)

The PacketViper OTR solution directly addresses this new threat vector by not permitting open access from within the ICS environment. PacketViper OTR was designed for these specific types of threats, and does not require exact threat mapping to be effective. PacketViper OTR is built upon a zero-trust model which locks in communication between control systems and devices without the need for micro segmentation, while at the same time providing visibility, anomaly detection, event alerting, and threat prevention in one solution, without the need for complex orchestration and integration. The OTR solution starts with building policies which are specific to communication streams between critical devices. For instance, a PLC communicating with a control system, on specific ports.

This trust is a vital component in the technology that guarantees continuity between the control systems and the critical downstream devices, while protecting the environment from untrusted connections and ports.

Pipedream, as with many attack vectors, requires reconnaissance and attack tools which utilize specific ports. Regardless if the attack vector begins with a workstation from within the environment, or from a new device, our zero-trust mechanism monitors specific behaviors which guarantees access will not be granted, as OTR monitors IP, port and even communication frequency, which an attacker will not be able to decipher or avoid.

The OTR solution's automated policy propagation not only prevents access to remote devices, it also isolates and contains the threat, notifies the enterprise, and propagates the detected event policy to all PacketViper OTR devices through a proven process specific to PacketViper.

Upon detection of an untrusted connection, a wire-speed policy change is triggered across the entire PacketViper OTR enterprise, which immediately prevents the attacker from attacking every connected location. Regardless if the ICS network is flat, routed, or otherwise engineered, the attacker will have no ability to connect to any location that is protected by a PacketViper OTR device once the policy is shared and applied. The OTR solution is so effective, that should the attacker be physically present at a remote location and attempt to by-pass any PacketViper OTR device by physically disconnecting it, the upstream and downstream OTR devices will isolate and contain the attack to that specific location.

Below we list various components of the malware toolkit, along with how PacketViper OTR can help protect OT and ICS environments against Pipedream and a host of other similar attack mechanisms and vectors.

Reference Advisory: CISA AA22-103A - APT Cyber Tools Targeting ICS/SCADA Devices

Capabilities: Pipedream utilizes several different protocols, including Omron's proprietary FINS, Modbus, and Schneider Electric's implementation of CODESYS for reconnaissance, manipulation, and Disabling of PLC's. PLC Credential Capturing, bruteforce, and DOS

Scope: Critical Infrastructure utilizing Schneider, Omron, CoDeSYS-based PLC's, and OPC UA operations

- Schneider Electric MODICON and MODICON Nano PLCs, including, but not limited to, TM251, TM241, M258, M238, LMC058, and LMC078;
  - Run a rapid scan that identifies all Schneider PLCs on the local network via User Datagram Protocol (UDP) multicast with a destination port of 27127 (Note: UDP 27127 is a standard discovery scan used by engineering workstations to discover PLCs and may not be indicative of malicious activity);
  - Brute-force Schneider Electric PLC passwords using CODESYS and other available device protocols via UDP port 1740 against defaults or a dictionary word list (Note: this capability may work against other CODESYS-based devices depending on individual design and function, and this report will be updated as more information becomes available);
  - Conduct a denial-of-service attack to prevent network communications from reaching the PLC;
  - Sever connections, requiring users to re-authenticate to the PLC, likely to facilitate capture of credentials;
  - Conduct a 'packet of death' attack to crash the PLC until a power cycle and configuration recovery is conducted; and
  - Send custom Modbus commands (Note: this capability may work against Modbus other than in Schneider Electric PLCs).

- OMRON Sysmac NJ and NX PLCs, including (but not be limited to) NEX NX1P2, NX-SL3300, NX-ECC203, NJ501-1300, S8VK, and R88D-1SN10F-ECT;
  - Scanning for OMRON using (Factory Interface Network Service (FINS) protocol;
  - Parsing the Hypertext Transfer Protocol (HTTP) response from OMRON devices;
  - Retrieving the media access control (MAC) address of the device;
  - Polling for specific devices connected to the PLC;
  - Backing up/restoring arbitrary files to/from the PLC; and
  - Loading a custom malicious agent on OMRON PLCs for additional attacker-directed capability.

- OPC Unified Architecture (OPC UA) servers.
  - The APT actors' tool for OPC UA has modules with basic functionality to identify OPC UA servers and to connect to an OPC UA server using default or previously compromised credentials. The client can read the OPC UA structure from the server and potentially write tag values available via OPC UA.

Risk: Actors could compromise Windows-based workstations, present within either information technology (IT) or OT environments, which could exploit an ASRock motherboard driver with known vulnerabilities. Actors could elevate privileges, move laterally within an OT environment, and disrupt critical devices or functions

Pipedream relies on several components to flourish:

- **EvilScholar:**

  - **Threat Description:** A capability designed to discover, access, manipulate, and disable Schneider Electric PLCs. It contains a CODESYS library that potentially allows an impacted device to target other manufacturers equipment.
  - **OTR Countermeasures:** PacketViper OTR is configured with a one-to-one port level trust relationship between critical devices. Any deviant connections attempting to discover, access, and or manipulate critical infrastructure other than pre-established trusts will be detected, alerted, and blocked - at wire speed - by the PacketViper OTR appliance. PacketViper OTR utilizes proprietary zero false positive threat detection, traffic anomaly sensors and unidirectional/bi-directional Security Policies to detect and restrict anomalies. Any scans, or access attempts from unauthorized systems or IP would be detected and remediated.

- **Badomen:**

  - **Threat Description:** A capability designed to scan, identify, and interact with Omron software and PLCs.

  - **OTR Countermeasures:** PacketViper OTR is configured with a one-to-one port level trust relationship between critical devices. Any deviant connections attempting to discover, access, and or manipulate critical infrastructure other than pre-established trusts will be detected, alerted, and blocked - at wire speed - by the PacketViper OTR appliance. PacketViper OTR utilizes proprietary zero false positive threat detection, traffic anomaly sensors and unidirectional/bi-directional Security Policies to detect and restrict anomalies. Any scans, or access attempts from unauthorized systems or IP would be detected and remediated.

- **Mousehole:**
  - **Threat Description:** A tool for interacting with OPC-UA servers. This includes reading and writing node attribute data, enumerating the Server Namespace and associated NodeIds, and brute forcing credentials.
  - **OTR Countermeasures:** PacketViper OTR is configured with a one-to-one port level trust relationship between critical devices. Any deviant connections attempting to discover, access, and or manipulate critical infrastructure other than pre-established trusts will be detected, alerted, and blocked - at wire speed - by the PacketViper OTR appliance. PacketViper OTR utilizes proprietary zero false positive threat detection, traffic anomaly sensors and unidirectional/bi-directional Security Policies to detect and restrict anomalies. Any scans, or access attempts from unauthorized systems or IP would be detected and remediated.
- **Dust Tunnel:**
  - **Threat Description:** Custom remote operational implant capability to perform host reconnaissance and command and control.
  - **OTR Countermeasures:** PacketViper OTR is configured with a one-to-one port level trust relationship between critical devices. Any deviant connections attempting to discover, access, and or manipulate critical infrastructure other than pre-established trusts will be detected, alerted, and blocked - at wire speed - by the PacketViper OTR appliance. PacketViper OTR utilizes proprietary zero false positive threat detection, traffic anomaly sensors and unidirectional/bi-directional Security Policies to detect and restrict anomalies. Any scans, or access attempts from unauthorized systems or IP would be detected and remediated.
- **Lazy Cargo:**
  - **Threat Description:** A user-mode Windows executable that drops and exploits a vulnerable ASRock driver to load an unsigned driver.
  - **OTR Countermeasures:** PacketViper OTR protects the critical boundaries which restrict access from both foreign and domestic entities to the protected critical workstations. The appliance limits both external to internal and internal to external connections. This capability would prevent C2C communications to or from a workstation through these malware tools. PacketViper OTR is configured with a one-to-one port level trust relationship between critical devices. Any deviant connections attempting to discover, access, and or manipulate critical infrastructure other than pre-established trusts will be detected, alerted, and blocked - at wire speed - by the PacketViper OTR appliance. PacketViper OTR utilizes proprietary zero false positive threat detection, traffic anomaly sensors and unidirectional/bi-directional Security Policies to detect and restrict anomalies. Any scans, or access attempts from unauthorized systems or IP would be detected and remediated.

About PacketViper

PacketViper provides transformative and trusted cybersecurity solutions for organizations seeking to modernize the cybersecurity of converging OT and IT networks. PacketViper customers cover multiple public and private sector industries. For more visit packetviper.com.