VEDERE LABS

Industroyer2 und INCONTROLLER

Neue Erkenntnisse und Schutz gegen aktuelle, ICS-spezifische Schadprogramme durch Forescout

28. Juli 2022

1. Zusammenfassung

Im neuen Bedrohungsbericht präsentiert Vedere Labs von Forescout eine umfassende, öffentliche technische Analyse von Industroyer2 und INCONTROLLER (auch bekannt als PIPEDREAM), die neuesten ICS-spezifischen Schadprogramme, die fast zeitgleich am 12. und 13. April beschrieben wurden.

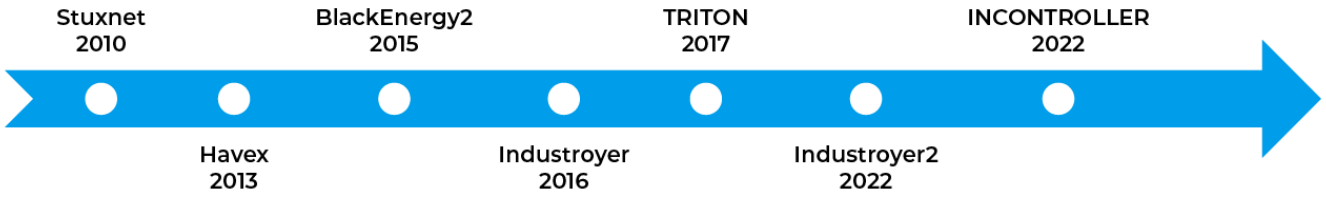
Obwohl Forscher:innen beide Schadprogrammfamilien bereits zuvor analysiert hatten, können wir folgende Neuigkeiten präsentieren:

- Eine Analyse einer Funktion in Industroyer2, mit der die gemeinsame Adresse der ASDU des Ziels erlangt werden soll. Obwohl diese Funktion aufgrund der hardkodierten Konfiguration unseres Musters nicht genutzt wurde, hätte dieses Tool in früheren Phasen der Auskundschaftung verwendet werden können, um Informationen über das Ziel zu erlangen.
- Eine Analyse der Ähnlichkeiten bei der IEC-104-Implementierung in Industroyer zeigt, dass es sich wahrscheinlich um eine modifizierte Version einer öffentlich verfügbaren Implementierung handelt.
- Die bisher ausführlichste Beschreibung von Lazycargo, einem Teil von INCONTROLLER, der vor kurzem veröffentlicht wurde, wird genutzt, um andere Elemente des Schadprogramms auszuführen.

Der Bericht enthält außerdem eine Liste mit Indikatoren für Gefährdungen und empfohlenen Gegenmaßnahmen.

2. Die Entwicklung von ICS-Schadprogrammen

ICS-spezifische Schadprogramme sind im Vergleich zu Commodity-Malware wie Ransomware oder Online-Banking-Trojanern immer noch sehr selten. Industroyer2 und INCONTROLLER orientieren sich an bisher bekannten Schadprogrammen, z.B. Stuxnet, Havex, BlackEnergy2, Industroyer und TRITON, die – wie in der nachstehenden Zeitleiste dargestellt – industrielle Steuerungssysteme ins Visier nehmen.



Industroyer2 nutzt betriebssystemspezifische Wiper und ein dediziertes Modul, um über das IEC-104-Industrieprotokoll zu kommunizieren. INCONTROLLER ist ein komplettes Toolkit mit Modulen, die über industrielle Netzwerkprotokolle wie OPC UA, Modbus, CODESYS, Machine Expert Discovery und Omron FINS Anweisungen versenden oder Daten von ICS-Geräten abfragen. Darüber hinaus besitzt Industroyer2 eine extrem spezifische Konfiguration, während INCONTROLLER auf unterschiedliche Ziele ausgerichtet ist.

Sowohl Industroyer2 als auch INCONTROLLER wurden entdeckt, bevor sie physische Probleme verursachen konnten. Industroyer2 wurde vermutlich von Sandworm APT entwickelt, einer Hackergruppe, die mit dem russischen Nachrichtendienst GRU in Verbindung gebracht wird, der hinter den Attacken auf das ukrainische Stromnetz 2015 und 2016 steckt. Industroyer2 wurde im Anschluss an 2022 erfolgte Maßnahmen gegen APT, wie die Auflösung des Botnetzes Cyclops Blink, entdeckt. Allerdings gibt es immer noch keine eindeutigen Hinweise auf die Akteure hinter INCONTROLLER, ihre Motive oder ihre Ziele.

Die beiden neuen Schadprogramme zeigen, dass der Missbrauch von oftmals aufgrund von Designfehlern unsicheren nativen Funktionen von OT-Geräten auch weiterhin die bevorzugte Strategie von realen Angreifern ist.

Vedere Labs machte vor kurzem gleich 56 durch Designfehler verursachte Schwachstellen in OT-Geräten unter der Bezeichnung OT:ICEFALL bekannt; davon betroffen sind auch Omron-Steuerungen, die von INCONTROLLER attackiert werden. Das Auftauchen neuer Schwachstellen und neuer Schadprogramme, die Schwachstellen in aufgrund von Designfehlern unsicheren OT-Geräten ausnutzen, bestätigt den Bedarf an robuster OT-kompatibler Netzwerküberwachung und Deep Packet Inspection-Technologie.

3. Gegenmaßnahmen

Kunden von Forescout eyeInspect sollten die nachstehenden Empfehlungen durchgehen, um sich zu vergewissern, ob sie gegen Industroyer2 und INCONTROLLER geschützt sind.

1. Allgemeine Empfehlungen

- Verfolgen Sie die Veröffentlichung neuer Inhalte wie Scripts und IoCs im OT-Portal oder durch Ihre Forescout-Kontaktpersonen.
- Überwachen Sie Schwachstellen im Netzwerk von Steuerungssystemen und HMIs.
- Sorgen Sie für die lückenlose Überwachung von Verbindungen zu Geräten außerhalb der dokumentierten Normen für das Gerät und seiner Umgebung, insbesondere bei HTTP- und Telnet-Verbindungen zu diesen Geräten.
- Überwachen Sie unautorisierte Telnet-Verbindungsversuche, einschließlich der Verwendung von Standardzugangsdaten.
- Identifizieren Sie ICMP-Nutzung und insbesondere mögliche Ping Sweeps anhand der ICMP-Indikatoren in der Industrial Threat Library, um mögliche Port-Scans und Identifizierungen zu entdecken.
- Weitere Konfigurationsoptionen können auf eyeInspect aktiviert werden, um die Erkennung von Eindringlingen an bekannten Knoten durchzuführen. Es sind diverse Konzepte wie Protokoll-Blacklisting und Kommunikations-Whitelisting mit Verkehrsregeln verfügbar.
- Das Script für Add-Ons zur Erkennung von Bedrohungen enthält weitere Prüfungen für Lateral Movement sowie Manipulation von Benutzerkonten und kann Versuche identifizieren, Administratorenrechte zu erlangen.
- Folgende Protokolle, die von den beiden neuen Schadprogrammen genutzt werden, sollten umfassend auf Anzeichen von Anomalien überwacht werden: IEC-104 (2404/TCP), OPC UA (4840/TCP, 4843/TCP), Modbus (502/TCP), Machine Expert Discovery (27126/UDP, 27127/UDP), CODESYS (1740-1743/UDP, 11740-11743/TCP, 1105/TCP) und Omron FINS (9600/TCP, 9600/UDP). Weiter unten finden Sie spezifische Empfehlungen für die einzelnen Protokolle in eyeInspect.

Weitere Informationen und technische Analysen finden Sie im vollständigen Bericht.


VEDERE LABS