VEDERE LABS

Industroyer2 et INCONTROLLER

De nouvelles découvertes, et comment Forescout offre une protection contre les plus récents logiciels malveillants spécifiques aux SCI

28 juillet 2022

1. Résumé

Dans notre nouveau rapport sur les menaces, l'équipe Vedere Labs de Forescout présente l'analyse technique publique la plus détaillée sur Industroyer2 et INCONTROLLER (également connu sous le nom de PIPEDREAM), les exemples le plus récents de logiciels malveillants spécifiques aux SCI, diffusés publiquement quasi simultanément les 12 et 13 avril.

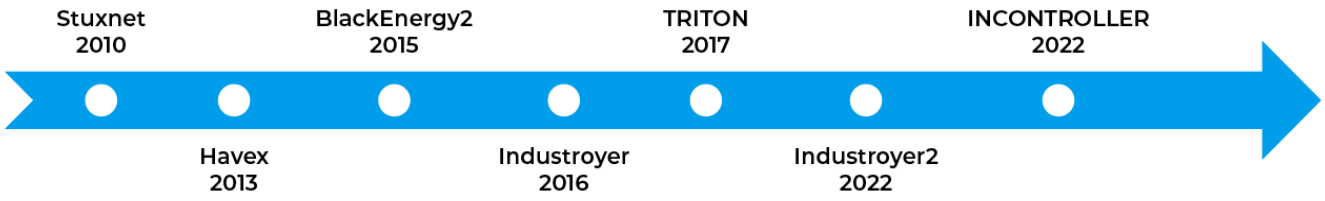
Bien qu'il existe des rapports antérieurs sur les deux familles de logiciels malveillants analysées dans cette recherche, nous apportons ici de nouvelles contributions :

- Une analyse d'une fonctionnalité dans Industroyer2 permettant de découvrir l'adresse commune de l'ASDU de la cible. Bien qu'elle n'ait pas été activée compte tenu de la configuration codée en dur de notre échantillon, il pourrait s'agir d'un outil utilisé lors des étapes de reconnaissance précédentes pour recueillir des informations sur la cible.
- Une analyse de la similitude de l'implémentation du IEC-104 dans Industroyer, qui révèle qu'il s'agit très probablement d'une version modifiée d'une implémentation disponible publiquement.
- La description publique la plus détaillée à ce jour de Lazycargo, une partie d'INCONTROLLER qui a été récemment diffusée publiquement et qui est utilisée pour exécuter d'autres parties du malware.

Le rapport contient également une liste d'indicateurs de compromission et de mesures d'atténuation recommandées.

2. L'évolution des logiciels malveillants ciblant les SCI

Les logiciels malveillants spécifiques aux SCI sont encore très rares par rapport aux logiciels malveillants de base tels que les rançongiciels ou les chevaux de Troie bancaires. Industroyer2 et INCONTROLLER font suite à de précédents exemples connus de logiciels malveillants ciblant les systèmes de contrôle industriel, tels que Stuxnet, Havex, BlackEnergy2, Industroyer et TRITON, présents dans la ligne du temps ci-dessous.



Industroyer2 exploite des curseurs spécifiques au système d'exploitation et un module dédié pour communiquer via le protocole industriel IEC-104. INCONTROLLER constitue lui un kit d'outils complet contenant des modules permettant d'envoyer des instructions à des appareils ICS ou de récupérer des données à partir de ceux-ci à l'aide de protocoles de réseau industriel, tels que OPC UA, Modbus, CODESYS, Machine Expert Discovery et Omron FINS. En outre, Industroyer2 a une configuration très ciblée, tandis que INCONTROLLER est davantage réutilisable sur différentes cibles.

Industroyer2 et INCONTROLLER ont tous deux été interceptés avant de causer des perturbations physiques. Industroyer2 serait développé et déployé par l'APT Sandworm, lié au GRU russe, qui était à la source des attaques initiales sur le réseau électrique ukrainien en 2015 et 2016. L'incident Industroyer2 fait suite à une activité récente contre l'APT en 2022, comme la perturbation du botnet Cyclops Blink. Il n'y a toujours pas de preuves concluantes au sujet des acteurs derrière INCONTROLLER, de leurs motivations ou de leurs objectifs.

Ces deux nouveaux logiciels malveillants montrent que l'usage abusif des capacités natives des équipements OT, souvent non sécurisées par conception (« insecure-by-design »), reste le modus operandi préféré des attaquants du monde réel. Vedere Labs a récemment divulgué un ensemble de 56 vulnérabilités « insecure-by-design » dans des équipements OT, dénommé OT:ICEFALL, qui comprenait des contrôleurs Omron ciblés par INCONTROLLER. L'émergence de nouvelles vulnérabilités et de nouveaux logiciels malveillants exploitant la nature non sécurisée par conception des technologies opérationnelles confirme la nécessité de disposer de capacités robustes de surveillance de réseau et d'inspection approfondie des paquets.

3. Atténuations

Les clients de Forescout eyeInspect peuvent suivre les recommandations ci-dessous pour s'assurer qu'ils sont protégés contre Industroyer2 et INCONTROLLER.

1. Recommandations générales

- Suivre la publication de contenus supplémentaires tels que les scripts et les IoC sur le portail OT ou par l'intermédiaire de vos représentants Forescout.
- Surveiller l'exposition du réseau pour les systèmes de contrôle et les IHM.
- Surveiller en détail les connexions aux dispositifs fonctionnant en dehors des normes documentées pour le dispositif et l'environnement, en accordant une attention particulière aux connexions HTTP et Telnet à ces dispositifs.
- Surveiller les tentatives de connexion Telnet non autorisées, y compris l'utilisation des informations d'identification par défaut.
- Détecter l'utilisation d'ICMP et surtout les éventuels balayages ping des indicateurs ICMP de la bibliothèque de menaces industrielles consacrée à la détection d'éventuels balayages et découvertes de ports**.**
- Des configurations supplémentaires peuvent être appliquées à eyeInspect pour effectuer une détection d'intrusion sur des nœuds connus. Certaines approches sont disponibles, telles que la liste noire de protocoles et la liste blanche de communication avec des règles de trafic.
- Le script « Threat Detection Add-Ons » contient des vérifications supplémentaires pour les mouvements latéraux et la manipulation de comptes d'utilisateurs, ce qui peut révéler des tentatives d'obtention de droits administratifs.
- Les protocoles exploités par les deux nouveaux logiciels malveillants doivent être surveillés de près pour détecter tout signe d'anomalie : 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) et Omron FINS (9600/TCP, 9600/UDP). Nous présentons ci-dessous des recommandations spécifiques à chaque protocole dans eyeInspect.

Pour plus d'informations et d'analyses techniques, lisez ici le rapport complet.


VEDERE LABS