VEDERE LABS

Industroyer2 e INCONTROLLER

Nuove scoperte: in che modo Forescout protegge contro i più recenti malware ICS

28 luglio 2022

1. Sintesi

Nell'ultimo report sulle minacce, Vedere Labs di Forescout presenta l'analisi tecnica pubblica più dettagliata di Industroyer2 e INCONTROLLER (anche noto come PIPEDREAM), i nuovi esemplari di malware ICS rilasciati al pubblico quasi simultaneamente, il 12 e 13 aprile.

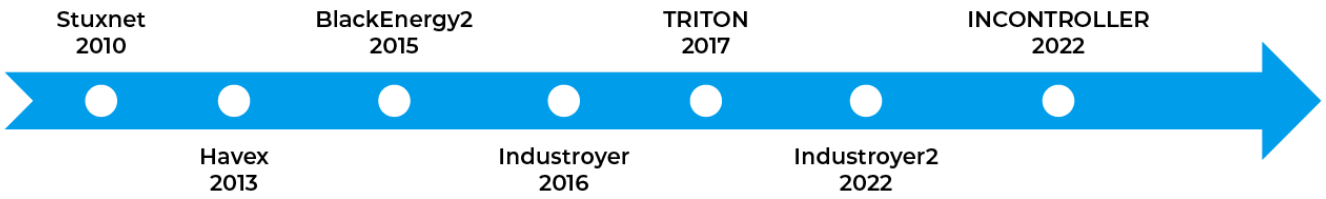
Anche se abbiamo pubblicato altri report in passato su entrambe le famiglie di malware analizzate in questo studio, presentiamo ora i seguenti nuovi contributi:

- Un'analisi della funzionalità di Industryoer2 per scoprire i Common Address ASDU del target. Pur non avendolo usato, vista la codifica rigida del nostro campione, potrebbe essere stato utilizzato in fasi di riconoscimento precedenti per raccogliere informazioni sul target.
- Un'analisi delle somiglianze dell'implementazione di IEC-104 in Industroyer che mostra che si tratta probabilmente di una versione modificata di un'implementazione disponibile pubblicamente.
- La descrizione pubblica più dettagliata finora di Lazycargo, una parte di INCONTROLLER che è stata resa pubblica recentemente ed è utilizzata per eseguire altre parti del malware.

Il report contiene inoltre una lista di indicatori di compromissione e le misure attenuative raccomandate.

2. L'evoluzione dei malware ICS

I malware ICS sono ancora molto rari rispetto ai commodity malware come i ransomware o i trojan bancari. Industroyer2 e INCONTROLLOER seguono esempi precedenti noti di malware che hanno come obiettivo i sistemi di controllo industriale come Stuxnet, Havex, BlackEnergy2, Industroyer e TRITON , così come indicato nella linea temporale qui sotto.



Industroyer2 sfrutta wiper specifici per OS e un modulo dedicato per comunicare attraverso il protocollo industriale IEC-104. INCONTROLLER è un toolkit completo che contiene moduli che inviano istruzioni o recuperano dati da dispositivi ICS tramite protocolli di rete industriali, come OPC UA, Modbus, CODESYS, Machine Expert Discovery e Omron FINS. Inoltre, Industroyer ha una configurazione altamente specifica per un target, mentre INCONTROLLER è più riutilizzabile per diversi target.

Entrambi i malware sono stati scoperti prima di causare interruzioni fisiche. Si ritiene che Industroyer2 sia stato sviluppato e distribuito dal gruppo Sandworm APT, legato a Russian GRU, responsabile degli attacchi alla rete elettrica ucraina nel 2015 e 2016. L'incidente legato a Industroyer2 si verifica dopo le recenti attività eseguite contro l'APT nel 2022, come la neutralizzazione della botnet Cyclops Blink . Non vi è ancora alcuna prova inconfutabile sui creatori di INCONTROLLER, le loro motivazioni o i loro obiettivi.

Entrambi i malware mostrano che lo sfruttamento delle capacità native dei dispositivi OT, spesso nate già con falle di sicurezza, continua a essere il modus operandi favorito per gli attacchi al mondo reale. Vedere Labs ha recentemente rilasciato un set di 56 vulnerabilità innate nei dispositivi OT chiamato OT:ICEFALL, che include i controller Omron obiettivo di INCONTROLLER. La comparsa di nuove vulnerabilità e malware che sfruttano le

falle di sicurezza innate dell'OT dimostra la necessità di un efficiente monitoraggio reti che tenga conto dei dispositivi OT e di congrue capacità di ispezione approfondita dei pacchetti.

3. Misure attenuative

I clienti Forescout eyeInspect possono seguire le raccomandazioni che seguono per garantire la protezione contro Industroyer2 e INCONTROLLER.

1. Raccomandazioni generali

- Seguire il rilascio di contenuti addizionali come script e IoC sull'OT Portal o attraverso il vostro rappresentante Forescout.
- Monitorare l'esposizione della rete per sistemi di controllo e HMI.
- Monitorare accuratamente le connessioni a dispositivi al di fuori dalla norma per il dispositivo o l'ambiente, con speciale attenzione a connessioni HTTP o Telnet.
- Monitorare tentativi di connessione Telnet non autorizzati, compreso l'utilizzo di credenziali di default.
- Rilevare l'uso di ICMP e specialmente i possibili ping sweep attraverso gli indicatori ICMP presenti nella Industrial Threat Library dedicata all'individuazione di eventuali port scan.
- È possibile adottare configurazioni aggiuntive su eyeInspect per eseguire la rilevazione delle intrusioni sui nodi noti. Sono disponibili diversi approcci, come il protocol blacklisting o il whitelisting delle comunicazioni con regole di traffico.
- Lo script Threat Detection Add-Ons contiene controlli aggiuntivi per movimento laterale e manipolazione account utente. Con questo strumento è possibile scoprire eventuali tentativi di acquisizione di diritti di amministratore.
- Eseguire un attento monitoraggio per segnali di anomalie sui protocolli sfruttati da entrambi i nuovi malware: 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) and Omron FINS (9600/TCP, 9600/UDP) . Di seguito, presentiamo raccomandazioni specifiche per ogni protocollo in eyeInspect.

Per maggiori informazioni e analisi tecniche, si prega di leggere l'intero report a questo link.


VEDERE LABS