Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Organo direzione informatica della Confederazione ODIC
Servizio delle attività informative della Confederazione SIC

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI

Sintesi del rapporto tecnico sul caso di spionaggio alla RUAG

Il MELANI/GovCERT ha analizzato il caso di cyberspionaggio contro la RUAG per fare chiarezza e garantire protezione. Il Consiglio Federale ha deciso di pubblicare il presente rapporto in modo che altre organizzazioni possano verificare che le proprie reti non siano vittime di infezioni simili e per illustrare il modus operandi del gruppo di hacker.

Gli hacker hanno usato un malware della famiglia Turla, in circolazione da parecchi anni. La variante rilevata nella rete della RUAG non ha funzionalità rootkit ma ricorre a tecniche di camuffamento per non essere individuata. Gli hacker sono stati molto pazienti durante l'infiltrazione e i movimenti laterali. Hanno attaccato solo vittime designate, adottando a questo scopo diverse misure tra cui un elenco d'indirizzi IP e un approfondito rilevamento dell'impronta digitale («fingerprinting») prima e dopo l'infezione iniziale. Una volta entrati nella rete, si sono mossi lateralmente infettando altri dispositivi e ottenendo maggiori privilegi. Uno dei loro obiettivi principali era l'Active Directory, attraverso la quale controllare altri dispositivi e usare le autorizzazioni e le appartenenze ai gruppi richiesti per accedere ai dati ritenuti di interesse. Il malware utilizzava HTTP per trasferire i dati all'esterno, dove erano installati svariati server di comando e di controllo (C&C). I server C&C avevano il compito di inviare nuovi comandi ai dispostivi infettati, per esempio nuovi dati binari, file di configurazione o comandi batch. Nella rete infiltrata gli hacker hanno utilizzato delle named pipes per la loro comunicazione interna, così da renderne difficoltosa la rilevazione. La comunicazione era strutturata secondo un sistema gerarchico, quindi non tutti i dispositivi infettati comunicavano con i server C&C. Tra i sistemi utilizzati troviamo i cosiddetti droni di comunicazione e droni di lavoro. Questi ultimi non comunicavano con il mondo esterno ma venivano utilizzati per sottrarre ed inviare dati ai primi che si occupavano, poi, di trasferirli all'esterno. Stimare il danno arrecato dagli hacker è difficile e non è lo scopo del presente rapporto. Abbiamo tuttavia rilevato schemi interessanti nei proxy log: gli hacker hanno alternato fasi di calma, in termini sia di richieste sia di quantità di dati trasferiti, a periodi di attività molto intensa con numerose richieste e grandi quantità di dati trafugati.

Nel rapporto formuliamo alcune raccomandazioni sulle contromisure che riteniamo maggiormente efficaci per proteggersi da questo genere di attacchi al sistema, all'Active Directory e a livello di rete. È importante notare che molte contromisure non sono costose, ma richiedono una discreta mole di lavoro. Sebbene sia difficile proteggere al cento per cento un'organizzazione da simili aggressori, confidiamo di poterli stanare perché tutti commettono errori. L'organizzazione attaccata deve essere preparata a individuare le tracce e a scambiare informazioni con altre parti per seguire da vicino gli hacker.

La seguente infografica illustra la cronologia del caso di cyberspionaggio: