Dipendente dell’Aeroporto utilizzava gli impianti della SACAL per “estrarre” Criptovalute. Video

Data: Invalid Date | Autore: Redazione

Polizia di Stato: denunciato dipendente dell’Aeroporto di Lamezia Terme. Utilizzava gli impianti della SACAL per “estrarre” criptovalute.
CATANZARO, 30 OTT - La Polizia Postale di Reggio Calabria e Catanzaro ha denunciato un dipendente della Società Aeroportuale Calabrese che utilizzava gli impianti della SACAL per “estrarre” criptovalute.

L’uomo, attirato dal miraggio dei guadagni offerti dalle nuove opportunità della tecnologica informatica, aveva approfittato della sua posizione lavorativa all’interno dello scalo aeroportuale di Lamezia Terme, per istallare un malware e sfruttare l’infrastruttura informatica della SACAL s.p.a., che gestisce gli aeroporti calabresi per “estrarre” ovvero produrre moneta virtuale, mettendo in pericolo la sicurezza dell’infrastruttura critica.

E’ quanto è emerso dalle indagini a carico di un tecnico addetto all’infrastruttura informatizzata dell’aeroporto di Lamezia Terme, che aveva avviato il business illegale pensando di passare inosservato.

I tecnici della SACAL, società che gestisce l’aeroporto, allarmati da alcune anomalie sui sistemi informatici della rete tecnologica aeroportuale, hanno immediatamente informato la Polizia di

Frontiera, che ha richiesto l'intervento degli esperti della Polizia Postale.

Gli investigatori, con la collaborazione delle autorità aeroportuali, hanno analizzato approfonditamente le partizioni della rete informatica interna all'hub aeroportuale, scoprendo la presenza, in due differenti locali tecnici, di una vera e propria "MINING FARM", ovvero di una rete abusiva composta da ben cinque potenti elaboratori elettronici, denominati "Mining RIG", termine con il quale si indicano in gergo tecnico i sistemi utilizzati per la creazione bitcoin o altre criptovalute, collegati alla rete Internet esterna attraverso i sistemi dedicati alla gestione dei servizi aeroportuali ed alimentati attraverso la fornitura di energia elettrica dell'Aeroporto.

Tale architettura consentiva all'utilizzatore del sistema integrato con la rete aeroportuale, di approvvigionarsi della criptovaluta "Ethereum", prodotta senza sostenere le ingenti spese di energia elettrica necessaria per il funzionamento h24 delle apparecchiature e sfruttando la connettività fornita dagli impianti info-telematici della SACAL, compromettendo la sicurezza ed esponendo i sistemi di gestione dello scalo.

All'esito dei primi accertamenti il personale della Specialità ha informato la Procura della Repubblica di Lamezia Terme, che ha immediatamente coordinato una complessa e meticolosa attività d'indagine di tipo tecnico-informatico e tradizionale.

Infatti se da un lato le attività tecniche hanno consentito di esaminare gli indirizzi IP abbinati alle macchine installate, di individuare il sito del Pool "Ethermine" (utilizzato per minare criptovaluta Ethereum), e di porre in essere un attento monitoraggio del sito e dell'infrastruttura tecnologica, dall'altro sono subito partiti mirati servizi di appostamento ed osservazione, svolti anche attraverso telecamere appositamente installate nei luoghi interessati, che hanno consentito agli investigatori di individuare il 41enne dipendente della SACAL.

Il tempestivo intervento degli operatori ha consentito di prevenire i rischi per la sicurezza dell'infrastruttura aeroportuale, provvedendo alla disinstallazione dei sistemi abusivi, posti sotto sequestro e quindi al ripristino delle condizioni di funzionamento degli impianti e della sicurezza dei servizi aeroportuali.

Il caso di specie è rappresentativo di un fenomeno in crescita, con l'avvento della moneta virtuale si sono moltiplicati infatti gli attacchi di cybercriminali che, in qualsiasi modo, cercano di prelevare fraudolentemente energia o sfruttare la potenza di calcolo dei sistemi informatici di grosse industrie, centrali elettriche o, come in questo caso, di aeroporti, per il funzionamento degli elaboratori destinati ad estrarre cripto valuta, attraverso azioni che mettono in serio pericolo la sicurezza ed lo stesso funzionamento dei plessi industriali colpiti.

L'Autorità Giudiziaria lametina, che ha convalidato il sequestro di tutte le apparecchiature elettroniche abusivamente installate nei sistemi aeroportuali, ha disposto ulteriori approfondimenti per accertare l'eventuale coinvolgimento di altri soggetti.

Clicca QUI per il video