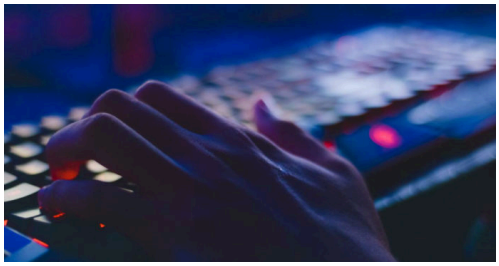

Tecnologia - *Cybersicurezza, report Swascam: da gennaio 700 vittime di attacchi ransomware*

Roma - 14 nov 2022 (Prima Notizia 24) **242 obiettivi colpiti nel solo mese di settembre, registrato un aumento del 116% rispetto ai 112 di gennaio.**

Da gennaio di quest'anno, le vittime colpite da cyberattacchi sono più che raddoppiate. E' quanto risulta dal report del terzo trimestre di Swascam - compagnia specializzata in sicurezza informatica - inerente le cybergang ransomware. Sono stati 700 gli obiettivi attaccati ed esposti alla pubblicazione dei propri dati in 76 paesi nel terzo trimestre di quest'anno, di cui 242 nel solo mese di settembre con una crescita del 116% rispetto ai 112 attacchi registrati a gennaio. 36 i gruppi ransomware che utilizzano il data leak in attività censiti tra luglio e settembre, con un aumento del 16% rispetto ai 31 del secondo trimestre.Una maggiore estensione di nazioni coinvolte, il 22,5% in più in confronto ai 62 Stati in cui risiedevano le realtà colpite tra aprile e giugno di quest'anno. Questo il bottino di guerra delle cybergang nel Q3 2022, secondo il terzo rapporto trimestrale "Gang Ransomware" redatto dal SOC e Threat Intelligence team di Swascan.Una analisi condotta attraverso la piattaforma proprietaria italiana di cyber Threat Intelligence e rilasciata on line sul sito della società italiana di cybersicurezza, grazie alla quale si ha traccia aggiornata dell'attività cybercriminale nel web a otto mesi dall'invasione russa dell'Ucraina. La parte del leone, come usuale dalla scomparsa di Conti Team a pochi giorni dall'attacco contro Kiev, la fa la cyebrgang russa LockBit, con il 33.4% dei data leak nel terzo trimestre. Distanziata al secondo posto BlackBasta, di probabile origine sudafricana, con il 7.7%, e al terzo posto a parimerito ALPHV/BlackCat e Hive con il 6.8% di data leak ciascuna. Il terzo trimestre è stato inoltre caratterizzato dall'emergere di nuove gang ransomware: BianLian, Yanluowang, IceFire, 0mega, Cheers, Redalert, Daixin, Donut Leaks, Bl00dy, Industrial SPY. Con 10 vittime pubblicate nel mese di luglio, il debutto di BianLian è paragonabile in dimensioni all'emergere di BlackBasta nel mese di aprile.29 le aziende vittime in Italia di pubblicazione di dati per mancato pagamento del riscatto nel periodo preso in esame, che fanno del nostro Paese il sesto al mondo per numero di realtà con dati esfiltrati e resi pubblici. Questo fa scendere l'Italia fuori dalla top 5 delle nazioni più colpite, "forse sintomo di una maggiore propensione a cedere al riscatto, pena il terribile danno d'immagine e di business Continuity che sovente accompagna questi cyber incident", commenta il ceo di Swascan, Pierguido Iezzi. Il rapporto analizza le specifiche delle gang più importanti, prende in considerazione i diversi settori colpiti e dà notizia della diffusione in rete del codice di LockBit 3.0 avvenuta il 21 settembre, subito utilizzato da altri gruppi ransomware per ulteriori attacchi."Quest'ultimo dato - considera Iezzi - lascia prevedere che nei prossimi mesi dal leak del codice di Lockbit nascano diverse nuove gang. Le conseguenze potrebbero essere quelle di dover far fronte a una nuova impennata di attacchi e ad un ulteriore abbassamento dell'asticella - dal punto di vista di know-how e

capacità tecniche - per gli aspiranti Criminal Hacker. Diventa dunque essenziale - conclude Iezzi - continuare a lavorare su resilienza e capacità di assorbimento degli impatti in azienda".Un ulteriore aumento delle gang RaaS, quindi, secondo l'esperto, non è da escludere."Il continuo utilizzo del ransomware, in un periodo così critico dal punto di vista geo-politico - sottolinea il CEO di Swascan Pierguido Iezzi - potrebbe ben presto trasformarsi in una lama a doppio taglio. Non solo il danno economico e di business Continuity causato dall'infezione in sé e per sé, ma anche il rischio che i dati colpiti dai Criminal Hacker vengano sottratti in maniera massiva. Non dobbiamo dimenticare che la maggior parte delle gang opera nei territori dell'Europa orientale. Una zona che per contingenze politiche al momento è tagliata fuori da contatti con l'occidente e che si vedrà presto costretta a sopperire in qualche modo all'assenza di know-how tecnologico fino ad oggi "importato" dall'occidente. I Criminal Hacker, in particolare le gang ransomware, potrebbero quindi trasformarsi nei "mercanti" di questo traffico illecito di conoscenze e tecnologie, avendo un accesso privilegiato - e ovviamente del tutto illegale - alle strutture che mantengono questo vantaggio competitivo".

(Prima Notizia 24) Lunedì 14 Novembre 2022

Sede legale : Via Costantino Morin, 45 00195 Roma
E-mail: redazione@primanotizia24.it