AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

Tecnologia - *Tecnologia, Palo Alto Networks: “Continuiamo a seguire il ransomware Conti"*

Roma - 27 ott 2021 (Prima Pagina News)

La società è sulle tracce del codice pericoloso.

l gruppo di cybercriminali Conti ha rivendicato sul proprio sito web l'attacco a San Carlo. Il ransomware Conti si distingue perché uno dei più spietati tra le decine che monitoriamo.Come rilevato da Unit 42 di Palo Alto Networks, il gruppo ha attaccato per oltre 12 mesi organizzazioni in cui le interruzioni IT potevano avere conseguenze pericolose per gli individui: ospedali, operatori del 118, servizi medici di emergenza e commissariati di polizia. Conti si distingue anche per la sua inaffidabilità: molte vittime sono state imbrogliate e, nonostante il pagamento del riscatto, non hanno recuperato i propri dati. L’FBI ha collegato Conti a più di 400 attacchi IT contro organizzazioni in tutto il mondo, tre quarti delle quali hanno sede negli Stati Uniti, con richieste fino a 25 milioni di dollari, che fanno di Conti uno dei gruppi più interessati al guadagno. Unit 42 ha seguito Conti per oltre un anno per aiutare le aziende agli attacchi. Sembra essere uno dei tanti gruppi di criminali che ha sfruttato il fiorente ecosistema del ransomware-as-a-service (RaaS) acquistando un accesso alle reti delle loro vittime da altri autori di minacce e procurandosi infrastrutture, malware, strumenti di comunicazione e riciclaggio di denaro da altri fornitori RaaS. La maggior parte utilizza gli stessi metodi di accesso comuni a molti attacchi ransomware, come e-mail di phishing, sfruttamento di applicazioni non protette esposte su Internet, mancanza di autenticazione a più fattori (MFA), così come i tipici percorsi utilizzati per conservare e migliorare l’accesso, ad esempio attraverso l’uso di Cobalt Strike o PowerShell. Questi approcci non sono particolarmente intelligenti o sofisticati, ma sono spesso efficaci. La metodologia di Conti segue di frequente l’approccio della “doppia estorsione” per cui gli attaccanti non solo bloccano i file della vittima e chiedono il riscatto, ma se ne impossessano, minacciando di pubblicarli sul web o di diffonderli in altro modo se la loro richiesta non viene soddisfatta.

(Prima Pagina News) Mercoledì 27 Ottobre 2021

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it