Nuova fuga di dati sul gruppo di pirati Conti

Il presunto membro della gang di ransomware Conti che ne sta diffondendo i dati come ritorsione per il loro supporto alla Russia ha pubblicato altro materiale, tra cui uno strumento di decrittazione

Purtroppo lo **strumento di decrittazione non funziona per ripristinare i documenti crittati dalle versioni recenti dell'attacco ransomware** Conti, ma i dati forniti sono comunque preziosi.

Contengono, tra gli altri segreti dell'organizzazione, il **codice sorgente per il ransomware Conti e il malware TrickBot insieme a tattiche, tecniche e procedure** dei cybercriminali.

Come riportato in un articolo di Threatpost, gli analisti di CyberArk hanno pubblicato un elenco dei contenuti divulgati, spiegandone l'importanza anche nell'attuale conflitto. Sono infatti in corso attacchi digitali all'Ucraina, oltre quelli bellici, e c'è anche **rischio che i cyberattacchi si estendano ad altri paesi**, come sottolineato da un documento dell'agenzia per cybersicurezza statunitense CISA.

Tra il materiale divulgato ci sono **messaggi di chat con le comunicazioni interne di Conti** tra giugno e novembre 2020, che danno anche accesso agli username dei partecipanti. C'è anche

il **contenuto della cache del pannello di amministrazione** che ha permesso di scoprire che Conti fa ampio uso di programmi Open Source.

Questa seconda fuga di dati contiene inoltre **credenziali e materiale legati al malware per il furto di credenziali Pony** e le conversazioni dei cybercriminali riguardo alcuni degli strumenti che utilizzano. Tra questi Cobalt Strike, un programma legittimo usato per i **penetration test** e sfruttato dai pirati per identificare vulnerabilità.

Nei documenti divulgati c'è anche il **materiale formativo utilizzato dalla gang per istruire i propri membri** sui vari aspetti delle loro attività criminali e **informazioni sul trojan TrickBot**, incluse parti del codice.

Gli analisti però sottolineano che **le fughe di notizie Conti non avranno un forte impatto sull'organizzazione di cybercriminal**i. Sono infatti relative solo a uno dei sei gruppi che la compongono, per quanto il più importante. Gli altri non hanno avuto alcun impatto e Conti, dopo aver riorganizzato la sua infrastruttura, ha continuato a operare.

https://www.securityinfo.it/2022/03/03/nuova-fuga-di-dati-sul-gruppo-di-pirati-conti/?utm_source=rss&utm_medium=rss&utm_campaign=nuova-fuga-di-dati-sul-gruppo-di-pirati-conti