

BlackCat: conosciamo meglio questo ransomware



BlackCat (alias ALPHV) è una famiglia di ransomware emersa a metà novembre 2021 che ha rapidamente guadagnato notorietà per la sua sofisticazione e innovazione. Operando con un modello di business ransomware-as-a-service (RaaS), BlackCat è stato osservato mentre cercava affiliati in noti forum di criminalità informatica, offrendo loro la possibilità di sfruttare il ransomware e mantenere l'80-90% del pagamento del riscatto. Il resto sarebbe stato pagato all'autore di BlackCat.

A partire da dicembre 2021, poco più di un mese dopo essere emerso, il gruppo BlackCat ha il settimo maggior numero di vittime elencate tra i gruppi monitorati da Unit 42 – e la sua lista continua a crescere.

Le vittime si estendono in vari settori, tra cui edile, assicurativo, trasporti e altro – rendendo l'impatto del gruppo ancora più vasto. Gli affiliati di BlackCat hanno chiesto riscatti fino a 14 milioni di dollari – quasi tre volte la richiesta media di 5,3 milioni di dollari a inizio 2021.

L'emergere di BlackCat è parte di un trend preoccupante, con nuove minacce che possono avere un impatto devastante in un breve lasso di tempo. Il successo del gruppo è attribuito in parte alla personalizzazione dei suoi attacchi e agli algoritmi efficienti che alimentano la crittografia.

BlackCat ha adottato un approccio aggressivo nel citare pubblicamente le vittime, elencandone più di una dozzina sul loro sito in poco più di un mese. Il maggior numero di vittime del gruppo finora sono organizzazioni statunitensi, ma

BlackCat e i suoi affiliati hanno attaccato anche aziende in Europa, Filippine e altri paesi. Le vittime appartengono a diversi settori, tra cui edilizia e ingegneria, retail, trasporti, servizi commerciali, assicurazioni, , servizi professionali, telecomunicazioni, componenti auto e prodotti farmaceutici.

L'uso del ransomware BlackCat è cresciuto rapidamente per una serie di ragioni. Attività di marketing efficaci dedicate agli affiliati hanno probabilmente contribuito – oltre a offrire una quota allettante dei pagamenti del riscatto, il gruppo ha sollecitato gli affiliati pubblicando annunci su forum come Ransomware Anonymous Market Place (RAMP).

Il malware stesso è codificato nel linguaggio di programmazione Rust e nonostante non sia il primo malware a utilizzarlo, è uno dei primi, se non il primo, ransomware a farlo. Sfruttando questo linguaggio di programmazione, gli autori sono in grado di elaborarlo facilmente su varie architetture. Date le sue numerose opzioni native, Rust è altamente personalizzabile, il che facilita la capacità di sfruttarlo e individuare gli attacchi.

Gli attori di BlackCat, spesso indicati come la “gang BlackCat”, utilizzano numerose tattiche che stanno diventando sempre più comuni. In particolare, tecniche di estorsione in alcuni casi, tra cui trafugare i dati delle vittime prima della distribuzione del ransomware, minacce di esporli se il riscatto non venisse pagato e attacchi DDoS (distributed denial-of-service).

Per ulteriori informazioni, visitare <https://unit42.paloaltonetworks.com/blackcat-ransomware/>

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/blackcat-conosciamo-meglio-questo-ransomware/>