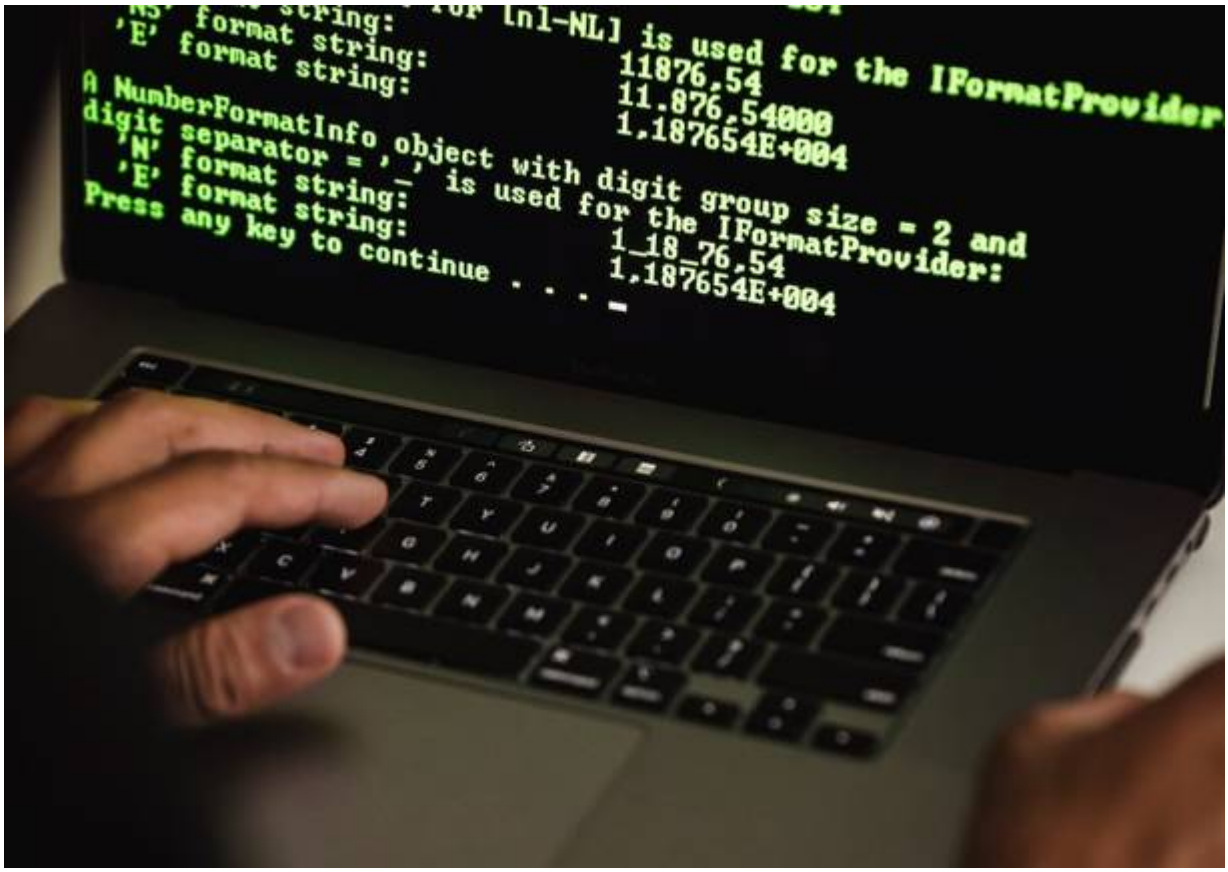
VareseNews

Scacco matto alla più grande gang di attacchi informatici

Pubblicato: Domenica 25 Febbraio 2024



La notizia. Una vasta operazione internazionale ha colpito duramente i criminali informatici di **LockBit**. La **National Crime Agency** (NCA) del Regno Unito ha sequestrato l'intera infrastruttura della cyber-gang e arrestato due affiliati in Polonia e Ucraina. Altri due sospetti di origine russa sono stati incriminati dall'FBI statunitense. Sono stati bloccati 200 crypto wallet, dove sono raccolti i fondi pagati per i riscatti di dati, ed è stato diffuso il codice per lo sblocco dei dati sotto sequestro. Il ransomware LockBit 3.0 ha causato danni in tutto il mondo, incluso un attacco ransomware contro i data center di Westpole in Italia nel dicembre 2023, che paralizzò per alcuni giorni anche molti servizi della Pubblica Amministrazione Digitale.

I cattivi. **LockBit è un'organizzazione criminale strutturata come un'azienda, che offre il ransomware come servizio (RaaS)**. Il loro software, **LockBit 3.0,** è stato sviluppato e perfezionato nel tempo per permettere agli acquirenti di effettuare attacchi ransomware. Questo tipo di attacco crittografa i dati della vittima e richiede un riscatto. Se il riscatto non viene pagato, i dati possono essere diffusi online. LockBit è stato identificato come la variante di ransomware più distribuita nel mondo nel 2022 e ha continuato a essere una minaccia significativa nel 2023. Questo ransomware è stato utilizzato per attaccare organizzazioni in vari settori critici, inclusi servizi finanziari, alimentari, istruzione, energia, governativi, sanitari, produzione e trasporti. Le versioni in continuo aggiornamento e sviluppo da parte della gang, vengono messe a disposizione di individui o gruppi (noti come "affiliati") per distribuire il ransomware in cambio di pagamento anticipato, quote di abbonamento o parte dei profitti.

In Italia, LockBit è una delle gang cyber più attive, con diversi procedimenti penali aperti.

LockBit 3.0 è stata presentata nel 2023 e ha introdotto funzionalità BlackMatter, rendendola più difficile da individuare e risolvere. Questa versione crittografa i file delle vittime in pochi minuti e può eludere le soluzioni di sicurezza tradizionali, grazie a una crittografia ultraveloce e un pannello di amministrazione intuitivo, che semplifica la gestione dell'attacco per i cybercriminali.

I buoni. Un'operazione internazionale denominata "Operazione Cronos" ha messo a dura prova la cybergang LockBit, ribaltando completamente il loro data leak site con un tocco di "British humour". Dopo un countdown di quattro ore orchestrato dal National Crime Agency (NCA) del Regno Unito, il sito è stato trasformato, sostituendo le rivendicazioni delle vittime del ransomware con dettagli sull'operazione e sulla stessa gang. Il nuovo layout del sito include informazioni dettagliate sull'operazione Cronos e sulla cyber-gang LockBit, insieme a una parodia che ironizza sul ban di LockbitSupp da parte di forum underground. Ma non è tutto: il sito offre anche un Decryptor pronto all'uso per coloro che sono stati colpiti dall'attacco di LockBit.

Questa operazione ha anche portato a un arresto in Polonia, come risultato della cooperazione internazionale. Le autorità polacche, su richiesta della Francia, hanno arrestato un individuo sospettato di essere coinvolto nell'attività di LockBit, dimostrando l'efficacia della collaborazione globale contro il crimine informatico. Inoltre, **il Dipartimento di Giustizia degli Stati Uniti ha annunciato un atto d'accusa contro due cittadini russi per l'utilizzo della variante di ransomware LockBit**, aggiungendoli alla lista degli attori già accusati in relazione a LockBit. Infine, è iniziato un ulteriore countdown. Secondo quanto riportato sul data leak site di LockBit, ulteriori informazioni riguardanti operazioni internazionali contro il crimine informatico verranno rivelate presto, mantenendo alta l'attenzione sulle azioni volte a contrastare questo tipo di attività illecita.

Come hanno fatto? LockBit si è difesa in questi anni offrendo ricompense a chi la aiutasse a rinforzare i propri sistemi dalle intrusioni delle Forze dell'ordine e agenzie di sicurezza informatica. **La NCA è riuscita ad infiltrare alcuni suoi membri nei forum di discussione nel dark web, esterni a LockBit, dove le debolezze del loro software venivano identificate e trattate**. In questo modo hanno mirato ad una "porta di ingresso" non ancora blindata completamente e, con un intervento tempestivo, hanno preso il controllo della rete. LockBit ha avvisato immediatamente i suoi affiliati criminali offrendo suggerimenti per proteggersi dalla scoperta dei loro dati di identità, ubicazione e conti bancari. Ma era troppo tardi, almeno per questa volta.

"A volte perdendo una battaglia si trova un nuovo modo di vincere la guerra", Donald Trump.

di Giuseppe Geneletti