AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

Tecnologia - *Cybersecurity, cosa aspettarsi dai gruppi di estorsione in futuro secondo Palo Alto Networks*

Milano - 21 lug 2023 (Prima Pagina News) **Le previsioni di Palo Alto Networks.**

Le informazioni che contano davvero sul panorama delle minacce non descrivono quello che è successo, ma anticipano cosa avverrà. Ecco alcune previsioni chiave in termini di estorsione, secondo gli analisti di incident response e threat intelligence di Palo Alto Networks, .Previsione n. 1: il coinvolgimento deli Governi sarà fondamentale per interrompere le attività dei gruppi di estorsione.I divieti di pagamento a determinati gruppi e Paesi hanno cambiato il panorama del business di ransomware ed estorsioni. In alcuni casi, le preoccupazioni per le sanzioni possono aver influenzato un maggior numero di organizzazioni a rifiutarsi di pagare, riducendo le entrate e inducendo gli affiliati ad abbandonare i gruppi conosciuti per lavorare con gruppi non autorizzati.Previsione n. 2: assisteremo a un evento significativo di ransomware nel cloud. Finora, la maggior parte dei casi di risposta agli incidenti nel cloud ha mostrato che gli attori delle minacce puntano agli obiettivi più facili da colpire. Le organizzazioni spesso trascurano i controlli di sicurezza di base e non sfruttano le funzionalità di sicurezza offerte dai fornitori di servizi cloud o gli strumenti aggiuntivi. Sebbene gli attori delle minacce siano a conoscenza di queste lacune, nella maggior parte dei casi hanno scelto di non sfruttarli poiché gli ambienti cloud presentano ancora alcune complessità che devono superare. Tuttavia, è chiara la loro tendenza a concentrarsi sul cloud, dedicandosi ad attacchi che richiedono maggiori competenze, ma che potrebbero avere un ritorno migliore a causa del potenziale impatto operativo sulle aziende.Negli ultimi anni, Unit 42 ha monitorato individui o gruppi che rappresentano una minaccia per le organizzazioni attraverso l'accesso diretto e prolungato a risorse, servizi o metadati facendo evolvere i loro TTP in modo specifico per colpire i carichi di lavoro del cloud. Se da un lato il modello di responsabilità condivisa riduce l'onere degli utenti nel proteggere infrastruttura, piattaforma e software nel cloud, dall'altro abbiamo visto le imprese, in particolare le più grandi del mondo, trasferire quantità crescenti di dati e carichi di lavoro nel cloud pubblico.Per questo, il 2023 sarà l'anno in cui gli attori delle minacce punteranno a distribuire il ransomware negli ambienti cloud. Previsione n. 3: gli attori delle minacce individueranno nuovi mezzi di accesso. Gli esperti di incidenti di Palo Alto Networks stanno vedendo che gli attori delle minacce si avvalgono di diverse tecniche di accesso, tra cui SEO poisoning (specialmente aumentato dal malvertising), callback phishing e false installazioni e/o aggiornamenti software. Ciò è dovuto all'efficacia di elementi di social engineering e alla necessità di allontanarsi da metodi più tradizionali, che vengono comunemente individuati.Previsione n. 4: gli attori delle minacce aumenteranno i metodi di estorsione. I dati mostrano già un aumento del furto di dati in combinazione con la crittografia. Si prevede che questa tendenza continuerà, dato che gli attori delle minacce

rispondono alla riduzione del loro tasso di successo aumentando la pressione sulle vittime. Questo porta alla prossima previsione. Previsione n. 5: le estorsioni senza cifratura diventeranno più numerose. Poiché gli attori delle minacce hanno avuto successo aggiungendo metodi di estorsione al ransomware, alcuni gruppi hanno tratto la conclusione che l'estorsione può essere efficace anche da sola. Rinunciando alla fase di cifratura, gli attori delle minacce possono ridurre la complessità tecnica di un attacco, e ci si aspetta che altri gruppi esplorino questo approccio. Previsione n. 6: gli incidenti ransomware a sfondo politico aumenteranno. Il ransomware e l'estorsione sono ovviamente condotti a scopo di lucro. Tuttavia, in alcuni casi, queste attività possono essere collegate a motivazioni politiche.I gruppi possono utilizzare il ransomware per finanziare altre attività a carattere politico o per interferire con processi nazionali, destabilizzare le infrastrutture critiche, generare tensione nei confronti dei governi e seminare discordia. Previsione n. 7: le minacce interne porteranno a tentativi di estorsione. Solo nel 2023 ci sono stati più di 100.000 licenziamenti da parte di oltre 300 aziende tecnologiche. Alcune delle persone colpite serberanno rancore e proveranno a vendicarsi. Le minacce interne possono essere particolarmente pericolose perché è più probabile che i dipendenti sappiano dove sono custoditi i gioielli della corona. Nell'ambiente attuale, un insider può coprire la propria identità vendendo l'accesso e altre informazioni a gruppi di criminali informatici, rendendo l'azione potenzialmente più remunerativa. Previsione n. 8: gli aggressori infetteranno supply chain e codice sorgente delle vittime prima di utilizzare il ransomware per distrarre dall'infezione della catena di fornitura. La crescente frequenza di eventi ransomware, abbinata a una migliore capacità di gestione da parte delle aziende potrebbe far considerare questo tipo di infezione una routine. Gli attori delle minacce ne approfitteranno, distribuendo ransomware per distrarre dal reale scopo dei loro attacchi. Portato all'estremo, questo potrebbe consentire loro di rimanere nascosti mentre orchestrano attacchi che potrebbero colpire un gran numero di organizzazioni in tutto il mondo. Le aziende dovrebbero rivedere i piani di risposta agli incidenti per il ransomware e l'estorsione in vista del panorama futuro.Si prevede che gli attori delle minacce più motivati continueranno a cercare ulteriori leve per ottenere ciò che vogliono e che altri tipi di gruppi di minacce sfrutteranno le tecniche di criminalità informatica note. I responsabili della sicurezza dovrebbero considerare che la gestione delle odierne tecniche di estorsione va oltre la salvaguardia dei dati, per quanto fondamentale. È anche una responsabilità fondamentale per proteggere la reputazione dell'organizzazione e la sicurezza di dipendenti, partner e clienti.

(Prima Pagina News) Venerdì 21 Luglio 2023

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