



Primo Piano - Estorsioni tramite attacchi cyber, Palo Alto Networks: “Record pagamenti”

Roma - 23 ago 2021 (Prima Pagina News) **La nuova ricerca.**

Il pagamento medio di un riscatto ransomware è aumentato dell'82% dal 2020, raggiungendo la cifra record di 570.000 dollari nel primo semestre 2021, a causa di tecniche sempre più aggressive atte a costringere le aziende a pagare. Questo incremento segue quello del 171% avvenuto lo scorso anno, con un importo superiore a 312.000 dollari. Questi dati, elaborati da Unit 42, il gruppo di consulenza sulla sicurezza di Palo Alto Networks, testimoniano ciò di cui molti sono già consapevoli: la crisi del ransomware continua a intensificarsi, e i cyber criminali incrementano gli investimenti in operazioni redditizie. Si sapeva già che la situazione sarebbe peggiorata: gli attacchi ransomware hanno impedito di accedere ai computer, fatto lievitare i costi della carne, ridotto i rifornimenti di benzina, chiuso scuole, ritardato cause legali e costretto alcuni ospedali a rifiutare i pazienti. La nascita della “quadrupla estorsione” è uno dei trend più preoccupanti identificati da Unit 42 nella prima metà del 2021. Chi si avvale del ransomware oggi utilizza tradizionalmente fino a quattro tecniche per costringere le vittime a pagare: 1. Crittografia: le vittime pagano per riottenere l'accesso a dati e sistemi compromessi inaccessibili a causa della cifratura. 2. Furto di dati: gli hacker pubblicheranno informazioni sensibili se il riscatto non sarà pagato. (Questo trend ha preso realmente piede nel 2020). 3. Denial of Service (DoS): le bande ransomware lanciano attacchi di denial of service che portano alla chiusura dei siti pubblici delle vittime. 4. Molestie: i cyber criminali contattano clienti, partner, dipendenti e media per comunicare loro che l'azienda è stata attaccata. Nonostante sia raro che un'organizzazione venga colpita da tutte e quattro le tecniche, quest'anno abbiamo visto gruppi ransomware adottare approcci aggiuntivi quando un'azienda non procedeva con il pagamento dopo la crittografia e il furto di dati. Il doppio, rispetto a quanto descritto nel Unit 42 Ransomware Threat Report 2021, dedicato ai trend 2020, in cui si evidenziava la doppia estorsione come tendenza emergente. Da quando hanno adottato questi approcci, i cyber criminali sono diventati ancora più avidi. La richiesta media di riscatto è aumentata del 518% nella prima metà del 2021 a 5.3 milioni di dollari, da una media di 847.000 dollari nel 2020. La richiesta più elevata fatta a una singola vittima rilevata dal nostro team è salita a 50 milioni di dollari nei primi sei mesi del 2021, dai 30 dell'anno scorso. Inoltre, REvil ha testato di recente un nuovo approccio proponendo una chiave di decrittografia universale a tutte le organizzazioni colpite dall'attacco Kaseya, al costo di 70 milioni di dollari, scendendo poi velocemente a 50 milioni. Kaseya ha ottenuto poi una chiave universale, ma non è chiaro quale sia stato il pagamento, se effettuato. Il pagamento più elevato confermato finora è di 11 milioni di dollari da parte di JBS SA dopo un vasto attacco a giugno. Lo scorso anno, il riscatto più alto era stato di 10 milioni di dollari. Prevediamo che la crisi del ransomware continuerà a crescere nei prossimi mesi a mano a mano che i



gruppi ransomware perfezionano le tecniche per convincere le vittime a pagare e sviluppano nuovi approcci per rendere gli attacchi ancora più dirompenti. Ad esempio, abbiamo iniziato a osservare crittografia di software infrastrutturale critico, noto come hypervisor, che può compromettere numerose istanze virtuali in esecuzione su un singolo server. Ci aspettiamo un numero più elevato di attacchi ad hypervisor e altre infrastrutture software gestite nei prossimi mesi e anche a managed service provider e ai loro clienti, seguendo l'ondata di azioni che hanno sfruttato il software di gestione remota Kaseya per distribuire ransomware. Prevediamo che i riscatti continueranno la loro traiettoria verso l'alto, e ci aspettiamo che alcune gang continueranno a concentrarsi sulla fascia bassa del mercato, prendendo regolarmente di mira le piccole imprese che non hanno risorse significative da investire nella sicurezza informatica. Finora abbiamo osservato gruppi, tra cui NetWalker, SunCrypt e Lockbit, richiedere e ottenere pagamenti che vanno da 10.000 a 50.000 dollari. Nonostante sembrino più bassi rispetto ai riscatti più elevati osservati, pagamenti di questa entità possono impattare in modo significativo su una piccola realtà.

(Prima Pagina News) Lunedì 23 Agosto 2021