IL CYBERCRIME ORA COLPISCE TRAMITE IL "*SUPPLY CHAIN ATTACK*" PORTA D'ACCESSO È IL TRUST TRA FORNITORE E CLIENTE

IL FURTO DI CREDENZIALI È UN'ALTRA MINACCIA IN CRESCITA NEL PANORAMA DEL CRIMINE INFORMATICO

16 MILA ATTACCHI CYBER ALLE AZIENDE ITALIANE DA LUGLIO 2020 A GIUGNO 2021, LO RILEVA IL NUOVO REPORT DI YARIX, DIVISIONE DIGITAL SECURITY DI VAR GROUP

Treviso, 02 dicembre 2021 - *"Il panorama del cyber risk in Italia sta diventando sempre più preoccupante: non parliamo più di minacce sporadiche a un gruppo limitato di aziende, percepito dagli hacker come detentore di asset di valore, ma di attacchi sistemici sempre più aggressivi, pronti a colpire qualsiasi settore e qualsiasi azienda con dati da proteggere. Il report evidenzia bene questo orientamento: il team SOC ha registrato un trend in crescita con circa 5000 eventi in media al mese."* **Mirko Gatto, CEO di Yarix** commenta così i dati del nuovo rapporto della divisione Digital Security del colosso italiano **Var Group, che analizza l'esposizione italiana agli attacchi del cybercrime** riferito al periodo **luglio 2020 - giugno 2021.**
Il report è stato curato dagli analisti del ***Cognitive Security Operation Center*** (**YCSOC**) di Yarix, una cyber control room che, 24 ore su 24, monitora e gestisce la sicurezza delle reti aziendali e pubbliche attraverso funzionalità evolute basate su AI. La base dati è stata integrata dalle risultanze delle analisi del team **Cyber Threat Intelligence di Yarix (YCTI),** che scandaglia la rete – Clear, Dark e Deep Web - per identificare informazioni utili a prevedere in anticipo potenziali attacchi informatici.

I risultati in cifre

- **circa 57.000 eventi di sicurezza rilevati (+157% YOY)**: si tratta di possibili violazioni dei livelli di sicurezza informatica, tali da configurare una situazione di potenziale rischio;
- **di questi, quasi 16.000 si sono evoluti in incidenti di sicurezza (+225% YOY)**: si tratta delle situazioni più gravi, tali da pregiudicare l'utilizzo di asset aziendali, violare disposizioni aziendali o di legge, causare la perdita o la diffusione di dati, etc;
- **1.130 eventi critici (+280% YOY)**: offensive particolarmente gravose in termini di rischio e impatti sull'infrastruttura digitale dell'organizzazione. Richiedono interventi di Emergency Response per ripristinare la normalità dei sistemi, implementare le necessarie contromisure di prevenzione e compiere una successiva analisi post-incidente per rilevare l'origine della compromissione o dell'attacco;
- Tra i settori più colpiti emergono il **manufacturing e il fashion (28% degli attacchi),** seguiti da quello relativo a **Information Technology** e **Banking and Finance,** rispettivamente al **12% e al 10%.** Particolarmente **significativo l'aumento registrato** dal settore **Health,** che si attesta a **9%.**

Il trend – Furto di credenziali, dalla vendita all'attacco
Uno dei trend in costante aumento evidenziato dal team YCTI è il **furto di credenziali e informazioni sensibili e confidenziali** per la loro conseguente messa **in vendita nel Dark Web** e nei canali underground specializzati nella compravendita di informazioni. **Il team YCTI** formato da **analisti in grado di muoversi nel dark web con profili sotto copertura**, infiltrandosi in black market e forum e di interagire direttamente con i **threat actor**, ha riportato un totale di **423 eventi** significativi riconducibili a queste attività.
Le analisi evidenziano che i threat actor agiscono principalmente attraverso due metodologie che si distinguono, oltre che per il costo, anche per le informazioni fornite. Si può avere una semplice vendita, e in questo caso l'attività si limita alla sola cessione della credenziale compromessa per l'accesso dell'azienda target, oppure di una vendita accompagnata ad una già avviata attività di compromissione. In questo secondo caso, il threat actor fornisce un accesso completo all'azienda vittima, che può potenzialmente procurare uno o più accessi o una backdoor con privilegi amministrativi all'interno dell'infrastruttura. L'accesso avviene attraverso **tre step: attività di ricognizione (reconnaissance), privilege escalation e lateral movement.**

Il trend – Supply Chain attack
Nel corso del 2021 una nuova tipologia di compromissione ha preso piede nel panorama dei cyber attacchi: **quella della *Supply Chain*** o catena di approvvigionamento**.**
Gli attacchi diretti verso organizzazioni ben protette spesso comportano un costo e una complessità rilevante per gli attaccanti; può risultare quindi più semplice attaccare la catena di approvvigionamento, che offre un

numero maggiore di possibili target e consente di trovare più facilmente un anello debole. In caso di successo l'impatto può essere significativamente più esteso e non solo rivolto al target principale dell'attacco.
Questa tipologia prevede una compromissione in almeno due fasi, una prima di compromissione del "fornitore" e una seconda di compromissione dell'anello successivo della catena di fornitura.
Il rischio per le infrastrutture target è particolarmente elevato perché sfrutta una componente insita nella maggior parte dei rapporti di fornitura, cioè il ***trust*** che c'è tra fornitore e utilizzatore del servizio, presente sia sotto forma di rapporto contrattuale, sia di rapporto basato su una fiducia insita nel servizio o nel software stesso, dettata dal brand del fornitore o da rapporti di fiducia personali.
L'attacco alla Supply Chain può avvenire attraverso:

- **la compromissione di un fornitore di servizi informatici,** utilizzando come *testa di ponte* gli accessi privilegiati alle infrastrutture dei clienti. Questi accessi sono il vettore d'attacco perfetto per un attaccante, in quanto già presenti e per loro natura abilitati allo svolgimento di diverse attività all'interno del perimetro dell'azienda. Sfruttando la catena di fiducia che lega il cliente al fornitore, l'attaccante può così massimizzare il profitto con attacchi mirati verso tutte le aziende che utilizzano lo stesso fornitore. A questo si aggiunge un ulteriore e ormai "classico" secondo ricatto, cioè quello dovuto all'esfiltrazione di dati e al danno reputazionale legato alla pubblicazione di dati relativi a contratti, clienti e know how aziendale;
- **la compromissione di un software,** solitamente diffuso all'interno delle realtà aziendali, **utilizzato come vettore del payload malevolo dell'attaccante.** In questo caso il *trust* è implicito nella presenza del software stesso e non sono rare le situazioni in cui tali software siano esclusi dai controlli di sicurezza attivi, al fine di consentirne il corretto funzionamento.

Il metodo

- Il report restituisce una rielaborazione analitica dei dati provenienti dalle aziende monitorate dal SOC e corrispondenti alla base dei clienti di Yarix, nella quale trovano espressione, in maniera trasversale, i diversi settori dell'economia nazionale. **Le imprese rappresentate nel panel analizzato occupano,** in media, **oltre il migliaio di addetti e sviluppano fatturati superiori ai 50 milioni di euro**. I dati sono stati normalizzati statisticamente e resi omogenei in modo da poter essere utilizzati come output quantitativo fondato e utile a supportare considerazioni qualitative.
- La base di dati proveniente dal SOC è stata integrata con i dati provenienti dalle analisi svolte dal team YCTI. Ulteriori informazioni derivano da fonti interne e da collaborazioni con istituzioni, enti e altre aziende, nonché tenendo conto delle notizie provenienti dal circuito **FIRST** (Forum for Incident Response and Security Teams), la comunità internazionale più estesa e autorevole per la prevenzione e la gestione congiunta di incidenti di sicurezza.

***

Per ulteriori informazioni
Communication & Media Relations Var Group
Sara Lazzeretti
Mail: s.lazzeretti@vargroup.it
Mob. 3391705791

Ufficio stampa
Community Strategic Communications Advisers
var@communitygroup.it

Var Group S.p.A.
Var Group www.vargroup.it, con un fatturato di 396 milioni di Euro al 30 aprile 2020, oltre 2500 collaboratori 23 sedi in tutta Italia, 7 all'estero in Spagna, Germania, Austria, Romania, Svizzera e Cina, è uno dei principali partner per l'innovazione del settore ICT. Sostiene la competitività delle imprese del Made in Italy con offerte dedicate ai maggiori distretti italiani come: Manufacturing, Food & Wine, Meccanica industriale, Automotive, Fashion, Furniture Retail & Gdo. La proposta Var Group si rinnova quotidianamente grazie alla ricerca continua e alla stretta collaborazione con Start up e Poli Universitari. Le imprese si trovano di fronte a sfide sempre più complesse: devono poter contare su soluzioni innovative e specializzate. L'offerta Var Group trae la sua forza dalla profonda conoscenza dei processi aziendali e dall'integrazione di più elementi. È frutto del lavoro di Business Unit focalizzate nello sviluppo di progetti di: Customer Experience, Digital Process, Digital Cloud, Digital Security, Smart Services, Cognitive & Advanced Analytics e Business Technologies Solutions. Var Group appartiene al Gruppo Sesa S.p.A., operatore di riferimento in Italia nell'offerta di soluzioni IT a valore aggiunto per il segmento business con ricavi consolidati per Euro 1,776 miliardi al 30 aprile 2020. La società capogruppo Sesa S.p.A. è quotata sul segmento STAR del mercato MTA di Borsa Italiana.