YARIX, DIVISIONE DIGITAL SECURITY DI VAR GROUP: NELLA SECONDA METÀ DEL 2019 BOOM DI ATTACCHI HACKER CONTRO IL COMPARTO DEL GAMING (+50%)

NELLE VIOLAZIONI DI LIVELLO CRITICO, IL CYBERCRIME CONTINUA A MANIFESTARE LA CAPACITÀ DI AGIRE SU SCALA INDUSTRALE, STANDARDIZZANDO PROCEDURE E MASSIMIZZANDO IL RITORNO

Empoli, 28 aprile 2020 – Fari accesi sul settore del gaming (piattaforme di gioco online, dal poker alle scommesse) e sviluppo di tecniche di attacco informatico capaci di mettere a segno violazioni di grande magnitudo, a fronte di uno sforzo complessivo contenuto: il report elaborato da **Yarix**, la divisione Digital Security del colosso italiano **Var Group**, scatta la fotografia aggiornata della contrapposizione – continua e serrata – tra il cybercrime e le organizzazioni pubbliche e private, impegnate nella difesa del proprio perimetro di sicurezza digitale.
Curato dagli analisti del *Cognitive Security Operation Center* (C SOC) di Yarix, il report si riferisce al **secondo semestre 2019** e quantifica l'esposizione del sistema Italia agli attacchi hacker, a partire da un punto di osservazione 'di frontiera'. Il C SOC è, infatti, un sofisticato bunker informatico, che 24 ore al giorno monitora e gestisce la sicurezza delle reti aziendali e pubbliche, attraverso sistemi computazionali predittivi e cognitivi di ultima generazione.

"Il decremento nel numero di attacchi registrati nel secondo semestre 2019 non deve trarre in inganno: viviamo un momento di straordinaria esposizione e vulnerabilità informatica. Milioni di italiani si sono affacciati, nelle ultime settimane, allo smart working, accedendo alle reti aziendali dalla propria abitazione. Spesso in assenza delle necessarie protezioni di sicurezza." – commenta **Mirko Gatto, CEO di Yarix, Divisione Digital Security di Var Group** – "*In parallelo, assistiamo a movimenti assai preoccupanti da parte del cybercrime, articolato in gruppi che condividono lo stesso modus operandi e adottano tecniche pensate per funzionare su scala industriale. Mai come in queste ore è necessario dotarsi di strumenti e professionalità atte alla protezione della sicurezza informatica, sedimentando la necessaria cultura della cybersecurity presso tutti i livelli della propria organizzazione".*

I risultati in cifre (luglio/dicembre 2019)

- **19.599 eventi di sicurezza** rilevati (**-40%** su primo semestre): possibili violazioni dei livelli di sicurezza informatica definiti da ciascuna organizzazione, tali da configurare una situazione di potenziale rischio. Sul decremento registrato influisce anche la stagionalità degli attacchi, che nei mesi di agosto e dicembre – in concomitanza con le chiusure aziendali – tende generalmente a diminuire;
- **4.483incidenti di sicurezza** (**-53%** su primo semestre): 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;
- **28 eventi critici** (**+1%** su primo semestre): 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 e implementare le necessarie contromisure di prevenzione.

I comparti più colpiti – focus aziende Gaming

In linea con i dati emersi nel primo semestre, i settori del manufatturiero e dell'Information Technology restano ai primi posti in termini di attacchi subiti.
Cresce, al contempo, l'attenzione del cybercrime nei confronti delle piattaforme online di giochi e scommesse: sempre più popolare presso un pubblico ampio e trasversale, il comparto del Gaming registra, infatti, un +50% rispetto ai primi sei mesi del 2019.
Il **picco** si è verificato **nei mesi di ottobre/novembre 2019**, quando, in più occasioni, si è manifestata una nuova modalità di attacco che aumenta la capacità offensiva del classico format del

‘*denial of service’*. Oltre a saturare le risorse della rete attaccata, gli hacker generano traffico malevolo presentandosi in rete con un indirizzo IP identico a quello dell’azienda di gaming ‘vittima’. In questo modo, siti web terzi vengono inondati di richieste anomale, non collegate alla normale navigazione e in numero tale da saturare il numero di operazioni consentite. Ne consegue un danno serio e duplice:

- L’indirizzo IP dell’azienda di gaming attaccata vede ridursi la propria **reputazione** online (*blacklist*), fino a trovarsi nella condizione di non poter più raggiungere fornitori o servizi vitali per il business;
- Gli stessi **utenti** della piattaforma di gaming attaccata si trovano nell’impossibilità di giocare, come conseguenza del ‘denial of service’ generato dagli hacker (danno diretto di business).

Analisi qualitativa: cresce l’efficacia degli attacchi, a parità di sforzo

I dati rilevati da Yarix nel secondo semestre 2019 confermano la presenza in rete di **servizi e protocolli esposti** e privi di protezione. Attraverso semplici strumenti di indicizzazione e scansione automatica del web, gli hacker sono in grado di individuare queste falle e di infiltrarsi così nei sistemi informatici. Una situazione indicativa, quest’ultima, di **due situazioni allarmanti**:

- Imprese e istituzioni continuano, in massima parte, a sottodimensionare il rischio cyber;
- La massiccia diffusione dello smart working – in seguito all’**emergenza sanitaria in corso** – ha imposto alle imprese di rendere agibili, da remoto, servizi prima fruiti solo all’interno del perimetro fisico aziendale. È evidente che, in assenza di specifici accorgimenti di sicurezza digitale, le opportunità di aggressione del cybercrime andranno inesorabilmente aumentando.

Una ulteriore considerazione qualitativa riguarda il **modus operandi** degli attaccanti: l’analisi di una serie di **episodi reali – verificatisi in Italia tra settembre e dicembre 2019** – indica che gruppi affini di hacker impiegano procedure di attacco standard, assicurandosi così il massimo ritorno possibile a fronte di un ‘investimento criminale’ contenuto.
Nello specifico, la connotazione industriale degli attacchi in questione è evidente dalle modalità adottate, che permettono di infettare non solo la porzione di rete accessibile al singolo utente, ma l’intero sistema, laddove si trovano le informazioni sensibili e il backup di tutti i dati.
La **compromissione in due step**: la prima fase vede l’invio massivo di allegati malevoli, che, una volta insinuatisi nel singolo dispositivo, aprono il varco ad un secondo malware. È quest’ultimo a creare il vero canale d’accesso per l’hacker, che a questo punto è **in grado di bloccare l’intera organizzazione**, cifrando i sistemi e cancellando documenti potenzialmente vitali. Gli episodi illustrati nel report di Yarix hanno riguardato aziende molto diverse tra loro per dimensione e comparto: in tutti i casi, il modus operandi è stato il medesimo, con l’unica variante che i riscatti chiesti dai cybercriminali sono stati modulati, in termini di importo, in funzione del fatturato della vittima.

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 omogeni 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 ulteriori **informazioni di Threat Intelligence**, derivanti da fonti interne (Honeypot) e da collaborazioni con istituzioni, enti e altre aziende.

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
Mob. 345 7357751

Var Group Spa
Var Group www.vargroup.it, con un fatturato di 343 milioni di Euro al 30 aprile 2019, oltre 2200 collaboratori 23 sedi in tutta Italia, 5 all'estero in Spagna, Germania 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 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 1,55 miliardi al 30 aprile 2019. La società capogruppo Sesa S.p.A. è quotata sul segmento STAR del mercato MTA di Borsa Italiana.