ARRIVA IN ITALIA IL '*BIG GAME HUNTING*':
IL CYBERCRIME APRE LA STAGIONE DELLA CACCIA ALLA PREDA PIÙ GROSSA,
CON RICHIESTE DI RISCATTO CALCOLATE IN BASE A VERI E PROPRI BUSINESS PLAN

SECONDO YARIX, DIVISIONE DIGITAL SECURITY DI VAR GROUP,
IL PRIMO SEMESTRE 2020 CONTA 2610 ATTACCHI ALLE IMPRESE ITALIANE.
IL 31% DELLE VIOLAZIONI COLPISCE IL SETTORE BANKING E FINANCE (+143% SU H2 2019)

Empoli, 1 dicembre 2020 – **Yarix**, divisione Digital Security di **Var Group**, presenta la nuova edizione del rapporto che analizza l'esposizione del sistema Italia agli attacchi del cybercrime, a partire dal punto di osservazione 'di frontiera' del *Cognitive Security Operation Center* (CSOC) e del team di *Incident Response*, rispettivamente dedicati alla prevenzione/monitoraggio e alla gestione dei cyberattacchi.

"Riferito al primo semestre del 2020, il report evidenzia un trend di attacco a due velocità: a fronte di una media stabile di circa 3000 violazioni cyber al mese, le organizzazioni monitorate dal nostro SOC – dotate quindi di un sistema avanzato di osservazione e prevenzione – hanno evidenziato una flessione degli incidenti critici da gennaio a maggio, quindi nel pieno del delicato periodo del lockdown. Viceversa, il nostro team di Incident Response, che agisce su attacchi già in corso su imprese al di fuori del perimetro SOC e quindi non strutturate rispetto alla protezione dal rischio informatico, ha visto aumentare le richieste di intervento su attacchi critici già in corso, proprio nello stesso periodo. Una conferma, quindi, dell'importanza della prevenzione attraverso sistemi professionali e avanzati di cybersecurity in chiave preventiva", commenta **Mirko Gatto, CEO di Yarix, Divisione Digital Security di Var Group.**

I trend – Big Game Hunting
Rispetto al primo semestre 2020, gli analisti di Yarix mettono l'accento sulla trasformazione qualitativa degli attacchi, che anche in Italia sembrano recepire il trend, già affermato a livello globale, del Big Game Hunting.
"Il focus degli hacker si sposta dalla 'pesca a strascico' alla caccia alle prede più grosse: gli attacchi finalizzati alla richiesta di un riscatto (ransomware) vengono studiati con largo anticipo e in maniera sofisticata, scegliendo le vittime sulla base di un'analisi del web alla ricerca di accurate informazioni finanziarie. In base al volume di fatturato e agli asset economico-finanziari di ciascuna azienda, i cybercriminali identificano il proprio obiettivo, quantificando il riscatto da chiedere sulla base di un vero e proprio Business Plan", aggiunge **Gatto**.

La diffusione del Big Game Hunting attiva, dunque, una **corsa al rialzo nei riscatti**, così come traspare dai dati diffusi da *Coveware*, società specializzata nella gestione completa di incidenti da ransomware: a livello globale, il riscatto medio richiesto dal gruppo hacker Maze nel primo semestre 2020 è pari a 420.000 dollari, mentre Ryuk e Netwalker si attestano rispettivamente sui 282.590 e 176.190 dollari. Secondo Coveware, il **riscatto medio richiesto dai gruppi cybercrime è aumentato del 47% tra il primo e il secondo semestre di quest'anno**.

Anche in Italia, il cybercrime sembra recepire questa tendenza globale: nei primi sei mesi del 2020, **nei confronti di imprese italiane sono stati avanzate richieste di riscatto sopra i 10 milioni di euro, in almeno due casi**, e tra i 5 e i 10 milioni di euro in altrettante ricorrenze.

La caccia grossa degli hacker è, secondo Yarix, un trend destinato a consolidarsi sempre più, dal momento che giova non solo alle grandi organizzazioni di cybercrime ma anche ai **piccoli gruppi di attaccanti**. Questi ultimi sembrano, infatti, avere inteso che rispetto alla polverizzazione degli sforzi su aggressioni indiscriminate è più remunerativo impegnarsi nello studio accurato di una

singola grande organizzazione: aumenta così anche per loro la possibilità di chiedere un riscatto corposo.

I trend – online banking nel mirino

Con un'incidenza pari al 31% delle violazioni rilevate dal SOC di Yarix, il settore del banking/finance sale al primo posto tra i comparti più attaccati dagli hacker: rispetto al secondo semestre del 2019, il primo semestre 2020 fa registrare un **+143%** di possibili incidenti di cybersicurezza.
A catalizzare gli attacchi sono i servizi di **online banking** a disposizione degli utenti: l'inserimento delle proprie credenziali all'interno di pagine web *'fake'* – create ad arte dagli hacker per ricreare le vere piattaforme online delle banche – consegna ai cyber criminali le chiavi di accesso al conto. Al passo con le più recenti contromisure tecnologiche, gli hacker hanno dimostrato di essere anche in grado di utilizzare **canali SMS o voce, per convincere le vittime a fornire i codici OTP** necessari a concludere le operazioni bancarie più complesse.
In parallelo, le contromisure sul fronte della cybersecurity vanno facendosi sempre più sofisticate, includendo la leva della **Cyber Threat Intelligence**. L'obiettivo è monitorare l'attività sotterranea degli hacker, nei confronti della banca 'nel mirino', e contrastare con strumenti evoluti una tipologia di phishing altrettanto evoluta.

Ransomware – cronistoria di un cybercrime

Come in un libro giallo, i professionisti di Yarix hanno ricostruito **i 5 tempi del crimine perfetto**, dalla violazione alla richiesta di riscatto ransomware.

1. **Identificazione del punto di accesso**: anche in relazione all'ormai massiccia diffusione dello smart working, il phishing è tra gli strumenti più diffusi di compromissione del perimetro di sicurezza delle imprese. Consente, infatti, di violare device e dispositivi di navigazione non presidiati in termini di cybersecurity.
    - Sempre più spesso, inoltre, le credenziali non sono carpite direttamente dagli attaccanti, ma vengono acquistate in set su specifici **market all'interno del Dark Web**. Il costo base può variare in base ai privilegi di accesso (utenze base, utenze amministrative, utenze apicali, etc);
2. **L'acquisizione del controllo**: una volta ottenuto l'accesso iniziale, gli attaccanti proseguono infiltrando il livello amministrativo del sistema informatico, il domain controller e l'infrastruttura di backup;
3. **Compromissione e cifratura**: in pieno controllo dei server, gli attaccanti compromettono il backup e infettano il sistema con l'eseguibile per la cifratura, che in parallelo estendono anche al maggior numero possibile di host collegati.
    - Gli hacker stanno sviluppando tool sempre più sofisticati per **ridurre i tempi di permanenza all'interno della rete**, comprimendo la finestra temporale (tra prima violazione e inizio della cifratura) di un eventuale intervento di gestione dell'incidente che possa fare la differenza tra livello critico e livello distruttivo. L'importo medio dei riscatti richiesti sta aumentando anche per questa riduzione dei tempi di attacco.
4. **L'esfiltrazione**: oltre alla cifratura dei server, che implica spesso un blocco dell'operatività delle organizzazioni colpite, i cybercriminali possono minacciare di **rendere disponibili su pagine web pubbliche i dati sensibili**: è stata rilevata l'apertura di **numerosi blog**, utili proprio a questo scopo. La vittima si trova così in una situazione particolarmente critica, non solo dal punto di vista industriale/operativo, ma anche sul fronte legale e reputazionale.
5. **Il riscatto**: questa è la fase in cui il crimine giunge al suo compimento, con la richiesta di un riscatto. Un evento che deve essere gestito correttamente, evitando di assecondare il ricatto, attivando professionalità capaci di contenere e gestire il danno informatico e denunciando l'accaduto.

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.
- A partire dal presente report, le informazioni qualitative si basano anche sulle rilevazioni fornite dal **team Incident Response** di Yarix, che nell'ultimo anno ha contribuito a disinnescare alcuni tra i più importanti attacchi hacker sferrati contro imprese e organizzazioni italiane.

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 S.p.A.
Var Group www.vargroup.it, con un fatturato di 343 milioni di Euro al 30 aprile 2019, oltre 2500 collaboratori 23 sedi in tutta Italia, 7 all'estero in Spagna, Germania, 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 1,55 miliardi al 30 aprile 2019. La società capogruppo Sesa S.p.A. è quotata sul segmento STAR del mercato MTA di Borsa Italiana.