OLTRE 3.000 ATTACCHI CYBER IN ITALIA DA GENNAIO A MARZO:
IL PRIMO REPORT DI YARIX, DIVISIONE SICUREZZA DIGITALE DI VAR GROUP,
FOTOGRAFA UNA SITUAZIONE DI RISCHIO GENERALIZZATO PER LE IMPRESE

GDO NEL MIRINO DEL CYBERCRIME, OLTRE A MANIFATTURIERO E IT:
IL 16% DEGLI ATTACCHI INVESTE LA GRANDE DISTRIBUZIONE ORGANIZZATA

Treviso, 17 giugno 2019 – "*Per il cybercrime, anche in Italia, è iniziata l'era dell'industrializzazione: non più attacchi estemporanei, ma offensive ragionate e sistematiche. Finchè anche le imprese e i singoli fruitori della rete non adotteranno misure di protezione altrettanto sofisticate, il trend degli attacchi cyber disegnerà una curva che non potrà che essere costante, continuativa e ascendente*". **Mirko Gatto, CEO di Yarix**, la divisione sicurezza digitale del colosso italiano **Var Group**, commenta così i risultati del primo dei report che, con cadenza trimestrale, sarà curato dagli analisti del Cognitive Security Operation Center (**C SOC**) di Yarix: un bunker informatico, tra i più avanzati in Italia, che 24 ore al giorno monitora e gestisce la sicurezza delle reti aziendali e pubbliche, attraverso sistemi computazionali predittivi e cognitivi di ultima generazione.

Tra i maggiori player italiani nel comparto della cybersecurity, al servizio di imprese ed enti governativi, aziende sanitarie, scuole e università, **Yarix quantifica e interpreta** in questo report **l'esposizione del sistema Italia agli attacchi del cybercrime**, a partire dal punto di osservazione 'di frontiera' del proprio SOC.

Il metodo

- Il report si riferisce al periodo gennaio/marzo 2019 e 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.

I risultati in cifre

- **12.020 eventi di sicurezza** rilevati: si tratta di possibili violazioni dei livelli di sicurezza informatica definiti da ciascuna organizzazione, tali da configurare una situazione di potenziale rischio;
- **3.162 incidenti di sicurezza**: a fronte dei circa 12.000 eventi rilevati, poco più di 3.000 sono evoluti in 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;
- **14 eventi critici**: 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;
- Se la maggioranza degli eventi di sicurezza rilevati è stata perpetrata ai danni dei comparti manufatturiero (37%) e IT (17%) – in linea con i trend nazionali degli ultimi mesi -, sorprende il terzo posto della **Grande Distribuzione Organizzata** (**16**%)
    - Il trend ricalca quanto già accaduto all'estero, con modalità e fini analoghi agli attacchi rivolti ad un'altra categoria, quella delle grandi catene alberghiere. Anche in Italia, la GDO rappresenta un obiettivo particolarmente appetibile per il cybercrime, perché, innanzitutto, permette di accedere ad un flusso di denaro continuo e importante.

Controllare la rete informatica della GDO significa paralizzarne l'attività e, di conseguenza, permette di richiedere riscatti a molti zeri. Non solo. Attraverso finti portali per carte fedeltà o la simulazione di premi, gli attaccanti sono in grado di mettere nel mirino anche gli utenti della GDO, impossessandosi di dati personali, informazioni sulle abitudini di acquisto e altre notizie che potranno poi essere utili per attacchi successivi. In questo senso, **il caso della GDO dimostra che le strategie di cyber-attacco ricalcano le strategie di marketing delle aziende, comprendendone le logiche e utilizzandole a proprio vantaggio**.

Analisi qualitativa: i megatrend della cyersecurity in Italia

Nel seguito, le considerazioni degli analisti di Yarix relativamente ai trend emergenti della sicurezza informatica in Italia, a partire dai dati rilevati nel primo trimestre 2019.

- **L'approccio industriale del cybercrime**: l'obiettivo di colpire il maggior numero di organizzazioni, a fronte di investimenti ridotti, in termini di denaro e tempo, viene perseguito con una strategia duplice:
    - Implementare campagne phishing massive e con l'impiego di malware già disponibili nel **deep web**. Le risorse necessarie ad arrecare danni significativi sono a disposizione di chiunque sia motivato a ricercarle;
    - Studiare da vicino gli obiettivi più promettenti, analizzando le abitudini di fruizione della rete e i **profili social personali dei vertici delle aziende** o delle organizzazioni da colpire.
- **Il ruolo delle email**: in questo contesto di crescente industrializzazione degli attacchi informatici, l'email resta il principale vettore di intrusione. Permette, infatti, di raggiungere contemporaneamente molti utenti, con l'intento sia di rubare password e credenziali sia di compromettere il client per renderlo parte di una più ampia 'botnet' malevola. Nel seguito, le campagne di phishing più aggressive del primo trimestre 2019:
    - **Sextortion**: scoppiata nel mese di gennaio, la campagna ha veicolato richieste di denaro in criptovalute, minacciando di rivelare la frequentazione di siti web a luci rosse;
    - **Fattura sospesa**: email malevole inducono, tramite link, al download di allegati pericolosi, appartenenti alla famiglia dei malware bancari, dei ransomware e dei trojan;
    - **Campagna email tramite PEC**: nel mese di marzo ha fatto la sua apparizione una campagna particolarmente aggressiva, in quanto veicolata tramite l'utilizzo di caselle PEC. Una nuova versione del malware Gootkit ha infettato utenze aziendali e della pubblica amministrazione, consentendo ai cybercriminali di prendere il controllo di dispositivi e acquisire dati sensibili. Un'anomalia – rilevata dagli analisti Yarix – ha consentito di stimare con sufficiente grado di probabilità che il file malevolo possa essere di provenienza russa, ucraina, bielorussa o cinese: il malware, infatti, si chiude immediatamente nel caso in cui la lingua settata nel dispositivo da infettare sia riconducibile ad una di queste nazioni;
- **L'esposizione inconsapevole delle potenziali vittime**: aziende e istituzioni continuano a manifestare un approccio superficiale nei confronti della sicurezza informatica, lasciando esposti e senza alcuna protezione servizi o protocolli, che possono rappresentare altrettanti varchi di accesso ai propri dati.
    - Attraverso semplici strumenti di indicizzazione e scansione automatica del web, gli attaccanti sono in grado di individuare immediatamente i servizi esposti e, tramite queste falle, infiltrarsi nei sistemi informatici;
    - Attraverso la disseminazione di 'Honeypot' – trappole digitali usate come strumenti di Threat Intelligence -, Yarix ha geolocalizzato le minacce sferrate a livello globale. Nazioni come l'Irlanda, la Russia e l'Olanda si trovano ai primi posti perché qui hanno

sede molte connessioni non presidiate, da cui transitano le aggressioni informatiche rilevate dagli Honeypot.

- L'introduzione di protocolli GDPR e d'avvio di percorsi di cybersecurity presso alcune aziende non sono argini sufficienti per contenere gli attacchi informatici, sempre più sofisticati e massivi. L'esposizione del comparto manufatturiero esemplifica questo assunto: la presenza, nelle aziende, di **sistemi ICS/SCADA non presidiati e non aggiornati** spiana il terreno ai cybercriminali. Violazioni di questi sistemi, oltre ad essere di semplice esecuzione, consentono di arrecare danni particolarmente gravosi, che possono obbligare l'azienda ad interrompere la produzione e ogni attività.

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 290 milioni di € al 30 aprile 2018, 1600 collaboratori e una presenza su tutto il territorio italiano grazie a 23 sedi capillarmente distribuite, è uno dei principali partner per l'innovazione del settore ICT. Sostiene la competitività delle imprese con offerte dedicate ai più importante settori italiani come: Manufacturing, Food & Wine, Meccanica industriale, 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, frutto del lavoro di Divisioni focalizzate nello sviluppo di progetti di Digital Transformation, Digital Industries, Digital Cloud, Digital Security. 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. La società capogruppo Sesa S.p.A. è quotata sul segmento STAR del mercato MTA di Borsa Italiana.