del 09 Luglio 2019

IL TIRRENO
Pistoia

estratto da pag. 1, 20

EMPOLI

Sventato attacco degli hacker No al ricatto da 2,5 milioni

La Var Group di Empoli ha respinto l'attacco a un'azienda bolognese di un gruppo di hacker russi: volevano 2,5 milioni. / IN CRONACA

IL CASO

Azienda empolese ferma i cyber-criminali Gli hacker avevano chiesto 2,5 milioni

Eccezionale intervento della divisione sicurezza della Var Group contro l'aggressione informatica di un gruppo russo

EMPOLI. Una task force di super-esperti, oltre 160 ore di lavoro, 3.500 macchine scandagliate, alla ricerca di un malware capace di paralizzare un'intera rete aziendale: è in questi dati l'eccezionale dell'intervento messo in campo da Yarix, la divisione sicurezza digitale del colosso italiano Var Group del Gruppo Sesa, per la gestione dell'attacco hacker subito dalla Bonfiglioli, azienda bolognese tra i più importanti produttori internazionali di riduttori industriali.

IL RISCATTO

Con la capacità di reazione dell'azienda e una imponente mobilitazione di risorse professionali, è stato possibile disinnescare una richiesta di riscatto di oltre 2,5 milioni di euro e ripristinare la piena funzionalità delle macchine. «Le imprese strategiche per il made in Italy sono nel mirino dei cybercriminali. Lo conferma anche il report del nostro Security operation center: nei primi 3 mesi del 2019, le aziende manufatturiere hanno subito il maggior numero di attacchi, superando i settori dell'It e della Gdo – spiega **Mirko Gatto**, Ceo di Yarix – l'attacco subito da Bonfiglioli esemplifica le capacità sempre più evolute di insinuarsi nei sistemi informativi e la necessità di ricorrere a competenze professionali strutturate come argine agli hacker». Competenze che hanno avuto la meglio. «Consideriamo la cybersecurity un asset funzionale agli obiettivi di business del gruppo – sottolinea **Enrico Andrini**, chief digital officer di Bonfiglioli Riduttori – ma è una materia in continua evoluzione: per questo, in occasione dell'attacco, abbiamo immediatamente attivato la collaborazione con Yarix».

I FATTI

Sferrato l'11 giugno, l'attacco è stato perpetrato da un gruppo Apt (Advanced persistent threat) utilizzando un malware 0 day. Virus di questo tipo risultano molto aggressivi perché realizzati ad hoc per un target aziendale specifico e capaci di restare nascosti: solo analisti specializzati sono in grado di individuarli, rilevando azioni e componenti utilizzati sugli endpoint compromessi. Attaccando la rete di Bonfiglioli, il gruppo ha poi agito con un ransomware che ha cifrato numerosi sistemi e compromesso l'accessibilità ai file criptati. La violazione ha poi ceduto il passo al più classico schema criminale, la richiesta di riscatto: "2,5 milioni e tutto tornerà a posto". Richiesta rifiutata da Bonfiglioli, che ha invece chiesto l'intervento dei professionisti di Yarix.

LA GESTIONE

«In 3 giorni abbiamo contenuto l'aggressione, mentre la completa distruzione del malware è stata completata in 10. Considerando la portata dell'attacco, è stato possibile grazie al lavoro coordinato di più team: gli esperti in analisi forense, incident response e malware analysis hanno operato sul posto in collegamento costante con gli ethical hacker del Security operation center di Yarix, attivi da remoto», rivela **Diego Marson**, chief technical officer di Yarix. Cioè la ge-

Paralizzata la rete della Bonfiglioli In 160 ore di lavoro sanate 3.500 macchine

stione dell'attacco ha richiesto un insieme articolato di interventi. Ad una prima fase di contenimento – culminata nell'isolamento del malware – è seguita la fase di eradicazione, che ha richiesto l'impiego di software intelligenti di ultima generazione, l'Edr. Yarix ha usato un sistema di avanguardia, capace di distinguere e interpretare, sul piano qualitativo oltre che quantitativo, i comportamenti "cattivi' tra quelli consueti dei normali processi.

L'IDENTIKIT

Indicazioni tecniche emerse durante la gestione dell'attacco, come l'utilizzo del ransomware Ryuk, condurrebbero al presunto profilo criminale degli hacker responsabili: un gruppo di e-criminali russi conosciuto come Grim Spider, noto per l'utilizzo di malware sofisticati come quello adottato con Bonfiglioli. Il gruppo, attivo da agosto 2018, agisce preferibilmente su obiettivi aziendali di grandi dimensioni a scopo di estorsione e ricatto.

CYBERSECURITY

Insieme ad altri dispositivi avanzati, il software Edr compone oggi la nuova architettura di sicurezza digitale pensata per Bonfiglioli. L'intero sistema di protezione è collegato al Security operation center di Yarix, che consente un monitoraggio continuo di ogni movimento anomalo attorno al perimetro informatico aziendale. Intervenendo su una cultura aziendale già predisposta e consapevole dei rischi, lo schema di presidio così disegnato da Yarix per Bonfiglioli realizza uno scudo molto strutturato. E importante è stata la scelta del Gruppo Bonfiglioli, che ha pubblicamente denunciato il tentativo di violazione ed estorsione subito. Sottrarsi al ricatto del cybercrime significa, infatti, gettare le basi per una cultura più matura e condivisa della legalità digitale, scardinando il meccanismo alla base del cosiddetto "pizzo 2.0" e innescando un circuito virtuoso di denuncia, responsabilità e trasparenza. —


IL TIRRENO

Iscrizioni online, assenze via sms a mensa la rivoluzione è servita

ESTATE

Anfore e latine: la vergognosa natura morta dei fondali maremmani

CODACONS