VAR GROUP PER BONFIGLIOLI: LE MIGLIORI COMPETENZE DI CYBERSECURITY AL SERVIZIO DI UNA ECCELLENZA ITALIANA, CONTRO LA NUOVA CRIMINALITÀ DIGITALE

ATTACCO HACKER NEUTRALIZZATO ANCHE GRAZIE ALL'INTERVENTO DI YARIX, DIVISIONE DIGITAL SECURITY VAR GROUP: IN CAMPO, UNA TASK FORCE DI ESPERTI E IL SUPPORTO DEL SECURITY OPERATION CENTER

Empoli, 8 luglio 2019 – 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: sta in questi dati l'eccezionalità dell'intervento messo in campo da **Yarix** – la divisione sicurezza digitale del colosso italiano **Var Group** – per la gestione dell'imponente attacco hacker subito dal **Gruppo Bonfiglioli**, tra i più importanti produttori internazionali di riduttori industriali. A valle di una eccezionale capacità di reazione dell'azienda e di una imponente mobilitazione di risorse professionali, è stato possibile disinnescare una richiesta di riscatto pari a oltre 2,5 milioni di euro e ripristinare la piena funzionalità delle macchine.

"*Le imprese strategiche per il Made in Italy restano al centro delle attenzioni dei cybercriminali, che trovano in questa tipologia di aziende un bersaglio appetibile e vulnerabile ad attacchi mirati, condotti sulla base di periodi di analisi anche molto lunghi. Lo conferma anche il report realizzato dal 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.*" – commenta **Mirko Gatto, CEO di Yarix, Var Group Company** – *"L'attacco subito da Bonfiglioli esemplifica in maniera inequivocabile le capacità sempre più 'evolute' del cybercrime di insinuarsi nei sistemi informativi e la necessità di ricorrere a competenze professionali strutturate, in termini di numero e competenze di operatori specializzati, come unico argine nei confronti degli hacker".*

"*Consideriamo la cybersecurity un asset strategico e funzionale agli obiettivi di business del Gruppo. Per questo abbiamo sempre investito in strumenti e processi di protezione, oltre che in formazione e condivisione di una cultura della sicurezza informatica*" – sottolinea **Enrico Andrini, Chief Digital Officer di Bonfiglioli Riduttori**– *Siamo consapevoli tuttavia che si tratti di una materia in continua evoluzione: per questa ragione, in occasione dei recenti eventi, abbiamo immediatamente attivato la collaborazione con Yarix, partner in grado di affiancarci con competenze specialistiche nella gestione di un attacco difficilmente individuabile".*

La dinamica
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 particolarmente aggressivi in quanto realizzati ad hoc per un target aziendale specifico e capaci di restare nascosti: solo analisti specializzati (team Cert e Incident Response) sono in grado di individuare questi attacchi, rilevando in modo puntuale le azioni e i componenti utilizzati sugli endpoint compromessi.
Attaccando la rete di Bonfiglioli, il gruppo ha agito in un secondo momento con un ransomware che ha cifrato numerosi sistemi e compromessa l'accessibilità ai file criptati. La violazione ha poi ceduto il passo al più classico degli schemi criminali, con una richiesta di riscatto, prontamente rifiutata da Bonfiglioli, che ha successivamente richiesto l'intervento di un pool di professionisti di Yarix, divisione Digital Security di Var Group.

La gestione
"In 3 giorni abbiamo contenuto l'aggressione digitale, mentre la completa distruzione del malware è stata completata nell'arco di 10 giorni. Considerando la portata dell'attacco, questo importante risultato è stato possibile in forza del combinato disposto del lavoro coordinato di più team: gli esperti in analisi forense, incident response e malware analysis, attivi in situ, hanno operato in collegamento costante con gli ethical hacker del Security Operation Center di Yarix, attivi da remoto", rileva **Diego Marson, Chief Technical Officer di Yarix.**

In dettaglio, la gestione dell'attacco ha richiesto un insieme articolato in interventi. Ad una prima fase di **contenimento** – culminata nell'isolamento del malware fino ad interrompere ogni possibile comunicazione verso i sistemi remoti – è seguita la **fase di eradicazione**, che ha richiesto l'impiego di **software intelligenti di ultima generazione**. Nello specifico, i professionisti di Yarix hanno utilizzato un sistema EDR (*Endpoint Detection&Response*) di avanguardia, capace di distinguere e interpretare, sul piano qualitativo oltre che quantitativo, **i comportamenti 'malevoli'** tra quelli consueti espressi dai normali processi informatici.

Il profiling tecnico – l'identikit degli e-criminali
Indicazioni tecniche emerse durante la gestione dell'attacco, come pure l'utilizzo del ransomware Ryuk, condurrebbero al presunto profilo criminale degli hacker responsabili dell'aggressione: un gruppo di **e-criminali russi** conosciuto come **Grim Spider**, noto per l'utilizzo di malware sofisticati come quello adottato contro Bonfiglioli. Il gruppo sarebbe **attivo da agosto 2018** e agirebbe preferibilmente contro obiettivi aziendali di grandi dimensioni – **metodologia '*big game hunting*'** – a scopo di estorsione e ricatto.

Cybersecurity come *forma mentis* di prevenzione continuativa
Insieme ad altri dispositivi avanzati di cybersecurity, 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 continuativo (24/24) di ogni movimento anomalo attorno al perimetro informatico aziendale. Intervenendo su una cultura aziendale già predisposta e consapevole dei rischi del cybercrime, lo schema di presidio così disegnato da Yarix per Bonfiglioli realizza uno scudo molto strutturato e certamente capace di competere con la nuova criminalità informatica, in grado di cambiare pelle ed esternare modalità di intrusione diverse ad ogni attacco.

Proprio alla luce di questa considerazione, risulta tanto più importante 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 tra le imprese attaccate.

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.