ECO DI BIELLA

Unione Industriale Biellese

13-05-2017

IL FATTO Chiesti dei riscatti

Attacchi degli hacker nel Biellese

Sarebbero state colpite società anche nel Biellese da parte degli hacker che hanno messo a segno il gigantesco attacco informatico dei giorni scorsi che ha mandato kappaò organizzazioni all'apparenza blindate di ben 74 paesi del mondo. Ora sta indagando la Polizia postale. Gli estorsori del web stanno colpendo nel Biellese da almeno due anni. E' toccato ad aziende, professionisti e scuole. «Noi abbiamo preferito pagare», racconta Massimo Angelico dell'omonimo Lanificio e presidente della Pallacanestro Biella.

● Caneparo a pagina

IL FATTO Nel mondo messe ko società di 74 paesi. Minimo il riscatto: 300 euro

Attacco hacker anche nel Biellese

Estorsori del web in provincia: in due anni assalti ad aziende, professionisti, scuole

Ha colpito a caso anche nel Biellese, come succede ormai da almeno due anni, anche se per gli ultimi casi ancora non si conoscono i particolari, il gigantesco attacco informatico a livello planetario che ha mandato kappaò organizzazioni all'apparenza blindate in ben 74 Paesi del mondo. Sono stati lanciati virus del riscatto, noti come ransomware, il più famigerato dei quali è "Wanna Cry", voglio piangere, attivato addirittura da strumenti digitali una volta utilizzati dagli 007 statunitensi. I cybercriminali hanno sfruttato la falla di un software Microsoft. In questo modo il virus si è diffuso facilmente attraverso la rete interna di centinaia di organizzazioni.

Come fanno. Tutto comincia da mail apparentemente innocue di persone e società conosciute che contengono in realtà un virus che "sequestra" i file dei computer. Poi viene chiesto un riscatto. Anche il Biellese è sotto attacco di questi hacker, gente che smanetta col computer con la facilità di un italiano medio ad avvolgere gli spaghetti nella forchetta. Sono stati attaccati studi tecnici di geometri, professionisti in genere, piccoli imprenditori, innumerevoli società e aziende tessili di piccole e medie dimensioni. E persino due scuole, l'Iti e il Liceo Classico.

Come spiegano da sempre dalla sezione di Biella della Polizia Postale, si tratta di file eseguibili dopo che sono stati scaricati sul computer e sono in grado di criptare, letteralmente "blindandoli", i file salvati sul computer, di norma tutti i documenti "Pdf", "Exel" e "Word". In pratica, il proprietario del computer che quei file li ha realizzati, non sarà più in grado di aprirli.

Il riscatto. Gli hacker chiedono a questo punto un riscatto sempre via mail, di norma 500 dollari, cifra che raddoppia dopo alcuni giorni. «Una volta colpiti dal virus - spiegano dalla Questura - allo stato non vi è alcuna possibilità tecnica per effettuare una decriptazione dei file, tenendo anche in considerazione il fatto che neppure l'eventuale pagamento assicura la descriptazione. Si tratta di un virus del genere "ransomware" che sta a significare, appunto, "richiedendo un riscatto" (ransom in Inglese, ndr). In effetti il sistema chiede il pagamento di una somma che raddoppia dopo un certo periodo...».

Il dettaglio. I banditi della Rete si affidano a un file-esca allegato ad una mail. Sono bravi, utilizzano linguaggi simili a quelli dell'azienda che stanno prendendo di mira. E spesso dall'altra parte c'è chi ci casca, magari per fretta o per distrazione e apre l'allegato. Il virus a quel punto si propaga, infettando ogni cosa e facendo sparire importanti file dai computer. Difficile individuare il luogo da cui vengono inviate le mail. E' infatti semplice, per questi hacker, utilizzando ad esempio "proxi" come "Thor", camuffare il loro indirizzo "IP" e sfuggire all'individuazione.

Contromisure. E' necessario aggiornare il sistema ai più recenti antivirus, impostare backup periodici dei propri dati su unità esterne, mantenere sempre aggiornato il browser web e tutti i plugin installati, usare la massima attenzione prima di aprire gli allegati delle mail, astenersi dal download di applicazioni potenzialmente pericolose, attenzione alla comparsa delle finestre Uac in Windows e alle autorizzazioni concesse ai file eseguibili. Tali finestre di Uac hanno intestazione di colore giallo e recano il messaggio "Consentire al programma seguente (...) di apportare modifiche al computer?": sono quelle che debbono essere trattate con maggiore attenzione. Se non si è sicuri dell'identità e della legittimità del file, premere il pulsante "No"...».

• **Valter Caneparo**

Attacco col virus "Wannacry" (voglio piangere)

Wannacry, ovvero "voglio piangere". Questo il nome dell'attacco informatico che ha colpito numerose organizzazioni e aziende in diversi Paesi del mondo, con Russia, Ucraina e Taiwan tra i bersagli più sofferenti. Un attacco "di proporzioni mai viste", segnalano alcuni esperti di sicurezza su Twitter. Sugli schermi dei computer presi di mira, che si bloccano e non possono essere riavviati, appare un messaggio che chiede un riscatto in bitcoin (la moneta elettronica). Tra i paesi colpiti Spagna, Gran Bretagna, Usa, Cina, Italia (colpite alcune università, Portogallo, Vietnam, Russia e Ucraina. Il "malware" non ha ancora un'origine nota, e intanto la mappa delle infezioni si amplia.

LA STORIA Qualche mese fa anche il Lanificio Angelico è stato preso di mira dai banditi della Rete

«Siamo stati costretti a pagare il riscatto»

«Costa meno pagare i ricattatori dopo l'attacco informatico che far mettere le mani sul sistema a un tecnico. Dopo che tutto si è risolto, è però necessario alzare le difese al massimo aggiornando tutti i sistemi...». A parlare è Massimo Angelico dell'omonimo Lanificio nonché presidente di Pallacanestro Biella. Anche la sua società, prima dell'inverno scorso, era stata presa di mira dagli estorsori del web. E' solo uno degli innumerevoli casi registrati anche nel Biellese.

La mail-esca. «Tutto è cominciato per colpa di una mail e del suo allegato zippato camuffato da fattura che è stato purtroppo aperto - ricorda l'imprenditore tessile -. In breve il virus ha infettato buona parte del sistema, non solo in azienda a Ronco, ma anche in altre sedi...». Com'è accaduto a centinaia di altre società, i file sono stati criptati e sono pertanto diventati irrecuperabili, a meno di non averne copia da qualche parte. Ecco perché è consigliabile effettuare sempre un back up di tutti i dati.

Il riscatto. Gli hacker hanno quindi inviato ad Angelico una richiesta contenente le istruzioni per pagare un riscatto con la moneta elettronica Bitcoin. «Ci hanno chiesto mi pare il corrispettivo di 300 dollari - prosegue Massimo Angelico -. Dopo aver stabilito che ci sarebbe costato meno pagare piuttosto che far intervenire un tecnico con il rischio, peraltro reale, che non sarebbe comunque riuscito a recuperare i file, abbiamo preferito versare quanto richiesto. Ottenuta la chiave di sblocco, tutto è magicamente tornato a posto...».

• **V.Ca.**

IL CASO Massimo Angelico