Polizia di Stato

Polizia Postale:No More Ransom

La Polizia di Stato scende in campo insieme a numerosi *partners* europei, tra i quali Europol, Eurojust e la Commissione Europea con un progetto per combattere il fenomeno del ransomware a livello globale.La piattaforma, supportata da un complesso consorzio di partners pubblici e privati, mette a disposizione nuovi strumenti di decriptazione e nuovi linguaggi per contrastare meglio questa nuova tipologia di malware.Il ransomware è un tipo di malware che blocca i dispositivi della vittima o ne cifra i dati, chiedendone di pagare un riscatto per riottenere il controllo del dispositivo e lo sblocco dei file criptati.Secondo la valutazione IOCTA 2016 (Internet Organised Crime Threat Assessment) di Europol, nell'ultimo anno il numero di varianti cryptoware si è moltiplicato ma è già da un triennio che le forze di polizia di mezzo mondo hanno intensificato gli sforzi per combattere questi criminali informatici che utilizzano i ransomware per sottrarre alle loro vittime grandi quantità di denaro.La lotta a questo tipo di malware rappresenta indubbiamente una priorità per le forze di polizia europee: quasi i due terzi degli Stati membri stanno conducendo investigazioni su queste forme di attacco informatico, un problema che non colpisce solo i dispositivi dei singoli cittadini, ma che miete vittime anche tra le aziende e le reti governative dei vari Stati.Per questo motivo, la Polizia Postale e delle Comunicazioni, unitamente ad Europol ed altri 30 *partners* internazionali, tra polizie dell'Unione Europea ed attori del settore privato, ha dato vita al progetto No More Ransom, il cui scopo è quello di introdurre un nuovo livello di cooperazione tra forze di polizia, CERT-EU (Computer Emergency Response Team for the EU institutions, agencies and bodies) e il settore privato, con lo specifico scopo di combattere insieme il dilagante fenomeno del ransomware.Il progetto, a cui hanno aderito 19 Stati membri in collaborazione con società private del settore, mette nella disponibilità degli utenti, rimasti vittime del malware, tools gratuiti per la decodifica dei propri dispositivi facilitando lo sblocco dei dati.E' stato, quindi, realizzato un portale online, www.nomoreransom.org, disponibile in lingua inglese, olandese, francese, italiano, portoghese e russo (ma presto tradotto anche in altre lingue), dove i cittadini possono trovare informazioni su cosa sono i ransomware e su come proteggersi.Gli otto *tools* gratuiti attualmente disponibili consentiranno ad una molteplicità di utenti di decriptare con successo i propri dispositivi senza dover sottostare al ricatto dei criminali di corrispondere cifre di denaro senza alcuna garanzia, peraltro, di rientrare in possesso dei propri dati.Tuttavia, la sensibilizzazione resta un punto fondamentale per evitare che i ransomware abbiano la meglio.Ecco alcune semplici misure di protezione che possono scongiurare danni irreversibili:avere sempre un sistema di back-up attivo in modo che l'infezione da ransomware non distrugga i dati personali per sempre;utilizzare efficaci software antivirus per proteggere il sistema dai ransomware;mantenere aggiornati tutti i software presenti sul computer;tenere riservate le password dei propri account per scongiurare accessi abusivi;non aprire gli allegati e non cliccare sui link contenuti nelle email provenienti da sconosciuti verificandone prima il nome del mittente e l'oggetto.*"Campagne massive di ransomware, quali cryptowall o cryptolocker, che tanto scompiglio hanno destato tra pubbliche amministrazioni, imprese e privati cittadini di mezzo mondo* - sostiene Roberto DI LEGAMI, Direttore della Polizia Postale e delle Comunicazioni - *sono conseguenza anche della presenza di un mercato virtuale nel quale sono ampiamente disponibili software malevoli di elevato livello di sofisticazione. Modello illegali noti come Cyber-crime-as-a-service, o per stare ancora più in tema, come Ransom-as-a-service, infatti, modificheranno sempre di più i tradizionali modelli di criminalità, consentendo anche a soggetti sprovvisti di approfondite competenze tecnologiche di portare a termine con successo, tra l'altro, attività estorsive come quelle in parola. La magnitudo del fenomeno ha sinora spinto gli investigatori a concentrarsi sull'attribuzione del reato ai relativi autori, tralasciandone di fatto le vittime. Il progetto NoMoreRansom* - prosegue DI LEGAMI - *rappresenta un valido esempio di cambio di passo, laddove alle vittime di ransomware si consente, da oggi, di ripristinare la funzionalità dei propri dispositivi infettati dal virus, semplicemente attraverso un accesso alla piattaforma, dalla quale potranno scaricare gratuitamente i software di decriptazione.Il progetto NoMoreRansom è frutto di una sapiente opera di partenariato tra i settori pubblico e privato, e di una costante collaborazione internazionale con i principali organismi europei, quali Europol ed Eurojust. Mi piace ricordare* - conclude DI LEGAMI - *che da tempo sosteniamo che la lotta contro la criminalità informatica è una responsabilità di tutti, che non può non realizzarsi attraverso la diffusione di una cultura globale della sicurezza in Rete. Per questo motivo, la Polizia Postale delle Comunicazioni investe sforzi significativi anche nel campo della prevenzione, attraverso importanti campagne di sensibilizzazione come la presente".*