Ranflood, ecco come funziona lo strumento italiano open source anti ransomware

Un nuovo strumento – **gratuito e open-source** – per contrastare **gli attacchi informatici a base di ransomware**: si chiama Ranflood e lo ha messo a punto un gruppo di ricercatori dell'**Università di Bologna** e di **ARPAE Emilia-Romagna**. Il software funziona come una "trappola dinamica" che insegue il virus e gli somministra dei file-esca, guadagnando così tempo per svelare l'attacco in corso e prendere contromisure.

La soluzione è stata testata in ambiente controllato su alcuni dei ransomware più noti, tra cui **WannaCry** (che mise in ginocchio la sanità inglese nel 2017) e LockBit (il virus usato nel 2021 per disabilitare i servizi della Regione Lazio). I risultati – pubblicati su *Computer & Security*, tra le riviste più prestigiose nel campo della sicurezza informatica – sono molto positivi, con un potenziale di protezione dagli attacchi che arriva fino al 94%.

I ransomware sono tra i virus informatici più pericolosi e insidiosi: una volta entrato nel computer della vittima, il virus sequestra i dati dell'utente rendendoli inservibili se non dietro il pagamento di un riscatto. Si stima che nel 2021 attraverso i ransomware siano stati estorti 20 miliardi di dollari in tutto il mondo, a cui si sommano costi sommersi incalcolabili che utenti e imprese devono sostenere, dovuti ai disservizi causati dall'attacco e ad apparati informatici resi inservibili.

Proprio per cercare soluzioni utili a contrastare questo fenomeno è nato **Ranflood**, frutto di oltre due anni di lavoro comune reso possibile da una convenzione tra il **Dipartimento di Informatica – Scienza e Ingegneria** dell'**Università di**

Bologna e il **Servizio Sistemi Informativi e Innovazione digitale** di **ARPAE Emilia-Romagna**.

Ma come opera questo sistema? Il punto di partenza è il funzionamento degli attacchi ransomware: una volta all'interno del sistema informatico, il virus si mette al lavoro e nel giro di poco tempo riesce a rendere illeggibili tutti i file presenti. Una volta terminato l'attacco, l'unico modo per accedere al sistema è attraverso la chiave in possesso dei criminali responsabili.

"Questo progetto parte da una nuova interpretazione di una tecnica di contrasto ai virus già nota, ***basata sul predisporre delle 'trappole', o file-esca****, che svelano la presenza di malintenzionati nel sistema",* spiega **Saverio Giallorenzo**, ricercatore al Dipartimento di Informatica – Scienza e Ingegneria dell'Università di Bologna, tra gli autori dello studio. *"Da questa base di partenza, con Ranflood siamo riusciti* ***a rendere la trappola 'dinamica'****: il sistema, cioè, insegue il virus per somministrargli i file-esca, che quindi non servono più solo per svelare un attacco, ma anche* ***per sviarlo e salvare i dati reali della vittima****".*

"Con Ranflood questa dinamica ***viene contrastata****: il sistema* ***riesce a 'tenere a bada' il virus****, facendogli sprecare tempo, in modo da dare all'utente la possibilità di reagire",* spiega **Simone Melloni**, del Servizio Sistemi Informativi e Innovazione digitale di ARPAE Emilia-Romagna, tra gli autori dello studio. *"Per farlo, Ranflood sfrutta due fattori. Prima di tutto, confonde i dati veri presenti nel sistema* ***con migliaia di file-esca*** *generati in tempi rapidissimi: attaccando questi dati fittizi il virus perde tempo inutilmente. In secondo luogo, questo stesso meccanismo* ***sottrae al virus risorse della macchina attaccata****, rallentando così la velocità della sua azione malevola".*

I test di laboratorio realizzati finora hanno restituito risultati molto promettenti sull'efficacia di Ranflood. Nel frattempo, gli studiosi sono già al lavoro su nuovi metodi di contrasto all'attività dei ransomware, che tengano conto delle nuove tecnologie e delle innovazioni che i cyber-criminali sfruttano per estorcere denaro.

Lo studio è stato pubblicato sulla rivista *Computer & Security* con il titolo "Data Flooding against Ransomware: Concepts and Implementations". Per l'Università di Bologna (Dipartimento di Informatica – Scienza e Ingegneria) hanno partecipato **Davide Berardi**,**Saverio Giallorenzo**, **Andrea Melis**, **Loris Onori** e **Marco Prandini**, insieme a **Simone Melloni** di ARPAE Emilia-Romagna (Servizio Sistemi Informativi e Innovazione Digitale).

Per approfondire

https://www.key4biz.it/ranflood-ecco-come-funziona-lo-strumento-italiano-open-source-anti-ransomware/453265/