IL SECOLO XIX

Quotidiano

Consiglio Nazionale delle Ricerche

Data 18-06-2019
Pagina 22
Foglio 1 / 2

LO STUDIO DURERÀ TRE ANNI

Caccia ai software mangia-dati La sfida parte dal Cnr di Genova

Annientò i cervelloni di diverse maxi-imprese, ora un team si occuperà degli eredi del malware Duqu

Francesco Margiocco

Quando nel 2011 un gruppo di scienziati dell'Università di Budapest lo ha stanato, Duqu era attivo da anni e aveva avuto il tempo di attaccare sistemi informatici di grandi industrie e rubare montagne di dati sensibili. Oggi i suoi eredi ne onorano la memoria, e continuano a trafugare. Duqu appartiene alla famiglia dei malware steganografici, software malevoli capaci di nascondersi e di agire indisturbati.

La differenza con un malware normale sta nel modo in cui il software malevolo sottrae i dati, e che Luca Caviglione, ricercatore dell'Istituto di matematica applicata e tecnologie informatiche del Cnr di Genova, spiega così: «Un malware classico inserisce le informazioni rubate nei pacchetti di informazioni lecite che viaggiano in rete, i bit. Un malware steganografico le nasconde nel tempo di trasmissione tra un bit e l'altro».

Caviglione è parte in causa. Con un gruppo internazionale di studiosi e un finanziamento milionario dell'Unione europea vuole fermare gli eredi di Duqu. «Prima analizzeremo le tecniche di comportamento dei malware steganografici; questo richiederà tempo perché finora il fenomeno è stato pochissimo studiato. Poi creeremo dei modelli matematici perché il computer possa riconoscere e fermare questi software da sé, in base all'esperienza, con quello che oggi chiamiamo "machine learning"»; e che è un insieme di operazioni logiche e algebricheche permettono al software di imparare dall'esperienza: osservare, analizzare, dare risposte.

È il compito del progetto Simargl: realizzare in tre anni un sistema di "machine learning" che fermi questi moderni cavalli di Troia. Del gruppo Simargl fanno parte, oltre all'istituto del Cnr, l'Università tecnica di Varsavia, l'Università di Hagen, la multinazionale dell'elettronica Thales, la multinazionale delle telecomunicazioni Orange e un'altra decina tra aziende e centri di ricerca.

I lavori sono partiti da poco più di un mese, il giorno della festa del lavoro, il primo maggio. «Anche se non è partner della ricerca, Europol, l'agenzia dell'Unione europea per la lotta al crimine, ci segue molto da vicino», dice il ricercatore polacco Wojciech Mazurczyk, che sta passando l'estate a Genova, in distacco dall'ateneo tedesco di Hagen, per avviare il progetto insieme a Caviglione. «Il compito mio e di Luca, all'interno del gruppo, è capire come fanno i malware a nascondere dentro il traffico di rete le informazioni che rubano».

Con una parte dei finanziamenti, a settembre, Caviglione pagherà uno studente di dottorato di ricerca, e un ricercatore, per lavorare con lui. Il tempo corre, e dovranno fare in fretta: l'Identity Theft Resource Center, organizzazione californiana specializzata in cyber-sicurezza, segnala che i furti di dati sensibili, a danno su tutti dell'industria e della sanità, sono aumentati in un anno del 126%. —

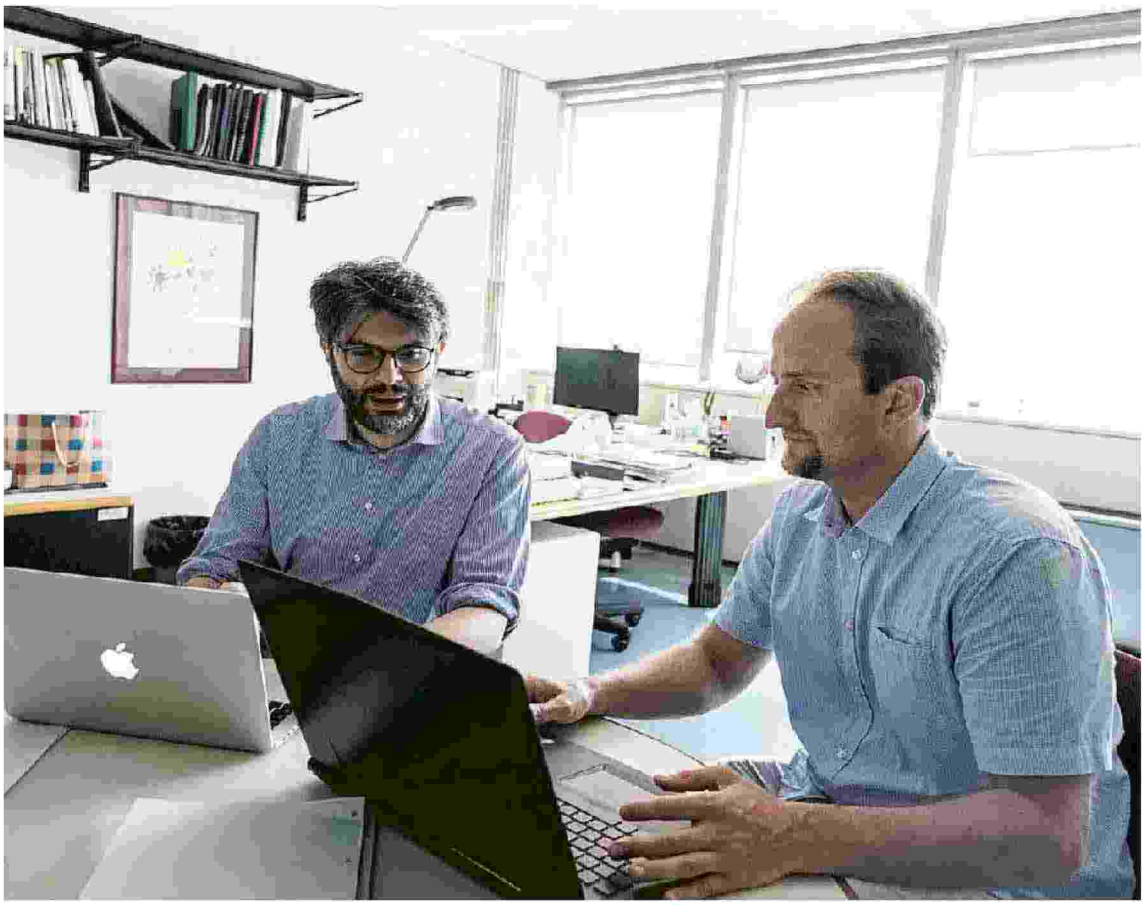
«Europol, l'agenzia dell'Unione europea per la lotta al crimine, ci segue da vicino»

IL SECOLO XIX

Quotidiano

Consiglio Nazionale delle Ricerche

Data 18-06-2019
Pagina 22
Foglio 2 / 2



Luca Caviglione (a sinistra) e Wojciech Mazurczyk al lavoro GENTILE


IL FUTURO È IN CITTÀ

Caccia ai software mangia-dati La sfida parte dal Cnr di Genova

I Centri in vetrina: Tursi mette online il calendario con tutte le proposte

Inizia l'era Guerrini a Palazzo Reale