ISSN 2611-4259

www.ictedmagazine.com

ICT ED MAGAZINE

INFORMATION COMMUNICATION TECHNOLOGIES EDUCATION MAGAZINE

PERIODICO DELLE TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE PER L'ISTRUZIONE E LA FORMAZIONE

ANNO V - N. 1 - APRILE 2022

ICTEDMAGAZINE
Information Communication Technologies Education Magazine
Periodico delle Tecnologie della Comunicazione e dell'Informazione per l'Istruzione e la Formazione
Registrazione al n.157 del Registro Stampa presso il Tribuna-le di Catanzaro del 27/09/2004
ISSN 2611-4259 ICT Ed Magazine (on line)

Rivista trimestrale
Anno V- N° 1 - Aprile 2022
Data di pubblicazione Aprile 2022
Via Pitagora, 46 – 88050 Vallefiorita (CZ)

Direttore Responsabile
Editore-responsabile intellettuale
Luigi A. Macrì
direzione@ictedmagazine.com

Editing e revisione editoriale
Maria Brutto

Redazione
Claudia Ambrosio
Maria Brutto
Mario Catalano
Benedetto Fucà
Ippolita Gallo
M. F. Oraldo Paleologo
Paolo Preianò
Davide Sorrentino

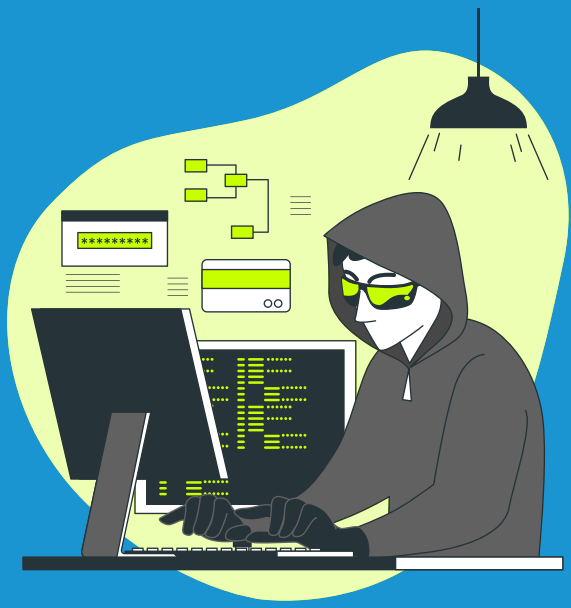
Hanno collaborato
Maria Letizia Belmonte
Giovanna Brutto
Andrea Cortese
Concetta Fava
Marco Di Paolo
Ludovica Zoccali

Webmaster
Rocco Voci - Synapsis

Impaginazione
Manuela Gaetano - CSV Calabria Centro

ICTEDMagazine è un periodico trimestrale, in formato digitale, delle tecnologie dell'informazione e della comunicazione per l'istruzione e la formazione; un progetto editoriale che vede impegnati docenti, genitori, tecnici, esperti e professionisti delle diverse categorie del sapere. Il nostro obiettivo è di contribuire a migliorare la consapevolezza dei genitori e della Società tutta, relativamente alle problematiche legate all'uso delle tecnologie con particolare attenzione ai minori, agli studenti, ed a tutti coloro che vivono una condizione sociale debole. Vengono, inoltre, trattati temi che riguardano la sicurezza e la protezione del proprio computer dai continui attacchi esterni nonché indicazioni a docenti e studenti su tematiche relative a istruzione, formazione, didattica e orientamento scolastico. Altre sezioni, su tematiche relative a ricerca e innovazione, scienze e saperi, rischi di dipendenza dalla rete, robotica educativa e informatica forense, intendono offrire approfondimenti che coronano una visione interdisciplinare orientata ad una prospettiva olistica del Sapere.

Luigi A. Macrì
Direttore responsabile ictedmagazine.com



Il materiale inviato non si restituisce, anche se non pubblicato. I contenuti degli articoli non redazionali impegnano i soli autori. Ai sensi dell'art. 6 - L. n.663 del 22/04/1941 è vietata la riproduzione totale o parziale senza l'autorizzazione degli autori o senza citarne le fonti.

Tutti i diritti riservati
www.ictedmagazine.com © 2022

Cyberwar e "Fuoco Digitale": l'altra faccia della guerra Russia - Ucraina

di Luigi A. Macrì
Direttore responsabile ictedmagazine.com
direzione@ictedmagazine.com

Una guerra più sottile e meno evidente, ma molto pericolosa e difficile da fronteggiare, parallela a quella che vediamo nei notiziari e nei reportage dalla Ucraina, è quella degli attacchi informatici.

Lo scopo principale della cyberwar, guerra cibernetica o informatica, è di minare, utilizzando azioni di sabotaggio informatico, i sistemi necessari per il funzionamento di uno Stato e di un'economia, come l'energia elettrica, la distribuzione del gas e dell'acqua, reti finanziarie e commerciali.

In questo numero, nell'articolo Cyberwar: sicurezza e prevenzione, mettiamo in evidenza, tra l'altro, che "negli ultimi due anni migliaia di aziende nel mondo hanno subito gravi disagi economici e logistici causati da attacchi-ricatti informatici"; ci soffermiamo, inoltre, sul ruolo che la disinformazione e le false notizie, tema che trattiamo molto spesso nei nostri articoli, hanno in questo contesto storico che stiamo vivendo.

Gli attacchi informatici non sono una novità ma la guerra tra Russia e Ucraina che vedono coinvolti interessi globali rischia di diventare una vera guerra informatica che può essere letale per gli interessi e l'economia di una nazione quanto una guerra tradizionale.

Di recente, il 24 febbraio scorso, quando è partita l'offensiva della Russia nei confronti dell'Ucraina, un gruppo di cybersicurezza estone di nome Eset ha intercettato ed identificato un attacco Wiper che consiste in un malware che aveva cancellato il sistema informatico di una banca ucraina e di un'agenzia governativa. Gli aggressori, per coprire le loro tracce, hanno usato, come spesso succede, un certificato digitale appartenente ad una piccola società, in questo caso, di giochi con sede a Cipro denominata Hermetical Digitale Ltd. Sembrerebbe che questo software, definito con il nome di "Hermeticwiper" che si è poi diffuso in Lituania e in Lettonia, faceva parte della guerra informatica parallela già in atto tra la Russia e l'Ucraina.

Gli attacchi informatici contro l'Ucraina sono incominciati prima dell'invasione con le truppe di terra. Il governo ucraino ha segnalato un cyber attacco il 14 gennaio che ha preso di mira siti governativi come quello del ministero degli esteri e del consiglio della difesa. Nel mese di febbraio gli esperti di sicurezza informatica dell'Ucraina hanno segnalato un attacco DDoS (distributed-denial-of-service), contro due delle maggiori banche del Paese che è stato realizzato con l'invio di un numero spropositato di richieste di accesso ad un sito tale da mandarlo in blocco.

Gli attacchi informatici avvengono anche in parallelo e per ostacolare situazioni sul campo; una prossima mossa degli hacker russi potrebbe essere quella di disabilitare il sistema informatico utilizzato dai treni per spostare le truppe al fronte ed inceppare le linee telefoniche utilizzate dai militari.

Nadiya Kostyuk, docente alla Georgia Tech School of Public Policy, ha dichiarato al Rest of World che la Russia ha utilizzato negli ultimi anni l'Ucraina come laboratorio per operazioni di attacchi informatici come quando hacker russi, nel 2015 e 2016, hanno oscurato porzioni di territorio dell'Ucraina, nel 2017 hanno lanciato il virus Notpetya il quale, prima di diffondersi in tutto il mondo, ha attaccato agenzie governative ucraine, gruppi bancari e la centrale nucleare di Chernobyl. Gli hacker russi sono stati anche collegati ad attacchi negli Stati Uniti di tipo ransonware ovvero attacchi informatici con richiesta di riscatto.

Nel 2020 gli hacker russi hanno dimostrato una grande capacità di infiltrarsi di nascosto nelle reti governative utilizzando la vulnerabilità nel software della rete informativa Solarwinds inserendosi nei sistemi informatici di uffici governativi e agenzie di molti paesi, compresi gli Stati Uniti, curiosando all'interno di quei sistemi per almeno un anno senza essere scoperti.

Questa situazione impone l'organizzazione di task force in ogni nazione per fronteggiare gli attacchi informatici e di una normativa specifica che possono tener conto delle diverse problematiche ad essa connesse. Lo scorso 2 marzo su Twitter compare una notizia ed un appello diffuso dal numero due del governo Ucraino, Mykhailo Fedorov, ministro per la trasformazione digitale, che dice: "Stiamo creando un esercito IT. Abbiamo bisogno di talenti digitali". Questa notizia, approvata pienamente dal presidente ucraino Zelensky che ha invitato ad unirsi all'esercito

informatico, ha subito visto l'adesione di migliaia di esperti provenienti da diverse nazioni.
Sebbene Putin continua a dire che non ha scatenato una guerra ma solo "un'operazione speciale nei confronti dell'Ucraina", una dichiarazione di guerra nei confronti della Russia c'è stata, quella del gruppo di hacher Anonymous che hanno rivendicato attacchi DDoS contro obiettivi russi e preso dati dal produttore di armi bielorusso Tetraedr.
Sono molti gli aspetti che rendono unica questa guerra che vede un'informazione veicolata massicciamente anche attraverso i dispositivi mobili come i cellulari; ma la realizzazione di gruppi di "fuoco digitale", organizzati e progettati per intervenire in una zona di guerra in rapida evoluzione è davvero senza precedenti. Una cosa è certa, tra i due anni di pandemia e questa guerra su più fronti, che di fatto con le sanzioni è diventata globale e coinvolge tutti, il mondo intero e la nostra vita non sarà più la stessa. Noi siamo profondamente consapevoli che è giunta l'ora di dichiarare la guerra, in un mondo globale e interconnesso, anacronistica e non conveniente per le nazioni e per i loro popoli, che poi sono, come stiamo vedendo, i primi a pagare. Solo quando le grandi potenze mondiali si uniranno per fare guerra all'inquinamento globale, all'egoismo, per permettere la ripresa di un equilibrio naturale che sembra compromesso, e combattere la povertà e lo sfruttamento, allora potremo dire che è iniziata davvero un'era di speranza e di pace.
Tra le tante iniziative molto valide di solidarietà e di riflessione per la pace tra i popoli, sento il dovere di segnalarvi una iniziativa, una petizione on line diffusa in più lingue, della quale sono il promotore insieme al professore Gaetano Mollo dal titolo Una nuova politica planetaria per un'etica della cooperazione. I link della petizione in lingua italiana e in lingua inglese, presto in spagnolo, sono disponibili di seguito nella sitografia. Vi invito a sottoscriverla e a diffonderla al fine di sensibilizzare le persone per realizzare quella che oggi sembra davvero un'utopia, nella quale vogliamo però credere, la pace nel mondo.

Sitografia:

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
https://www.reuters.com/world/europe/ukrainian-government-foreign-ministry-parliament-websites-down-2022-02-23/
https://www.npr.org/2022/01/19/1074172805/more-than-70-ukrainian-government-websites-have-been-defaced-in-cyber-attacks?t=1649059137352
https://www.wired.com/story/russia-ukraine-ddos-nft-nsa-security-news/
https://restofworld.org/2022/russias-cyber-war-ukraine-risks-death-collateral-damage/
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
https://www.cisa.gov/uscert/russia
https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/
https://www.thedailybeast.com/anonymous-hackers-claim-responsibility-for-cyberattacks-against-russian-state-news-site-rtcom

Petizione in lingua italiana:
https://www.change.org/p/petizione-per-una-nuova-politica-planetaria-per-un-etica-della-cooperazione
Petizione in lingua inglese:
https://www.change.org/p/a-new-planetary-politics-for-an-ethics-of-cooperation