07/04/2022

snewsonline.com

Argomento: Exprivia: si parla di noi

EAV: € 209
Utenti unici: 1.767

https://www.snewsonline.com/domenico-raguseo-la-guerra-diversa/

Domenico Raguseo: la guerra diversa

di Redazione - 7 Aprile 2022

Domenico Raguseo, Head of CyberSecurity Exprivia, penna già varie volte presente sulle colonne di S News, presenta un approfondimento dall'incalzante attualità e di sicuro interesse.

Buona lettura!

La guerra diversa

Nella storia della cybersecurity ci sono alcuni "eventi" che finiscono nella storia della letteratura per qualche ragione: da Mirai a Stuxnet, da WannaCry a Zeus, da Petya a Non-Petya, solo per citarne alcuni.

Il 2022 temo si unirà alla già ampia serie di eventi nefasti come l'anno in cui, per la prima volta, il conflitto tradizionale che vede i contendenti combattere su terra, acqua e cielo per la prima volta li vedrà combattere una guerra diversa, ma con conseguenze potenzialmente fatali anche su quello che in molti chiamano il cyber-spazio, e cioè milioni di dispositivi interconnessi tra di loro che, semplifico, definiamo internet.

RIVISTA
Scarica l'ultimo numero in versione PDF.

Nr. 61 Novembre-Dicembre 2021
Dahua: l'innovazione della sicurezza sempre al tuo fianco

Fiere ed eventi

Secon 2022
Dal 20.04.2022 al 22.04.2022
KINTEX
Seoul, Korea

Focus Tour 2022
Dal 22.04.2022 al 22.04.2022
Bari, Italy

Securex Poland
Dal 25.04.2022 al 27.04.2022
MTP Poznań Expo
Poznań, Polonia

Domenico Raguseo: la guerra diversa

Domenico Raguseo, Head of CyberSecurity Exprivia, penna già varie volte presente sulle colonne di S News, presenta un approfondimento dall'incalzante attualità e di sicuro interesse.

Buona lettura!

La guerra diversa

Nella storia della cybersecurity ci sono alcuni "eventi" che finiscono nella storia della letteratura per qualche ragione: da Mirai a Stuxnet, da WannaCry a Zeus, da Petya a Non-Petya, solo per citarne alcuni.

Il 2022 temo si unirà alla già ampia serie di eventi nefasti come l'anno in cui, per la prima volta, il conflitto tradizionale che vede i contendenti combattere su terra, acqua e cielo per la prima volta li vedrà combattere una guerra diversa, ma con conseguenze potenzialmente fatali anche su quello che in molti chiamano il cyber-spazio, e cioè milioni di dispositivi interconnessi tra di loro che, semplifico, definiamo internet. Ovviamente la prima volta è una stigmatizzazione volontaria: il carattere stesso di internet, dove i confini e gli attori sono meno definiti che nel mondo reale, non penso consenta di definire in maniera inequivocabile la prima volta che uno stato ha deciso di arrecare danno all'altro stato tramite internet, ma sicuramente è l'anno in cui a questo evento i mass media, i social networks e l'opinione pubblica ha dato maggiore risalto per una serie di ragioni.

Sicuramente ha contribuito il grado di consapevolezza del fatto che i servizi digitali da cui dipendiamo sono irreversibili, tanto che per fermare un pronto soccorso ad un ospedale non è necessario un missile ma un ransomware. Stessa cosa si direbbe per voli aerei, infrastrutture critiche.

Se qualche anno fa la cosa poteva lasciare qualcuno sorpreso, i ripetuti incidenti (fino anche alla prima morte di un paziente che non ha potuto essere ricoverato a causa di un ransomware presso un ospedale) hanno fatto concretamente sorgere il timore che qualcosa di fatale potesse accadere, e questo ha fatto sì che l'opinione pubblica sentisse questo conflitto più vicino, non solo geograficamente, ma anche digitalmente. Se infatti la probabilità di un missile può essere considerata ancora lontana, così come le immagini di distruzione, la probabilità che qualcosa di nefasto possa accadere ai servizi digitali da cui dipendiamo, ha sicuramente contribuito a far percepire la guerra più vicina.

Ovviamente se l'opinione pubblica può essere stata sorpresa, molto meno lo sono stati gli addetti ai lavori, soprattutto i contendenti, che per limitare i danni hanno a loro volta chiesto e provato ad escludersi o ad escludere l'avversario da internet. Se l'uno chiede infatti che l'ICANN (Internet Corporation for Assigned Names and Numbers) revochi domini rilasciati all'avversario e spenga i DNS (Domain Name Systems) sul territorio dell'avversario, l'altro studia come disconnettersi da internet di sua

spontanea volontà per le stesse o opposte ragioni. Si ha la sensazione di vedere le fazioni combattere per un ponte che entrambi sono interessati a possedere, perché entrambi hanno il timore che a controllarlo sia l'avversario, dimenticando però che in questo caso il ponte è internet e staccarne un pezzo minerebbe i principi stessi su cui internet è stato fondato e di conseguenza minerebbe tutti i servizi e l'economia ad esso collegato, dai social networks a swift (e transazioni bancarie in genere), sino a milioni di altri servizi che tramite internet vengono erogati.

La guerra su internet ha delle specificità che la differenziano notevolmente da battaglie sugli elementi tradizionali.
La prima è che a combattere non ci sono persone con elmetto, ma gruppi spesso transnazionali e transterritoriali che appoggiano l'uno o l'altro. Se nel 1972 Lorenz in una conferenza parlò di come il batter d'ali di una farfalla in Brasile potesse provocare un tornado in Texas, oggi con internet un attaccante in un emisfero può, senza lasciare la sua scrivania, bloccare il portale del Ministero della Difesa di uno dei contendenti. Immaginate pertanto migliaia di attaccanti seduti sulle scrivanie di mezzo mondo che combattono usando le tastiere. I rischi di danni collaterali sono possibili, e cioè di malware creati per attaccare un obiettivo ma che per qualche ragione si diffondono, colpendo anche terzi non coinvolti direttamente nel conflitto.

A rendere più preoccupante questo fenomeno è il fatto che, se in genere chi attacca è motivato da un profitto economico, in questo caso l'attaccante potrebbe essere motivato semplicemente dal creare danni all'avversario. Non sorprende che se negli anni scorsi abbiamo parlato di ransomware (ricatti per estorcere criptovalute alla vittima), in guerra si parla di attacchi wiper dove i dati sono distrutti. Pertanto, si tratta di attacchi molto veloci e violenti, che riducono la possibilità di ridurre i rischi.

Inoltre non dimentichiamo che i malware creati durante il conflitto verranno utilizzati anche dopo il conflitto e le vulnerabilità zero-day saranno sfruttate da attaccanti negli anni a venire.

di Domenico Raguseo