Corriere DELLE Comunicazioni it

http://www.corrierecomunicazioni.it/it-world/43765_intelligenza-artificiale-arma-finale-contro-il-cybercrime-as-a-service.htm

Intelligenza artificiale arma finale contro il cybercrime as a service

05/10/16

Si apre una nuova frontiera per il mercato della sicurezza informatica alle prese con la nuova generazione di malware. Corcom è andato nel quartier generale di Netscout System, nella Silicon Valley. Il Cmo Jim McNiels: "Alle aziende servono nuove strategie difensive oggi che i 'cattivi' si sono spostati in rete, dove c'è valore da rubare"

di Antonio Dini

È la nuova frontiera. La sicurezza informatica, che nell'era delle reti sta vivendo una seconda giovinezza. Dopo che il mercato degli attori tradizionali ha visto rapidi consolidamenti e cambiamenti di fronte, nel settore emergono nuove realtà piccole e dinamiche per fare fronte a una esigenza di mercato: **la difesa da un'intera generazione di nuovi malware**, software creati da malintenzionati con l'obiettivo di rubare dati e identità digitali.

L'ultima moda nella parte oscura della rete sono gli attacchi con ransomware, cioè software che chiedono i riscatti. Dopo l'infezione da parte di un vettore nascosto, magari nell'allegato di una mail o in un sito truffaldino. Il "carico" o payload del vettore di attacco infetta il computer crittando con una chiave conosciuta solo dal suo autore tutto il contenuto del disco rigido. In questo modo l'utente non può più aprire i suoi documenti.

Un esempio tra i più recenti è il **ransomware Polyglot, anche conosciuto come MarsJok**, che secondo gli esperti di Kaspersky Lab appartenente imita un altro famigerato trojan, cioè CTB-Locker. Una geografia complessa, ricca di nomi e di tecnologie i cui risultati sono sempre gli stessi: dati compromessi, richieste di riscatto in Bitcoin che poi non portano allo sblocco dei dati (ma attenzione, Kaspersky sostiene di aver trovato il modo di sbloccare Polyglot senza bisogno di pagare, che è comunque sconsigliato).

È in questo contesto che ci possiamo chiedere quali siano in realtà le soluzioni con le quali si potranno risolvere alla radice questi problemi.

Qui entrano in gioco aziende come **Netscout Systems, che CorCom ha potuto visitare nel suo quartier generale della Silicon Valley**, a margine dell'incontro organizzato da NetEvents a Saratoga, in California.

«Siamo arrivati a un punto di svolta – dice a CorCom **Jim McNiel, Chief marketing officer di Netscout** – in cui la visibilità sulla rete e la capacità di analizzare i pacchetti non basta più: occore anche l'intelligenza artificiale capace di capire cosa sta succedendo e prvedere in maniera non deterministica se quello davanti al quale ci troviamo è un attacco oppure traffico lecito».

Netscout, che si definice "guardiana del mondo connesso", ha un osservatorio privilegiato perché dal 1986, anno in cui è stata fondata da Anil Singhal come Network General, raccoglie il traffico delle reti e cerca di dargli un senso. Nel tempo si sono succedute diverse tecnologie e acquisizioni mirate: l'ultima delle quali è l'acquisto della parte di telecomunicazioni di Danaher Corporation, che include **Arbor Networks, Fluke Networks, Tektronix Communications e VSS Monitoring**. Un pugno di tecnologie preziose per Netscout che le danno accesso a soluzioni per tutti i livelli di comunicazione digitale, da quello del trasporto dati a quello delle applicazioni e della presentazione delle informazioni.

«È nata una nuova forma forma di criminalità online - dice McNiel – che potremmo definire "**cybercrime as a service**". È un mercato organizzato e segmentato, dove anche chi non ha competenze tecnologiche di avanguardia può utilizzare, pagando solo per quel che gli serve, i più moderni strumenti malware in circolazione. Basta poco per avere a disposizione una Botnet da milioni di Pc (tra l'altro, Roma risulta essere la terza città di Europa, Medio Oriente e Africa per numero di Pc "zombie", secondo un rapporto Norton by Symantec) e lanciare un attacco Ddos, cioè un attacco che satura i canali di comunicazione di una rete, "spegnendo" l'accesso sia ai servizi di front end che a quelli interni dell'azienda. La stima è che un attacco di questo genere costi, almeno alle aziende Usa, fra i due e i quattro milioni di dollari per ciascuna vittima.

«Le aziende – dice McNiel – devono avere una strategia che assicuri loro una funzionalità 24/7 del loro business, sennò perdono oltre che soldi anche reputazione, credibilità e competitività». Mantenere tutto in funzione oggi è più difficile perché i "cattivi" si sono decisamente spostati in rete, dove c'è valore da rubare, ma anche perché il mondo digitale è diventato estremamente complesso e vulnerabile. Oggi ci sono 15 miliardi di apparecchi connessi con un indirizzo IP. Sono più delle persone che si connettono in rete (3 miliardi) o del totale della popolazione umana (7,3 miliardi) se è per questo, inclusa quella parte che non sa neanche cosa sia Internet o un computer.

Il Brasile, che è la nona economia al mondo, circa un decimo di quella americana, è l'epicentro dei più grandi attacchi Ddos del pianeta. Gli esempi dei mondiali di calcio e delle Olimpiadi tenutesi in quel Paese sono un chiaro caso di quanto sia necessario avere visibilità nella rete e capire le differenze nei dati che vengono raccolti.

La parola chiave è "**business assurance", la possibilità cioè di dare la garanzia della continuità di funzionamento della rete** e dei servizi delle aziende cliente. Dentro ci sono i big data, la capacità di analizzare le informazioni raccolte da apparecchi presso i clienti dei servizi che "annusano" il traffico di rete e lavorano per dargli un senso.

È la stessa cosa che fa Javelin, come spiega a CorCom il suo responsabile delle operazioni, Greg Fitzgerald: «Oggi è una corsa: quanto velocemente si trova la macchina compromessa per riuscire a

spegnerla. Prima ci volevano mesi, adesso minuti. Riusciamo a cogliere gli attaccanti nell'atto dell'attacco e magari anche a trovare le tracce ancora fresche di quello che stanno facendo. Ma per riuscirci serve l'intelligenza artificiale, servono meccanismi automatici che consentano di cogliere i cambiamenti all'interno di una rete».

L'eterna lotta fra guardie e ladri, che nel tempo è diventata sempre più complessa, nel mondo cyber acquista una dimensione inedita che fa fare la sua comparsa alle prime "guardie artificiali". Quando arriveranno anche i "ladri artificiali", cioè le AI a disposizione dei cattivi? Manca meno di quel che sembra.

 05 Ottobre 2016

TAG: saratoga netevents, malware, security, artificial intelligence