Evoluția amenințărilor cibernetice odată cu dezvoltarea inteligenței artificiale

Predicții referitoare la IA

Convergența IA cu 5G va accelera dezvoltarea terapiei digitalizate

"In 2018 we saw a great deal of hype around AI in healthcare but we also saw it become a reality—in everything from predictive analytics for chronic disease management, to workflow enhancement in radiology as well as administrative and financial use cases that bring operational efficiency. In 2019 we are going to see voice and video, coupled with AI, being used to help accelerate the shift of the point of care from the hospital, to the patient, wherever they are. The convergence of AI with 5G will also accelerate the development of digital therapeutics that are more personalized, adaptive and take advantage of AR and VR. Mental health and substance abuse treatment will be where we see early adoption. Clinicians that embrace AI as an augmenter or assistant, not as a threat of replacement or obsolescence, will be able to differentiate themselves both to their patients and their peers"

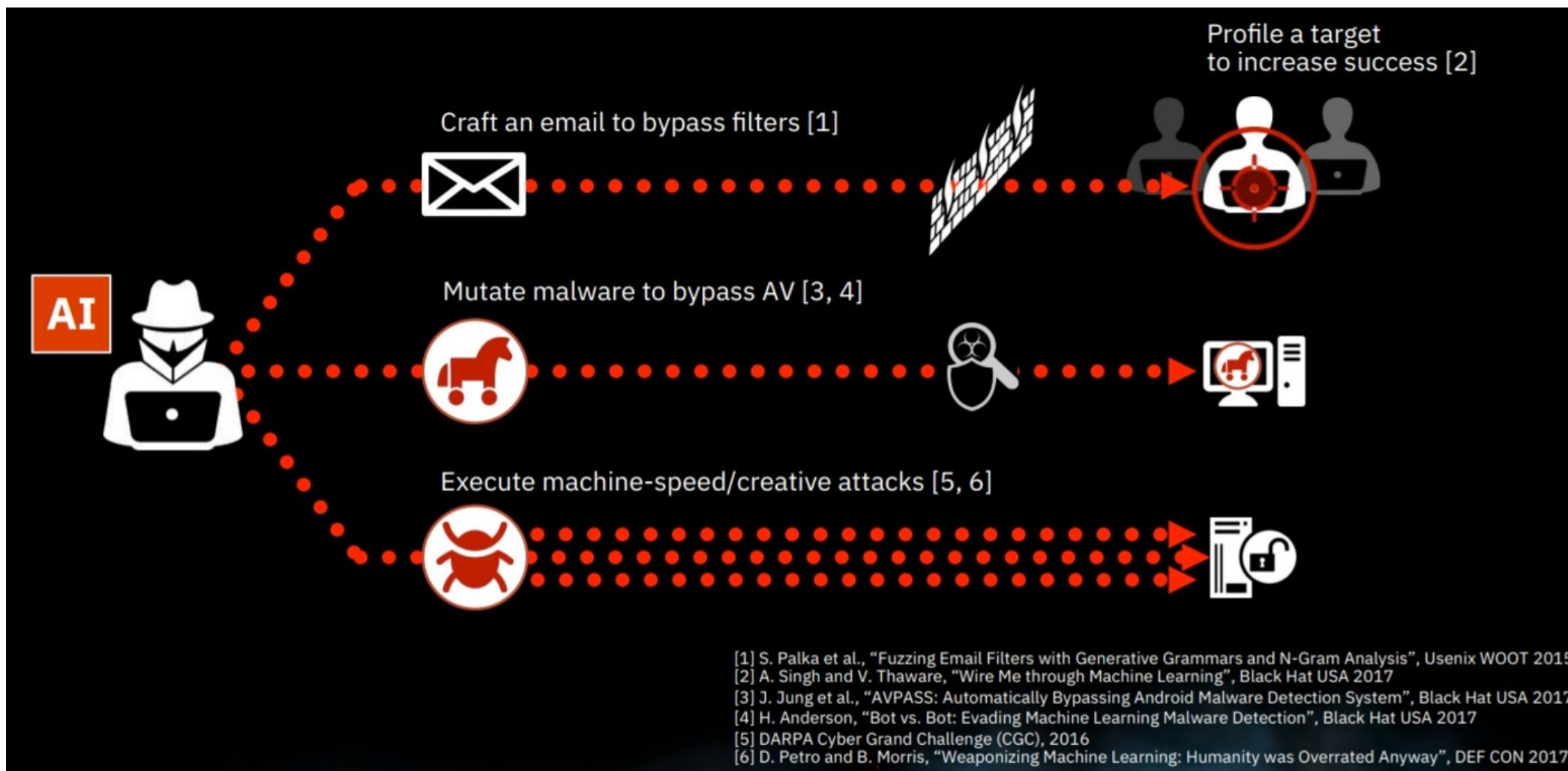Jennifer Esposito, General Manager, Health & Life Sciences, Intel

Predicții referitoare la IA

Atacuri cibernetice bazate pe IA

- Primele semne ale unor atacuri cibernetice bazate pe IA au fost observate în 2017 când o companie din India a suferit un atac cu o formă de malware ce folosea tehnici rudimentare de machine learning pentru a observa și a învăța modele de comportament al utilizatorilor din rețea.

- Între timp, tot mai multe atacuri cibernetice folosesc algoritmi intelligenți pentru tintirea victimelor si evitarea detecției.

- 62% dintre participanții la un sondaj efectuat la conferințța Black Hat USA 2018 consideră că în următorul an vom observa cel puțțin un atac cibernetic bazat pe IA.
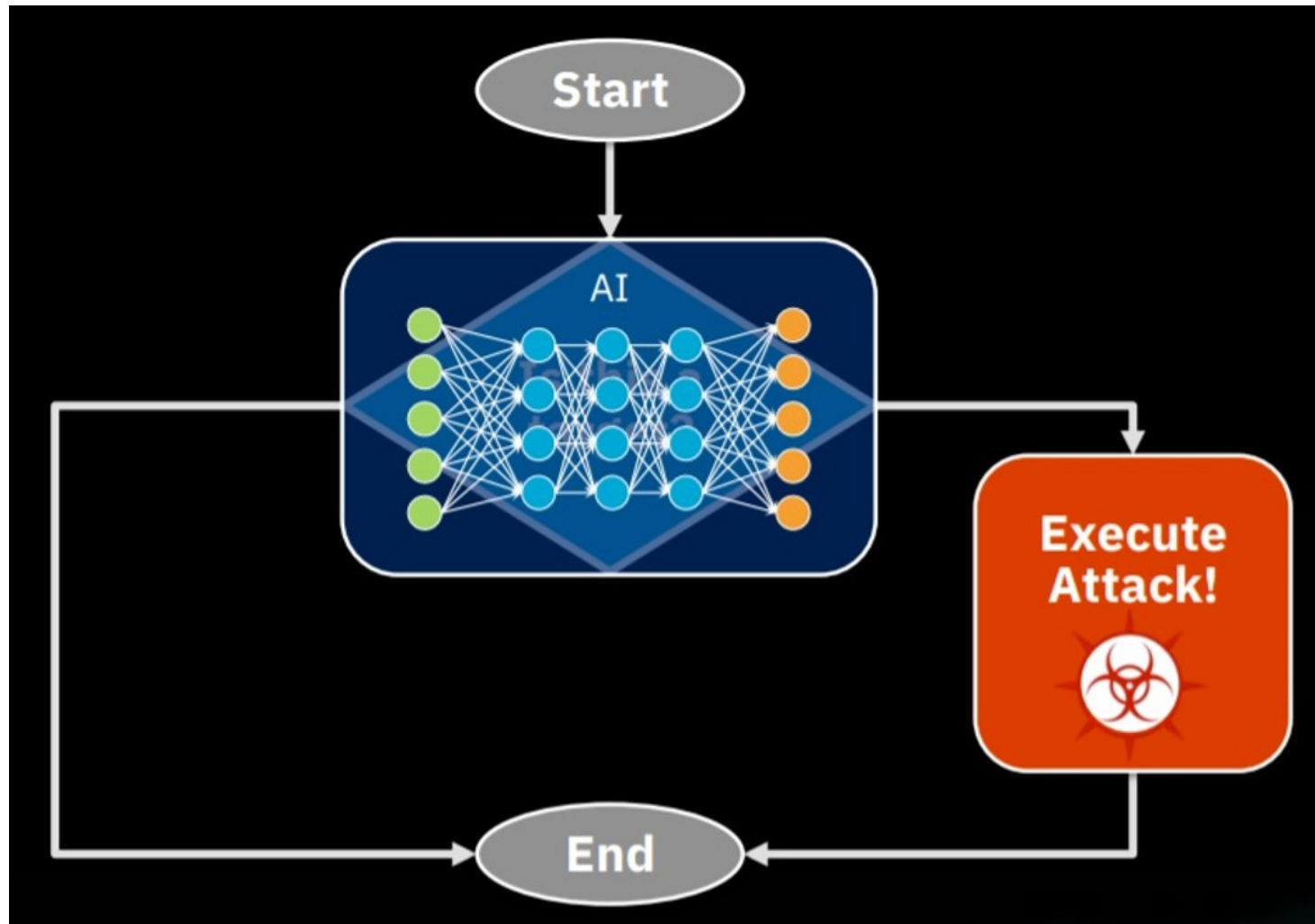
DeepLocker

IBM research presented at BlackHat USA 2018

Profile a target to increase success [2]

Craft an email to bypass filters [1]

Mutate malware to bypass AV [3, 4]

Execute machine-speed/creative attacks [5, 6]

[1] S. Palka et al., "Fuzzing Email Filters with Generative Grammars and N-Gram Analysis", Usenix WOOT 2015
[2] A. Singh and V. Thaware, "Wire Me through Machine Learning", Black Hat USA 2017
[3] J. Jung et al., "AVPASS: Automatically Bypassing Android Malware Detection System", Black Hat USA 2017
[4] H. Anderson, "Bot vs. Bot: Evading Machine Learning Malware Detection", Black Hat USA 2017
[5] DARPA Cyber Grand Challenge (CGC), 2016
[6] D. Petro and B. Morris, "Weaponizing Machine Learning: Humanity was Overrated Anyway", DEF CON 2017

AI-powered targeted attacks

Source: IBM research presented at BlackHat USA 2018

Ce am putea face?

Big Data Security Analytics

http://www.deliblogic.com/legends-big-data-security-analytics/

Vă mulțumesc!

Cătălin Pătrașcu

✉ catalin.patrascu@outlook.com

in /catalin.patrascu

☎ /+40-785.257.443