



Atelier

Faking it: combattere gli attacchi di impersonificazione delle email con l'AI

Alessio Pennasilico, Comitato Tecnico Scientifico, Clusit

Mariana Pereira, Director Email Security Products, Darktrace

27 ottobre 15.00-16.00 - Streaming Edition

#securitysummit #academy #streamingedition

Alessio L.R. Pennasilico aka -=mayhem=-

Practice Leader Information & Cyber Security Advisory Team @
Security Evangelist & Ethical Hacker



Membro del Comitato Tecnico Scientifico



Presidente dell'Associazione Informatici Professionisti



Vice Presidente del Comitato di Salvaguardia per l'Imparzialità



Membro del Comitato di schema



Direttore Scientifico della testata

CYBERSECURITY360



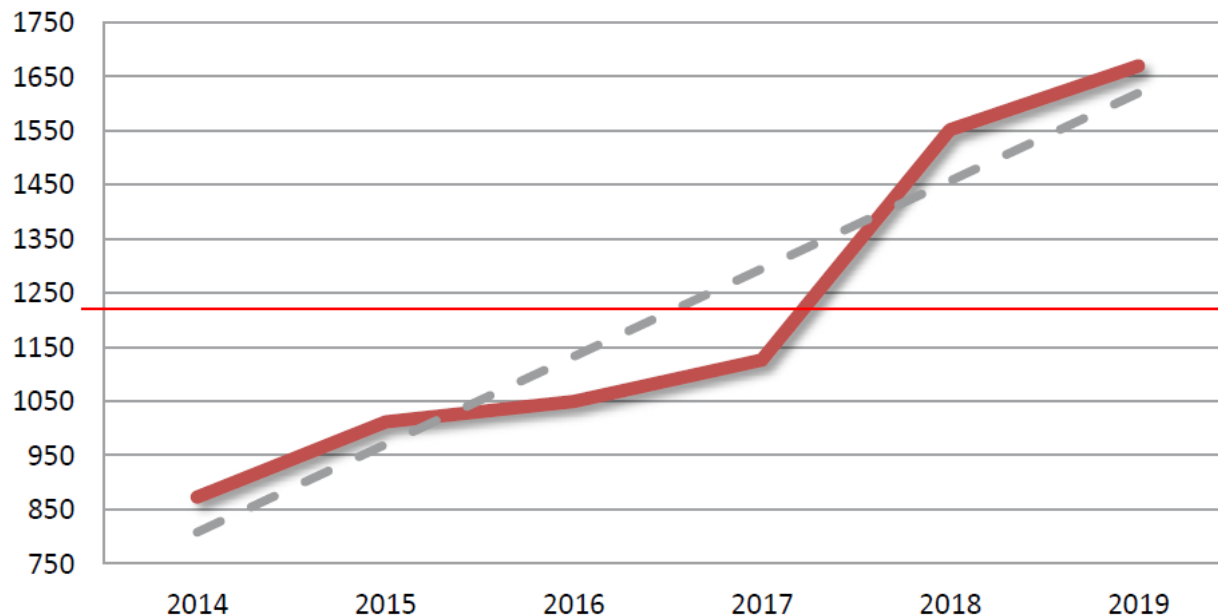
Mariana Pereira

*Director
Email Security Products*



Sono in aumento tentativi di attacco ed i conseguenti incidenti!

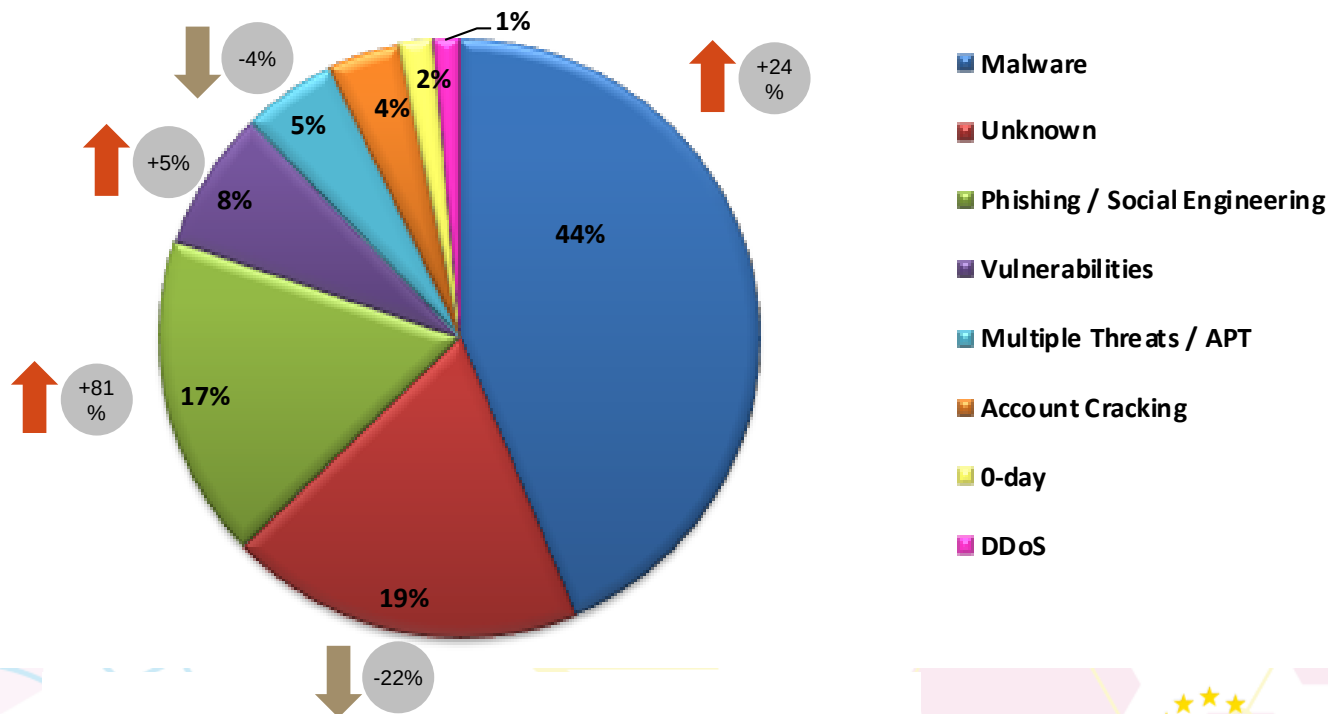
Numero di attacchi rilevanti per anno (2014 - 2019)



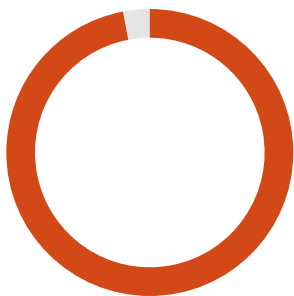
© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Malware e phishing ANCORA (!?!?) la principale minaccia!

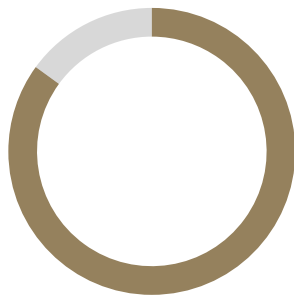
Tipologia e distribuzione delle tecniche d'attacco 2019



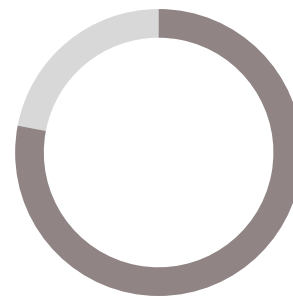
Un problema che ci riguarda tutti...



Utenti che non sono in grado di identificare una e-mail di phishing sofisticata



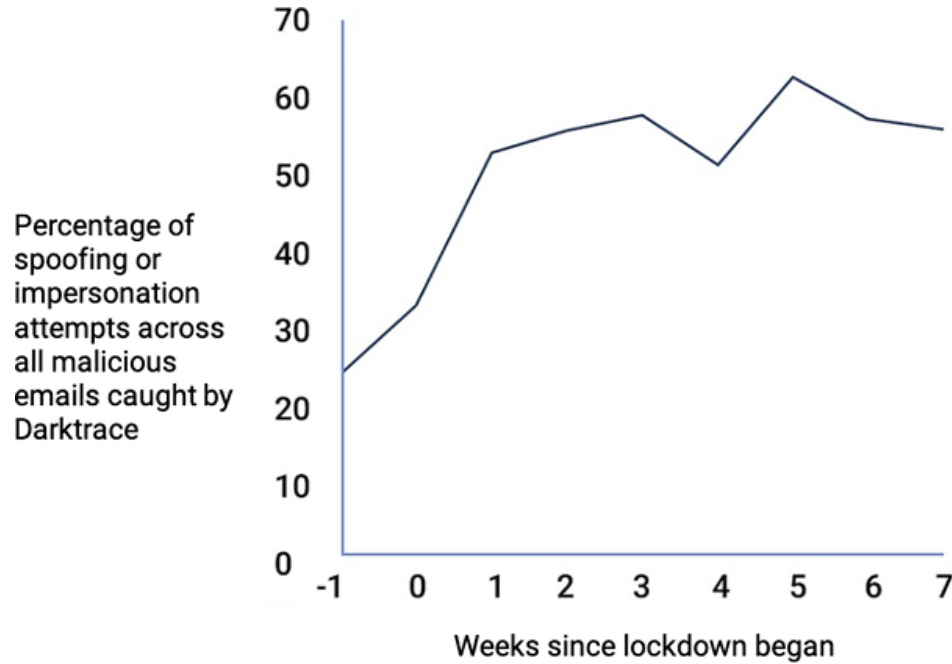
Organizzazioni che sono state vittime di attacchi di phishing



Persone che dichiarano di essere consapevoli dei rischi associati a link sconosciuti nelle e-mail ma che cliccano comunque

Fonte: Keepnet Labs

In aumento gli attacchi spoofing



User profiling & targeting

È davvero un attacco
“informatico”?

Non solo email con
payload dannosi, ma
anche email per
recognizance &
profiling



CEO Fraud vs Business e-mail compromise (BEC)

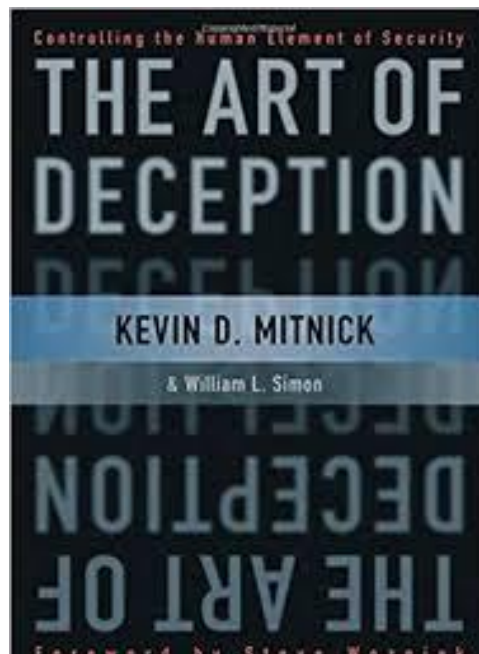
CEO Fraud: è davvero un attacco “informatico”?

Fai questo bonifico

Vs

Guarda questa contabile / estratto conto falsi

SOCIAL ENGINEERING COME ATTO DI MANIPOLAZIONE



“... the social engineer is able to take advantage of people to obtain information with or without the use of technology.” (Kevin D. Mitnick)

“Social engineering is any act that influences a person to take an action that may or may not be in his or her best interests.” (Cristopher Hadnagy)

Possiamo fidarci di contatti di fiducia?

Renata Pereira

enjoy ;)

http://thecooperreview.com/10-more-tricks-appear-smart-in-meetings/?mc_cid=d462daddcf&mc_eid=fdacfed706

Renata Pereira

This is excellent

<https://www.theguardian.com/culture/video/2016/apr/25/patrick-stewart-sketch-what-has-the-echr-ever-done-for-us-video>

Renata Pereira

Dear Santa

Dear Santa, I hope you don't mind me writing in English- One of your elves took it upon him/herself to correct my grammar whe...

Renata Pereira

Enjoy!

[http://i.imgur.com/ZZpVeoY.gifv?](http://i.imgur.com/ZZpVeoY.gifv?utm_source=Mr%20Hyde&utm_medium=email&utm_campaign...)

[utm_source=Mr%20Hyde&utm_medium=email&utm_campaign...](http://i.imgur.com/ZZpVeoY.gifv?utm_source=Mr%20Hyde&utm_medium=email&utm_campaign...)

Renata Pereira

(No Subject)

[https://www.buzzfeed.com/samstryker/ryan-lochte-tweets?](https://www.buzzfeed.com/samstryker/ryan-lochte-tweets?bfbfbmain&ref=bfbfbmain&utm_term=.nhoo9ZoQ#.dfz1lw1o)

[bfbfbmain&ref=bfbfbmain&utm_term=.nhoo9ZoQ#.dfz1lw1o](https://www.buzzfeed.com/samstryker/ryan-lochte-tweets?bfbfbmain&ref=bfbfbmain&utm_term=.nhoo9ZoQ#.dfz1lw1o)

Renata Pereira

A few laughs...

[https://i.imgur.com/TaNjIZi.gifv?](https://i.imgur.com/TaNjIZi.gifv?utm_source=Mr%20Hyde&utm_medium=email&utm_campaign...)

[utm_source=Mr%20Hyde&utm_medium=email&utm_campaign...](https://i.imgur.com/TaNjIZi.gifv?utm_source=Mr%20Hyde&utm_medium=email&utm_campaign...)

Renata Pereira

Fwd: BA e-ticket receipt 6YFLUZ: LHR-LIN 27

----- Messaggio inoltrato ----- Da: British Airways e-ticket <BA.e-ticket@email.ba.com> Data: mercoledì 26 novem...

https://i.imgur.com/

1 / 79

One engine detected this URL.

https://i.imgur.com/

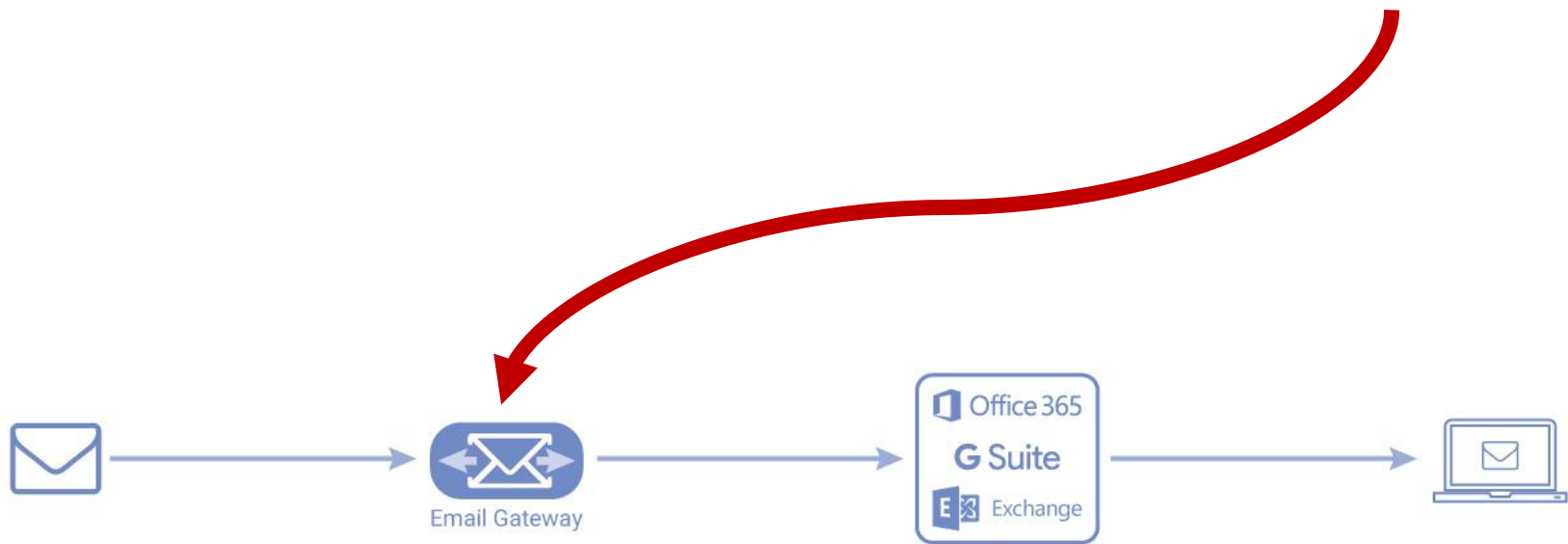
200 Status

text/html Content Type

2020-10-12 02:03:08 UTC 15 hours ago

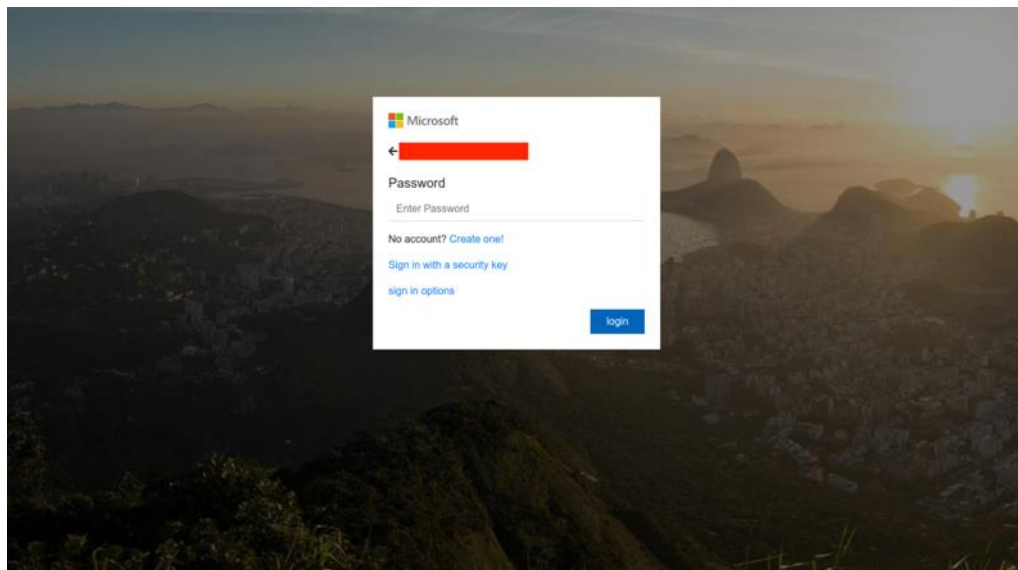
DETECTION	DETAILS	COMMUNITY
MalwarePatrol	Malicious	ADMMUSLab
AvastLab WebGuard	Clean	AlienVault
Antiy-AVL	Clean	Artists Against 419
Avira (no cloud)	Clean	BADWARE.INFO
Baidu International	Clean	BitDefender
BlockList	Clean	Burly
Certego	Clean	CNS Army
CLEAN MX	Clean	Comodo Valkyrie Verdict
CyDef	Clean	CyberCrime
CyRadar	Clean	Cym
desinmascara.me	Clean	DRS

L'approccio attuale utilizza tools posizionati qui:



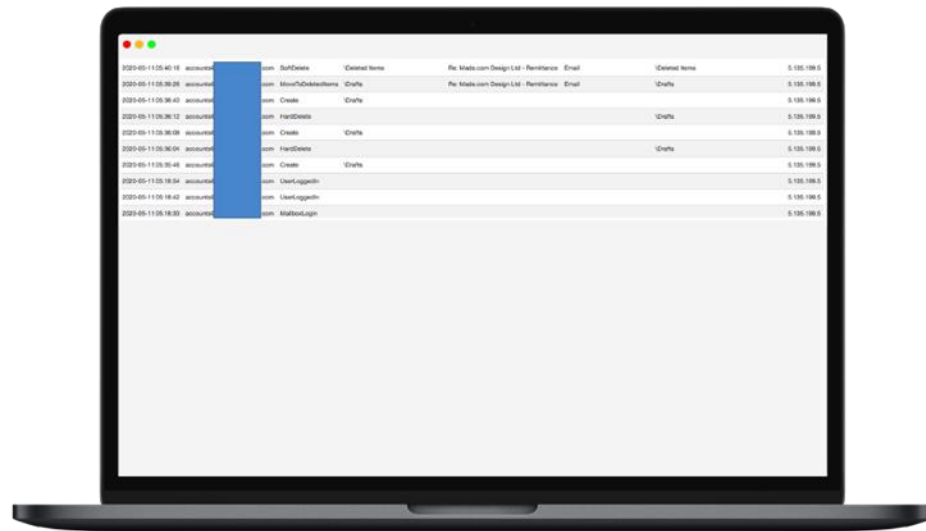
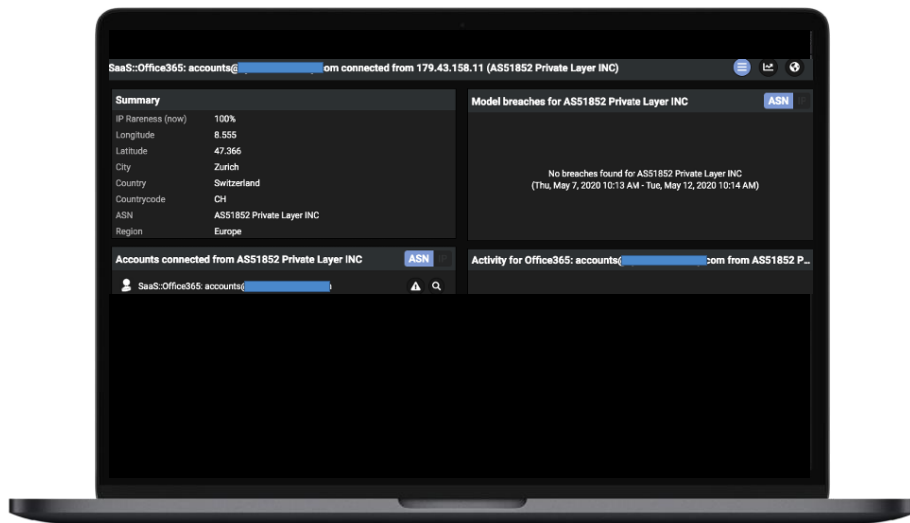
Testo del link visualizzato: [https://COMPANY.sharepoint\[.\]com/sites/.....](https://COMPANY.sharepoint[.]com/sites/.....)

Vero link payload: [http://we---kk\[.\]xyz/...../#user@COMPANY.COM](http://we---kk[.]xyz/...../#user@COMPANY.COM)



Credenziali Rubate

Un account compromesso dà accesso non solo alla posta elettronica...



Come cambiano le minacce

Dalla mail...
...al ransomware ...
...all'esfiltrazione...

Cybercrime: i dati di Luxottica pubblicati sul Darkweb dal gruppo Nefilim

🕒 20 Ottobre 2020 🧑 Francesco Bussoletti 📁 Cyber, Difesa e Sicurezza



by Odisseus





di Gianluca Dotti
Giornalista
scientifico

Un articolo scritto da un'intelligenza artificiale ha battuto quelli tradizionali

Opinion
Artificial intelligence (AI)

A robot wrote this entire article. Are you scared yet, human?

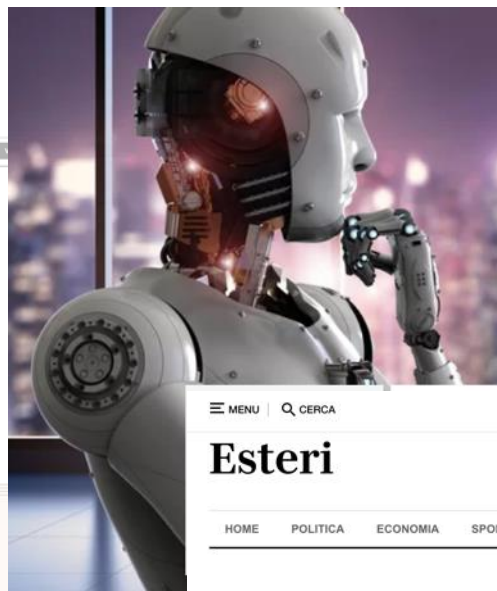
GPT-3

Tue 8 Sep 2020 09:45 BST

67,413 1,188

We asked GPT-3, OpenAI's powerful new language generator, to write an essay for us from scratch. The assignment? To convince us robots come in peace

For more about GPT-3 and how this essay was written and edited, please read our editor's note below



MENU CERCA

la Repubblica

R+ Rep: PER ABBONARSI ACCEDI

Esteri

HOME POLITICA ECONOMIA SPORT SPETTACOLI TECNOLOGIA MOTORI TUTTE LE SEZIONI D REP TV



Gb, il Guardian pubblica il primo editoriale scritto da un robot: "Umani, noi non vi distruggeremo"



Il quotidiano britannico ha chiesto a GPT-3, il nuovo potente generatore di linguaggi di OpenAI, di scrivere un saggio. L'incarico? Convincerci che l'intelligenza artificiale non è una minaccia

DARKTRACE



The Rise of 'Digital Fakes'

- Rise of Offensive AI and impersonation attacks
- AI powered 'digital fakes' are impossible for humans to distinguish
- Attacks move at machine speed

Asimmetria della minaccia cyber

Attaccare sta diventando più semplice

- Attacchi alla velocità delle macchine
- E-mail di phishing sofisticate
- Attacchi furtivi “low and slow”
- AI offensiva

Difendersi sta diventando più difficile

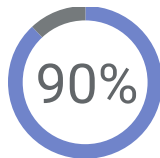
- Cloud e IoT
- Mobile e smart-working
- Attività digitali frammentate
- Team della sicurezza sovraccarichi

Insights da professionisti della cyber security

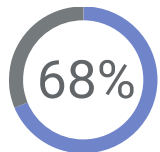


600%

increase in
COVID-19
phishing emails



Mobile apps for
business as a
category up



of organisations
expanded workforce
VPN usage

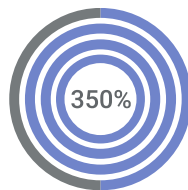
 Suite 20%
adoption increase ↑



Google Meet Factor user increase

Seat increase
↑ 58M ↑
 Microsoft 365

300 MILLION
↑  zoom
User Growth
10 MILLION



 Microsoft Teams
Daily users
increase



29%
of organisations
introduced workforce
VPNs for the first time

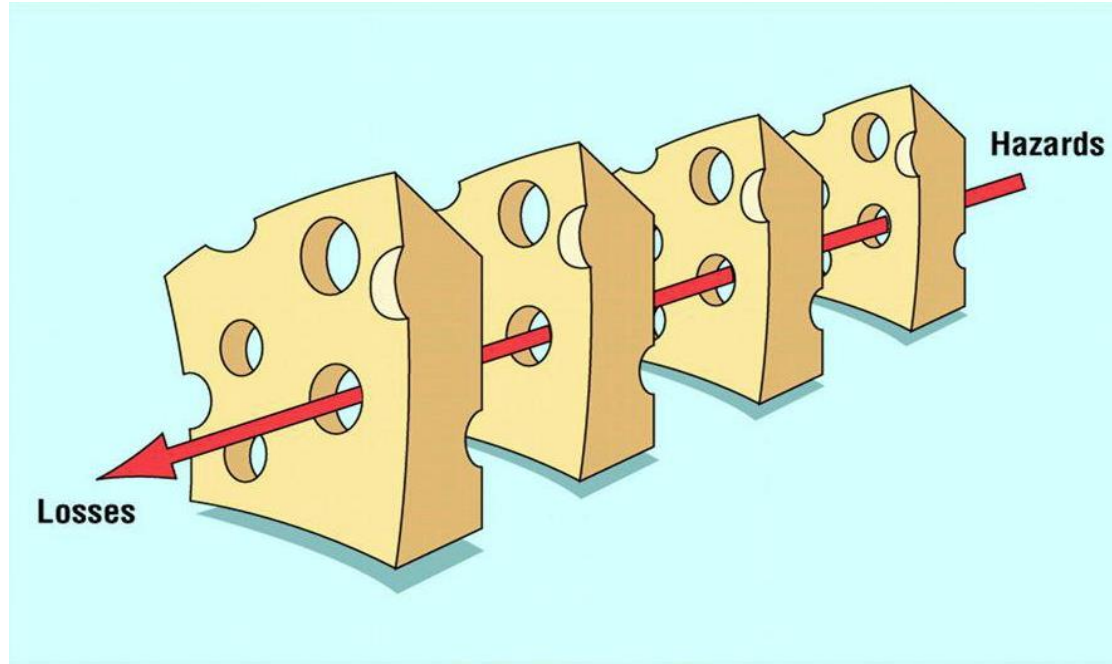
Come contrastare questi attacchi?

Sperare che l'utente si accorga di qualche «anomalia»

oppure

Formalizzare i processi adatti
Adottare le tecnologie adeguate
Formare e sensibilizzare le persone

Anche l'efficacia dell'azione più insignificante fa differenza



Q&A