ITS DIGITAL ACADEMY MARIO VOLPATO
ISTITUTO SALESIANO SAN MARCO
COESIONE ITALIA 21-27 VENETO
Cofinanziato dall'Unione europea
REPVBBLICA ITALIANA
REGIONE DEL VENETO
ISTITUTI TECNICI SUPERIORI IT'S MY FUTURE

DAINESE
ANDREA

Cybercrime

Istituto Salesiano San Marco
ITS Crossmedia Communication Specialist

No AI were harmed during the making of these slides.

WHOAMI

Andrea Dainese – CISO

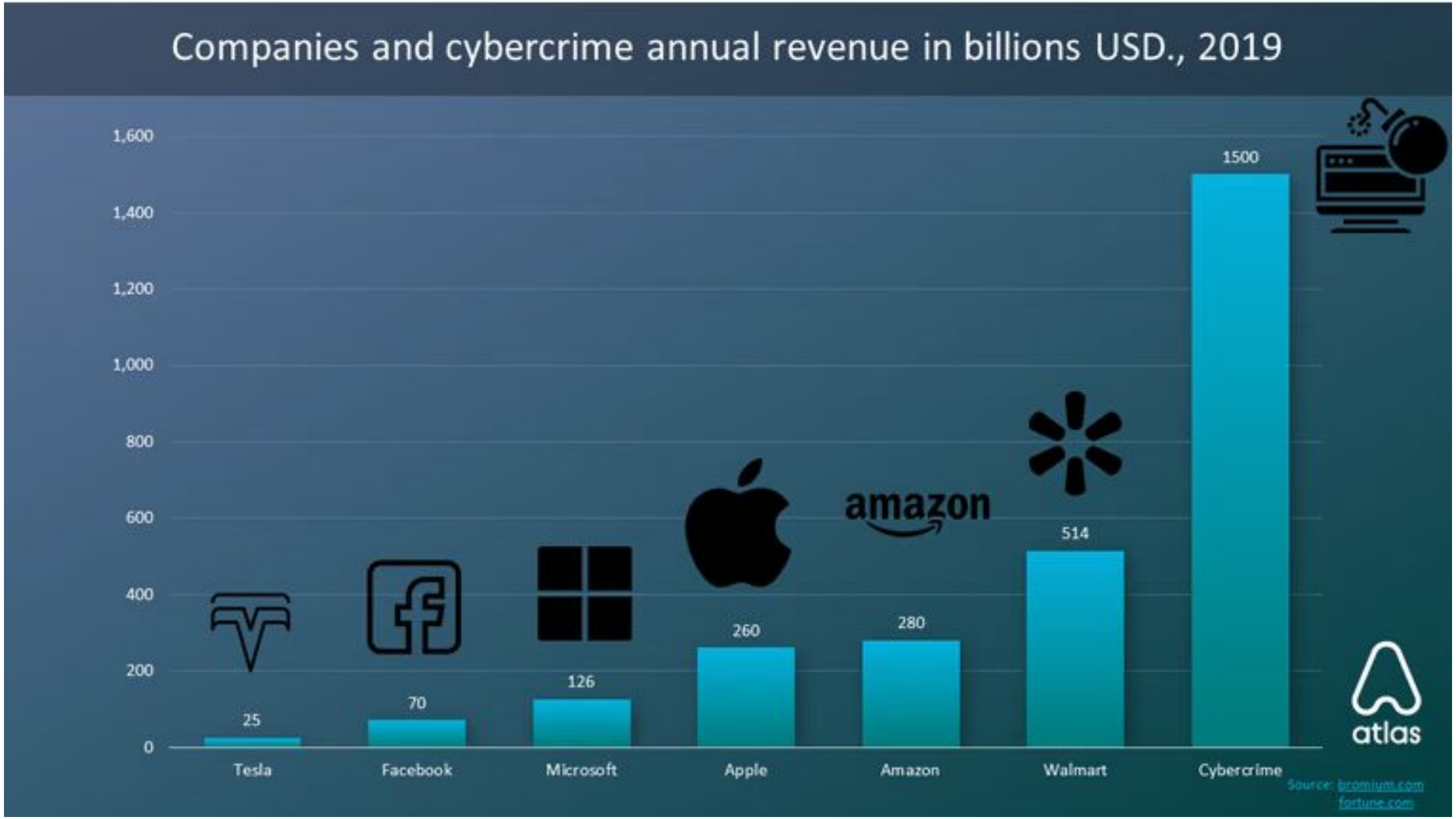
- Senior Network & Security Architect with 15+ years' experience in securing complex IT and OT infrastructures
- Focused on cyber security strategies, GDPR/ISO 27001 compliance and Automation
- Incident Response Team
- Cisco (CCIE), VMware, Red Hat… certified
- Father of Unified Networking Lab (UNetLab)
- Privacy and digital security evangelist – expert counselor-mediator in Cyberbullying

https://adainese.it

~~HACKERS~~

CYBERCRIME

CYBERCRIME REVENUE

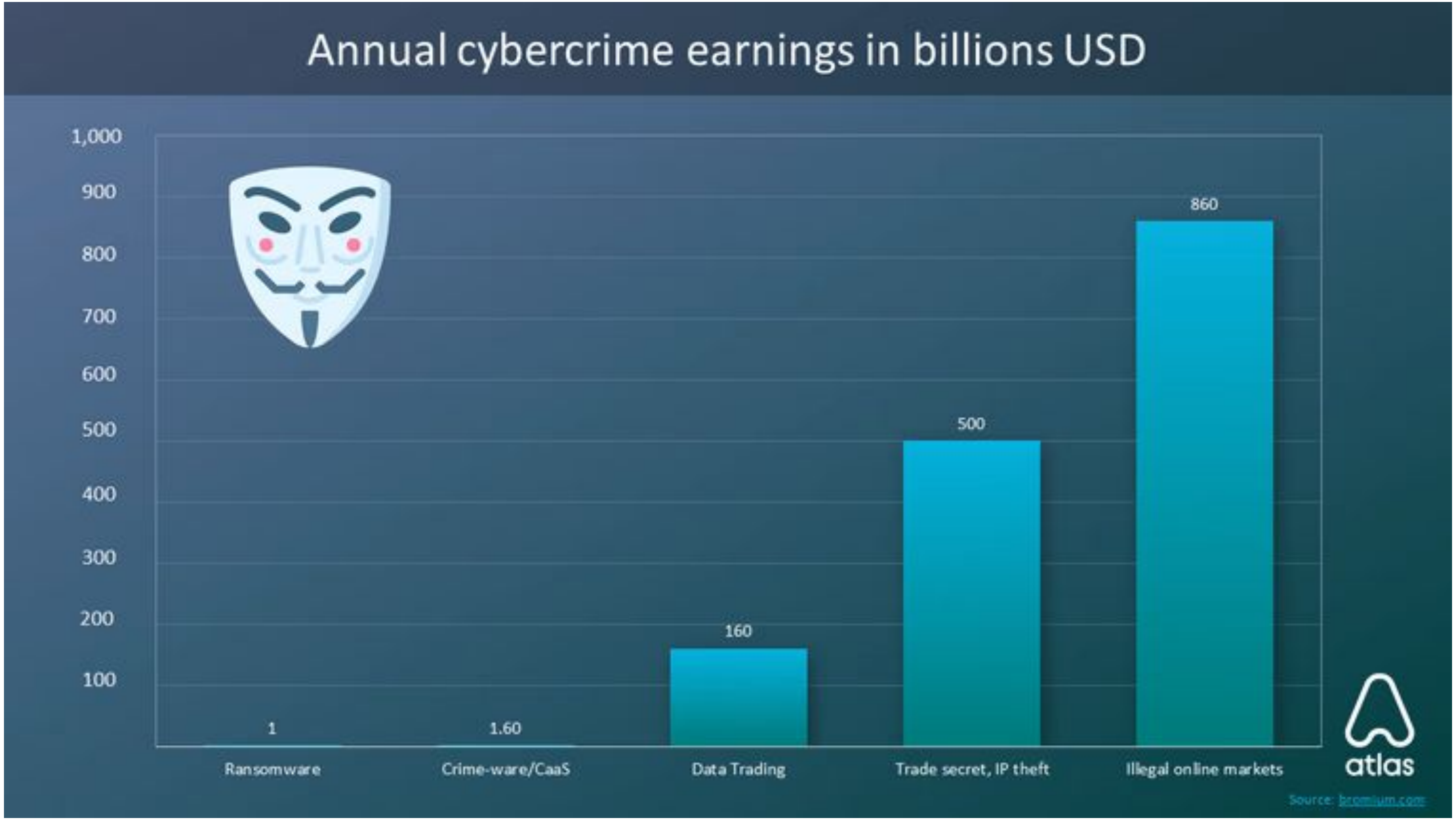


Companies and cybercrime annual revenue in billions USD., 2019

Source: bromium.com fortune.com

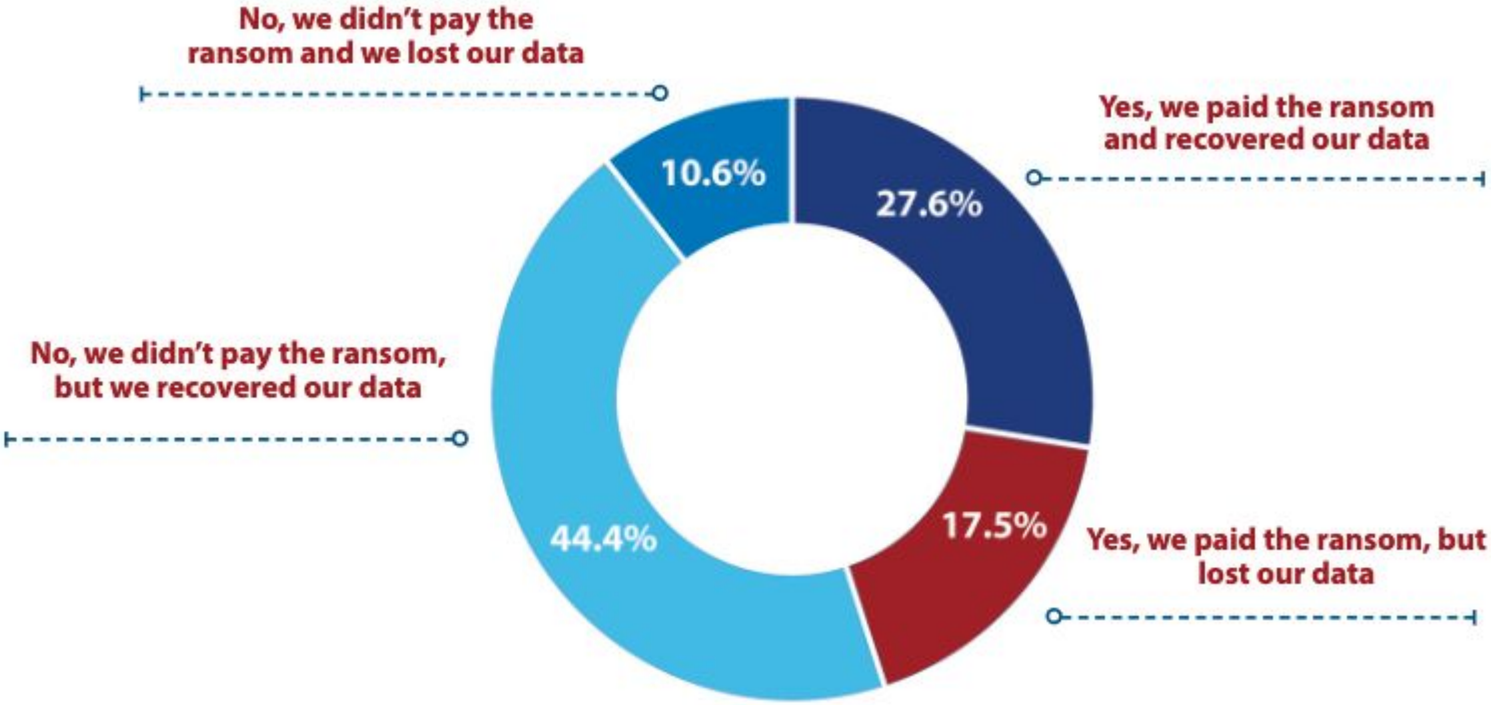
https://atlasvpn.com/blog/cybercrime-annual-revenue-is-3-times...

CYBERCRIME REVENUE

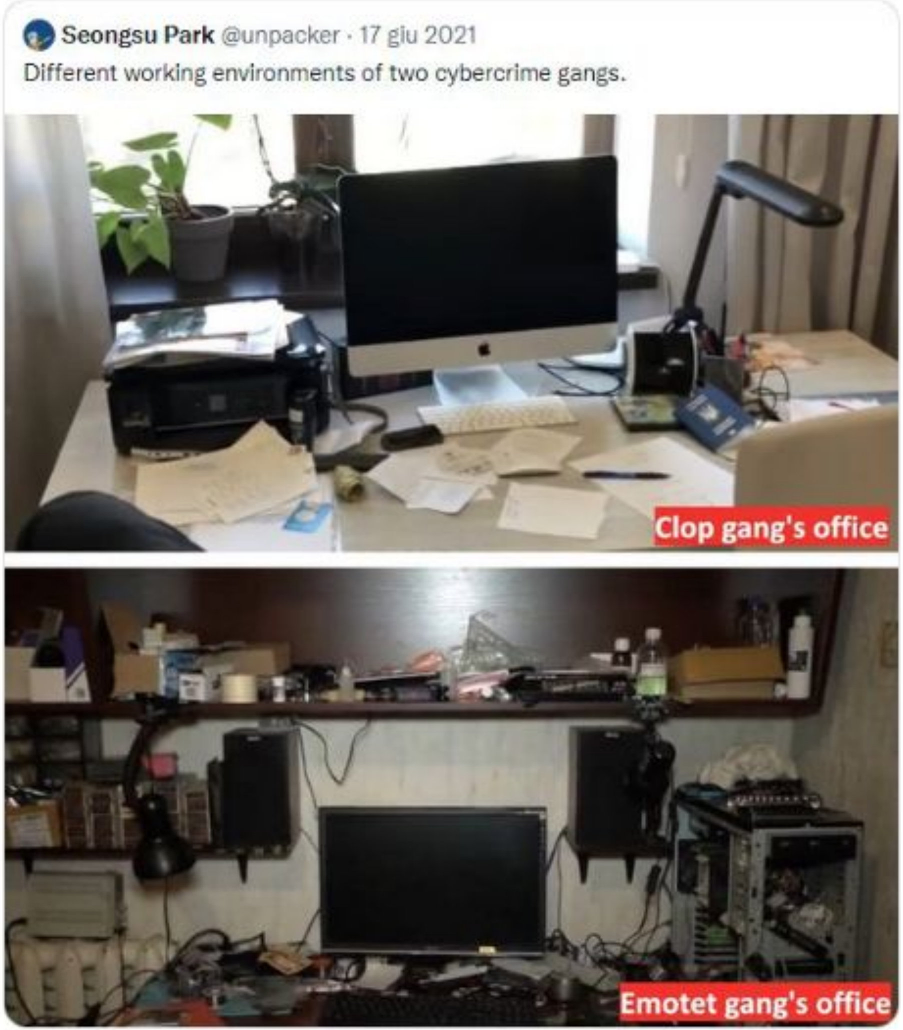


https://atlasvpn.com/blog/cybercrime-annual-revenue-is-3-times...

PAYING RANSOM



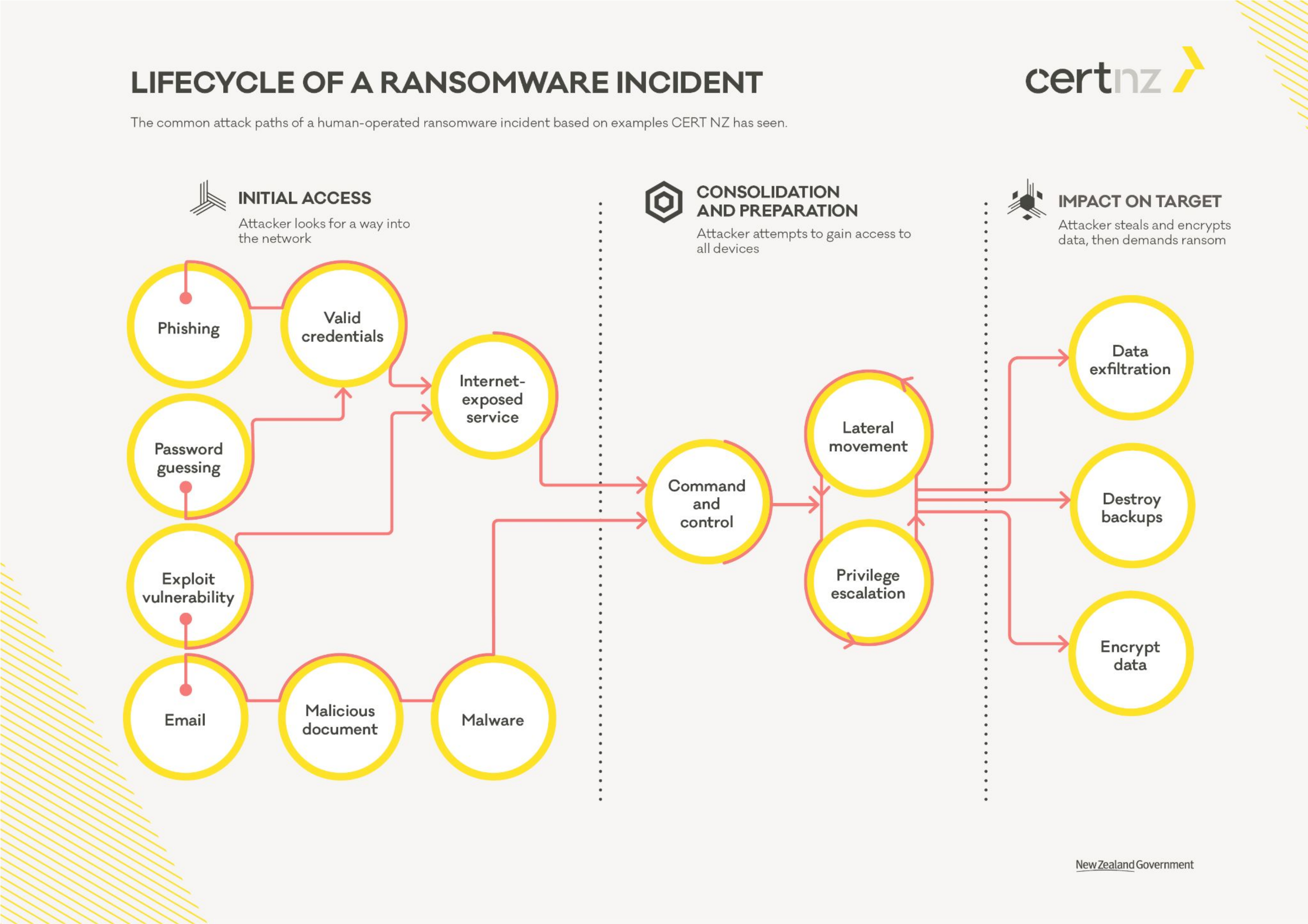
https://www.imperva.com/.../CyberEdge-2019-CDR-Report-v1.1.pdf



Seongsu Park @unpacker · 17 giu 2021

Different working environments of two cybercrime gangs.

RANSOMWARE



LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.

INITIAL ACCESS

Attacker looks for a way into the network

Phishing

Valid credentials

Password guessing

Internet-exposed service

Exploit vulnerability

Email

Malicious document

Malware

CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

Command and control

Lateral movement

Privilege escalation

IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom

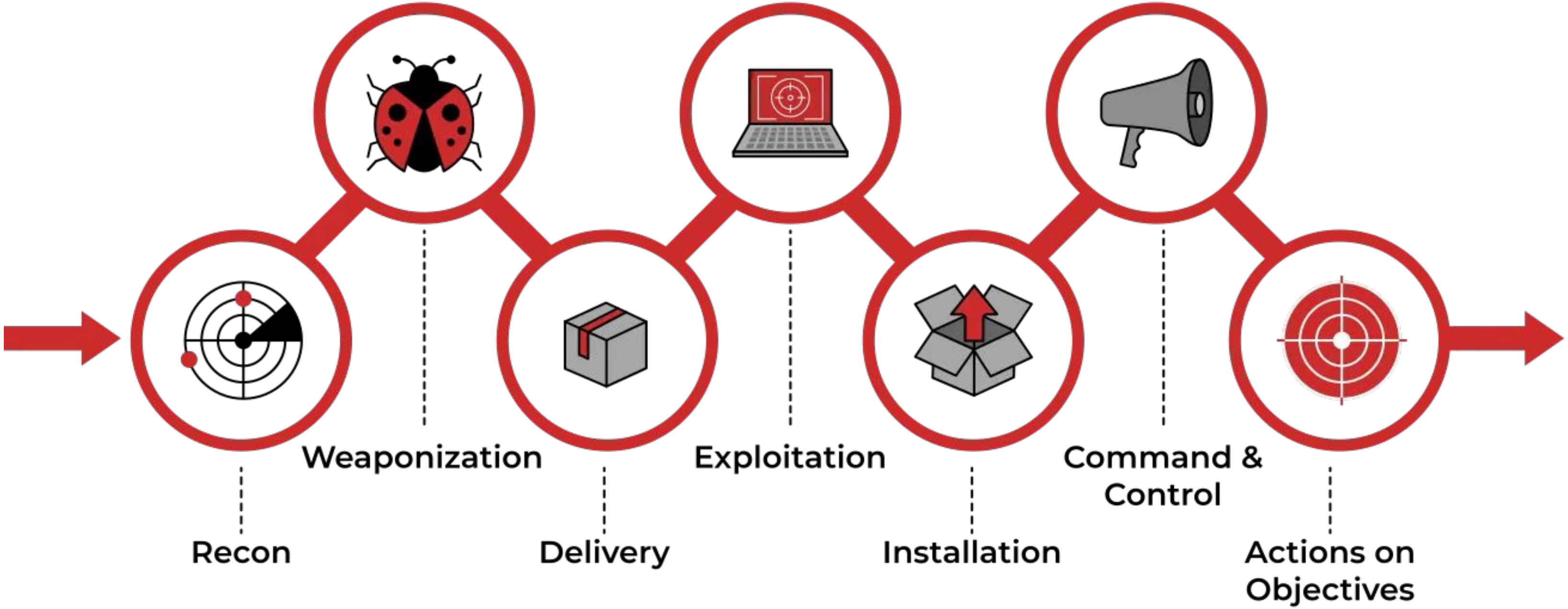
Data exfiltration

Destroy backups

Encrypt data

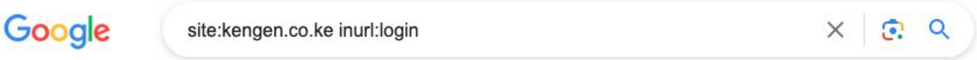
New Zealand Government

CYBER KILL CHAIN

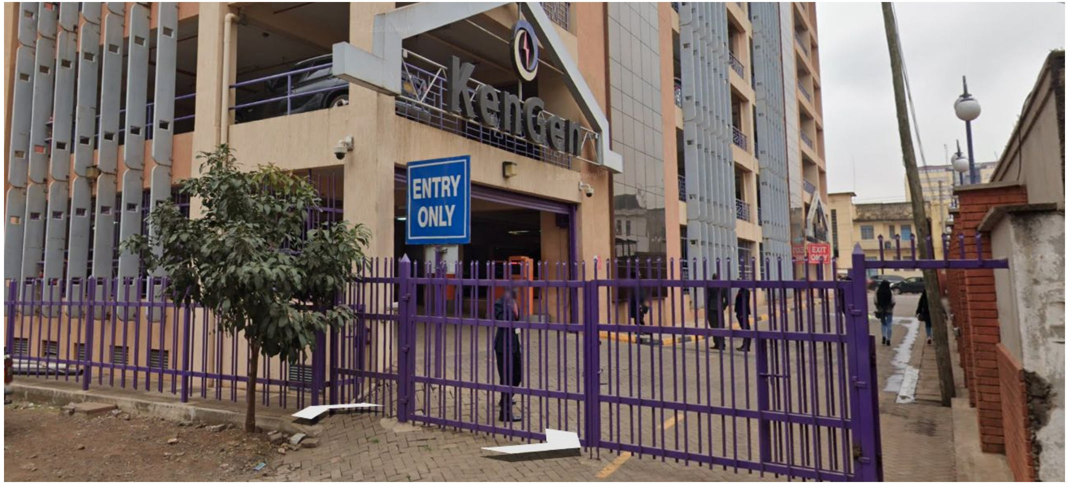


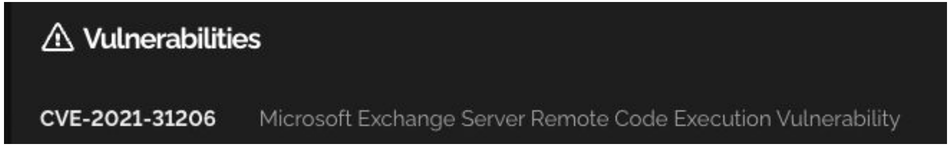
https://www.lockheedmartin.com/.../cyber/cyber-kill-chain.html

RECON PHASE

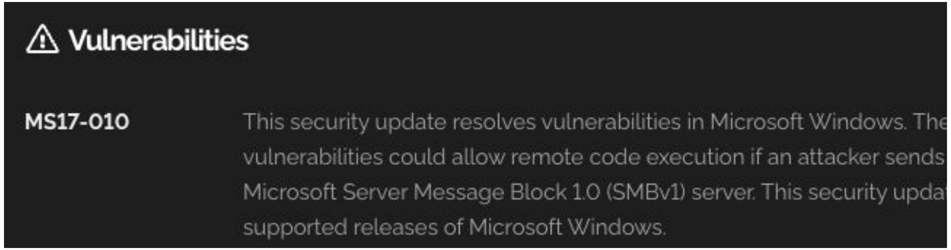

Google

site:kengen.co.ke inurl:login

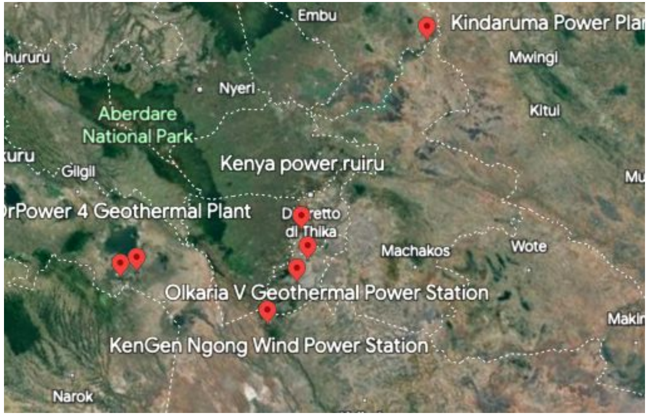



⚠ Vulnerabilities

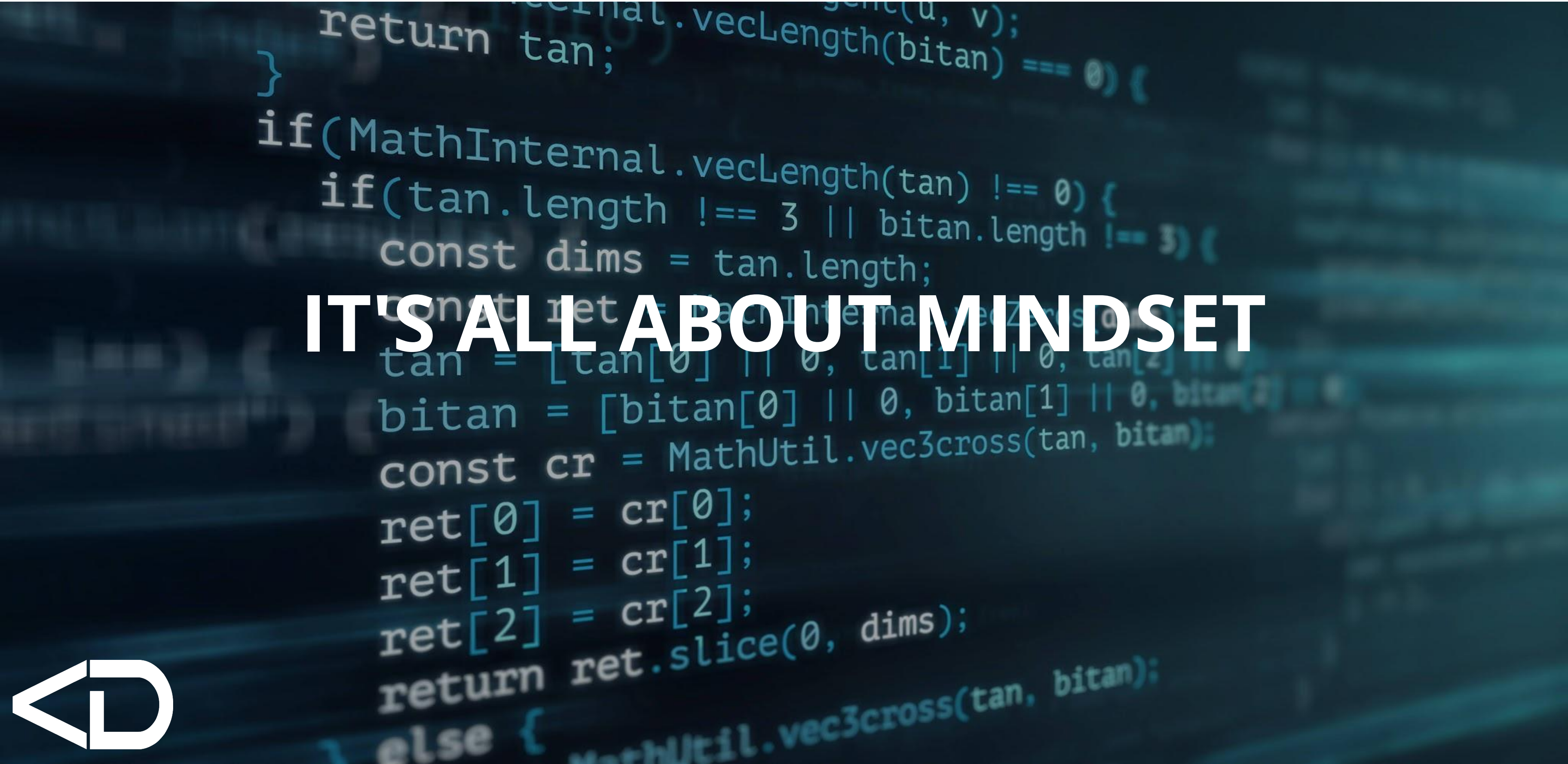
CVE-2021-31206 Microsoft Exchange Server Remote Code Execution Vulnerability


⚠ Vulnerabilities

MS17-010 This security update resolves vulnerabilities in Microsoft Windows. The
vulnerabilities could allow remote code execution if an attacker sends
Microsoft Server Message Block 1.0 (SMBv1) server. This security upda
supported releases of Microsoft Windows.

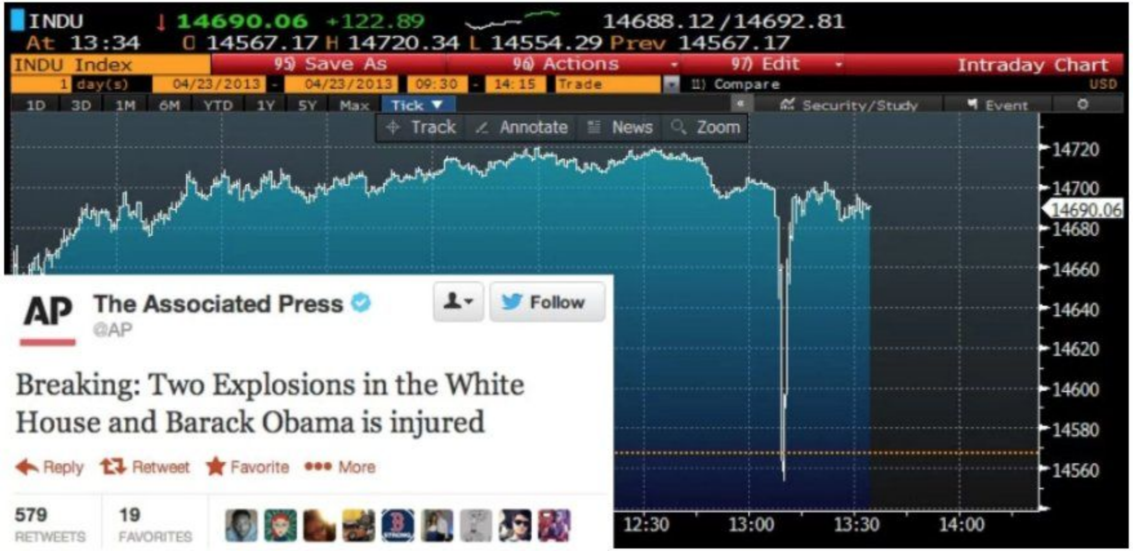


IT'S ALL ABOUT MINDSET



```
    return tan;
}
if(MathInternal.vecLength(tan) !== 0) {
    if(tan.length !== 3 || bitan.length !== 3) {
        const dims = tan.length;
        tan = [tan[0] || 0, tan[1] || 0, tan[2]
        bitan = [bitan[0] || 0, bitan[1] || 0, bitan[2
        const cr = MathUtil.vec3cross(tan, bitan);
        ret[0] = cr[0];
        ret[1] = cr[1];
        ret[2] = cr[2];
        return ret.slice(0, dims);
    } else {
```

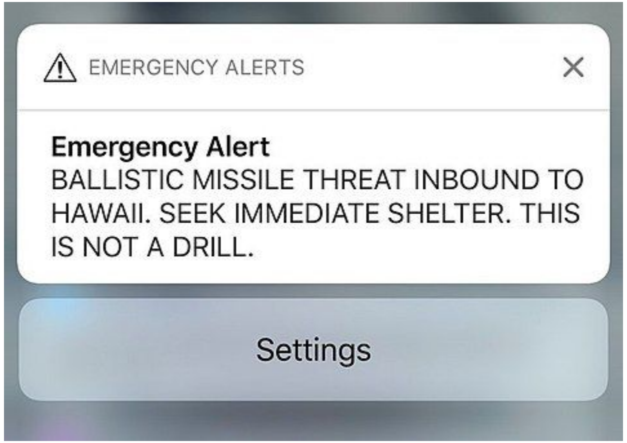
FAKE NEWS/CHAT



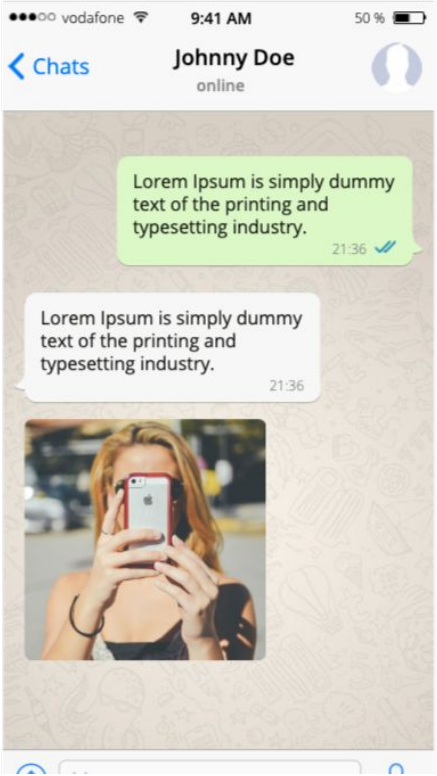
The Associated Press
@AP
Follow

Breaking: Two Explosions in the White House and Barack Obama is injured

579 RETWEETS 19 FAVORITES


EMERGENCY ALERTS

Emergency Alert
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.

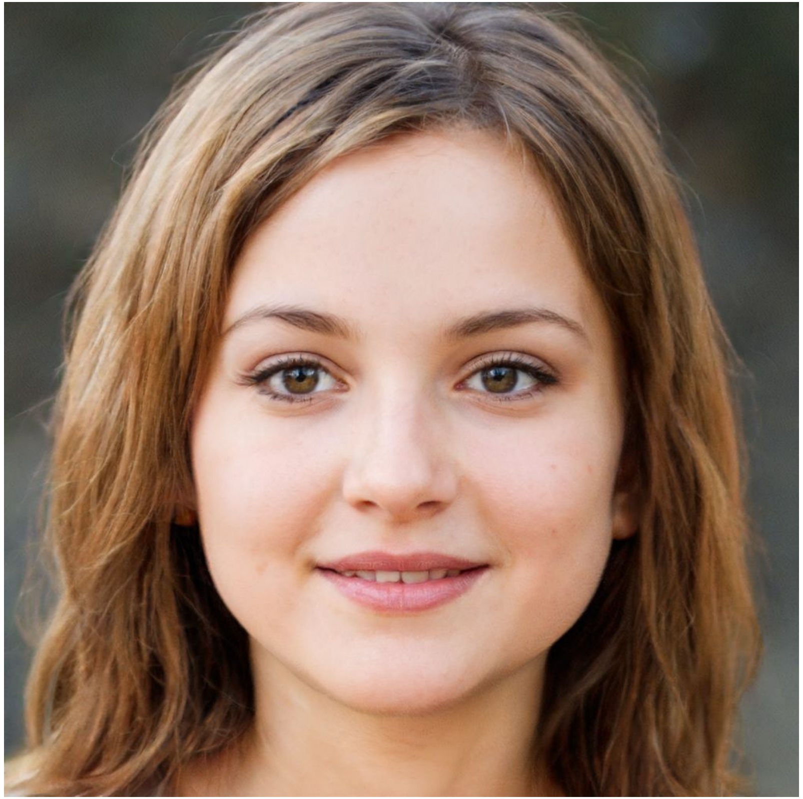


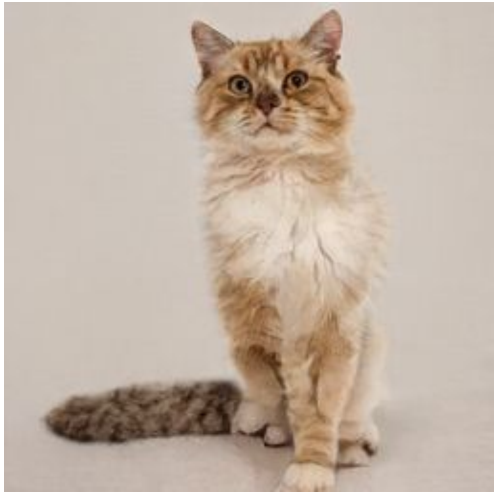
Johnny Doe
online

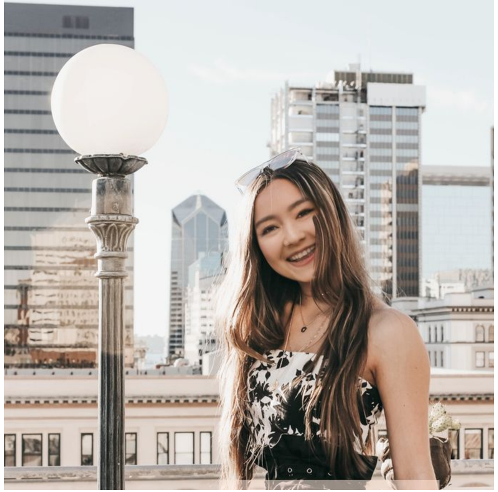
Lorem Ipsum is simply dummy text of the printing and typesetting industry. 21:36

Lorem Ipsum is simply dummy text of the printing and typesetting industry. 21:36

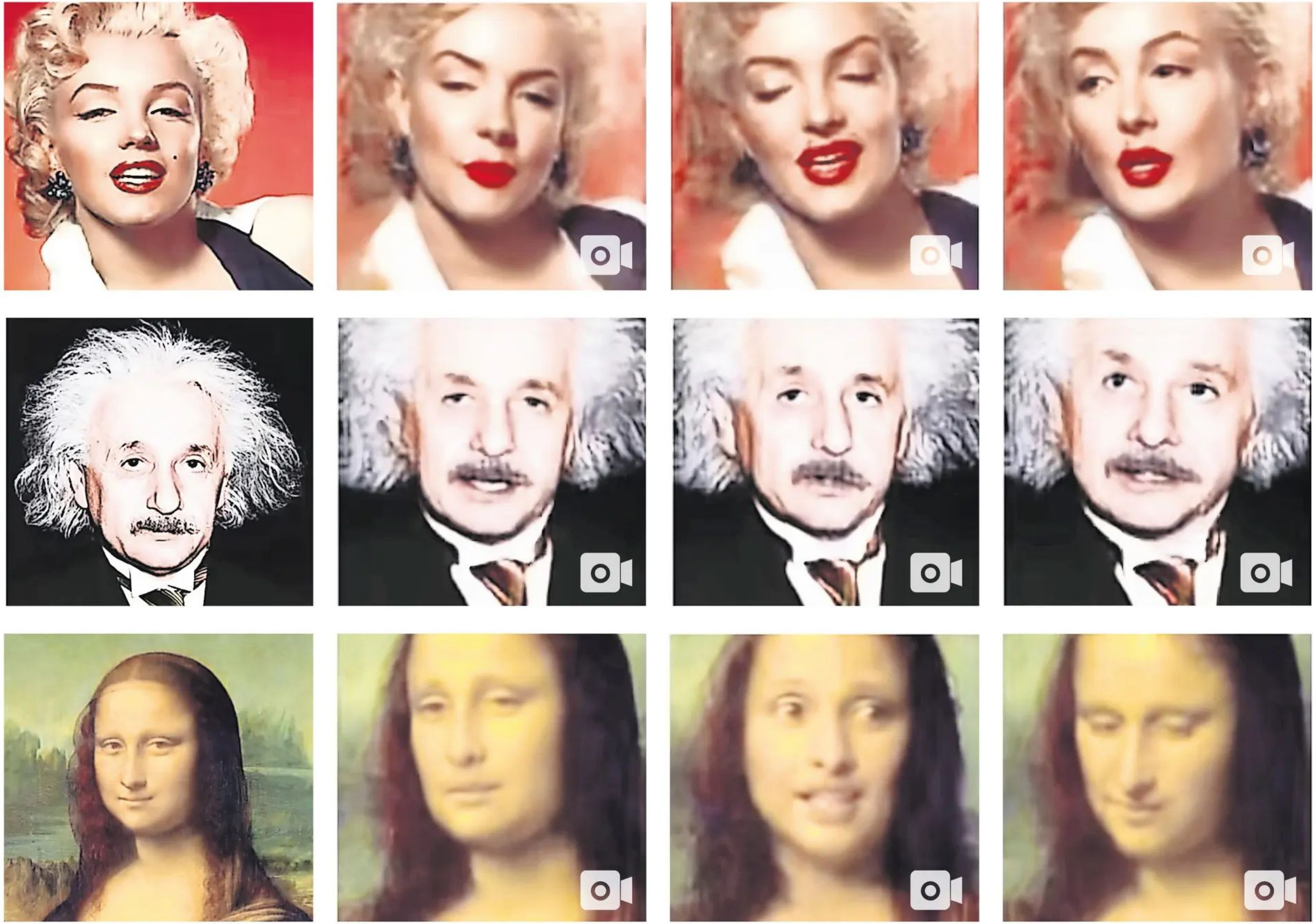
FAKE PICTURES







FAKE VIDEOS



SURVEILLANCE

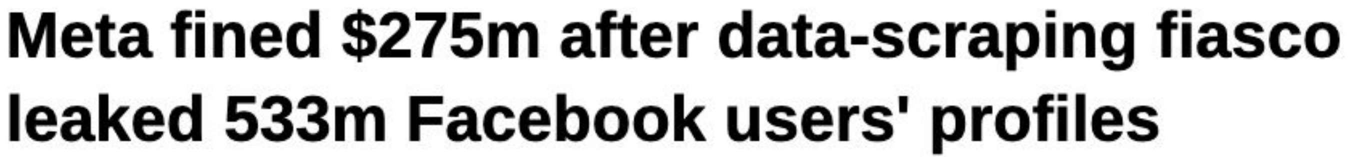
Scientists […] reported […] that they had devised a computer algorithm that can identify 99.98 percent of Americans from almost any available data set with as few as 15 attributes, such as gender, ZIP code or marital status.
https://www.nytimes.com/…/data-privacy-protection.html

How Target Knew a High School Girl Was Pregnant Before Her Parents Did
https://techland.time.com/…school-girl-was-pregnant…/

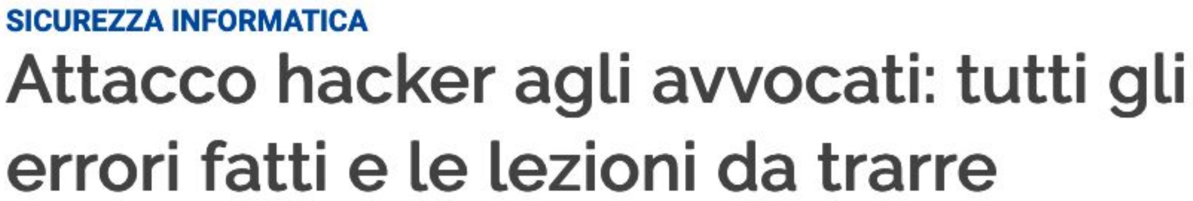
Facebook’s second most powerful executive, Sheryl Sandberg, has apologised for the conduct of secret psychological tests on nearly 700,000 users in 2012, which prompted outrage from users and experts alike.
https://www.theguardian.com/…/facebook…psychological-experiments

[…] a tool that could end your ability to walk down the street anonymously, and provided it to hundreds of law enforcement agencies, ranging from local cops in Florida to the F.B.I. and the Department of Homeland Security. […] Clearview AI, devised a groundbreaking facial recognition app. You take a picture of a person, upload it and get to see public photos of that person, along with links to where those photos appeared.
https://web.archive.org/…/technology/clearview-privacy-facial-recognition.html

DATA BREACH

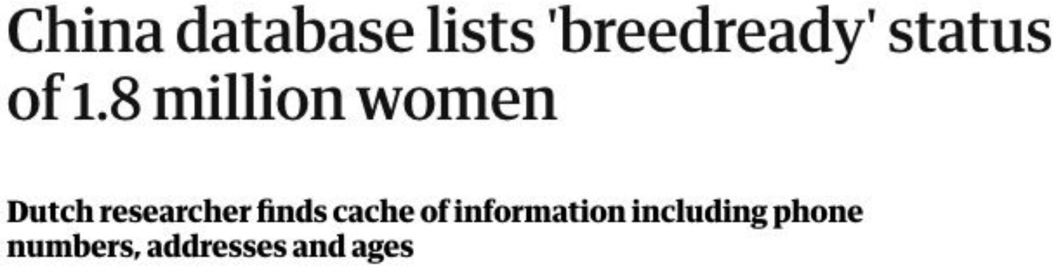


Meta fined $275m after data-scraping fiasco leaked 533m Facebook users' profiles



SICUREZZA INFORMATICA

Attacco hacker agli avvocati: tutti gli errori fatti e le lezioni da trarre



China database lists 'breedready' status of 1.8 million women

Dutch researcher finds cache of information including phone numbers, addresses and ages

MEDIA MISUSE

EZ (68 anni) -> Sergio Mattarella

“Ti hanno ammazzato il fratello cazzo... Non ti basta?”

(Non avrei dovuto. Voglio andare dal presidente e scusarmi)

MC (40 anni) -> Laura Boldrini

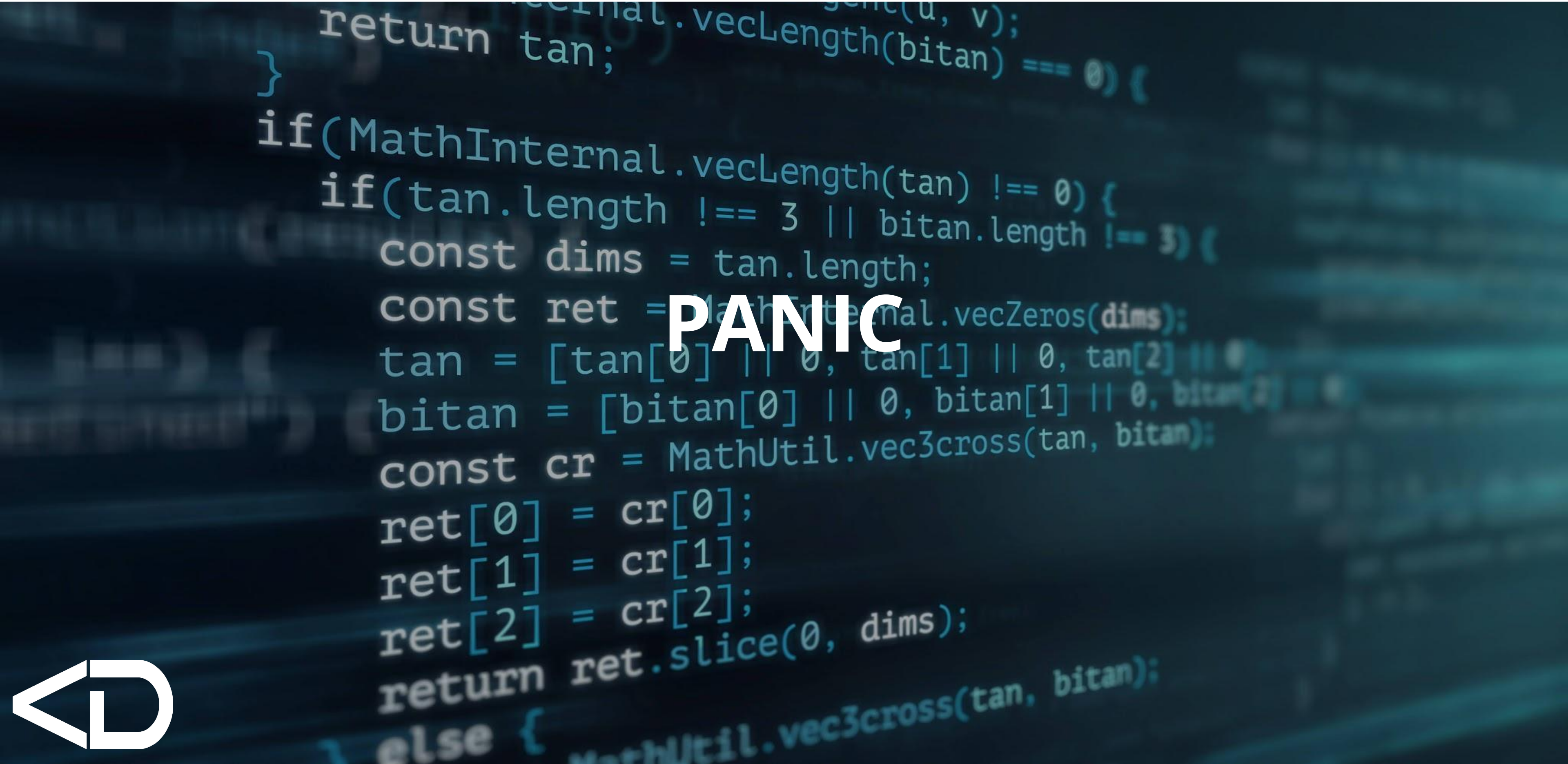
“Mi sa tanto che ha bisogno di una bella pallottola”

(Sono un uomo tranquillo, odio la violenza e i soprusi)

GF (61 anni) -> Laura Boldrini

“Boldrini sei una puttana andicappata vattene a casa fai la cosa giusta per una volta vaiii viaaa”

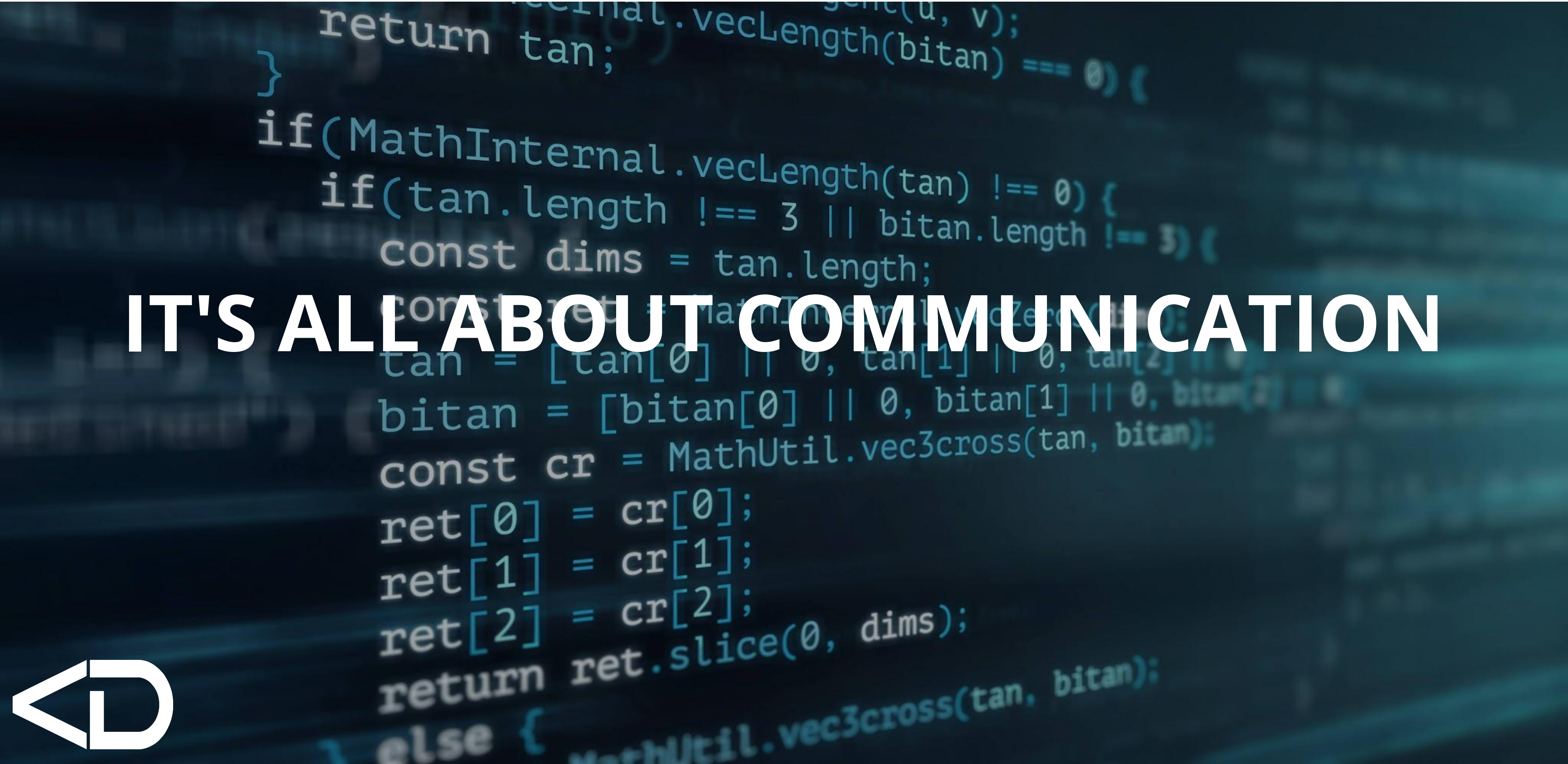
(Mi stanno facendo nera di insulti, me li merito ho fatto una cosa orrenda da sentirmi male)



PANIC

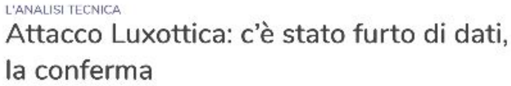
CRISIS

IT'S ALL ABOUT COMMUNICATION



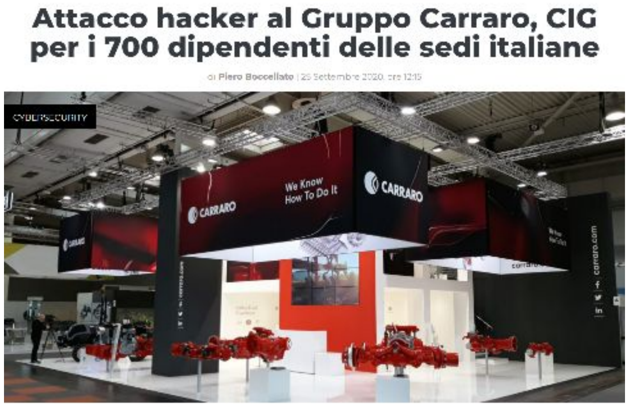
```
        ...ernal.vecLength(bitan) === 0) {
    return tan;
}
if(MathInternal.vecLength(tan) !== 0) {
    if(tan.length !== 3 || bitan.length !== 3) {
        const dims = tan.length;
        const ret = MathInternal.vecZero(dims);
        tan = [tan[0] || 0, tan[1] || 0, tan[2] || 0];
        bitan = [bitan[0] || 0, bitan[1] || 0, bitan[2] || 0];
        const cr = MathUtil.vec3cross(tan, bitan);
        ret[0] = cr[0];
        ret[1] = cr[1];
        ret[2] = cr[2];
        return ret.slice(0, dims);
    } else {
        ... MathUtil.vec3cross(tan, bitan);
```

FEAR



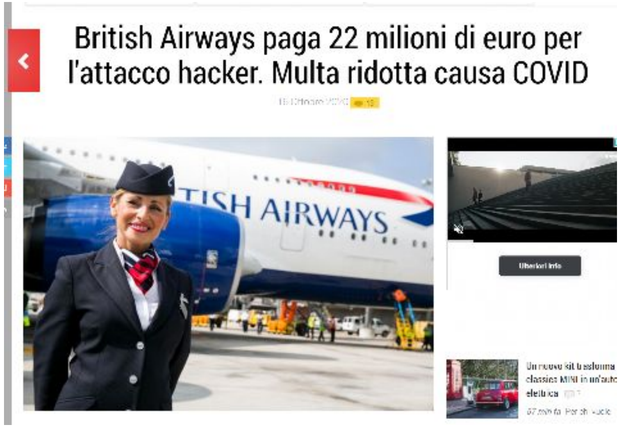
L'ANALISI TECNICA

Attacco Luxottica: c'è stato furto di dati, la conferma



Attacco hacker al Gruppo Carraro, CIG per i 700 dipendenti delle sedi italiane

di Piero Boccellato | 25 Settembre 2020, ore 12:15

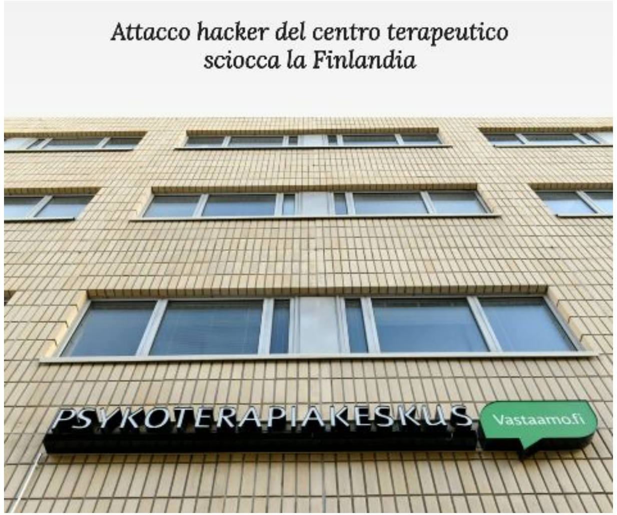


British Airways paga 22 milioni di euro per l'attacco hacker. Multa ridotta causa COVID

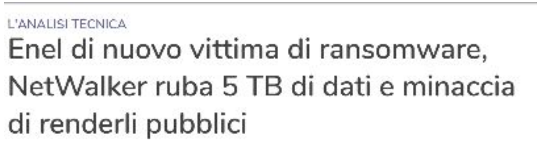
16 Ottobre 2020 👁 13

Un nuovo kit trasforma classica MINI in un'auto elettrica

57 min fa Perch Auto

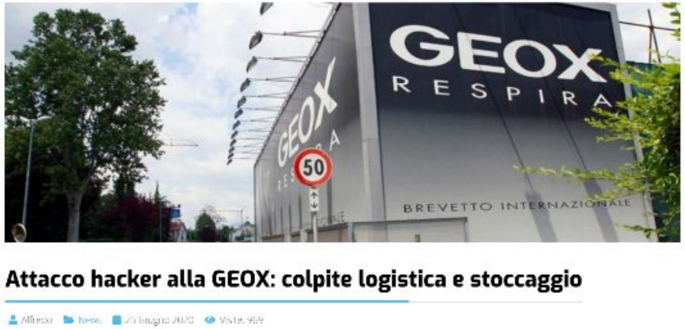


Attacco hacker del centro terapeutico sciocca la Finlandia



L'ANALISI TECNICA

Enel di nuovo vittima di ransomware, NetWalker ruba 5 TB di dati e minaccia di renderli pubblici



Attacco hacker alla GEOX: colpite logistica e stoccaggio

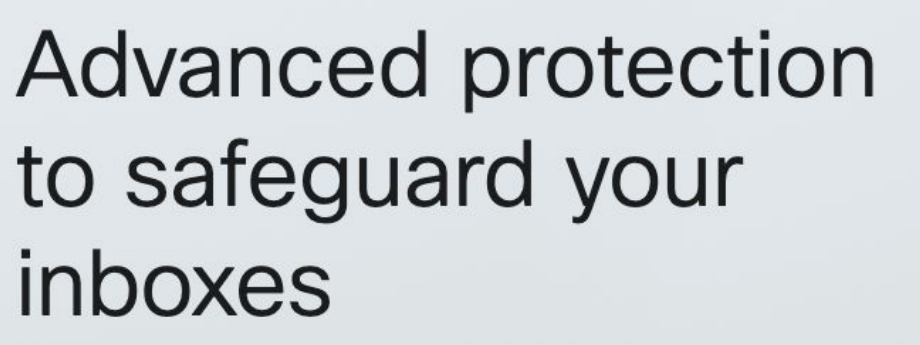
Alfredo News 25 Giugno 2020 Viste: 959

AWARENESS

Security Awareness Training That Works!

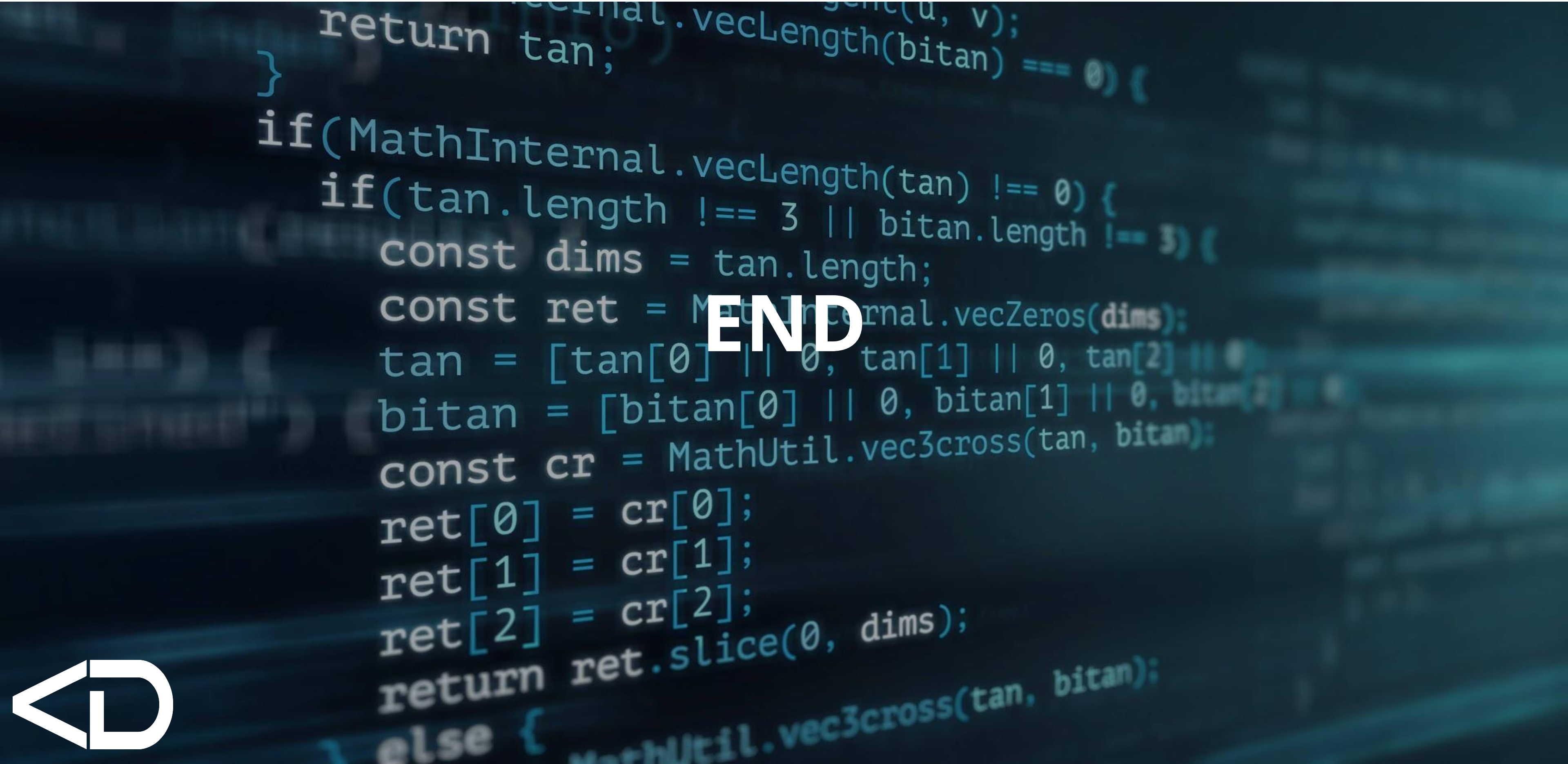
Break the attack chain

Protect your people from advanced email attacks and identity-based threats. Defend sensitive data from theft, loss and insider threats.



Advanced protection to safeguard your inboxes

ETHIC or THE DARK WAY?



END