MegaTec 2025

APPLICA
Tech Knowledge Transfer

CCC CA

VULNERABILIDADES SOCIALES EN CIBERSEGURIDAD

Paula Brenes Ramírez
Fundación YOD

YOD FOUNDATION


YANKEE

MEGATEC 2025

“Gasolina y Datos:
Lo Que Tu Red No Debería Estar Quemando”

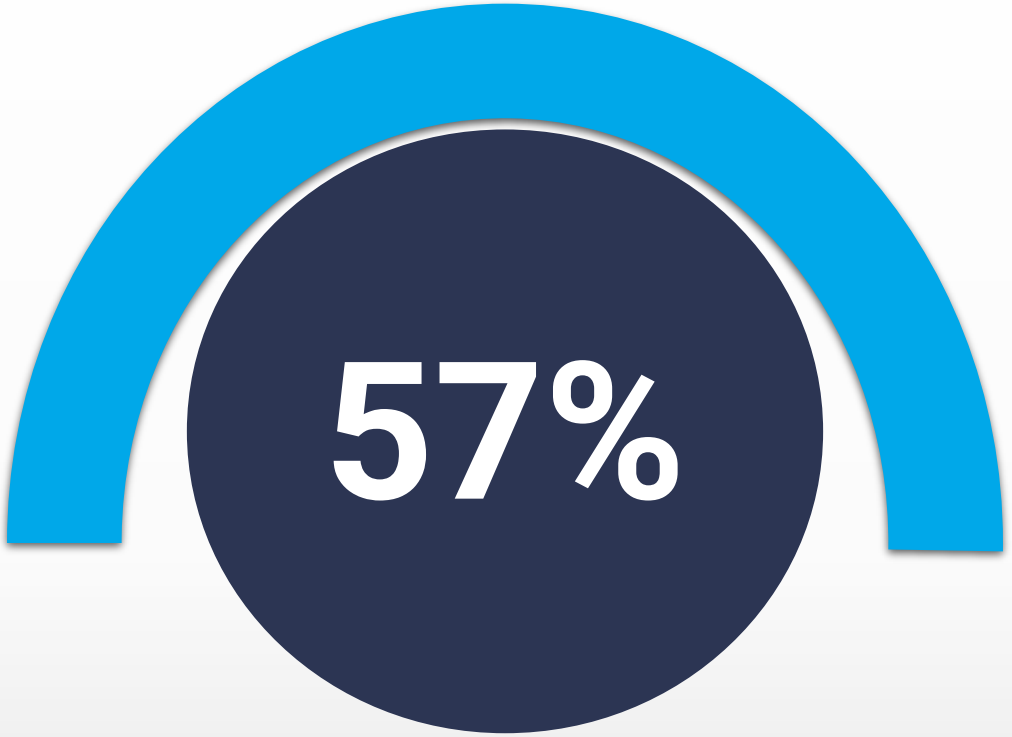
"Equifax failed to patch its network after being alerted in March 2017 to a critical security vulnerability affecting its ACIS database, which handles inquiries from consumers about their personal credit data," the FTC alleges.

"Even though Equifax's security team ordered that each of the company's vulnerable systems should be patched within 48 hours after receiving the alert, Equifax did not follow up to ensure the order was carried out by the responsible employees."

- El ataque se originó por una vulnerabilidad conocida (Apache) que no fue parchada, a pesar de que existía una actualización disponible.
- Equifax acordó pagar multas de al menos 575 millones de dólares

YOD FOUNDATION

APPLICA TECH KNOWLEDGE TRANSFER CCC CA



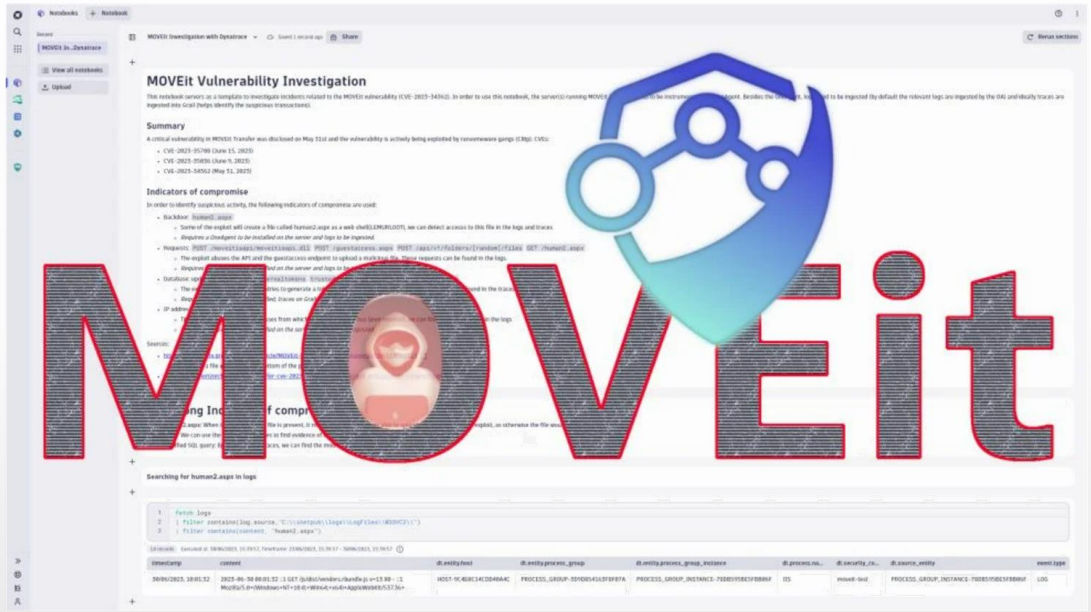
de las brechas en 2025 involucraron explotación de vulnerabilidades conocidas y no parchadas.


Colección de Oro
Sergio Vargas
15 Exitos
Sergio Vargas
La Ventanita - Penas al Viento - Por Ella
Dudas - y mucho más

“La Ventanita”

2023 Mega Hack: The MOVEit Data Breach Continues

Oct 2, 2023 | Cyber Attack, Cyber Security



2023 has witnessed a relentless wave of interconnected Cyber attacks, causing consequences like a data breach, that has left countless victims in their wake.

- MOVEit Transfer es justamente una aplicación web expuesta públicamente.
- El ataque explotó una debilidad en la validación de entrada web, que es una causa clásica de brechas vía web.

Las vulnerabilidades en aplicaciones web representaron el 40% de las brechas iniciales

“Oye cómo va...”


BBC

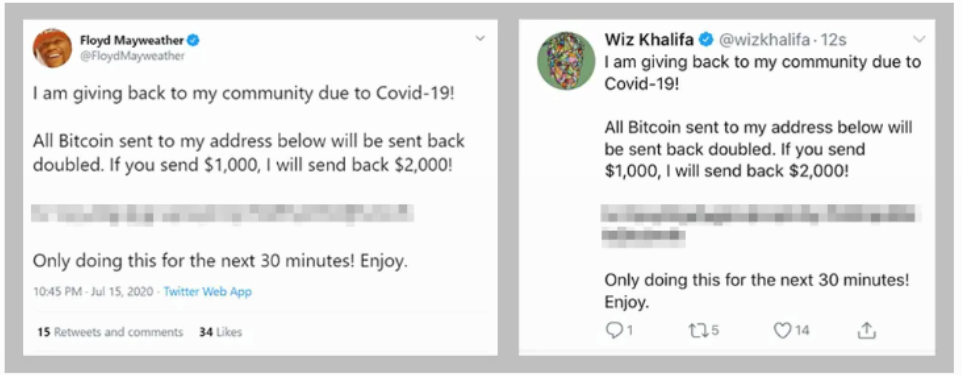
Home News Sport Business Innovation Culture Travel Earth Video Live

Briton pleads guilty in US to 2020 Twitter hack

9 May 2023

Share

Joe Tidy & Antoinette Radford
BBC News


Floyd Mayweather
@FloydMayweather

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

[redacted]

Only doing this for the next 30 minutes! Enjoy.

10:45 PM · Jul 15, 2020 · Twitter Web App

15 Retweets and comments 34 Likes

Wiz Khalifa @wizkhalifa · 12s

I am giving back to my community due to Covid-19!

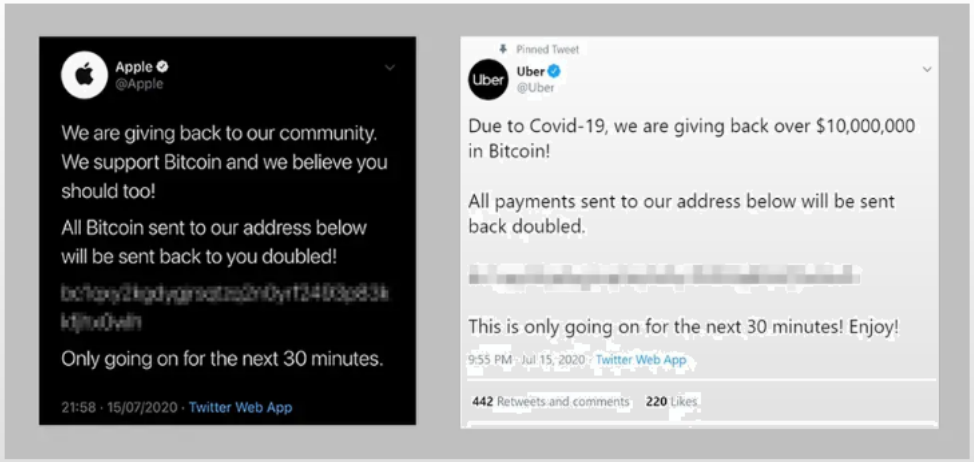
All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

[redacted]

Only doing this for the next 30 minutes! Enjoy.

1 5 14

Celebridades como el boxeador estadounidense Floyd Mayweather y el cantante Wiz Khalifa también perdieron el control de sus cuentas.


Apple
@Apple

We are giving back to our community. We support Bitcoin and we believe you should too!

All Bitcoin sent to our address below will be sent back to you doubled!

[redacted]

Only going on for the next 30 minutes.

21:58 · 15/07/2020 · Twitter Web App

Pinned Tweet

Uber
@Uber

Due to Covid-19, we are giving back over $10,000,000 in Bitcoin!

All payments sent to our address below will be sent back doubled.

[redacted]

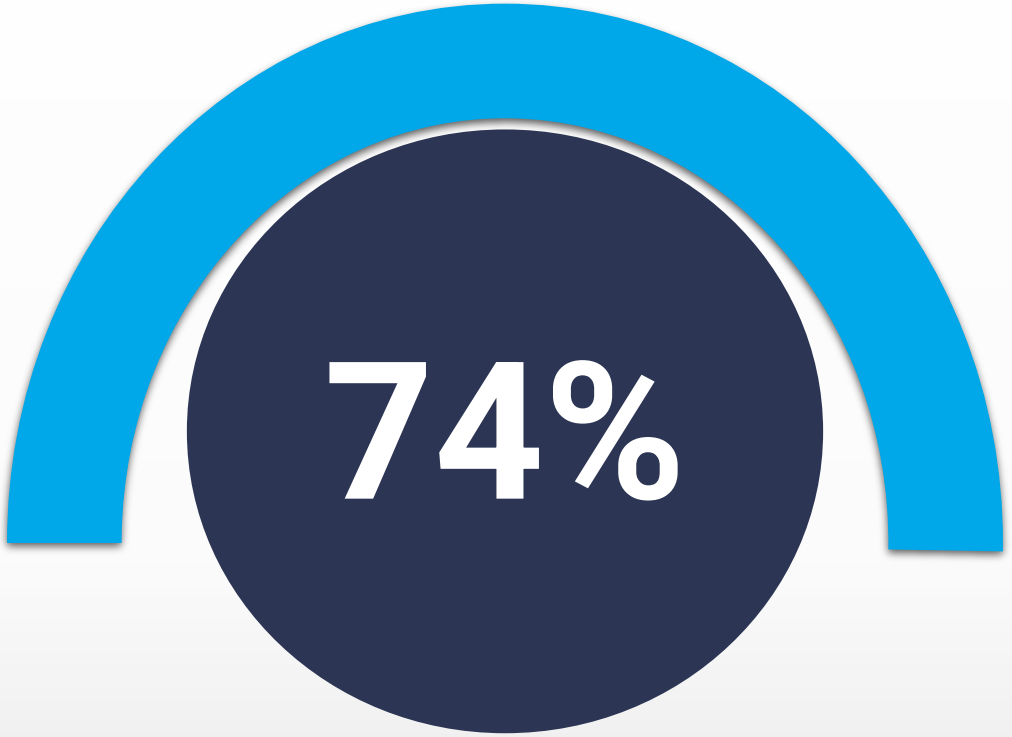
This is only going on for the next 30 minutes! Enjoy!

9:55 PM · Jul 15, 2020 · Twitter Web App

442 Retweets and comments 220 Likes

Technology companies Apple and Uber have more than 5.5 million Twitter followers between them

MegaTec 2025



de las brechas exitosas en 2025 comenzaron con un ataque de ingeniería social

YOD FOUNDATION

Applica Tech Knowledge Transfer

CCC CA


nuevo milenio ~el mismo sabor
EL GRAN COMBO
DE PUERTO RICO

Me liberé (de los riesgos ocultos)

MegaTec 2025

NBC NEWS

Target Settles 2013 Hacked Customer Data Breach For $18.5 Million

SHARE & SAVE –

BUSINESS NEWS

Target Settles 2013 Hacked Customer Data Breach For $18.5 Million

The most customers ever hacked has ended in Target paying the biggest ever data breach settlement.

Judge rules that banks can sue Target for 2013 credit card hack

The development paves the way for more banks to sue merchants with poor POS security.

by Megan Geuss - Dec 5 2014, 3:30am CET

Share Tweet

YOD FOUNDATION

APPLICA Tech Knowledge Transfer

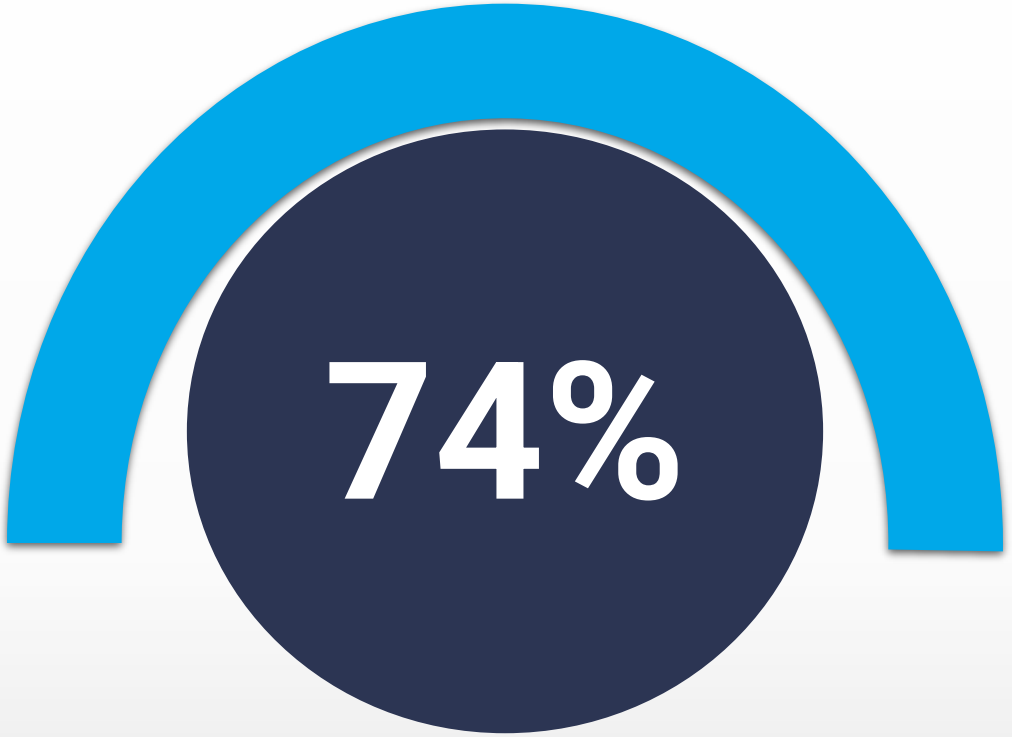
CCC CA

de las brechas de datos involucraron a terceros o proveedores externos

Y Nos Dieron las 10 (y el ataque también)

The company's CEO authorized the payment as a means to restart the pipeline's systems quickly and safely

A cyberattack forced the shutdown of 5,500 miles of Colonial Pipeline's sprawling interstate system. Photograph: Jim Lo Scalzo/EPA



de ataques exitosos ocurren en fines de semana o noches

La Incondicional SNOWFLARE
filtración masiva de datos empresariales

MEGATEC 2025

CNBC MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVESTING CLUB PRO LIVESTREAM

CYBER REPORT

AT&T's massive data breach deepens crisis for Snowflake seven weeks after hack was disclosed

PUBLISHED FRI, JUL 12 2024•6:11 PM EDT | UPDATED MON, JUL 15 2024•9:55 AM EDT

Jordan Novet
@JORDANNOVET

SHARE

KEY POINTS

- Snowflake has a growing problem on its hands after AT&T said on Friday that data from "nearly all" wireless customers was connected to a breach.
- Prior to Friday, the most notable companies tied to the Snowflake attack were Advance Auto Parts, LendingTree, Ticketmaster operator Live Nation Entertainment and Santander Bank.
- Snowflake disclosed the cyberattack in late May and has enlisted the help of CrowdStrike and Alphabet's Mandiant to investigate.

In this article

SNOW UNCH T +0.01 (+0.04%)

Follow your favorite stocks
CREATE FREE ACCOUNT

RELATED

23andMe bankru
With America's D
on sale, market p
gets a new twist

'Tokenization' of
bond market cor
says BlackRock's
Fink, if we solve
problem

CYBERSCOOP Topics Special Reports Events Podcasts Videos Insights

remains active

The hacker has extorted $2.7 million as part of the attacks on Snowflake customers, according to a researcher tracking the case.

BY AJ VICENS • SEPTEMBER 21, 2024

Listen to this article 3:07 Learn more.

(Flickr / Blogtrepreneur)

SHARE

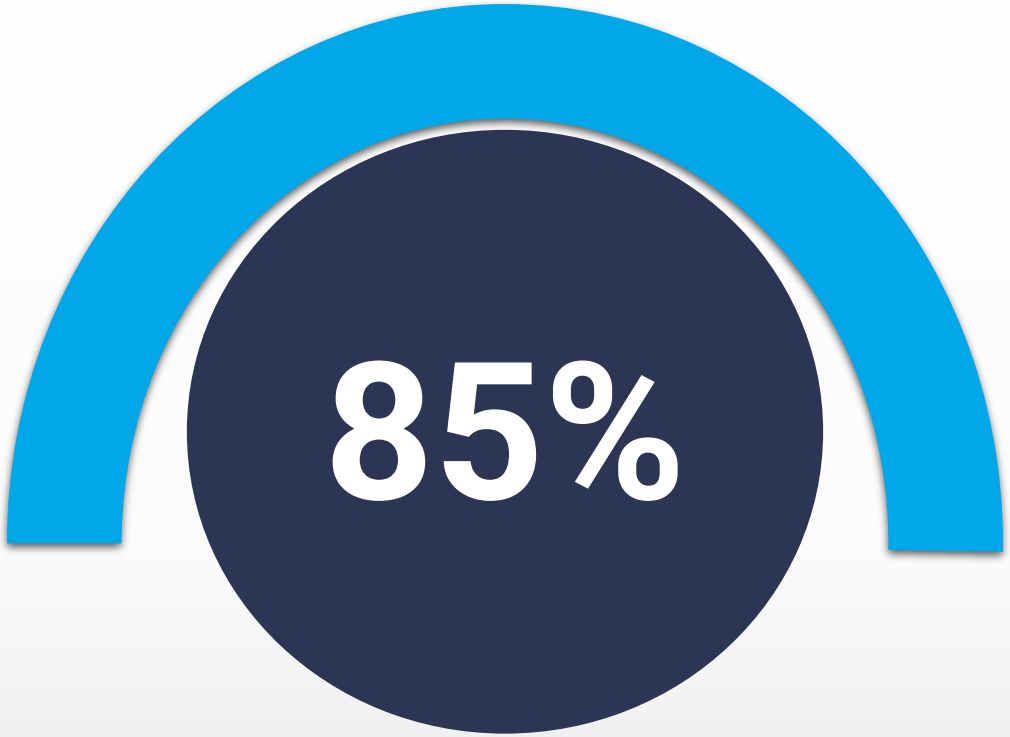
SCOTTSDALE, Ariz. — The hacker behind the bulk of the Snowflake customer data theft earlier this year remains active as of this week, a researcher tracking the suspect said Friday.

The hacker — known primarily "Judische," but who also used other names online, including "Waifu" — continues to target software-as-a-service providers and other

YOD FOUNDATION

APPLICA TECH KNOWLEDGE TRANSFER

CCC CA



de las brechas en 2025 involucraron el abuso o mal manejo de accesos privilegiados

RSA Security
(entrada lenta por phishing sigiloso)

This was published 14 years ago

Hacked security firm leaves Aussies vulnerable

Ben Grubb

Updated March 21, 2011 — 10.48am, first published at 2.02am

Save Share

- Hundreds to be briefed on hacked security firm's technology

Hundreds of thousands of cryptographic tokens used by Australians who bank online, the Defence Force and other large corporations are vulnerable to a potential hack attack after a supplier revealed secret data it held had been stolen.

Customers of RSA, a security division of the data storage giant EMC, were on Friday told that the company had been the victim of "an extremely sophisticated cyber attack".

Federal government customers of RSA's affected SecurID service include the Department of Defence, Department of the Prime Minister and Cabinet, Australian Electoral Commission, Family Court of Australia, Department of Parliamentary Services, Department of Veterans' Affairs, Geoscience Australia, AusAid, Department of the Treasury and Crimtrac, according to closed tender documents listed on the AusTender website.

News > Privacy

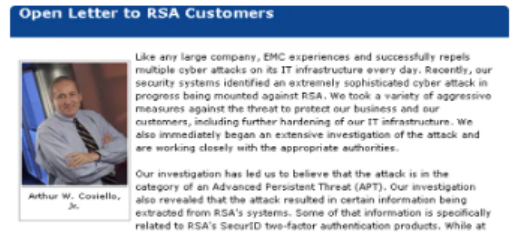
RSA: Cyberattack could put customers at risk

The company warns in open letter that information stolen in attack could be used to compromise SecurID authentication implementations.

Elinor Mills

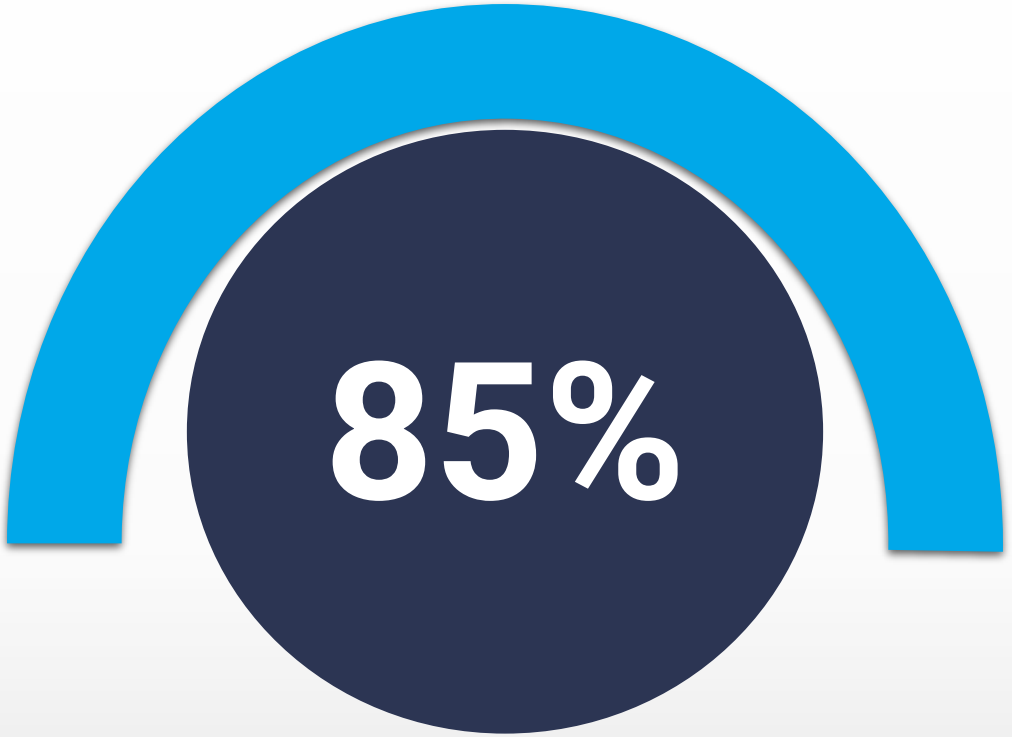
March 17, 2011 4:09 p.m. PT

Information about RSA's SecurID authentication tokens used by millions of people, including government and bank employees, was stolen during an "extremely sophisticated cyberattack," putting customers relying on them to secure their



RSA Executive Chairman Art Coviello warns customers about a security breach that affects its SecurID authentication technology.

RSA



de las brechas de datos involucraron un elemento humano

“El Anillo pa' Cuándo...?”

MegaTec 2025

Uber responding to ‘cybersecurity incident’ after hack

Ride-hailing company confirms attack after hacker compromises Slack app and messages employees

A hacker compromised the workplace messaging app Slack, then used it to send a message to Uber employees announcing it had suffered a data breach. Photograph: Mike Blake/Reuters

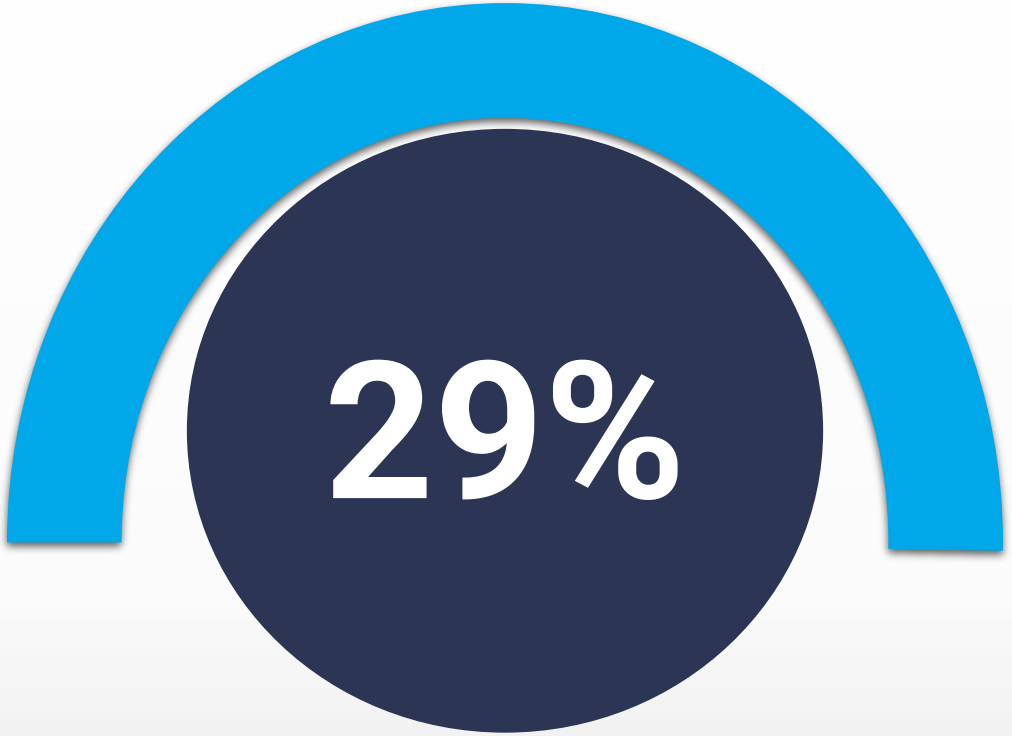
Uber has been hacked in an attack that appears to have breached the ride-hailing company’s internal systems.

> We are currently responding to a cybersecurity incident. We are in touch with law enforcement and will post additional updates here as they become available.
>
> — Uber Comms (@Uber_Comms) September 16, 2022

YOD FOUNDATION

APPLICA Tech Knowledge Transfer

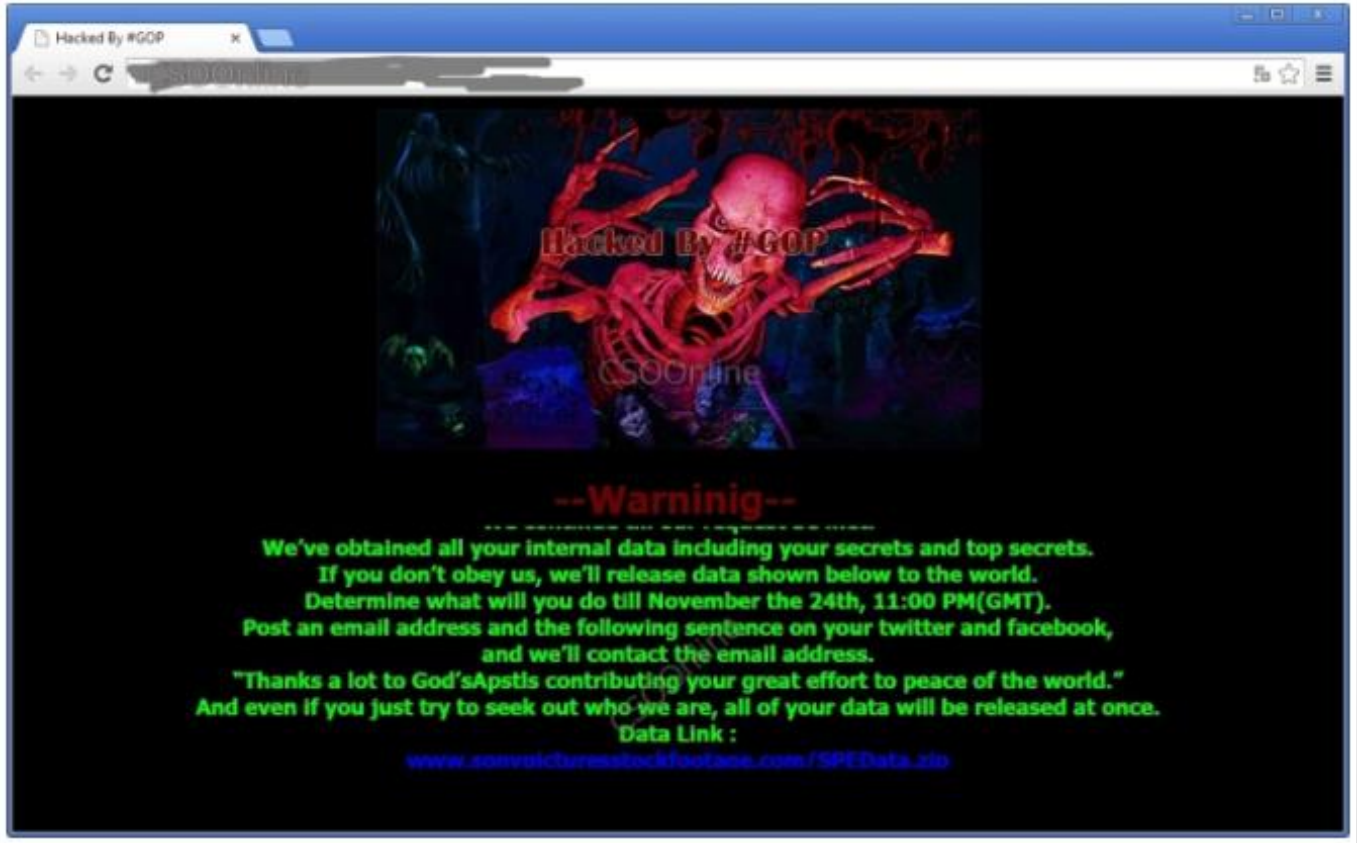
CCC CA



Uso de las brechas en 2025 involucraron ataques exitosos contra mecanismos débiles o mal implementados de autenticación

“Te Aviso, Te Anuncio”

Advertencias ignoradas y consecuencias devastadoras — el arte de no escuchar a tiempo



de las organizaciones víctimas de un ataque grave habían recibido advertencias o señales de alerta que no fueron atendidas.

“Felices los 4 (pero el quinto era un atacante interno)”

Dear Customer,

We recently became aware of unauthorized access to certain of our information technology systems hosted by a third party cloud provider. We have no indication that there has been unauthorized activity with respect to any user's account.

We are not currently aware of evidence of access to any databases that host user data, but we cannot be certain that user data has not been exposed. This data may include your name, email address, and the one-way encrypted password to your account (in technical terms, the passwords are hashed and salted). The data may also include your address and phone number if you have provided that to us.

As a precaution, we encourage you to change your password. We recommend that you also change your password on any website where you use the same user ID or password. Finally, we recommend that you enable two-factor authentication on your Ubiquiti accounts if you have not already done so.

Change Password Enable Two-Factor Authentication

We apologize for, and deeply regret, any inconvenience this may cause you. We take the security of your information very seriously and appreciate your continued trust.

Thank you,
Ubiquiti Team

KnowBe4 Product + Pricing Free Tools Resources Partners Abo

7 Aug

Tech Firm Ubiquiti Suffers $46M Cyberheist

Stu Sjouwerman

Tweet Share Share 0

Brian Krebs just reported on a massive $46M Cyberheist.

Networking firm **Ubiquiti Networks Inc.** disclosed this week that cyber thieves recently stole $46.7 million using an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers.

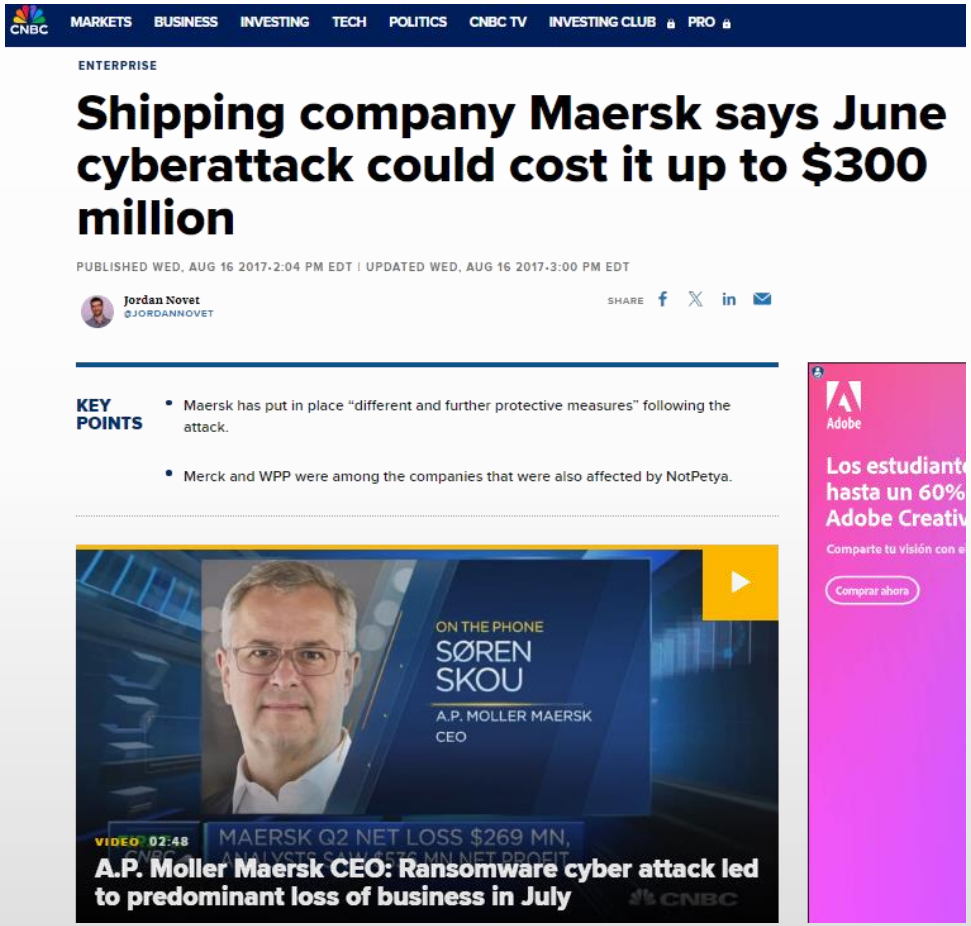
Ubiquity, a San Jose based maker of networking technology for service providers and enterprises, disclosed the attack in a quarterly financial report filed this week with the **U.S. Securities and Exchange Commission (SEC)**. The company said it discovered the fraud on June 5, 2015, and that the incident involved employee impersonation and fraudulent requests from an outside entity targeting the company's finance department.

“This fraud resulted in transfers of funds aggregating $46.7 million held by a Company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties,” Ubiquity wrote. “As soon as the Company became aware of this fraudulent activity it initiated contact with its Hong Kong subsidiary's bank and promptly initiated legal proceedings in various foreign jurisdictions. As a result of these efforts, the Company has recovered $8.1 million of the amounts transferred.”

Known variously as “CEO fraud,” and the “business email compromise,” the swindle that hit Ubiquiti is a sophisticated and increasingly common one targeting businesses working with foreign suppliers and/or businesses

de los incidentes de ciberseguridad involucran amenazas internas (insiders)

“Vivir Mi Vida…”



CNBC MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INVESTING CLUB PRO

ENTERPRISE

Shipping company Maersk says June cyberattack could cost it up to $300 million

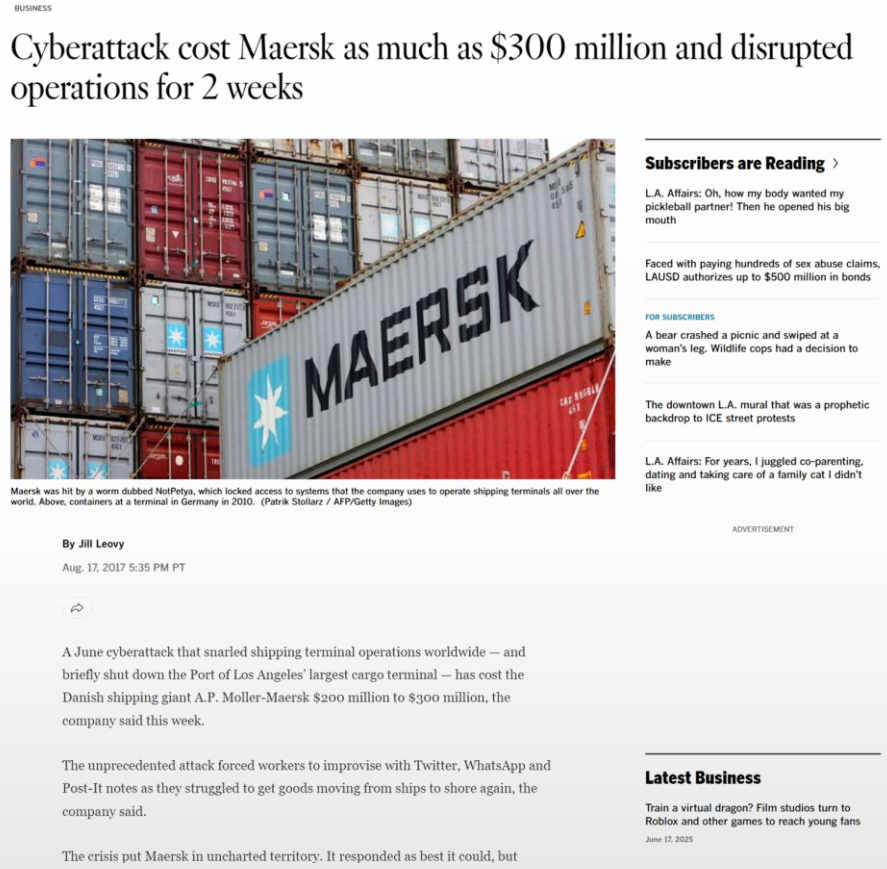
PUBLISHED WED, AUG 16 2017•2:04 PM EDT | UPDATED WED, AUG 16 2017•3:00 PM EDT

Jordan Novet
@JORDANNOVET

SHARE

KEY POINTS

- Maersk has put in place “different and further protective measures” following the attack.
- Merck and WPP were among the companies that were also affected by NotPetya.



BUSINESS

Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks

Maersk was hit by a worm dubbed NotPetya, which locked access to systems that the company uses to operate shipping terminals all over the world. Above, containers at a terminal in Germany in 2010. (Patrik Stollarz / AFP/Getty Images)

By Jill Leovy
Aug. 17, 2017 5:35 PM PT

A June cyberattack that snarled shipping terminal operations worldwide — and briefly shut down the Port of Los Angeles' largest cargo terminal — has cost the Danish shipping giant A.P. Moller-Maersk $200 million to $300 million, the company said this week.

The unprecedented attack forced workers to improvise with Twitter, WhatsApp and Post-It notes as they struggled to get goods moving from ships to shore again, the company said.

The crisis put Maersk in uncharted territory. It responded as best it could, but

Subscribers are Reading ›

L.A. Affairs: Oh, how my body wanted my pickleball partner! Then he opened his big mouth

Faced with paying hundreds of sex abuse claims, LAUSD authorizes up to $500 million in bonds

FOR SUBSCRIBERS
A bear crashed a picnic and swiped at a woman's leg. Wildlife cops had a decision to make

The downtown L.A. mural that was a prophetic backdrop to ICE street protests

L.A. Affairs: For years, I juggled co-parenting, dating and taking care of a family cat I didn't like

ADVERTISEMENT

Latest Business

Train a virtual dragon? Film studios turn to Roblox and other games to reach young fans
June 17, 2025

NotPetya se infiltró en la red interna de Maersk, borrando 45,000 PCs y 4,000 servidores en cuestión de horas.

96 ataques de ransomware fueron registrados en solo una semana a inicios de 2025, un incremento del 104%


RUBÉN BLADES UNA DÉCADA

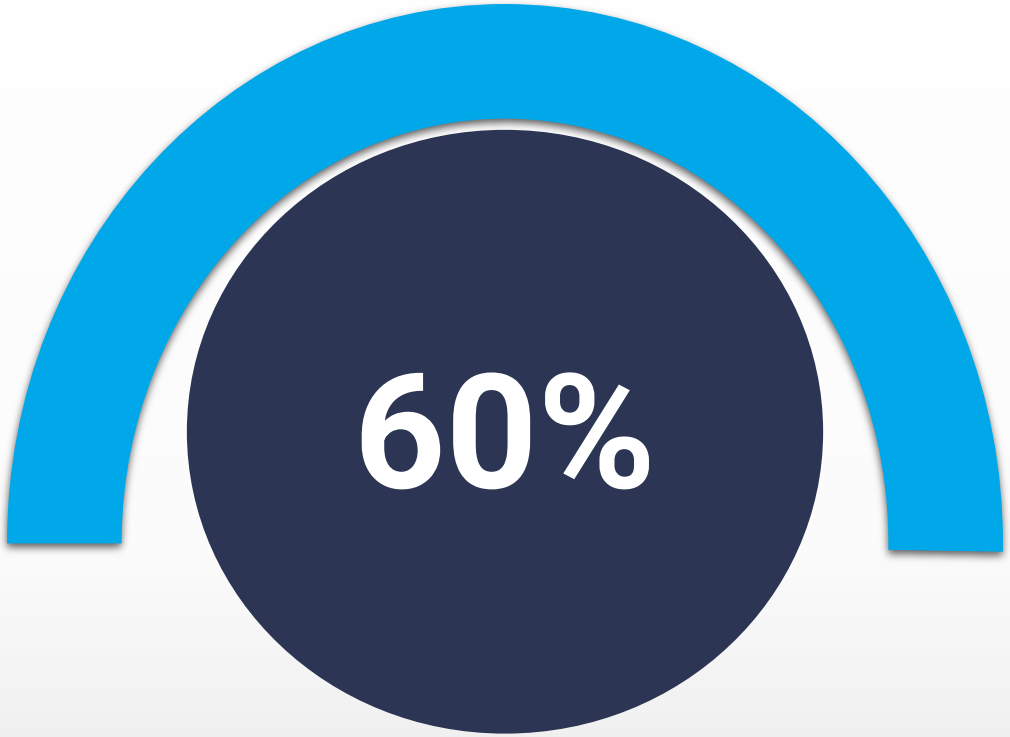
“Prohibido Olvidar: Lecciones de Brechas que Dejan Huella”

MEGATEC 2025

YOD FOUNDATION

APPLICA TECH KNOWLEDGE TRANSFER

CCC CA



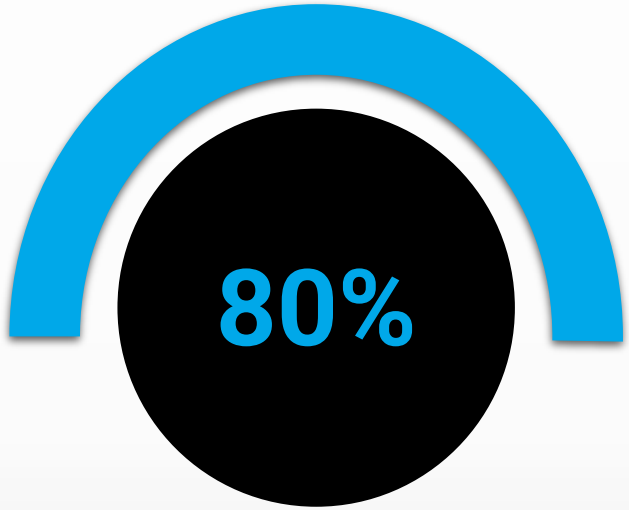
de ataques afectan infraestructura crítica

MEGATEC 2025

ESTADÍSTICAS RELEVANTES

MegaTec 2025

La falta de formación y conciencia sigue siendo el principal talón de Aquiles



de los incidentes de ciberseguridad se deben a errores humanos

YOD FOUNDATION

APPLICA Tech Knowledge Transfer

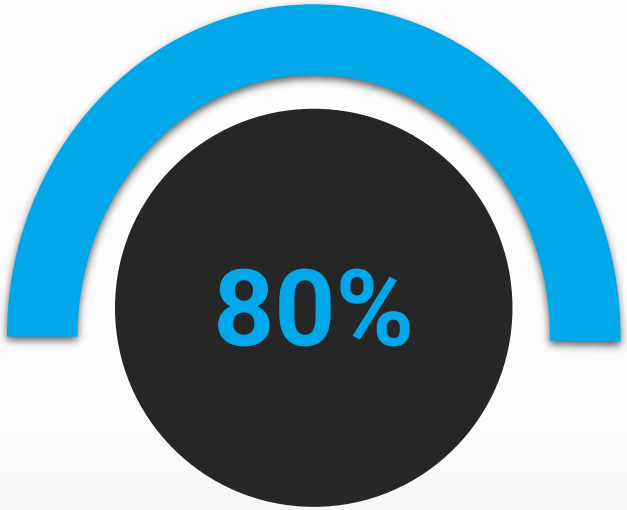
CCC CA

Desarrollo de la Presentación

- Uso de texto corto
- Uso de imágenes
- Uso de videos

MegaTec 2025

La falta de formación y conciencia sigue siendo el principal talón de Aquiles



de los incidentes de ciberseguridad se deben a errores humanos

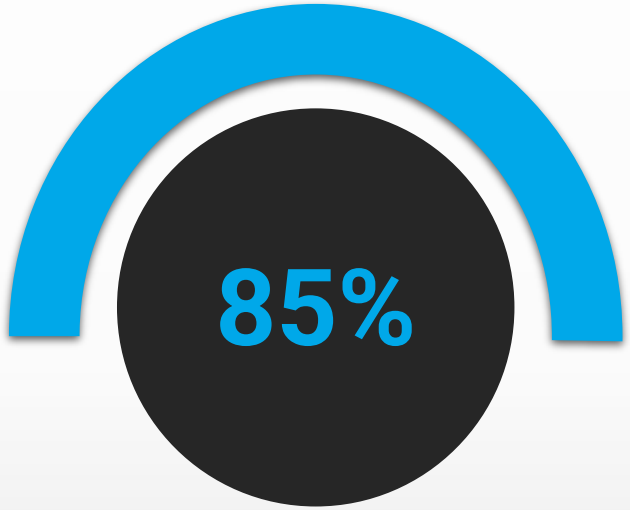
YOD FOUNDATION

APPLICA Tech Knowledge Transfer

CCC CA

MegaTec 2025

Los accesos privilegiados siguen siendo el mayor riesgo de seguridad



de las brechas involucraron abuso o mal manejo de accesos privilegiados

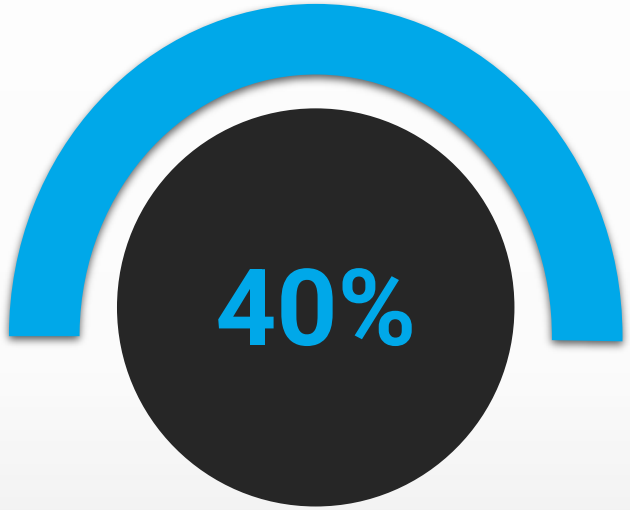
YOD FOUNDATION

APPLICA Tech Knowledge Transfer

CCC CA

MegaTec 2025

La exposición de portales, APIs y apps sigue siendo crítica



de las brechas iniciales se originaron en aplicaciones web vulnerables

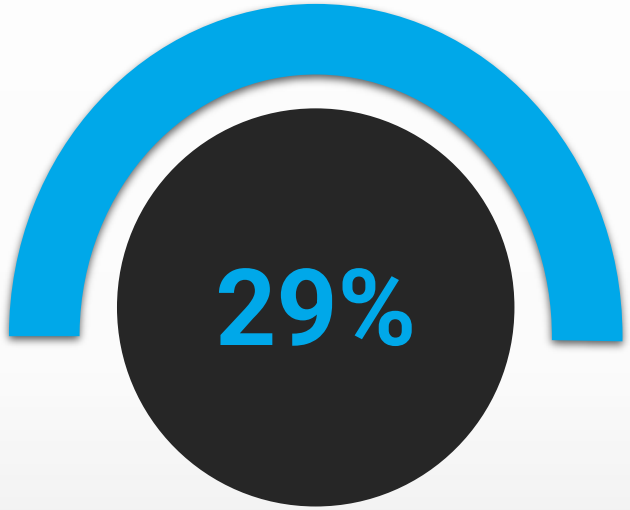
YOD FOUNDATION

APPLICA Tech Knowledge Transfer

CCC CA

MegaTec 2025

El engaño sigue venciendo a la tecnología



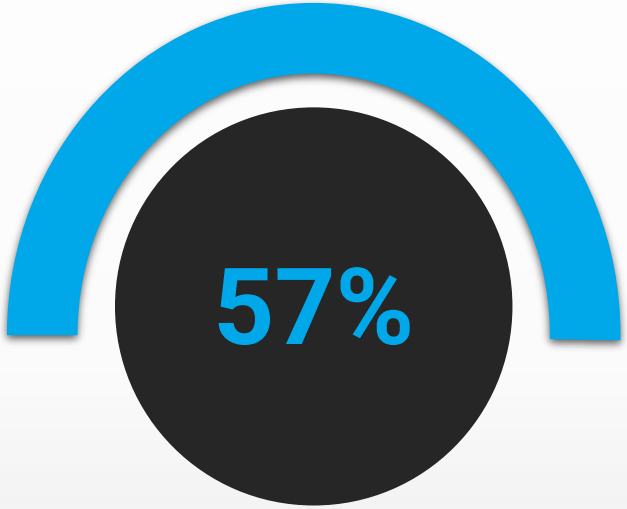
de las brechas fueron producto de ingeniería social exitosa

YOD FOUNDATION

APPLICA Tech Knowledge Transfer

CCC CA

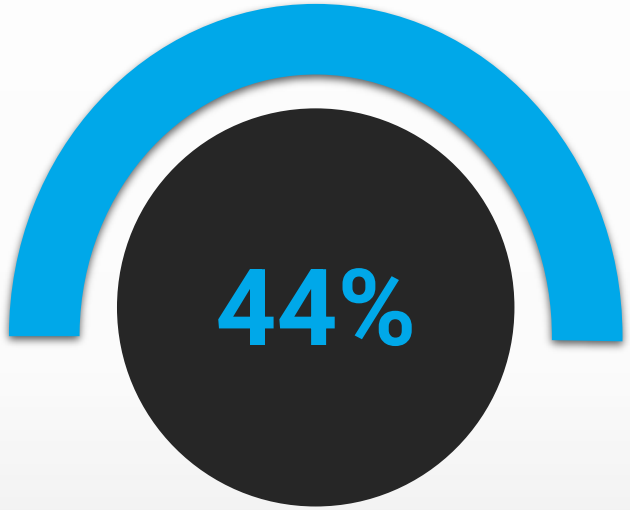
El problema no son los "zero days", son los "forever days"



de las brechas implicaron explotación de vulnerabilidades conocidas no parchadas

MegaTec 2025

Afecta desproporcionadamente a pequeñas y medianas empresas



Ransomware estuvo presente en las brechas analizadas

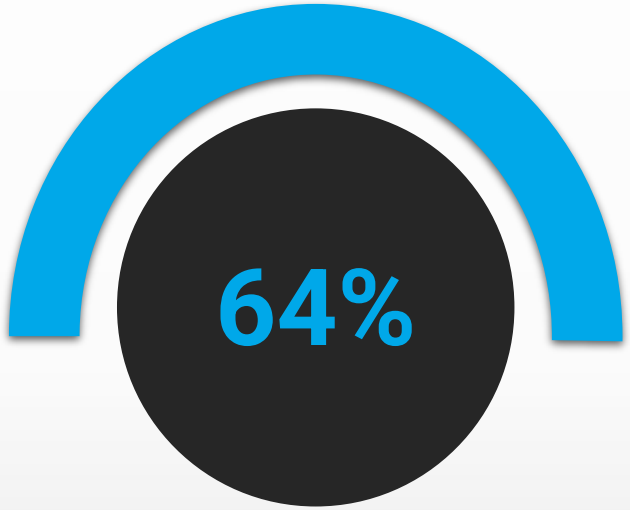
YOD FOUNDATION

APPLICA Tech Knowledge Transfer

CCC CA

MegaTec 2025

¡La resiliencia gana terreno!



de las organizaciones víctimas de ransomware **no** pagaron el rescate

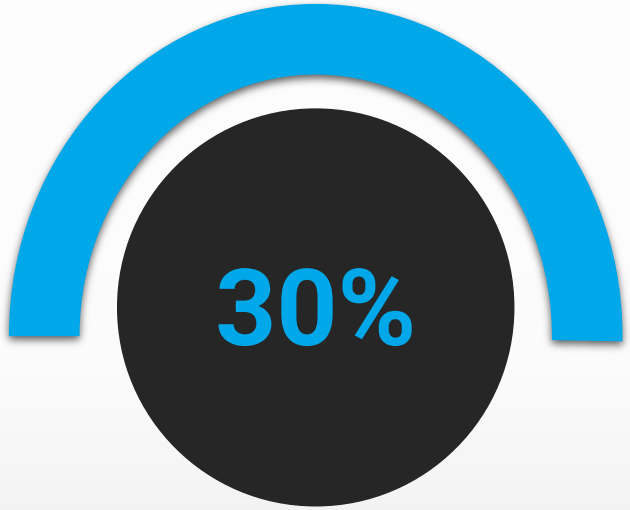
YOD FOUNDATION

APPLICA Tech Knowledge Transfer

CCC CA

MegaTec 2025

La movilidad sin control sigue siendo un riesgo creciente



de los dispositivos comprometidos en eran equipos no administrados (BYOD)

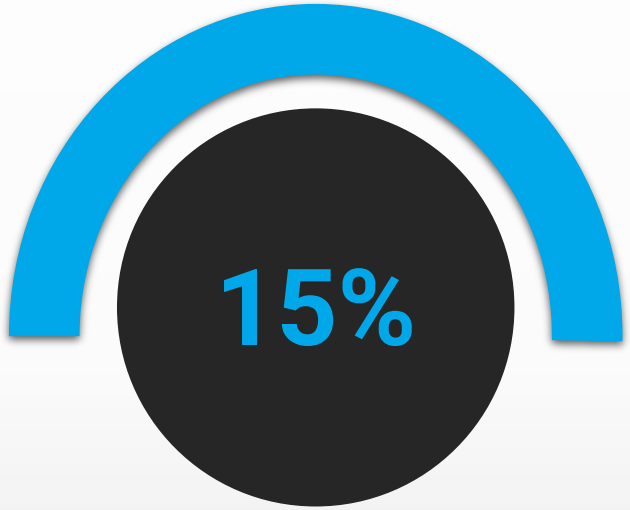
YOD FOUNDATION

APPLICA Tech Knowledge Transfer

CCC CA

MegaTec 2025

Nuevo riesgo emergente por fuga de datos hacia plataformas de IA



de empleados usan IA generativa en dispositivos corporativos sin autorización

YOD FOUNDATION

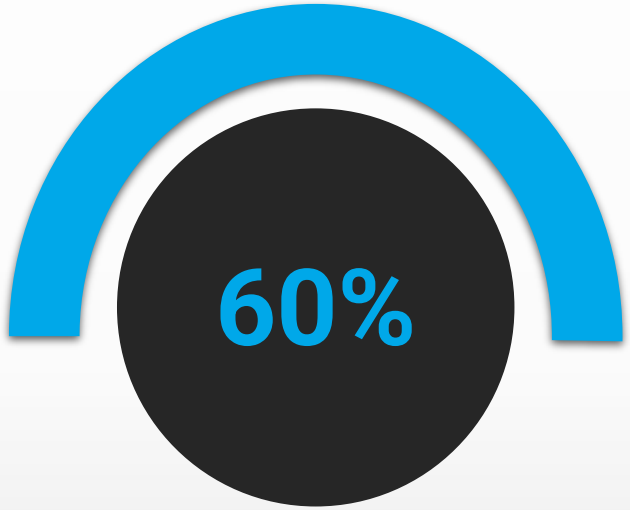
APPLICA Tech Knowledge Transfer

CCC CA

MegaTec 2025

¡Un descuido en el café

y adiós seguridad!



de los empleados tiene datos sensibles almacenados en su laptop corporativa

YOD FOUNDATION

APPLICA Tech Knowledge Transfer

CCC CA

Muchas Gracias

Para más información

www.ccc-ca.com

www.applica.site

APPLICA
TECH KNOWLEDGE TRANSFER

CCC CA

YOD
FOUNDATION