

LIVE Heathrow Airport

BREAKING NEWS



DELAYS AT  
HEATHROW AS  
CYBER ATTACK  
HITS EUROPEAN  
AIRPORTS

Cómo cambió mi *mindset* después de 100 ciberataques

BREAKING NEWS

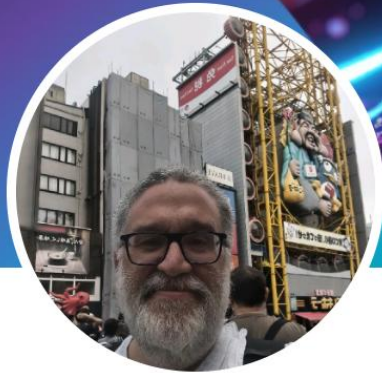
Disruption reported at several European airports

sky news .com

Heathrow Airport, Brussels and Berlin - causing flight delays and cancellations

BREAKING

# BIO (@MALLAVIBARRENA)



**Martiniano ("Marty") Mallavibarrena**  
**Martínez de Castro** ✓

He/Him

Cloud, RPA-Automation, AI, CyberSecurity and Criminal investigations.  
Hooked on retrocomputing. Japan lover. Tech Writer and speaker.

Moralzarzal, Community of Madrid, Spain · [Contact info](#)



SS&C Blue Prism



Udima Universidad a  
Distancia de Madrid



### RANSOMWARE



Le chantajea

### SPYWARE



Roba sus datos

### ADWARE



Le muestra publicidad  
sin parar

# Tipos de malware

### GUSANOS



Se propagan  
entre equipos

### TROYANOS



Introducen malware  
en su PC

### REDES DE ROBOTS



Convierten su PC  
en un zombi

LinkedIn

## Las 5 principales amenazas de malware contra las que debemos prepararnos en 2025

En 2024 hubo una buena cantidad de ciberataques de alto perfil, y empresas tan grandes como Dell y TicketMaster fueron víctimas de...

Hace 2 días



ADSLZone

## Un nuevo malware de Android está robando información de los usuarios

Los usuarios de Android se están exponiendo a un nuevo virus de Android que puede robar la información que hay en sus móviles.

Hace 5 días



iProUP

## Ciberseguridad: Conocé el nuevo malware que ataca a usuarios de macOS

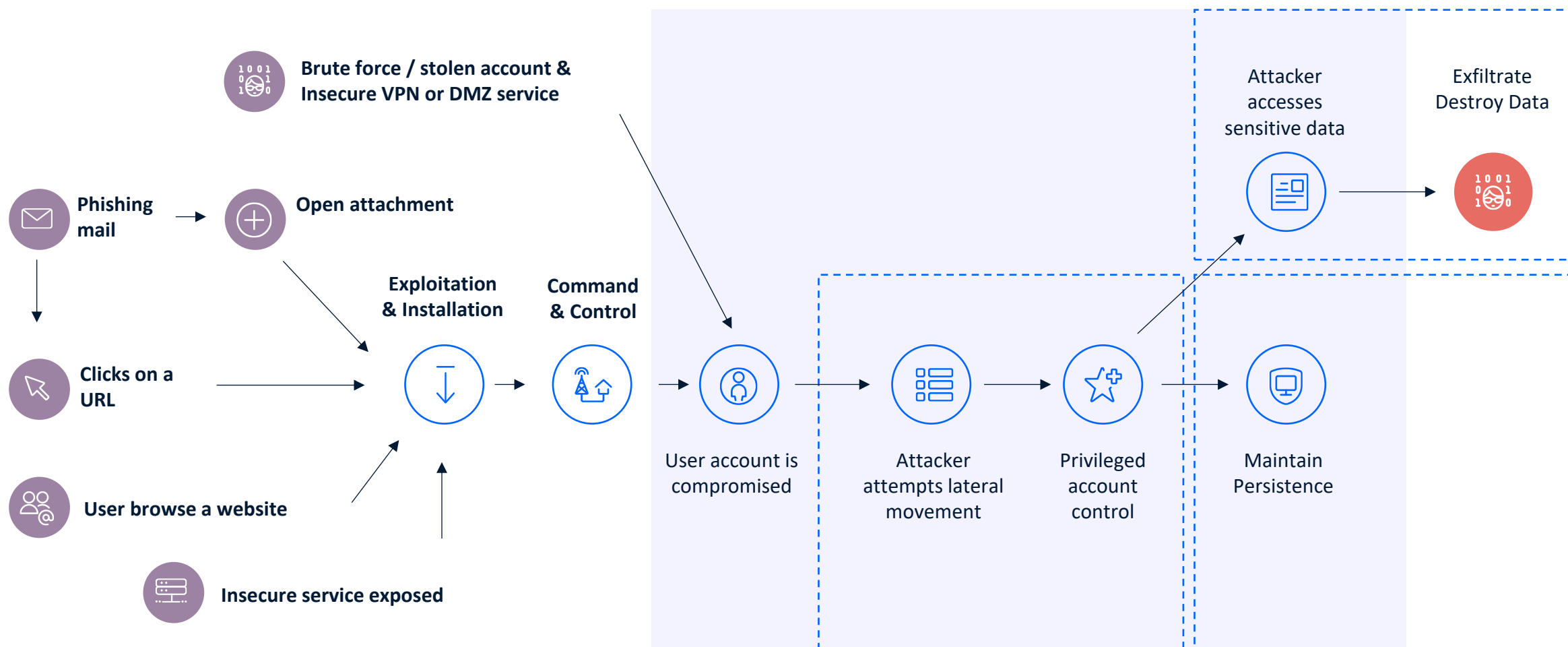
Expertos de Check Point Research advierten sobre una nueva versión del malware Banshee macOS Stealer, al aprovechar el código antivirus de...

Hace 1 día



# MALWARE & FAMILIAS

## Las distintas fases en un incidente de seguridad utilizando ransomware







## 02 – VORIV ZAKON – EL HONOR ENTRE LADRONES

**DarkMarket**

 ZENTRALE  
KRIMINALINSPEKTION  
OLDENBURG

 Rheinland-Pfalz  
GENERALSTAATSANWALTSCHAFT  
KOBLENZ

### DIESER DARKWEB-MARKTPLATZ WURDE BESCHLAGNAHMT

von der Landespolizei Niedersachsen, der Zentralkriminalinspektion Oldenburg in Zusammenarbeit mit Europol, dem Bundeskriminalamt, dem US-Justizministerium und dem Landeskriminalamt Rheinland-Pfalz im Auftrag der Generalstaatsanwaltschaft Koblenz (Rheinland-Pfalz).

### THIS DARKWEB MARKETPLACE HAS BEEN SEIZED

by the the State Police of Lower Saxony, Central Criminal Inspection Oldenburg in conjunction with Europol, Bundeskriminalamt, Federal Bureau of Investigation, U.S. Department of Justice and State Office of Criminal Investigation Rhineland-Palatinate, on behalf of the Attorney General's Office in Koblenz (Rhineland-Palatinate).

 Bundeskriminalamt

 Rheinland-Pfalz  
LANDESKRIMINALAMT

 CYBERCRIME  
INTELLIGENCE UNIT

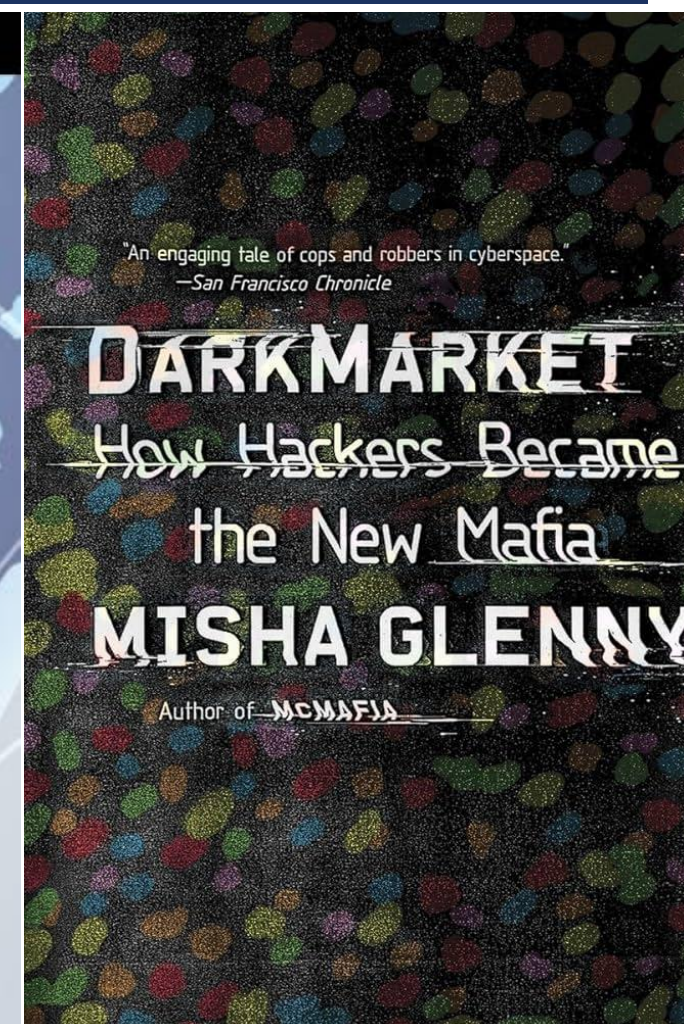
 POLIZEIDIREKTION  
OLDENBURG

 LANDESKRIMINALAMT  
NIEDERSACHSEN

 NCA  
National Crime Agency

 EUROPOL

 AFP  
AUSTRALIAN FEDERAL POLICE



## 03 – SIN PIEDAD

AL MENOS SIETE HOSPITALES REGISTRARON DEMORAS, LO QUE RETRASÓ EL INICIO DE TRATAMIENTOS

Hospitales fueron afectados por retrasos en entrega de resultados VIH y hepatitis tras el ciberataque al Instituto de Salud Pública

19.08.2025

El Hospital de Los Rios sufre un ciberataque de la  
a de 'ransomware' Qilin

## 4 – LOS SOSPECHOSOS HABITUALES





# 5 – SI HAY DEMANDA, SIEMPRE HABRÁ OFERTA. SIEMPRE.

The screenshot displays a dark web marketplace interface. At the top is a navigation bar with links: Home, Orders, Messages (with a red notification badge), Become a vendor, Balance, Support, and Pony&Orient Express. On the right of this bar are icons for a bell, a user profile, and a power button. Below the navigation bar is a breadcrumb trail: Home / Homepage.

The main content area is divided into three sections:

- Personal phrase:** Displays the text "all8s".
- User panel:** Shows a user profile for "Level 1" who joined on "03 May 2022". It also lists "Total sales: 0.00 USD" and "Total orders: 0.00 USD".
- Navigation:** A list of categories with item counts: Drugs (2915), Services (74), Security & Hosting (13), Miscellaneous (6), Jewellery & Art (0), Identification (68), Guides & Tutorials (1035), Fraud (1040), Counterfeit (32), Software & Malware (407), and Carded Items (121).

The central part of the page features a "Top list" of drug offerings in a grid:

- 50x XTC 220MG BLUE DOMINOS HIGH QUALITY CLEAN PILLS:** Sold by TheWizzardNL for USD 160.00. A green "Sold: 1" badge is present.
- Colombian Cocaine - 2,5gram:** Sold by NarcNL for EUR 1.00.
- 1KG MDMA CHAMPAGNE 89% PURE CRYSTALS HQ++:** Sold by TheWizzardNL for USD 1.00.
- Ketamin - 50gram:** Sold by NarcNL for EUR 1.00.
- XTC - 25pcs - Pink Red-Bulls:** Sold by NarcNL for EUR 1.00.
- x10 Oxycodone m30 30mg Worldwide Shipping:** Sold by Dimma for GBP 1.00. A green "Sold: 2" badge is present.
- x25 Oxycodone m30 30mg Worldwide Shipping:** Sold by Dimma for GBP 1.00. A green "Sold: 1" badge is present.
- {1GR} PURE COLOMBIAN COCAINE 100% (UNCUT) FREE UK-UK DEL:** Sold by CocaineMaster for GBP 1.00.
- MDMA - 50gram:** Sold by NarcNL for EUR 1.00.
- MDMA Champagne Crystals 92% | High Quality | 1G - 1000G MDMA WORLDWIDE SHIPPING:** Sold by SanikharExpress for EUR 1.00. A green "Sold: 4" badge is present.

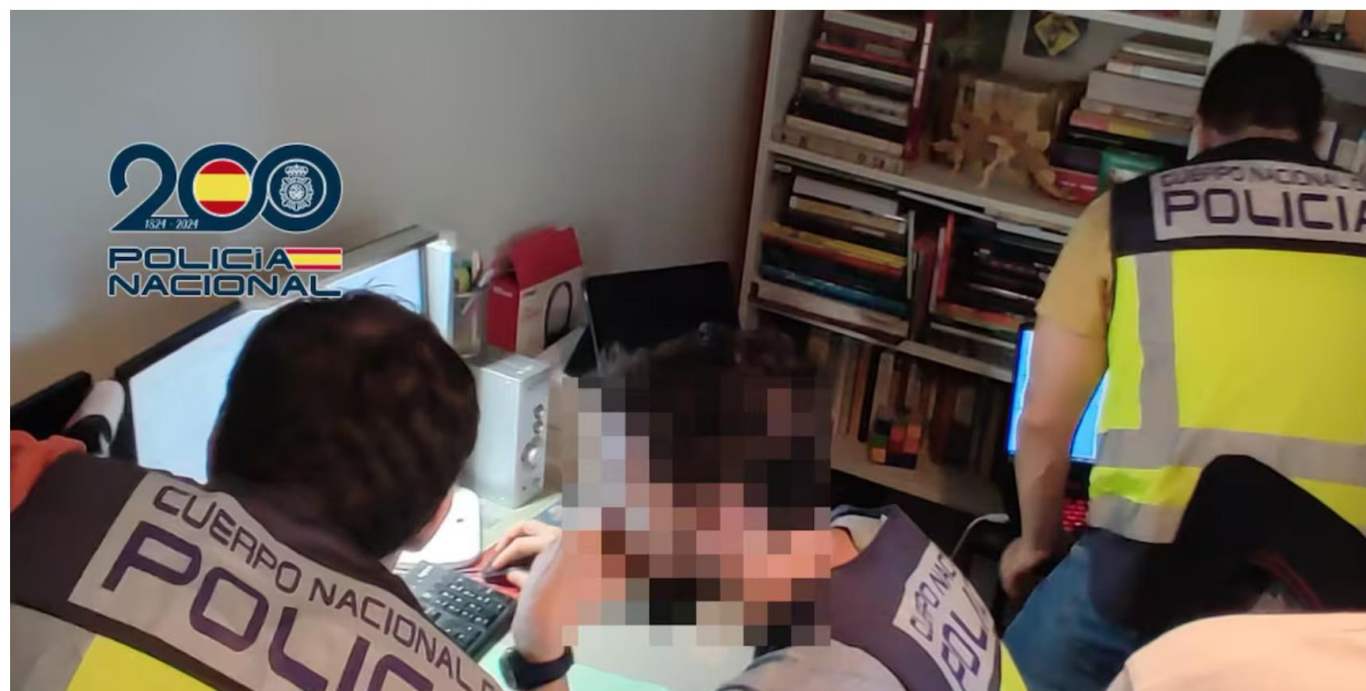
At the bottom of each listing is a button that says "Buy this position" followed by a plus icon and the price in USD.

## 6 – PERO ENTONCES.. ¿LOS CUERPOS POLICIALES?

CIBERATAQUES >

### **Una operación internacional desmantela la infraestructura de los ‘hackers’ prorrusos que atacaron España por el apoyo a Ucrania**

El grupo NoName057(16), vinculado al régimen de Putin, ciberatacó las webs de ministerios y empresas durante las elecciones generales de 2023



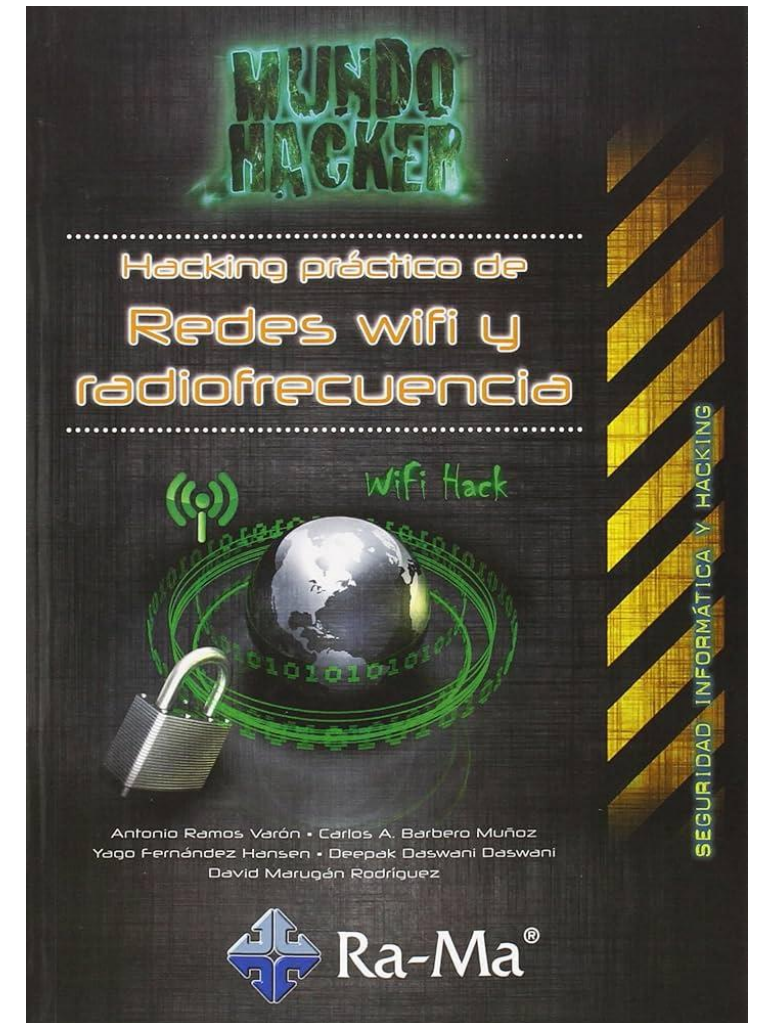


## 7 – LA LEY DE LA SELVA





## 8 – CONOCIMIENTO UBÍCUO (¡TODO ESTÁ EN YOUTUBE!)

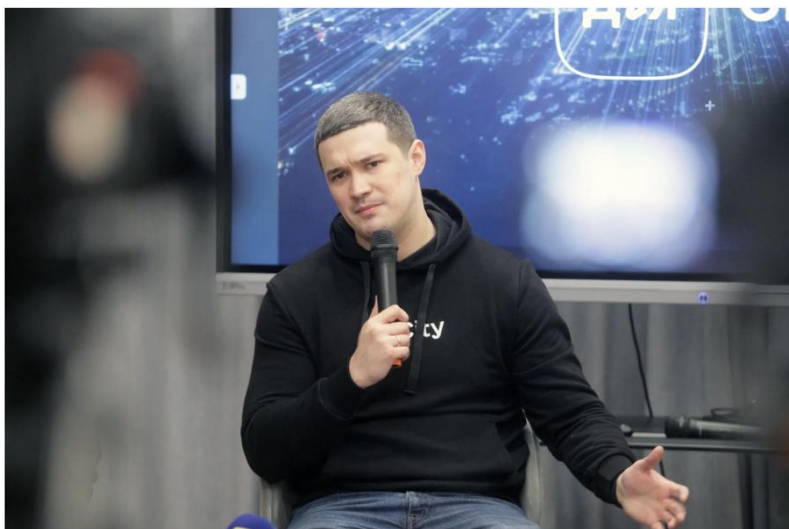




## 9 – VEN AL LADO OSCURO

### *Hackers voluntarios se enlistan en la guerra digital contra Rusia*

Las batallas en línea han desdibujado las fronteras entre hackers respaldados por países y aficionados patriotas, lo que dificulta que los gobiernos entiendan quién los está atacando y cómo tomar represalias.



Una foto de diciembre de Mijail Fedorov, ministro de transformación digital de Ucrania. “Estamos creando un ejército tecnológico”, tuiteó el sábado. Yevhen

## Cómo Rusia reclutó y formó a «batallones» de hackers

NUEVA SOCIEDAD 269 / MAYO - JUNIO 2017

En los últimos años, la defensa del ciberespacio se ha convertido en una de las principales preocupaciones del Kremlin. En 2013, el Ejército ruso lanzó una operación destinada a reclutar a especialistas en seguridad de la información, tal como lo revelaron el diario digital Meduza y The New York Times.

# 10 – LA GUERRA DE “LAS IA”

The screenshot displays the Microsoft Defender Endpoint Security interface. The top navigation bar includes 'Endpoint security', 'Endpoint detections', and a search bar. The main area is divided into four tabs: 'Details', 'Process table', 'Process tree', and 'Events timeline'. The 'Process tree' tab is active, showing a hierarchical view of running processes. A process tree is visible, starting from 'powershell.exe' and branching into 'powershell.exe', 'notepad.exe', 'cmd.exe', and 'payroll.exe'. The 'payroll.exe' process is highlighted with a green checkmark and a red 'Blocked' status. The right-hand pane provides detailed information about the selected 'payroll.exe' process, including its execution details, command line, file path, and SHA256 hash.

**Endpoint security** | [Endpoint detections](#) > Feb. 9, 2024 14:26:55

Search | Charlotte AI | Search@8f315ca1 | Customer ID

Details | Process table | **Process tree** | Events timeline

**payroll.exe**

**Blocked** Actions

**Execution details**

Host name  
SULK-FOX-USR1

User name  
WORKSHOP\SU...

Local process ID  
2328

Command line  
payroll.exe

File path  
\\Device\\HarddiskVolume2\\Users\\natasha\\Down  
loads\\payroll.exe

Executable SHA256  
017ac6ab8e84d6ebdf4e908db1246ae7514cffd2d9  
f252402164e56fb51c3fe4

Start time  
Feb. 9, 2024 14:2...

End time  
Feb. 9, 2024 14:2...

Duration  
<1s

**Associated detections**



Recap





GRACIAS

@MALLAVIBARRENA