

# Modus operandi de grupos criminales con impacto en Euskadi en 2025

A lo largo de 2025, se ha seguido un proceso de identificación y monitorización de las amenazas que han tenido un impacto potencial en Euskadi con objetivo de poner en marcha iniciativas que mitiguen el riesgo de la ciudadanía y de las entidades tanto públicas como privadas. Por este motivo, en la Agencia Vasca de Ciberseguridad Cyberzaintza, hemos analizado un total de **127 incidentes de especial relevancia**, cuya categoría corresponde a una peligrosidad alta, muy alta o crítica en base a la clasificación recogida en la guía CCN-STIC 817, de gestión de ciberincidentes.



Dicho análisis, engloba entre otros aspectos la identificación del «modus operandi» utilizado por los atacantes para llevar a cabo sus acciones maliciosas, lo que incluye las tácticas, técnicas y procedimientos. A continuación, utilizando como base el framework de Mitre ATT&CK se recoge la información extraída de los análisis realizados con el objetivo de que sirva a las organizaciones a priorizar y poner en marcha iniciativas que contribuyan a elevar su capacidad de resiliencia y, por ende, su nivel de madurez en ciberseguridad.

## Top técnicas (técnica más utilizada por cada táctica)

Táctica	Técnica más usada
Reconnaissance	Gather Victim Host Information - T1592
Resource Development	Acquire Infrastructure - T1583
Initial Access	Exploit Public-Facing Application - T1190
Execution	Command and Scripting Interpreter - T1059
Persistence	Boot or Logon Autostart Execution - T1547
Privilege Escalation	Exploitation for Privilege Escalation - T1068
Defense Evasion	Indicator Removal: File Deletion - T1070
Credential Access	Credentials from Password Stores - T1555
Discovery	File and Directory Discovery - T1083
Lateral Movement	Remote Services - T1021
Collection	Data from Local System - T1005
Command and Control	Application Layer Protocol - T1071
Exfiltration	Exfiltration Over C2 Channel - T1041
Impact	Data Encrypted for Impact - T1486

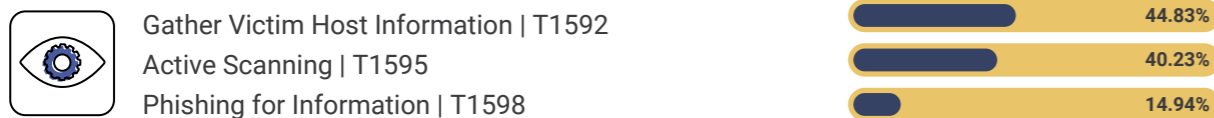


## Top 10 mitigaciones

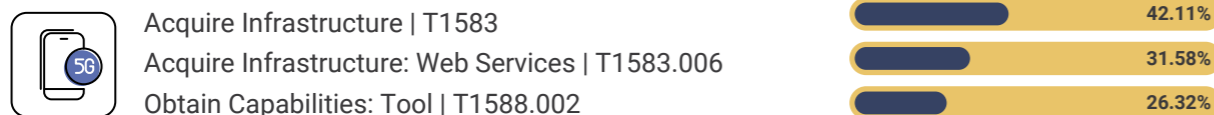
<b>M1026 Privileged Account Management</b> 	La gestión de cuentas privilegiadas se centra en implementar políticas, controles y herramientas para administrar de manera segura las cuentas privilegiadas (por ejemplo, cuentas SYSTEM, root o de administrador).	<b>M1038 Execution Prevention</b> 	Bloquear la ejecución de código en un sistema mediante control de aplicaciones y/o bloqueo de scripts.
<b>M1047 Audit</b> 	Realizar auditorías o análisis de sistemas, permisos, software inseguro, configuraciones inseguras, etc., para identificar posibles debilidades.	<b>M1031 Network Intrusion Prevention</b> 	Utilizar firmas de detección de intrusiones para bloquear el tráfico en los límites de la red.
<b>M1017 User Training</b> 	Formar a los usuarios para que reconozcan intentos de acceso o manipulación por parte de un adversario, con el fin de disminuir el riesgo de ataques exitosos de spearphishing, ingeniería social y otras técnicas que requieran la interacción del usuario.	<b>M1040 Behavior Prevention on Endpoint</b> 	La prevención basada en comportamiento en el endpoint se refiere al uso de tecnologías y estrategias para detectar y bloquear actividades potencialmente maliciosas, analizando el comportamiento de procesos, archivos, llamadas a API y otros eventos en el dispositivo final.
<b>M1018 User Account Management</b> 	Gestionar la creación, modificación, uso y permisos asociados a las cuentas de usuario.	<b>M1037 Filter Network Traffic</b> 	Emplear dispositivos de red y software en los endpoints para filtrar el tráfico de entrada, salida y movimiento lateral en la red.
<b>M1051 Update Software</b> 	Las actualizaciones de software garantizan que los sistemas estén protegidos frente a vulnerabilidades conocidas mediante la aplicación de parches y mejoras proporcionadas por los fabricantes.	<b>M1048 Application Isolation and Sandboxing</b> 	El aislamiento y el sandboxing de aplicaciones se refieren a la técnica de restringir la ejecución de código a un entorno controlado y aislado.

## Top 3 técnicas por cada táctica

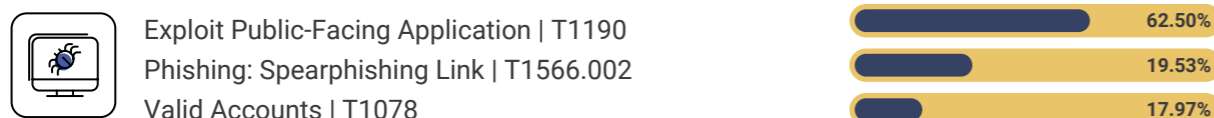
### Reconnaissance



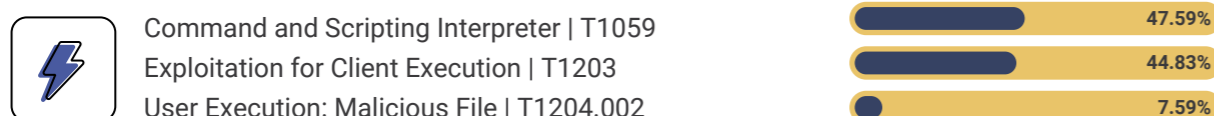
### Resource Development



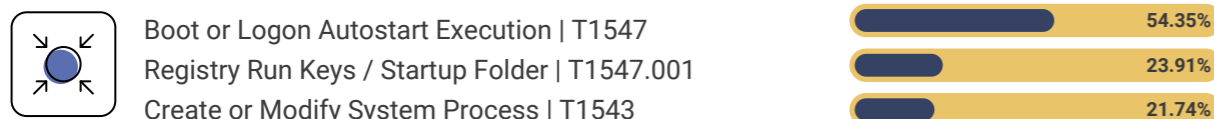
### Initial Access



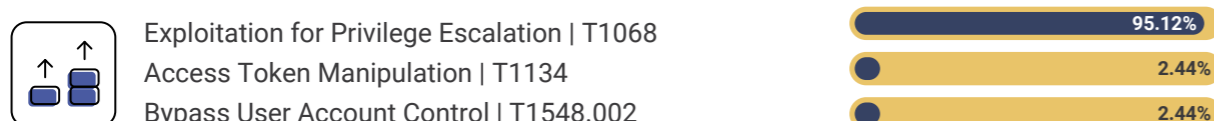
### Execution



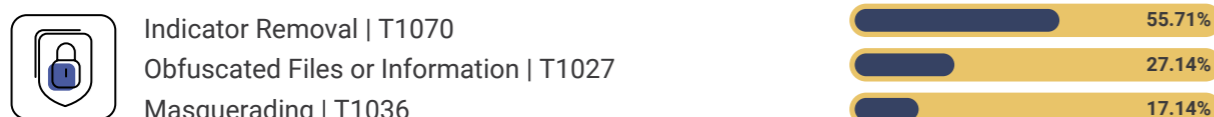
### Persistence



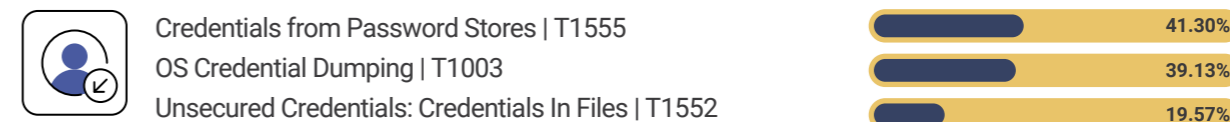
### Privilege Escalation



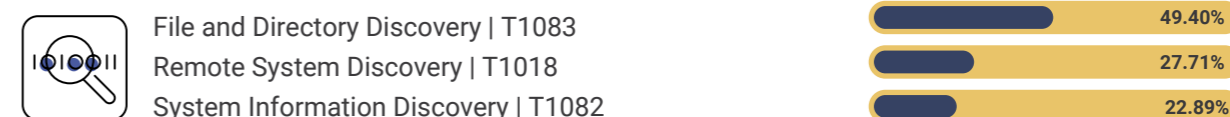
### Defense Evasion



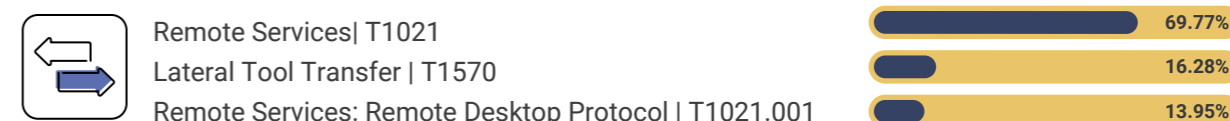
### Credential Access



### Discovery



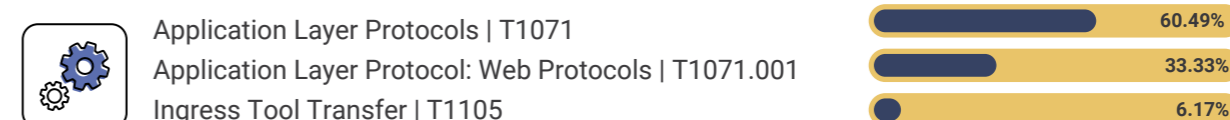
### Lateral Movement



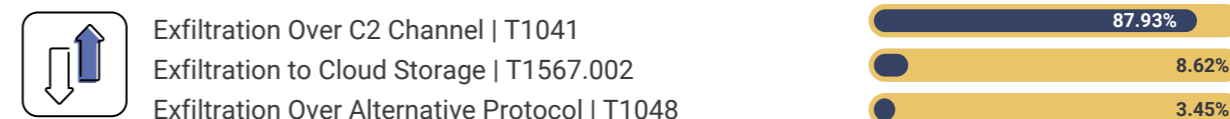
### Collection



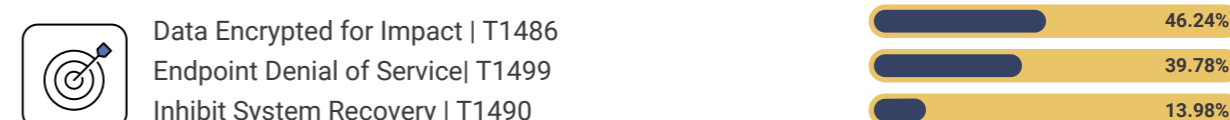
### Command and Control



### Exfiltration



### Impact



## CONCLUSIONES

- La explotación de aplicaciones públicas se consolida como el vector dominante. Las técnicas de reconocimiento evolucionan hacia la recopilación exhaustiva de información específica del objetivo.
- Los métodos de acceso a credenciales se centran en la explotación de almacenes de contraseñas que concentran credenciales de alto valor. Hay un cambio de estrategia hacia exfiltración de grandes volúmenes de datos en lugar de captura selectiva.
- Esta evolución revela adversarios que combinan oportunismo técnico con reconocimiento exhaustivo, priorizando vulnerabilidades sin parchear y maximizando la exfiltración masiva de información.

➔ Esto exige refuerzo urgente en gestión de parches, protección de almacenes de credenciales y monitorización de exfiltración.