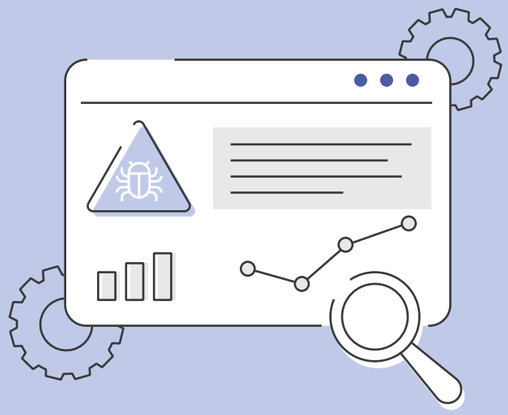
Modus operandi de grupos criminales con impacto en Euskadi

Durante 2023, 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, desde Cyberzaintza, Agencia Vasca de Ciberseguridad, hemos analizado un total de 99 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 10 técnicas (técnica más utilizada por cada táctica)

Táctica	Técnica más usada
Reconnaissance	Vulnerability Scanning - T1595.002
Resource Development	Malware - T1587.001
Initial Access	Phishing - T1566
Execution	Malicious File - T1204.002
Persistence	Registry Run Keys / Startup Folder File - T1547.001
Privilege Escalation	Exploitation for Privilege Escalation - T1068
Defense Evasion	Deobfuscate/Decode Files or Information - T1140
Credential Access	Brute Force - T1110
Discovery	File and Directory Discovery - T1083
Lateral Movement	Lateral Tool Transfer - T1570
Collection	Archive via Custom Method - T1560.003
Command and Control	Ingress Tool Transfer - T1105
Exfiltration	Exfiltration Over C2 Channel - T1041
Impact	Data Encrypted for Impact - T1468

Top 10 mitigaciones

A partir de las técnicas más utilizadas se identifican de manera priorizadas las mitigaciones.

User Training - M1017

12,85%

Capacitar a los usuarios para que estén al tanto de los intentos de acceso o manipulación por parte de un adversario para reducir el riesgo de éxito de spearphishing, ingeniería social y otras técnicas que involucran la interacción del usuario.

Behavior Prevention on Endpoint - M1040

10,08%

Utilizar capacidades para evitar que se produzcan patrones de comportamiento sospechosos en los sistemas de punto final. Esto podría incluir un proceso sospechoso, archivo, llamada a la API, etc.

Execution Prevention - M1038

12,00%

Los adversarios pueden usar nuevas DLL para ejecutar esta técnica. Identificar y bloquear software potencialmente malicioso ejecutado a través del secuestro de órdenes de búsqueda mediante el uso de soluciones de control de aplicaciones capaces de bloquear archivos DLL cargados por software legítimo.

Antivirus/Antimalware - M1049

8,92%

Utilizar firmas o heurísticas para detectar software malintencionado.

Network Intrusion Prevention - M1031

11,92%

Usar firmas de detección de intrusiones para bloquear el tráfico en los límites de la red.

Restrict Web-Based Content- M1021

7,92%

Restringir el uso de ciertos sitios web, bloquear descargas / archivos adjuntos, bloquear Javascript, restringir las extensiones del navegador, etc.

User Account Management - M1018

11,00%

Administrar la creación, modificación, uso y permisos asociados a las cuentas de usuario.

Audit - M1047

7,69%

Realizar auditorías o escaneos de sistemas, permisos, software inseguro, configuraciones inseguras, etc. para identificar posibles debilidades.

Privileged Account Management - M1026

10,77%

Administrar la creación, modificación, uso y permisos asociados a las cuentas privilegiadas, incluidos SYSTEM y root.

Disable or Remove Feature or Program - M1042

6,85%

Eliminar o denegar el acceso a software innecesario y potencialmente vulnerable para evitar el abuso por parte de los adversarios.

Top 3 técnicas por cada táctica

Reconnaissance

Vulnerability Scanning – T1595.002	60,00%
Active Scanning – T1595	20,00%
IP Addresses – T1590.005	20,00%

Resource Development

Malware – T1587.001	47,37%
Link Target – T1608.005	31,58%
Acquire Infrastructure – T1583	21,05%

Initial Access

Phishing – T1566	53,33%
Spearphishing Attachment – T1566.001	28,33%
Spearphishing Link – T1566.002	18,33%

Execution

Malicious File – T1204.002	43,64%
PowerShell – T1059.001	30,91%
Command and Scripting Interpreter – T1059	25,45%

Persistence

Registry Run Keys / Startup Folder – T1547.001	35,29%
Web Shell - T1505.003	35,29%
Account Manipulation – T1098	29,41%

Privilege Escalation

Exploitation for Privilege Escalation – T1068	50,00%
Boot or Logon Autostart Execution - T1547	25,00%
Group Policy Modification – T1484.001	25,00%

Defense Evasion

Deobfuscate/Decode Files or Information – T1140	44,44%
Obfuscated Files or Information – T1027	29,63%
Modify Registry – T1112	25,93%

Credential Access

Brute Force – T1110	44,44%
Exploitation for Credential Access – T1212	27,78%
Steal Web Session Cookie– T1539	27,78%

Discovery

File and Directory Discovery – T1083	43,75%
Network Share Discovery – T1135	31,25%
Process Discovery – T1057	25,00%

Lateral Movement

Lateral Tool Transfer – T1570	42,68%
Pass the Hash – T1550.002	28,57%
Remote Desktop Protocol – T1021.001	28,57%

Collection

Archive via Custom Method – T1560.003	36,36%
Automated Collection – T1119	36,36%
Adversary-in-the-Middle – T1557	27,27%

Command and Control

Ingress Tool Transfer – T1105	37,50%
Application Layer Protocol – T1071	31,25%
Encrypted Channel – T1573	31,25%

Exfiltration

Exfiltration Over C2 Channel – T1041	57,14%
Automated Exfiltration – T1020	21,43%
Exfiltration Over Alternative Protocol – T1048	21,43%

Impact

Data Encrypted for Impact – T1486	62,96%
Inhibit System Recovery – T1490	22,22%
Service Stop – T1489	14,81%

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza