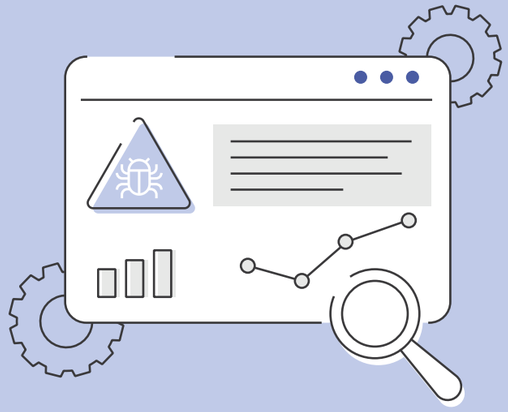
Modus operandi de grupos criminales con impacto en Euskadi

Durante 2022, 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 el Basque CyberSecurity Centre, hemos analizado un total de 75 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	Phishing for Information - T1598
Resource Development	Acquire Infrastructure: Domains - T1583.001
Initial Access	Phishing - T1566
Execution	User Execution: Malicious File - T1204.002
Persistence	External Remote Services - T1133
Privilege Escalation	Exploitation for Privilege Escalation - T1068
Defense Evasion	Obfuscated Files or Information - T1027
Credential Access	OS Credential Dumping: LSASS Memory – T1003.001
Discovery	System Information Discovery - T1082
Lateral Movement	Lateral Tool Transfer - T1570
Collection	Data from Local System - T1005
Command and Control	Application Layer Protocol: Web Protocols – T1071.001
Exfiltration	Exfiltration Over C2 Channel - T1041
Impact	Data Encrypted for Impact - T1486

Top 10 mitigaciones

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

User Training - M1017

5,66%

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.

Privileged Account Management - M1026

4,90%

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

Behavior Prevention on Endpoint - M1040

5,33%

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.

Network Intrusion Prevention - M1031

4,57%

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

Execution Prevention - M1038

5,11%

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.

User Account Management - M1018

4,35%

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

Antivirus/Antimalware - M1049

5,10%

Utilizar firmas o heurísticas para detectar software malintencionado.

Restrict Web-Based Content- M1021

4,13%

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

Disable or Remove Feature or Program - M1042

4,90%

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

Software Configuration - M1054

3,59%

Implementar cambios de configuración en el software (que no sea el sistema operativo) para mitigar los riesgos de seguridad asociados a la forma en que funciona el software.

Top 3 técnicas por cada táctica

Reconnaissance

Phishing for Information - T1598	18,18%
Active Scanning: Vulnerability Scanning – T1595.002	18,18%
Search Victim-Owned Websites - T1594	9,09%

Resource Development

Acquire Infrastructure: Domains – T1583.001	20,00%
Compromise Accounts - T1586	10,00%
Develop Capabilities: Exploits - T1587.004	10,00%

Initial Access

Phishing - T1566	20,00%
Phishing: Spearphishing Attachment – T1566.001	16,25%
External Remote Services - T1133	13,75%

Execution

User Execution: Malicious File – T1204.002	13,83%
Command and Scripting Interpreter: PowerShell – T1059.001	9,57%
Native API - T1106	8,51%

Persistence

External Remote Services - T1133	14,63%
Valid Accounts - T1078	12,20%
Scheduled Task/Job: Scheduled Task – T1053.005	12,20%

Privilege Escalation

Exploitation for Privilege Escalation - T1068	15,22%
Process Injection - T1055	13,04%
Create or Modify System Process: Windows Service – T1543.003	10,87%

Defense Evasion

Obfuscated Files or Information - T1027	7,48%
Valid Accounts - T1078	6,80%
Process Injection - T1055	6,12%

Credential Access

OS Credential Dumping: LSASS Memory – T1003.001	17,78%
Brute Force - T1110	11,11%
OS Credential Dumping: NTDS – T1003.003	8,89%

Discovery

System Information Discovery - T1082	9,88%
File and Directory Discovery - T1083	9,88%
Process Discovery - T1057	8,64%

Lateral Movement

Lateral Tool Transfer - T1570	15,38%
Exploitation of Remote Services - T1210	11,54%
Remote Services: Remote Desktop Protocol – T1021.001	11,54%

Collection

Data from Local System - T1005	17,65%
Screen Capture - T1113	17,65%
Automated Collection - T1119	11,76%

Command and Control

Application Layer Protocol: Web Protocols – T1071.001	21,62%
Data Encoding: Standard Encoding – T1132.001	10,81%
Remote Access Software - T1219	8,11%

Exfiltration

Exfiltration Over C2 Channel - T1041	47,37%
Exfiltration Over Web Service: Exfiltration to Cloud Storage – T1567.002	15,79%
Automated Exfiltration - T1020	15,79%

Impact

Data Encrypted for Impact - T1486	47,06%
Inhibit System Recovery - T1490	17,65%
Service Stop - T1489	11,76%

Basque CyberSecurity Centre