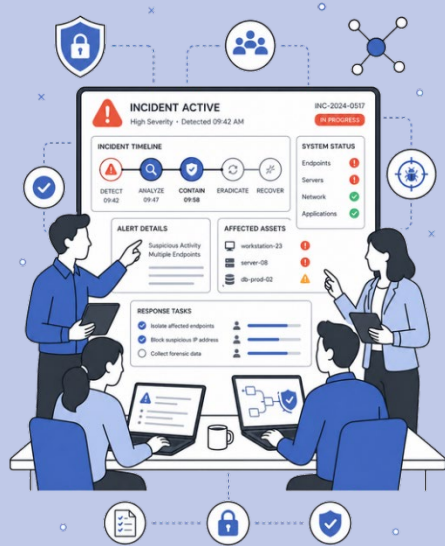




Euskadin eragina duten talde kriminalen modus operandi-a 2026ko lehen seihilekoan

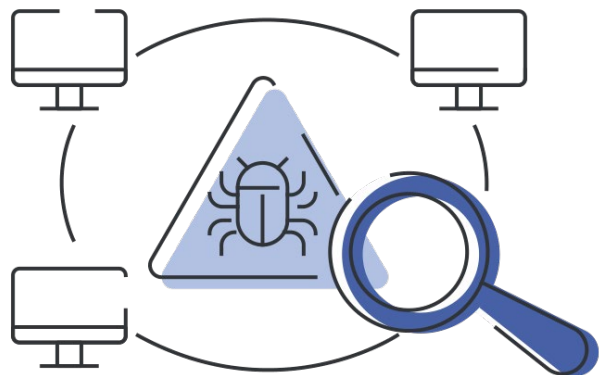
2026ko lehen seihilekoan zehar, Euskadin eragina izan dezaketen mehatxuak identifikatzeko eta monitorizatzeko prozesu bat jarraitu da. Zibersegurtasunaren Euskal Agentzian, Cyberzaintzan, garrantzi bereziko 200 gertakari aztertu ditugu guztira, eta horien kategoria arrisku-maila handiari, oso handiari edo kritikoari dagokio, CCN - STIC 817 gidaren sailkapenaren arabera.



Azterketa horretan erasotzaileek erabilitako «modus operandi» -aren identifikazioa sartzen da. Oinarri gisa MITRE ATT&CK framework-a erabiliz, egindako analisietatik ateratako informazioa jasotzen da –hileko buletinak, malware-txostenak eta MISP sistemaren konpromiso-adierazleak–, erakundeei zibersegurtasuneko erresilientzia-maila eta heldutasun-maila handitzen dituzten ekimenak lehenesten laguntzeko.

Top 10 taktikak (Teknika erabiliena taktika bakoitzeko)

TAKTIKA	TEKNIKA ERABILIENA
Reconnaissance	Gather Victim Network Information – T1590 BERRIA
Resource Development	Acquire Infrastructure – T1583
Initial Access	Exploit Public-Facing Application – T1190
Execution	Exploitation for Client Execution – T1203 BERRIA
Persistence	Boot or Logon Autostart Execution – T1547
Privilege Escalation	Exploitation for Privilege Escalation – T1068
Defense Evasion	Impair Defenses – T1562 BERRIA
Credential Access	OS Credential Dumping – T1003 BERRIA
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 arintze-neurriak

M1047 Audit Sistemen, baimenen, konfigurazio ez-seguruen eta softwarearen ikuskaritza egitea, egon daitezkeen ahuleziak identifikatzeko.	6.30%	M1031 Network Intrusion Prevention Intrusioak detektatzeko sinadurak erabiltzea sarearen mugetan trafiko maltzurra blokeatzeko.	5.30%
M1018 User Account Management Erabiltzaile-kontuen sorkuntza, aldaketa, erabilera eta baimenak kudeatzea.	5.70%	M1040 Behavior Prevention on Endpoint Potentzialki maltzurra izan daitekeen jarduera detektatzea eta blokeatzea, endpoint-eko prozesuen portaera aztertuta.	4.80%
M1038 Execution Prevention Baimendu gabeko kodearen exekuzioa blokeatzea, aplikazioak kontrolatuz eta script-ak blokeatuz.	5.60%	M1021 Restrict Web-Based Content NUEVO Webgune maliziosuetako eta deskarga ez-seguruetarako sarbidea mugatzen duten politikak eta teknologiak aplikatzea.	3.80%
M1026 Privileged Account Management SYSTEM, root edo administratzaile kontuak modu seguruan administratzeko politikak, kontrolak eta tresnak inplementatzea.	5.50%	M1049 Antivirus/Antimalware NUEVO Sinaduretan, heuristikan eta portaeraren analisian oinarritutako antibirus/antimalware soluzioak.	3.60%
M1017 User Training Erabiltzaileak trebatzea sarbide- edo manipulazio-saiakerak antzemateko, spearphishing arriskua murriztuz.	5.30%	M1022 Restrict File and Directory Permissions NUEVO Sistema eragileko fitxategi, direktorio eta konfigurazioetarako sarbidea erabiltzaile baimenduei mugatzea.	3.10%

Top 3 teknikak taktika bakoitzeko

Reconnaissance Gather Victim Network Information T159072.90% Gather Victim Host Information T15928.30% Active Scanning T15958.30%	Credential Access OS Credential Dumping T100366.10% LSASS Memory T1003.0018.00% Valid Accounts T10785.40%
Resource Development Acquire Infrastructure T158332.40% Compromise Infrastructure T158430.40% Establish Accounts T158514.20%	Discovery File and Directory Discovery T108318.80% Account Discovery T108716.30% Remote System Discovery T101814.20%
Initial Access Exploit Public-Facing Application T119031.90% Phishing T156631.90% Valid Accounts T107822.70%	Lateral Movement Remote Services T102170.40% Lateral Tool Transfer T15709.20% SMB/Windows Admin Shares T1021.0026.10%
Execution Exploitation for Client Execution T120343.30% Command and Scripting Interpreter T105925.20% PowerShell T1059.00110.60%	Collection Data from Local System T100535.70% Automated Collection T111910.70% Screen Capture T11139.50%
Persistence Boot or Logon Autostart Execution T154727.30% Create or Modify System Process T154322.70% Registry Run Keys / Startup Folder T1547.00112.10%	Command and Control Application Layer Protocol T107165.90% Web Protocols T1071.0018.50% Web Service T11027.10%
Privilege Escalation Exploitation for Privilege Escalation T106864.50% Process Injection T105513.10% Bypass User Account Control T1548.0025.60%	Exfiltration Exfiltration Over C2 Channel T104183.30% Exfiltration Over Alternative Protocol T10487.00% Exfiltration Over Web Service T15675.30%
Defense Evasion Impair Defenses T156229.40% Obfuscated Files or Information T102713.00% Indicator Removal T107010.90%	Impact Data Encrypted for Impact T148650.60% Data Destruction T148514.30% Inhibit System Recovery T14909.50%

ONDORIOAK — ALDERAKETA 2025 VS. 2026ko LEHEN SEHILEKOA

- 2026ko lehen seihilekoan 200 gertakari erregistratu dira, eta urteko guztizkoa 2025etik gorakoa da (127). Jarduera maleziatsuaren erritmoa nabarmen bizkortzen da.
- Defentsa-ihesean, T1070ek (Indicator Removal) T1562ri ematen dio lidergoa (Impair Defenses, % 42): aurkariak aktiboki desaktibatzen dituzte defentsak, arrastoak ezabatzeraz mugatu beharrean.
- Exfiltrazioa gehiago kontzentratzen da: T1041 % 87,9tik % 93,1era igaro da, aktoreek C2 kanalarekin irteera-kanalak bateratzen dituzten seinale.

- Hasierako sarbide-bektoreak berdinketa erakusten du: T1190 (Exploit Public-Facing Application) eta T1566 (Phishing) bektoreak nabarmentzen dira, eta 2025ean T1190-ren % 62,5aren aurka.
- Kredentzialetarako sarbidean, T1555 (Password Stores) T1003 (OS Credential Dumping, % 67,6) teknikak ordeztzen du: sistema eragilearen cache, memoria edo egituren kredentzialak zuzenean iraultzen dituen teknika oldarkorragoa.
- Gutxitze-neurriek banaketa uniformeagoa aurkezten dute (M1047 liderra da 2025ean, % 6,3 vs % 13.8 M1026), eta horrek defentsa-estrategia zabalagoa eskatzen du.