2024an Euskadin inpaktua izan duten gaizkile-taldeen modus operandia

2024an zehar, Euskadin balizko inpaktua izan duten mehatxuak identifikatu eta monitorizatu dira, herritarren eta erakunde publiko zein pribatuen arriskua arintzeko ekimenak martxan jartzeko. Bereziki garrantzitsuak izan diren 94 jazoera aztertu ditugu guztira, eta jazoera horiek arriskutsuak, oso arriskutsuak edo kritikoak izan dira, ziber-jazoerak kudeatzeko CCN-STIC 817.

Azterketa horretan, besteak beste, erasotzaileek ekintza horiek egiteko erabili duten «modus operandia» identifikatu da, hau da, taktikak, teknikak eta prozedurak. Ondoren, Mitre ATT & CKren framework-a oinarri hartuta, egindako azterketetatik ateratako informazioa jasotzen da, erakundeek erresilientzia-gaitasuna eta, ondorioz, zibersegurtasuneko heldutasun-maila handitzen lagunduko duten ekimenak lehenesteko eta abian jartzeko.

Tekniken Top 10a (taktika bakoitzean gehien erabili duten teknika)

Taktika	Teknikaren izena
Reconnaissance	Vulnerability Scanning - T1595.002
Resource Development	Exploits - T1587.004
Initial Access	Exploit Public Facing Application - T1190
Execution	Command and Scripting Interpeter - T1059
Persistence	Registry Run Keys / Startup Folder - T1547.001
Privilege Escalation	Exploitation for Privilege Escalation - T1068
Defense Evasion	Obfuscated Files or Information - T1027
Credential Access	Credentials In Files - T1552.001
Discovery	System Information Discovery - T1082
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

Arintze-neurrien top 10

M1026 Privileged Account Management

%14,30

Kontu pribilegiatuei lotutako sorkuntza, aldaketa, erabilera eta baimenak kudeatzea, SYSTEM eta root barne.

M1038 Execution Prevention

%9,53

Sistema batean kodearen exekuzioa blokeatzea, aplikazioak kontrolatuz eta/edo script-ak blokeatuz.

M1018 User Account Management

%12,54

Erabiltzaile-kontuei lotutako sorkuntza, aldaketa, erabilera eta baimenak kudeatzea.

M1031 Network Intrusion Prevention

%8,60

Arrotzak detektatzeko sinadurak erabiltzea, sarearen mugetako trafikoa blokeatzeko.

M1047 Audit

%11,97

Sistemen, baimenen, segurua ez den softwarearen, seguruak ez diren konfigurazioen eta abarren auditoretzak edo azterketak egitea balizko ahultasunak identifikatzeko.

M1049 Antivirus/Antimalware

%7,56

Sinadurak edo heuristikak erabiltzea asmo txarreko softwarea detektatzeko.

M1017 User Training

%11,81

Erabiltzaileak formatzea aurkari baten sartzeko edo manipulatzeko ahaleginak hautemateko, spearphisingaren, ingeniaritza sozialaren eta erabiltzailearen interakzioa eskatzen duten beste teknika batzuen bidezko eraso arrakastatsuen arriskua murrizteko.

T1032 Multi-factor Authentication

%7,05

Ebidentziaren bi faktore edo gehiago erabiltzea sistema bat egiaztatzeko, hala nola erabiltzaile-izena eta pasahitza, txartel fisiko adimendunaren token batekin edo tokenen sortzaile batekin batera.

M1040 Behavior Prevention on Endpoint

%9,95

Enpoint sistemetan portaera susmagarrien patroiak prebenitzeko tresnak edo gaitasunak erabiltzea. Horren barruan egon daitezke, besteak beste, susmagarriak izan daitezkeen prozesuekin, fitxategiekin eta API deiekin lotutako portaerak.

M1021 Restrict Web-Based Content

%6,68

Webgune batzuen erabilera mugatzea, deskargak/erantsitako fitxategiak blokeatzea, Javascript blokeatzea, nabigatzailearen luzapenak mugatzea, etab.

Taktika bakoitzaren tekniken top 3

Reconnaissance

Vulnerability Scannig | T1595.002	%72,73
Phishing for Information | T1598	%18,18
Active Scanning | T1595	%9,09

Resource Development

Exploits | T1587.004	%50,00
Acquire Infrastructure | T1583	%25,00
Compromise Infrastructure | T1584	%25,00%

Initial Access

Exploit Public Facing Application | T1190	%39,13
Spearphishing Attachment | 1566.001	%31,88
Phishing | T1566	%28,99

Execution

Command and Scripting Interpeter |1059	%45,00
Malicious File | T1204.002	%27,50
PowerShell | T1059.001	%27,50

Persistence

Registry Run Keys / Startup Folder | T1547.001	%53,85
Boot or Logon Autostart Execution | T1547	%23,08
Create or Modify System Process | T1543	%23,08

Privilege Escalation

Exploitation for Privilege Escalation | T1068	%42,11
Abuse Elevation Control Mechanism | T1548	%31,58
Process Injection | T1055	%26,32

Defense Evasion

Obfuscated Files or Information | T1027	%58,82
File Deletion | T1070.004	%23,53
Deobfuscate/Decode Files or Information | T1140	%17,65

Credential Access

Credentials In Files | T1552.001	%50,00
Unsecured Credentials | T1552	%27,27
OS Credential Dumping | T1003	%22,73

Discovery

System Information Discovery | T1082	%39,47
File and Directory Discovery | T1083	%36,84
Network Service Discovery | T1046	%23,68

Lateral Movement

Remote Services | T1021	%42,11
Remote Desktop Protocol | T1021.001	%31,58
SMB/Windows Admin Shares | T1021.002	%26,32

Collection

Data from Local System | T1005	%45,00
Archive Collected Data | T1560	%30,00
Audio Capture | T1123	%25,00

Command and Control

Application Layer Protocol | T1071	%42,50
Web Protocols | T1071.001	%32,50
Ingress Tool Transfer | T1105	%25,00

Exfiltration

Exfiltration Over C2 Channel | T1041	%66,67
Exfiltration to Cloud Storage | T1567.002	%20,00
Data from Cloud Storage | T1530	%13,33

Impact

Data Encrypted for Impact | T1486	%66,67
Inhibit System Recovery | T1490	%22,22
Application or System Exploitation | T1499.004	%11,11