

Euskadin eragina duten talde kriminalek zer modus operandi izan duten 2025an

2025ean, prozesu berezi bat burutu dugu, Euskadin eragina izan duten mehatxuak identifikatzeko eta monitorizatzeko. Asmoa da gero ekimen batzuk martxan jartzea, ea lortzen dugun arriskuak murriztea bai erakunde publiko eta pribatuentzat bai herritarrentzat berentzat. Hori dela eta, Cyberzaintza, Zibersegurtasunaren Euskal Agentzian, guztira, **eragin handiko 127 gertakari** aztertu ditugu, guztiak ere arrisku handi, oso handi edo kritikokoak, hala sailkaturik baitaude zibergorabeherak kudeatzeko CCN-STIC 817 gidan.



Analisi horretan, besteak beste, identifikatu da erasotzaileek zer «modus operandi» erabiltzen duten beren ekintza gaiztoak gauzatzeko, alegia, bai taktikak, bai teknikak bai eta prozedurak ere. Jarraian, ikus dezagun, oinarri gisa Mitre ATT & CKren frameworka erabiliz, analisiak zer informazio eman duten, ea, horrela, antolakundeek asmatzen duten zer ekimen lehenetsi eta jarri behar duten martxan, erresilientzia-gaitasun handiagoa izateko eta, beraz, zibersegurtasunean heldutasun-maila handiagoa erdiesteko.

Puntako teknika (taktika bakoitzean gehien erabiltzen den teknika)

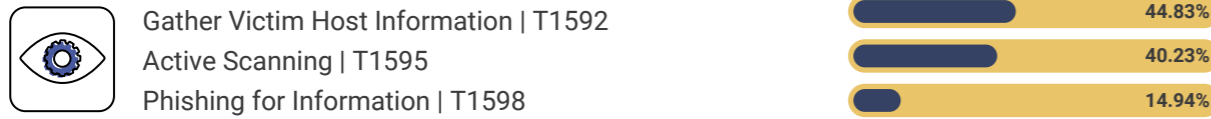
Taktika	Gehien erabiltzen den teknika
Reconnaissance	Gather Victim Host Information - T1592
Resource Development	Acquire Infrastructure - T1583
Initial Access	Exploit Public-Facing Application - T1190
Execution	Command and Scripting Interpreter - T1059
Persistence	Boot or Logon Autostart Execution - 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



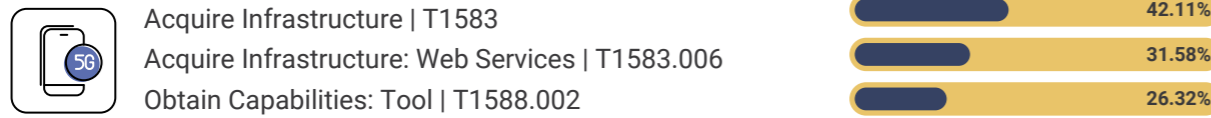
Puntako 10 arinketa (mitigazio)

M1026 Privileged Account Management 13.81%	Politika, kontrol eta tresna batzuk jartzen dira martxan, kontu pribilegiatuak arriskurik gabe administratzeko (adibidez, SYSTEM kontuak, root edo administratzailearenak); hori izaten da kontu pribilegiatuen kudeaketaren oinarria.	M1038 Execution Prevention 10.00%	Sistema batean kode-exekuzioa blokeatzea, aplikazioak kontrolatuz edo script-ak blokeatuz.
M1047 Audit 12.15%	Auditoretzak eta analisiak egitea, ikusteko ea puntu ahulik baduten sistemetan, software segurtasun-gabeetan, konfigurazio segurtasun-gabeetan eta abar.	M1031 Network Intrusion Prevention 8.92%	Sarketei antzemateko sinadurak erabiltzea, trafikoa, hartara, sareko mugetan blokeatzeko.
M1017 User Training 10.27%	Erabiltzaileak prestatzea, errazago konturatu daitezkeen aurkariak noiz ari zaizkien barrura sartu nahian edo manipulatu ahaleginean, ea, horrela, arrakastaz behintzat eraso gutxiago jotzen dizkieten spearphishinga erabiliz, edo ingeniariaritzaren soziala, edo erabiltzailearekiko elkarreragina eskatzen duten beste teknika batzuk.	M1040 Behavior Prevention on Endpoint 8,85%	Prebentzioaren oinarria endpointeko jokamoldea baldin bada, horrek esan nahi du teknologia eta estrategia batzuk erabiltzea, hartara errazago antza hartzeko jarduera maltzurak izan daitezkeenei. Horretarako, aztertuko dugu ea azken gailuan zer jokamolde izan duten prozesuek, artxiboek, APIra egindako deiek eta beste gertaera batzuek.
M1018 User Account Management 10.24%	Ondo kudeatzea nola sortu, aldatu, erabili edo baimentzen ditugun erabiltzaile-kontuak.	M1037 Filter Network Traffic 7.88%	Sareko gailuak eta softwarea erabiltzea endpointetan, sareko sarrerako, irteerako eta albo-mugimenduetako trafikoa iragazteko.
M1051 Update Software 10.14%	Softwarearen eguneratzeak bermatzen du sistemak ahultasun ezagunen aurrean babestuta egotea, fabrikatzaileek emandako adabakiak eta hobekuntzak aplikatuz.	M1048 Application Isolation and Sandboxing 7.74%	Aplikazioen isolamendua eta sandboxing-a kodearen exekuzioa ingurune kontrolatu eta isolatu batera mugatzeko teknikarekin lotuta daude.

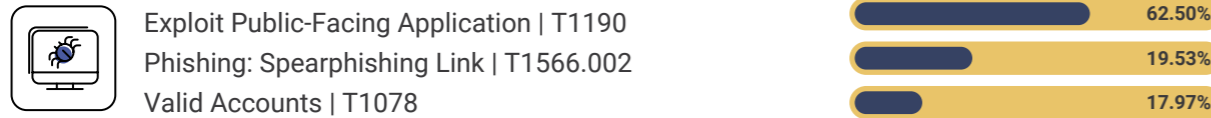
Reconnaissance



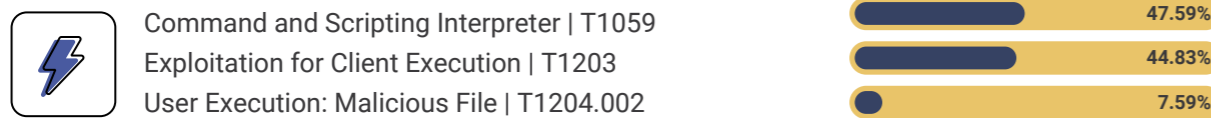
Resource Development



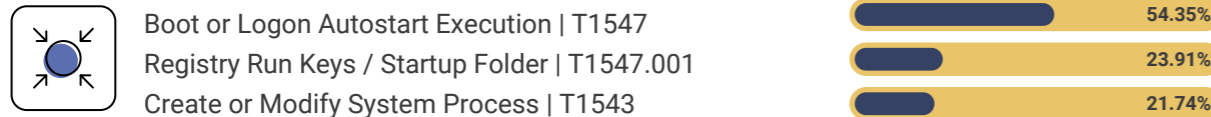
Initial Access



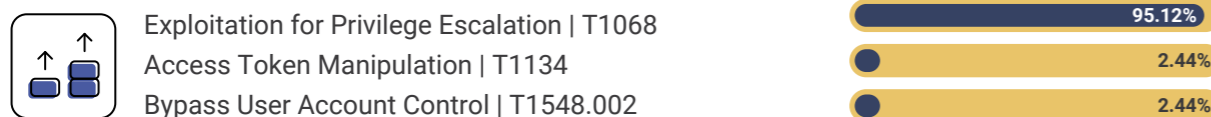
Execution



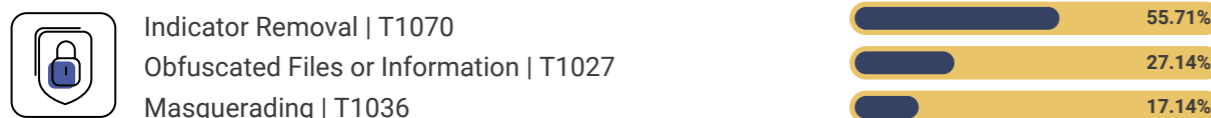
Persistence



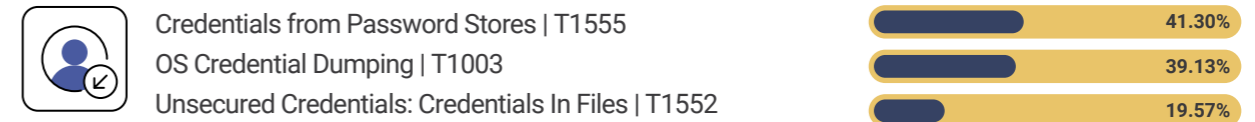
Privilege Escalation



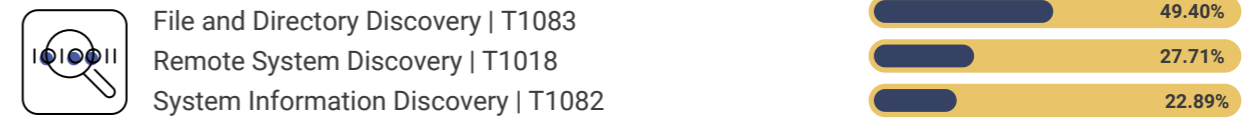
Defense Evasion



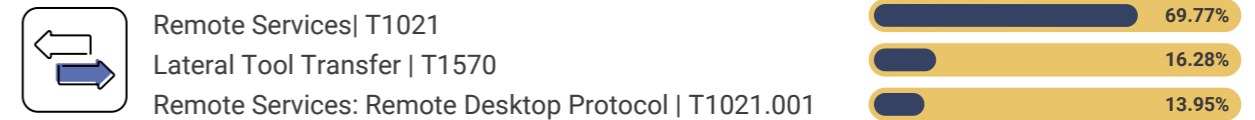
Credential Access



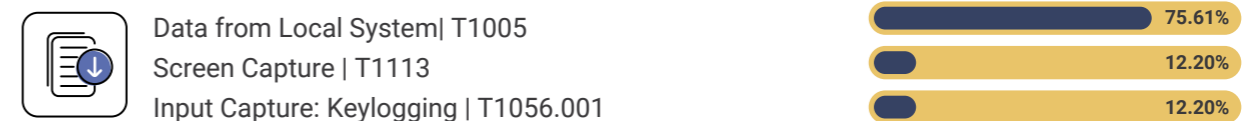
Discovery



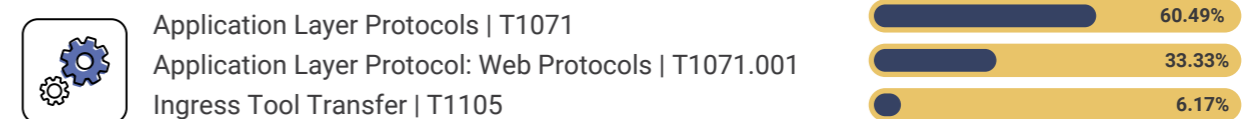
Lateral Movement



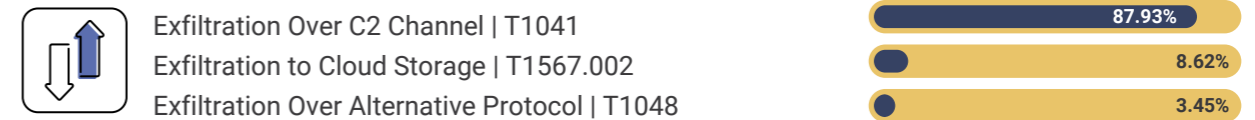
Collection



Command and Control



Exfiltration



Impact



ONDORIOAK

- Aplikazio publikoen ustiapena bektore nagusi gisa finkatzen da. Ezagutze-teknikek helburuari buruzko informazio zehatza zehatz-mehatz biltzeko joera dute.
- Kredentzialak eskuratzeko metodoen ardatza da balio handiko kredentzialak biltzen dituzten pasahitzen biltegiak ustiatzea. Estrategia aldatu egin da, eta datu-bolumen handiak kanporatzen dira, harrapaketa selektiboa egin beharrea.
- Bilakaera horrek agerian uzten du aurkariak direla, oportunitate teknikoa eta azterketa sakona konbinatzen dituztenak, adabakirik gabeko ahuleziak lehenetsiz eta informazioaren kanporatze masiboa maximizatuz.

➔ Horrek presazko laguntza behar du adabakien kudeaketan, kredentzialen biltegien babesean eta iragazketaren monitorizazioan.