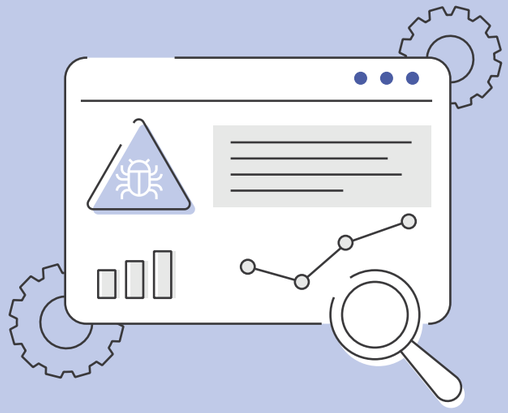
Basque CyberSecurity Centre

Euskadin eragina duten talde kriminalen portaera

2022an, Basque CyberSecurity Centre-an, herritarren eta erakunde publiko zein pribatuen arriskua arintzeko ekimenak abian jartze aldera, Euskadin eragin potentziala duten mehatxuak identifikatzeko eta monitorizatzeko prozesuaren zati gisa, garrantzi bereziko 75 gertakari aztertu ditugu guztira, eta horien kategoria arriskugarritasun handi, oso altu edo kritiko bati dagokio, CCN-STIC 817 gidan, ziberintzidenteen kudeaketari buruzkoan, jasotako sailkapenaren arabera.



Azterketa horretan, besteak beste, erasotzaileek beren ekintza maltzurrak gauzatzeko erabilitako «modus operandi» aren identifikazioa sartzen da, eta horren barruan sartzen dira taktikak, teknikak eta prozedurak.

Ondoren, Mitre ATT&CK framework-a oinarri gisa hartuta, egindako analisietatik ateratako informazioa jasotzen da, erresilientzia-gaitasuna eta, beraz, zibersegurtasuneko heldutasun-maila handitzen lagunduko duten ekimenak lehenesteko eta abian jartzeko balio izan diezaieten erakundeei:

Top 10 teknika (taktika bakoitzak gehien erabiltzen duen teknika)

Taktika	Gehien erabiltzen diren teknika
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 arintzeak

Teknika erabilienetatik abiatuta, arintzeak lehenesten dira.

User Training - M1017

5,66%

Erabiltzaileak trebatzea aurkari baten sarbide edo manipulazio saiakeren berri izan dezaten, spearphishing, gizarte-ingeniaritza eta erabiltzailearen interakzioa inplikatzen duten beste teknika batzuen arrakasta-arriskua murrizteko.

Privileged Account Management - M1026

4,90%

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

Behavior Prevention on Endpoint - M1040

5,33%

Gaitasunak erabiltzea, azken puntuko sistemetan portaera-eredu susmagarriak gerta ez daitezen. Horrek prozesu susmagarri bat, artxiboa, APIra deitzea eta abar barne har ditzake.

Network Intrusion Prevention - M1031

4,57%

Intrusioak detektatzeko sinadurak erabiltzea sarearen mugetako trafikoa blokeatzeko.

Execution Prevention - M1038

5,11%

Arerioek DLL berriak erabil ditzakete teknika hau exekutatzeko. Maltzurra izan daitekeen softwarea identifikatzea eta blokeatzea, bilaketa aginduak bahituz, software legitimoak kargatutako DLL fitxategiak blokeatzeko gai diren aplikazioak kontrolatzeko soluzioak erabiliz.

User Account Management - M1018

4,35%

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

Antivirus/Antimalware - M1049

5,10%

Sinadurak edo heuristikak erabiltzea asmo txarreko softwarea detektatzeko.

Restrict Web-Based Content- M1021

4,13%

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

Disable or Remove Feature or Program - M1042

4,90%

Beharrezkoa ez den eta kaltebera izan daitekeen softwarerako sarbidea ezabatzea edo ukatzea, aurkarien abusua saihesteko.

Software Configuration - M1054

3,59%

Softwarean konfigurazio-aldaketak ezartzea (sistema eragilea ez dena), softwareak funtzionatzen duen moduari lotutako segurtasun-arriskuak arintzeko.

Taktika bakoitzeko top 3 teknika

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