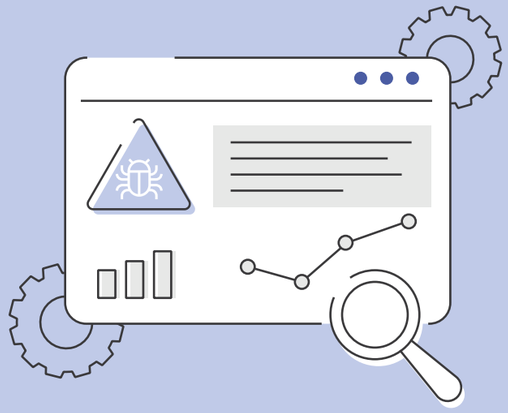
Euskadin eragina duten talde kriminalen modus operandi

2023an, Euskadin eragin potentziala izan duten mehatxuak identifikatu eta monitorizatzeko prozesuari jarraitu zaio, herritarren eta erakunde publiko nahiz pribatuen arriskua arinduko duten ekimenak abian jartzeko. Hori dela eta, Cyberzaintzak, Zibersegurtasunaren Euskal Agentziak, garrantzi bereziko 99 gertakari aztertu ditu guztira, eta horien kategoria arriskugarritasun handia, oso handia edo kritikoa da, ziberintzidenteen kudeaketari buruzko CCN-STIC 817 gidan jasotako sailkapenaren arabera.



Azterketa horrek, besteak beste, erasotzaileek beren ekintza maltzurrak gauzatzeko erabilitako «modus operandi»-aren, taktikak, teknikak eta prozedurak hartzen du barne. Mitre ATT & CK framework-a oinarri gisa hartuta, egindako analisietatik ateratako informazioa biltzen da, erakundeek erresilientzia- gaitasuna eta, beraz, zibersegurtasuneko heldutasun-maila handitzen lagunduko duten ekimenak lehenetsi eta abian jar ditzaten.

Taktika bakoitzak erabiltzen dituen 10 teknika onenak

Taktika	Teknikarik erabiliena
Reconnaissance	Vulnerability Scanning - T1595.002
Resource Development	Malware - T1587.001
Initial Access	Phishing - T1566
Execution	Malicious File - T1204.002
Persistence	Registry Run Keys / Startup Folder File - T1547.001
Privilege Escalation	Exploitation for Privilege Escalation - T1068
Defense Evasion	Deobfuscate/Decode Files or Information - T1140
Credential Access	Brute Force - T1110
Discovery	File and Directory Discovery - T1083
Lateral Movement	Lateral Tool Transfer - T1570
Collection	Archive via Custom Method - T1560.003
Command and Control	Ingress Tool Transfer - T1105
Exfiltration	Exfiltration Over C2 Channel - T1041
Impact	Data Encrypted for Impact - T1468

10 aringarririk onenak

Arintzeak lehentasunez identifikatzen dira, gehien erabiltzen diren tekniketatik abiatuta.

User Training - M1017

%12,85

Erabiltzaileak gaitzea arerioak sartzeko edo manipulatzeko egiten dituen saiakeren berri izan dezaten, spearphishing, gizarte-ingeniaritza eta erabiltzailearen interakzioa inplikatzen duten beste teknika batzuen arrakasta-arriskua murrizteko.

Behavior Prevention on Endpoint - M1040

%10,08

Amaierako puntuaren sistemetan portaera-eredu susmagarririk ez sortzeko gaitasunak erabiltzea. Horrek, prozesu susmagarri bat, artxiboa, APIrako deia eta abar, har litzake.

Execution Prevention - M1038

%12,00

Aurkariek DLL berriak erabil ditzakete teknika hori gauzatzeko. Bilaketa-aginduak bahituz exekutatutako software potentzialki maltzurra identifikatu eta blokeatzea, aplikazioak kontrolatzeko soluzioak erabiliz, software legitimoz kargatutako DLL fitxategiak blokeatzeko gai direnak.

Antivirus/Antimalware - M1049

%8,92

Sinadurak edo heuristikak erabiltzea asmo txarreko softwarea detektatzeko.

Network Intrusion Prevention - M1031

%11,92

Intrusioak detektatzeko sinadurak erabiltzea, sarearen mugetan trafikoa blokeatzeko.

Restrict Web-Based Content- M1021

%7,92

Web gune batzuen erabilera murriztea, deskargak / erantsitako fitxategiak blokeatzea, Javascript blokeatzea, nabigatzailearen luzapenak murriztea, etab.

User Account Management - M1018

%11,00

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

Audit - M1047

%7,69

Sistemen, baimenen, segurtasunik gabeko softwarearen eta konfigurazio ez-seguruen auditoretzak edo eskaneatzeak egitea, balizko ahuleziak identifikatzeko.

Privileged Account Management - M1026

%10,77

Kontu pribilegiatuen sorrera, aldaketa, erabilera eta baimenak administratzea, SYSTEM eta root barne.

Disable or Remove Feature or Program - M1042

%6,85

Beharrezkoa ez den eta kaltebera izan daitekeen softwarerako sarbidea ezabatzea edo ukatzea, aurkariek gehiegikeriak egin ez ditzaten

Taktika bakoitzeko 3 teknika onenak

Reconnaissance

Vulnerability Scanning – T1595.002 %60,00
Active Scanning – T1595 %20,00
IP Addresses – T1590.005 %20,00

Resource Development

Malware – T1587.001 %47,37
Link Target – T1608.005 %31,58
Acquire Infrastructure – T1583 %21,05

Initial Access

Phishing – T1566 %53,33
Spearphishing Attachment – T1566.001 %28,33
Spearphishing Link – T1566.002 %18,33

Execution

Malicious File – T1204.002 %43,64
PowerShell – T1059.001 %30,91
Command and Scripting Interpreter – T1059 %25,45

Persistence

Registry Run Keys / Startup Folder – T1547.001 %35,29
Web Shell - T1505.003 %35,29
Account Manipulation – T1098 %29,41

Privilege Escalation

Exploitation for Privilege Escalation – T1068 %50,00
Boot or Logon Autostart Execution - T1547 %25,00
Group Policy Modification – T1484.001 %25,00

Defense Evasion

Deobfuscate/Decode Files or Information – T1140 %44,44
Obfuscated Files or Information – T1027 %29,63
Modify Registry – T1112 %25,93

Credential Access

Brute Force – T1110 %44,44
Exploitation for Credential Access – T1212 %27,78
Steal Web Session Cookie– T1539 %27,78

Discovery

File and Directory Discovery – T1083 %43,75
Network Share Discovery – T1135 %31,25
Process Discovery – T1057 %25,00

Lateral Movement

Lateral Tool Transfer – T1570 %42,68
Pass the Hash – T1550.002 %28,57
Remote Desktop Protocol – T1021.001 %28,57

Collection

Archive via Custom Method – T1560.003 %36,36
Automated Collection – T1119 %36,36
Adversary-in-the-Middle – T1557 %27,27

Command and Control

Ingress Tool Transfer – T1105 %37,50
Application Layer Protocol – T1071 %31,25
Encrypted Channel – T1573 %31,25

Exfiltration

Exfiltration Over C2 Channel – T1041 %57,14
Automated Exfiltration – T1020 %21,43
Exfiltration Over Alternative Protocol – T1048 %21,43

Impact

Data Encrypted for Impact – T1486 %62,96
Inhibit System Recovery – T1490 %22,22
Service Stop – T1489 %14,81

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza