

## Laburpen exekutiboa

2024aren hasieran agertu zenetik, **RansomHub** taldea ransomware-mehatxu aktiboenetako bat bihurtu da, eta **ransomware-as-a-service (RaaS)** ereduaren barruan hedatzeko gaitasun handienetakoa duena.

RansomHub-ek berehala lortu du posizionatzea, **afiliatuen ekosistema oso aktibo** bati esker, baldintza bereziki errentagarriak eskaintzen baitizkie afiliatuei. Eredu horri esker, taldeak aldibereko intrusioak egin ahal izan ditu hainbat herrialde eta sektoretan, eta biktimak metatu ditu industria ugarian –teknologia, osasuna, manufaktura edo finantza-zerbitzuak, besteak beste–. Horrenbestez, onura ekonomikora bideratutako talde oso oportunistak gisa sendotu da.

Teknikoki, **Windows, Linux eta ESXi** inguruneetara egokitutako karga kaltegarriekin jarduten du, eta horrek aukera ematen dio azpiegitura hibridoek eraso egiteko. Hasierako sarbidea **kredentzial konprometituen, VPN zerbitzu kalteberen edo phishingaren** bidez lortu ohi du. Behin sartutakoan, erreminta legitimoak eta **“living off the land”** teknikak erabiltzen ditu alboko mugimendua egiteko, defentsak ekiditeko eta esfiltrazioa eta zifratzea prestatzeko.

Taldeak **estortsio bikoitzeko** estrategia bat exekutatzen du, eta lapurtutako datuak bere atarian argitaratzen ditu biktimak ordaindu ezean. RansomHub **arrisku handia** da antolakunde eta administrazio publikoentzat, bere gaitasun operatibo handiagatik, profesionalizazioagatik eta azkar hedatzen delako. Horregatik guztiagatik, gomendatzen da **urruneko sarbide-kontrolak indartzea, jarduera susmagarriak monitorizatzea eta sare-segmentazioa aplikatzea**, eta, gainera, **ziberinteligentzia-gaitasunak baliatzea, RansomHub-en kanpainei aurrea hartzeko**.

## Ransomware-taldea: RansomHub

RansomHub **RaaS ereduaren** arabera jarduten duen ransomware-talde bat da, 2024aren hasieratik aktibo dagoena. Lortutako hedapen azkarra egozten zaio afiliatuentzako oso errentagarria den programa bati eta ustez desegindako beste talde batzuetako eragileak bildu izanari, eta horrek gaitasun teknikoak indartu ditu hasieratik.

2025aren hasieran, **DragonForce taldeak** xurgatu zuen RansomHub-en azpiegitura, eta taldea gaur egun inaktibotzat jotzen da marka gisa, nahiz eta bere afiliatuek eta erremintek **arrisku handia izaten jarraitzen duten**.

## Eragindako herrialdeak eta sektoreak

RansomHub-ek hainbat eskualdetako antolakundeei eraso egin die, eragin berezia izanik Estatu Batuetan, Erresuma Batuan, Europan eta Australian. 2025ean, Espainiako zenbait enpresari ere eraso egin die.

Espanian, erasoak nagusiki kontzentratu dira teknologia, osasuna, elikadura eta manufaktura bezalako sektoreetan, eta zerbitzu profesionaletan ere bai.

Maila globalean, biktimak nagusiki **teknologia, eraikuntza, finantzak, osasuna eta manufaktura** sektoreetakoak dira.

Gainera, RansomHub-en biktima gehienak **enpresa txikiak** dira, eta horrek erakusten du ikuspegi oportunistak duela, defentsa-gaitasun eskasa duten helburuetara bideratua.

## Analisi teknikoa

Ikuspegi tekniko-operatibo batetik, RansomHub-ek hasierako eraso-bektore ugari erabiltzea du ezaugarri, hala nola kalteberatasun ezagunak, gizarte-ingeniaritzako teknikak eta malware osagarria erabiltzea hasierako sarbidea eta iraunkortasuna ezartzeko.

Exekuzio-fasean eta alboko mugimenduaren fasean, RansomHub-ek administrazio-erreminta legitimoak eta sareko utilitateak eta framework erasokorrak konbinatzen ditu payloadak zabaltzeko, urruneko scriptak exekutatzeko eta sistemen artean pibotatzeko. Gainera, Windows, Linux eta ESXi-ekin bateragarriak diren payloadak erabiltzen ditu taldeak, eta horrek aukera ematen dio eraginkortasun handiko ingurune korporatibo hibrido eta birtualizatuei eraso egiteko.

**Ezabatu** **gizarte-ingeniaritzako** **erreminta legitimoak** **erabiliz** **Google**-en idatzia, Windows eta Linux sistemen arteko eramangarritasunerako optimizatua.

**Zifratze hibridoko eskema, AES-256 (artxiboak zifratzeko) eta RSA-2048 (gakoak babesteko) konbinatzen dituena.**

**Hasierako sarbidea phishing zuzenduaren bidez, kalteberatasunen ustiapena** VPNetan (adibidez, Fortinet, SonicWall) eta **konprometitutako kredentzialen abusua.**

**Alboko mugimenduak eta esfiltrazioa, erreminta legitimoak erabiliz (LOLBAS),** hala nola AnyDesk, WinSCP eta RClone. PowerShell eta WMIren erabilera ere detektatu da, iraunkortasunerako eta urruneko exekuziorako.

**EDRren ihesa eta tampering-a zerbitzuak desaktibatuz, logak manipulatu eta bitar lausotuak erabiliz.** Aldaera batzuek anti-debugging eta anti-sandbox teknikak inplementatzen dituzte.

## MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
<b>Resource Development</b>	T1588.005 – Obtain Capabilities: Exploits
<b>Initial Access</b>	T1566 – Phishing T1190 – Exploit Public-Facing Application
<b>Execution</b>	T1059 – Command and Scripting Interpreter T1047 – Windows Management Instrumentation
<b>Persistence</b>	T1136 – Create Account T1098 – Account Manipulation
<b>Defense Evasion</b>	T1070 – Indicator Removal on Host T1222 – File and Directory Permissions Modification T1036 – Masquerading T1562 – Impair Defenses: Disable or Modify Tools
<b>Credential Access</b>	T1003 – OS Credential Dumping
<b>Discovery</b>	T1082 – System Information Discovery T1018 – Remote System Discovery T1057 – Process Discovery T1083 – File and Directory Discovery T1046 – Network Service Discovery
<b>Lateral Movement</b>	T1021.001 – Remote Services: Remote Desktop Protocol
<b>Command and Control</b>	T1219 – Remote Access Software
<b>Exfiltration</b>	T1048 – Exfiltration Over Alternative Protocol
<b>Impact</b>	T1486 – Data Encrypted for Impact T1489 – Service Stop T1490 – Inhibit System Recovery

## Arintze-neurriak

### Proaktiboak

- ❑ Logak babestea eta zentralizatzea, ezabatzea eragotziz eta artxibo-/direktorio-baimenetan egiten diren aldaketak monitorizatuz. (T1070 - Indicator Removal, T1222 - Permissions Modification)
- ❑ Sarea segmentatzea eta ostalarien arteko ikusgaitasuna mugatzea, prozesuen, sistemen eta direktorioen aurkikuntza murriztuz. (T1057 - Process Discovery, T1018 - Remote System Discovery, T1083 - File/Directory Discovery, T1082 - System Information Discovery)
- ❑ Offline backupak/backup aldaezinak inplementatzea eta zerbitzu kritikoak babestea, geldialdi susmagarrien edo susperraldia inhibitzeko ahaleginen aurkako alertekin. (T1486 - Data Encrypted for Impact, T1489 - Service Stop, T1490 - Inhibit System Recovery)
- ❑ RDP erabiltzaileak auditatzea eta mugatzea; zerbitzua desgaitzea ezinbestekoa ez bada; gatewayak eta MFA erabiltzea. (T1021.001 - Remote Services: Remote Desktop Protocol)

### Erreaktiboak

- ❑ Sandbox eta mikrosegmentazioa erabiltzea; driver kalteberak blokeatzea eta exploiten aurkako babesa aplikatzea; softwarea eguneratuta mantentzea eta mehatxu-inteligenzia erabiltzea. (T1203 - Exploitation for Client Execution)
- ❑ Antibirus bat erabiltzea, artxibo susmagarriak berrogeialdian automatikoki jartzeko, eta PowerShell desaktibatzea beharrezkoa ez denean. (T1059 - Command and Scripting Interpreter: PowerShell, T1047 - WMI)

## Ondorioak eta gomendioak

2024-2025ean hazkunde eta jarduera gehien izan duen ransomware-taldeetako bat da RansomHub, eta nabarmendu da afiliatuentzako oso errentagarria den RaaS ereduagatik eta tamaina desberdinetako antolakundeak konprometitzeko duen gaitasunagatik –bereziki enpresa txiki eta ertainak–. Bere malgutasun teknikoak –Windows, Linux eta ESXi-n jarduteko gai diren kargekin–, bai eta urruneko sarbideen eta konprometitutako kredentzialen ustiapenean duen ikuspegi oportunistak ere, mehatxu bereziki garrantzitsu bihurtu dute gaur egungo testuinguruan.

RansomHub-en jarduera gero eta handiagoak, RaaS ekosistemaren profesionalizazioarekin batera, nabarmen handitzen du arriskua tamaina guztietako antolakundeentzat, bereziki esposiziopeko urruneko sarbideak dituztenentzat edo kredentzialen kudeaketa ahula dutenentzat. Testuinguru horretan, funtsezkoa da defentsa sakon indartzea, jarduera susmagarriaren detekzio goiztiarra hobetzea eta erantzuteko eta berreskuratzeko plan sendoak ziurtatzea. Gainera, ziberinteligentzia-gaitasunen laguntza izateak aukera ematen du kanpainei aurrea hartzeko eta etorkizuneko erasoen inpaktu potentziala nabarmen murrizteko.

