

## Laburpen exekutiboa

**SpaceBears** taldea Ransomware as a Service Phobos-i estu lotutako **ransomware**-mehatxu berri eta sofistikatu gisa gailendu da. Talde horrek **estortsio bikoitzeko eredu** bat erabiltzen du, eta datuen zifratzea eta informazio hori publikoki filtratzeko mehatxuak konbinatzen ditu, biktimen gaineko presioa handituz. 2024an zehar, SpaceBears-ek arreta erakarri du egindako eraso-kanpaina erasokorregandik eta **antolakunde txiki zein handiei** eragiteko duen gaitasunagatik. Gainera, mehatxu-eragile horrek ondo antolatuta egoteko itxura du, euskarri globaleko sare bat du, eta dark webeko webgune bat erabiltzen du lapurtutako datuak filtratzeko.

Hedatutako neurri teknikoen artean, sarbide-bektore bat erabiltzen da, **RDP (Remote Desktop Protocol) protokoloko kalteberatasunak ustiaturik** eta **mezu elektronikoko kaltegarriak** (phishing) erabiliz. Gainera, **ihes-taktika aurreratuak** erabiltzen ditu, detektatzea saihesteko eta erasoaren eraginkortasuna maximizatzeko.

SpaceBears oso arriskutsua da; izan ere, talde horrek eragina du datuen **eskuragarritasunean**, zifratu egiten dituelako, eta **informazioaren osotasunari eta konfidentziasunari** eragiten die, argitaratzen badira. Gainera, SpaceBears-ek galera ekonomiko handiak, ospearen kalteak eta balizko arau-zehapenak eragin diezazkieke biktimei. Horregatik, **SpaceBears goi-mailako mehatxua da** antolakundeentzat, eta txosten honetan gomendatutako segurtasun-neurriak ezarri behar dituzte mehatxu hori prebenitzeko eta arintzeko.

## Ransomware-taldea: SpaceBears

**SpaceBears** taldea 2024ko apirilean agertu zen, **Phobos malwareari afiliatuta**. Gaur egun, ransomware-as-a-service (RaaS) familia aktiboenetako bat da.

**SpaceBears-ek estortsio bikoitzeko eredu** bat erabiltzen du, biktimaren **informazioa zifratzea** eta lapurtutako datu sentikorrek **filtratzeko mehatxua** konbinatuz. Horretarako, SpaceBears-ek dark webeko filtrazio-webgune bat erabiltzen du. Bertan, lapurtutako informazioaren zati bat argitaratzen du, eta presioa egiten die antolakundeei erreskatea ordaindu dezaten, mehatxu eginez informazio gehiago publiko egingo dutela euren eskaerak betetzen ez badira.

SpaceBears-en ezaugarri bereizgarri bat da bere filtrazio-webgunearen aurkezpenak duen **ikuspegi "korporatiboa"**. Enpresa-irudiak eta enpresa legitimo baten estiloa imitatzen duen tonu profesionala erabiltzen dituzte, eta horrek biktimen gaineko presioa areagotu dezake, beren eskaerak modu formalagoan eta egituratuagoan aurkezten dituztelako. Ikuspegi horrek estortsio-estrategia kalkulatu eta profesionala islatzen du, euren erasoaren eraginkortasuna maximizatzeko diseinatua.






## Eragindako herrialdeak eta sektoreak

SpaceBears-en biktimen artean enpresa txiki eta ertainak daude, eta tamaina handiagoko enpresa batzuk ere bai. Gehien kaltetutako sektoreen artean **informazioaren teknologiak, manufaktura eta zerbitzu profesionalak** daude, eta horiek ohiko jomugak dira, datuen kudeaketan eta sare-azpiegituretan dituzten kalteberatasunak direla-eta. Geografiari dagokionez, SpaceBears-ek hainbat eskualdetako antolakundeei eragin die, baina jarduera **Ipar Amerikan eta Europan** kontzentratzen du nagusiki. Gaur egun, **Espainiak bost biktima** erregistratu ditu guztira. Horietatik hiru azken hilabeteetan izan dira, eta horrek erakusten du herrialde horretako erasoak goranzko joeran daudela.

## Analisi teknikoa

SpaceBears-ek **phishing-mezuak** erabiltzen ditu edo **RDP protokoloan ezagunak diren kalteberatasunak** ustiatzen ditu biktimen sareetan infiltratzeko. Phobos ransomwarearekin lotu ohi den teknika bat da. Sartu ondoren, SpaceBears ransomwareak **bolumeneko segurtasun-kopiak eta datuak babesteko beste mekanismo batzuk desaktibatzen** ditu, eta horrek zaildu egiten du informazioa berreskuratzea erreskatea ordaindu gabe. Gainera, beste ransomware-aldaera batzuek bezala, SpaceBears-ek ihes-teknika aurreratuak erabil ditzake detektatzea saihesteko eta erasoaren eraginkortasuna maximizatzeko. Azkenik, ransomwareak **datuak zifratzen ditu** eta **estortsio bikoitza** egiten du onura ekonomikoak lortzeko.

### Ezaugarri tekniko nagusiak:

-  **Phobos-en oinarritutako ransomwarea:** SpaceBears-ek Phobos ransomwarearen oinarri-kode bera erabiltzen du, eta horrek banaketa azkarra eta efizientea egiteko aukera ematen dio.
-  **RDP kalteberatasun ezagunen ustiapena:** RDP protokoloko kalteberatasunak erabiltzen ditu biktimen saretarako urruneko sarbidea lortzeko, konfigurazio ez-seguruak edo kredentzial ahulak aprobetxatuz.
-  **Segurtasun-kopiak desaktibatzea:** Segurtasun-kopiak ezabatzen ditu, eta datuak leheneratzea blokeatzen du, erreskaterik ez badago.
-  **Zifratze sendoa erabiltzea:** AES-256 konbinazio bat erabiltzen du zifratze simetrikorako eta RSA-1024 zifratze asimetrikorako.
-  **Estortsio bikoitzeko eredia:** SpaceBears-ek estortsio bikoitzaren eredia hartu du: biktimen artxiboak zifratzeaz gain, datu sentikorak argitaratzeko mehatxua ere egiten du, erreskatea jaso ezean.

## MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
<b>Initial Access</b>	T1133 – External Remote Services T1566.001 – Phishing: Spearphishing Attachment
<b>Execution</b>	T1059.003 – Command and Scripting Interpreter: Windows Command Shell T1204.002 – User Execution: Malicious File
<b>Persistence</b>	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
<b>Privilege Escalation</b>	T1134 – Access Token Manipulation T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control
<b>Defense Evasion</b>	T1562.004 – Impair Defenses: Disable or Modify System Firewall T1562.001 – Impair Defenses: Disable or Modify Tools T1070.001 – Indicator Removal: Clear Windows Event Logs T1218.010 – System Binary Proxy Execution: Mshta
<b>Credential Access</b>	T1003.001 – OS Credential Dumping: LSASS Memory
<b>Discovery</b>	T1049 – System Network Connections Discovery T1057 – Process Discovery T1083 – File and Directory Discovery
<b>Lateral Movement</b>	T1021.001 – Remote Services: Remote Desktop Protocol
<b>Collection</b>	T1560.001 – Archive Collected Data: Archive via Utility
<b>Command and Control</b>	T1071.002 – Application Layer Protocol: Ingress Tool Transfer
<b>Exfiltration</b>	T1048 – Exfiltration Over Alternative Protocol
<b>Impact</b>	T1486 – Data Encrypted for Impact T1490 – Inhibit System Recovery

## Arintze-neurriak

### Proaktiboak

- ❑ Urruneko sarbideak mugatzea eta faktore anitzeko autentifikazioa aplikatzea. (T1133/T1021 - External Remote Services/ Remote Desktop Protocol)
- ❑ Hasiera automatikoko gakoak monitorizatzea eta babestea. (T1547.001 - Registry Run Keys / Startup Folder)
- ❑ Aplikazioen kontrola erabiltzea egokia denean, eta eguneratu gabe dauden edo ezinbestekoak ez diren erremintak ezabatzea. (T1562.001 - Impair Defenses)
- ❑ ASR eta Credential Guard gaitzea, NTLM eta Wdigest mugatzea eta pasahitz eskusiboak erabiltzea. (T1003.001 - OS Credential Dumping: LSASS Memory)
- ❑ Pribilegioak mugatzea, sarea segmentatzea, urruneko sarbideak kontrolatzea eta kontsultak eta artxiboetarako sarbideak auditatzea. (T1083 - File and Directory Discovery)
- ❑ Baimendu gabeko kodea exekutatzea prebenitzea, aplikazioen kontrola, scripten blokeoa eta, orobat, exekuzioa prebenitzeko beste mekanismo batzuk ezarriz. (T1059.003 - Command and Scripting Interpreter: Windows Command Shell)

### Erreaktiboak

- ❑ Eraso-azalera murrizteko arauak (ASR) gaitzea artxibo kaltegarriak exekutatzea saihesteko. (T1204 - User Execution: Malicious File)
- ❑ Sareko gailuak eta endpoint-eko softwarea erabiltzea sarearen sarrerako, irteerako eta alboko trafikoa iragazteko. (T1048 - Exfiltration Over Alternative Protocol)

## Ondorioak eta gomendioak

SpaceBears-ek arrisku handia planteatzen die antolakundeei, ez bakarrik datuak zifratzearen eta estortsio finantzarioaren zuzeneko kalteengatik, baita informazioaren eskuragarritasunean eta konfidentzialtasunean izan ditzakeen ondorioengatik eta ospe eta konfiantzari lotutako ondorioengatik ere. SpaceBears bezalako taldeek gizarte-ingeniaritza erabiltzen dute eta segurtasun-azpiegiturako kalteberatasunak ustiatzen dituzte, batez ere urruneko sarbidearekin lotutakoak, sare korporatiboetan efizientziaz infiltratzeko, informazioa zifratzeko eta antolakundeei estortsioa egiteko helburuarekin.

Horregatik guztiagatik, SpaceBears mehatxu aurreratua da, eta erantzun integral eta proaktiboa eskatzen du. Antolakundek prest egon behar dute magnitude horretako eraso bati aurre egiteko, segurtasun-teknologia aurreratuak ezarriz, langileen etengabeko prestakuntzaren bidez eta hondamendien aurrean berreskuratzeko estrategiak planifikatuz.

