

## Laburpen exekutiboa

Warlock **talde zibergaizkile** bat da, **ransomware-as-a-service (RaaS)** ereduaren arabera jarduten duena, eta, horrela, erasoan zuzeneko atribuzioa zailduz eta malwarearen hedapen-abiadura eta irismena zabalduz. 2025eko ekainean jendaurrean agertu zenetik, taldeak aste gutxi barru abiarazi zituen **eskala globaleko** konpromiso-kanpaina ugari, **Microsoft SharePoint-en kalteberatasunak ("ToolShell")** ustiatuz, inpaktu bereziarekin **azpiegitura kritikoetan eta teknologiaren eta telekomunikazioen sektorean**. Gainera, taldearen jarduera Storm-2603rekin (Txinako jatorriko taldea) lotu dute hainbat analistak, krimen/estatua eredu hibridoa sendotuz horrela.

Bere eragiketa-kateak barnean hartzen ditu hasierako sarbidea kalteberatasun ezagunen bidez (**CVE-2025-49704, CVE-2025-49706, CVE-2025-53770 eta CVE-2025-53771**), webshell-en hedapena, alboko mugimendua erreminta legitimoekin eta informazio sentikorraren esfiltrazioa. Beste RaaS talde batzuek ez bezala, Warlock-ek **lapurtutako datuen enkante pribatua** baliatu du datuak saltzeko dark web klasikoaren alternatiba gisa, ospe- eta betetze-arriskua handituz zifratzetik harago.

Horren ondorioz, Warlock **oso arriskutsua** da esposiziopeko SharePoint on-premises duten antolakundeentzat. Gainera, **eraso-probabilitatea handia** da, **oportunista eta modularra** delako. Izan ere, Warlock gai da esposizio-leihoak kapitalizatzeko antolakundearen sarbidea, iraunkortasuna eta kontrola azkar lortzeko, inpaktu operatiboa eta estortsio-presioa maximizatuz datuen lapurretaren eta monetizazioaren bidez.

## Ransomware-taldea: Warlock

Warlock **2025eko ekainean** sortu zen, Errusiako **RAMP** foroan argitaratutako **afiliatuak erakartzeko kanpaina** batetik abiatuta. Taldearen lehen kanpainetatik, taldea nabarmendu zen **esfiltratutako datuen enkante pribatua** egiteagatik, onura ekonomikoa maximizatuz eta bere eragiketen esposizio publikoa murriztuz.

Gaur egungo ikerketek erakusten dutenez, **lankidetzak teknikoak** du Txinako jatorria duen **Storm-2603** entitate gaiztoarekin, Microsoft SharePoint ustiatzeko "ToolShell" kalteberatasun-katea eskainiko zukeena. Eredu horrek **exploit-hornitzaileen eta ransomware-operadoreen arteko aliantza taktiko** baten hipotesia indartzen du, egile-harreman zuzena baino.

RaaS ekosisteman, Warlock-ek **operadore nagusi eta afiliatuen koordinatzaile** gisa jarduten du, azpiegitura, zifratzaileak eta ordainketak kudeatzeko zerbitzuak eskainiz; afiliatuek, berriz, hasierako intrusioa eta datuen esfiltrazioa exekutitzen dituzte.

## Eragindako herrialdeak eta sektoreak

Azken hilabeteetan berretsitako eta talde honi esleitutako intrusioek **gutxienez 61 antolakunde barne hartzen dituzte 21 herrialde desberdinetan**. Konpromisoak detektatu dira **Ipar Amerikan, Europan, Asian eta Afrikan**, eta bereziki **AEBn, Erresuma Batuan, Japonian, Indian eta Frantzian**. Gehien kaltetutako sektoreek barnean hartzen dituzte **teknologia, telekomunikazioak, finantza-zerbitzuak, manufaktura, nekazaritza, gobernu-organismoak eta funtsezko zerbitzuak**.





Gaur egun, Espainian Warlock-ek konprometitutako antolakunde bakarra detektatu da, baina aurreikusten da datozen hilabeteetan gehiago izatea.

## Analisi teknikoa

Warlock-ek antolakundeak konprometitzen ditu, Interneten esposiziopean dauden Microsoft SharePoint on-premises-en **ToolShell** kalteberatasun-katea ustiatuz. Sistemetara sartu ondoren, **iraunkortasuna** ezartzen du, **segurtasun-kontrolak desaktibatzen ditu** prozesu eta zerbitzuen aurrez konfiguratutako zerrenden bidez, **pribilegioak handitzen ditu** eta **alboko mugimenduak** egiten ditu living-off-the-land erreminten bidez. Ondoren, komunikazioak hasten ditu bere **aginte- eta kontrol-zerbitzariarekin (C2)**, eta **informazio-esfiltrazioa** egiten du hodeiko biltegiatze-zerbitzuetara.

Azkenik, Warlock-en fitxategi-zifratzaileak **eskala handian** zifratzen ditu fitxategiak, erreskate-oharrak uzten ditu (How\_to\_decrypt\_my\_data.txt), eta x2anylock luzapena gehitzen die fitxategiei.

### Ezaugarri tekniko nagusiak:

-  **Microsoft SharePoint** on-premises ustiatzea **CVE-2025-49704** eta **CVE-2025-49706** bidez eta **CVE-2025-53770** eta **CVE-2025-53771** bypass-en bidez (ToolShell).
-  **Alboko mugimenduak** egiten ditu **living-off-the-land** erreminten bidez (PsExec, Impacket eta WMI), eta **GPOren** abusua egiten du, payload modu masiboan hedatzeko.
-  **Datuak esfiltratzea** Rclone erremintaren bidez hodeiko biltegiatze-zerbitzuetara.
-  **.x2anylock luzapena** gehitzen die fitxategi zifratuei, eta erreskate-oharrak bidaltzen ditu (“**How\_to\_decrypt\_my\_data.txt**” eta “**How to decrypt my data.log**”).

## MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
<b>Initial Access</b>	<b>T1190</b> – Exploit Public-Facing Application <b>T1203</b> – Exploitation for Client Execution
<b>Execution</b>	<b>T1059.001</b> – Command and Scripting Interpreter: PowerShell
<b>Persistence</b>	<b>T1505.003</b> – Server Software Component: Web Shell <b>T1543.003</b> – Create or Modify System Process: Windows Service <b>T1053</b> – Scheduled Task/Job
<b>Defense Evasion</b>	<b>T1112</b> – Modify Registry <b>T1036</b> – Masquerading <b>T1562</b> – Impair Defenses <b>T1497</b> – Virtualization/Sandbox Evasion
<b>Credential Access</b>	<b>T1003.001</b> – OS Credential Dumping: LSASS Memory
<b>Discovery</b>	<b>T1082</b> – System Information Discovery <b>T1057</b> – Process Discovery <b>T1007</b> – System Service Discovery <b>T1135</b> – Network Share Discovery <b>T1083</b> – File and Directory Discovery
<b>Lateral Movement</b>	<b>T1021.006</b> – Remote Services: Windows Remote Management <b>T1021.002</b> – Remote Services: SMB/Windows Admin Shares
<b>Command and Control</b>	<b>T1105</b> – Ingress Tool Transfer
<b>Exfiltration</b>	<b>T1567.002</b> – Exfiltration Over Web Service: Exfiltration to Cloud Storage <b>T1041</b> – Exfiltration Over C2 Channel
<b>Impact</b>	<b>T1486</b> – Data Encrypted for Impact

## Arintze-neurriak

### Proaktiboak

- ❑ Sistemak aldian-aldian eskaneatzea kalteberatasunen bila, eta prozedurak ezartzea detektatutako kalteberatasunak konpontzeko. (T1190 - Exploit Public-Facing Application)
- ❑ 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. (T1082 - System Information Discovery)

### Erreaktiboak

- ❑ Ustiapen-fasean portaera anomaloa detektatzen duten segurtasun-aplikazioak (EMET edo WDEG) erabiltzea. (T1203 - Exploitation for Client Execution)
- ❑ Antibirus bat erabiltzea fitxategi susmagarriak berrogeialdian automatikoki jartzeko eta PowerShell desaktibatzea beharrezkoa ez denean. (T1059.001 - Command and Scripting Interpreter: PowerShell)
- ❑ Proxy zerbitzarien bidezko sareko nabigazioa mugatzea baimendu gabeko kanpoko zerbitzuak erabiltzea eragozteko. (T1567.002 - Exfiltration to Cloud Storage)

## Ondorioak eta gomendioak

Warlock mehatxu sofistikatu, modular eta oportunistak da, kalteberatasun ezagunak ustiatzera eta onura maximizatzen bideratua, lapurretaren, estortsioaren eta datuen enkantearen bidez.

### Lehentasuneko gomendioak:

- ❑ Adabaki-politika arinak inplementatzea eta zerbitzuen esposizioaren etengabeko egiaztapena.
- ❑ Urruneko sarbidea murriztea eta sarea segmentatzea alboko mugimenduak mugatzeko.
- ❑ Offline segurtasun-kopiak mantentzea eta haiek leheneratzea probatzea.
- ❑ Living-off-the-land jardura eta transferentzia susmagarriak identifikatzeko gai diren detekzio-mekanismoak (EDR/XDR) hedatzea.
- ❑ Underground foroak eta OSINT iturriak monitorizatzea, Warlock-i lotutako enkante pribatuak edo filtrazioak detektatzeko.

Neurri horiek aplikatzeak, zibersegurtasunaren ikuspegi proaktibo eta koordinatuarekin batera, aukera emango du eraso-azalera murrizteko, jardura anomaloa fase goiztiarretan detektatzeko eta balizko gorabeheren inpaktu operatiboa arintzeko.

