

## Laburpen exekutiboa

Sinobi ransomware bat da, zerbitzu gisa jarduten duena (RaaS), 2025eko erdialderako identifikatua eta ransomwarearen panoraman estortsio bikoitzeko talde gisa sortu dena. Malware honek biktimen informazio sentikorra lapurtzen du, eta dark webeko atarietan argitaratzen du, erreskate bat ordaintzeko presioa eginez filtratzea saihesteko. Bere kanpainak lotu izan dira **VPNaren kredentzial konprometituekin hasierako sarbidea lortzearekin** (zenbait kasu dokumentatu dira SonicWall kredentzialekin), **urruneko sarbideko bektoreen ustiapenarekin** eta informazioa esfiltratzeko **tresna legitimoen erabilerarekin** (*living-off-the-land*).

**Maila teknikoan**, malwareak sareko unitate lokal eta partekatuetako artxiboak zifratzen ditu, erreskate-oharrak eta **.SINOBI luzapenarekin** markatutako artxiboak utziz. Zifratzeko, Curve-25519 Donna erabiltzen du AES-128-CTRrekin batera, eta horrek ezinezkoa egiten du erasotzailearen Curve-25519 gako pribaturik gabe berreskuratu ahal izatea. Teknika hau beste ransomware-aldaera batzuen berdina da, Babuk-ena, esate baterako.

Operatiboki, badirudi Sinobik lehenagoko familien **kodea eta metodologia berrerabiltzen** dituen entitate gisa jokatzeko duela; Lynx familiarekiko antzekotasun garrantzitsuak ikusi dira (kodearen mailan, antzeko teknika kriptografikoak eta antzeko filtrazio-guneak). Horrek azkar eskalatzeko eta kanpaina korporatiboetan egokitzeko bide ematen du.

Delituzko negozioaren ikuspegitik, Sinobik datu-bitartekari eta estortsio bikoitzeko operadore gisa jarduten du. Horretarako, atari bat du Tor sarean, eta bertan biktimen zerrendak eta datu-zatiak argitaratzen ditu, eta presio-epeak eta larderia erabiltzen ditu erreskatea ordaintzera behartzeko.

## Ransomware-taldea: Sinobi

**Sinobi** 2025ean identifikatutako ransomware-talde bat da, eta **Lynx**-en bilakaera posibletzat jotzen da, oso antzeko kodea, filtrazio-guneen egiturak eta modus operandi dituztelako. **Ransomware-as-a-Service** (RaaS) eredu baten bidez jarduten du, afiliatuei **estortsio bikoitzeko** erasoak exekutatzeko tresnak eta euskarria eskainiz, sistemen zifratzea *dark web*eko atarietako datuen filtrazioarekin konbinatzen dutenak. Berretsitako erasoetan, ransomwareak “.SINOBI” luzapena jartzen die artxibo zifratuei eta erreskate-oharra sortzen du “README.txt” izenarekin.

## Eragindako herrialdeak eta sektoreak

Sinobi talde nahiko berria den arren, **2025aren erdialdetik** aurrera modu iraunkorrean hedatzen hasi da bere jarduera, helburu kopuru handi samarra lortu arte (87 biktima berretsi dira). Biktima horiek **Estatu Batuetakoak** dira nagusiki, eta ondoren Erresuma Batukoak, Kanadakoak eta Frantziakoak.

**Espanian**, gutxienez, industria- eta manufaktura-sektorean jarduten duen LASER AUTOMOTIVE VALENCIA SL enpresaren aurkako eraso bat berretsi da. Taldeak 2025eko urriaren 1ean aldarrikatu zuen eraso bere **leaksitean**.


Sinobik gehien erasotako sektoreei dagokienez, datu publikoek erakusten dute **manufakturan, eraikuntzan, energian, osasunean, hezkuntzan eta finantza-zerbitzuetan** zentratu direla batik bat.


## Analisi teknikoa


Sinobi RaaS motako ransomwarea da, eta erasoak konprometitutako kredentzialen bidez hasten ditu (adibidez, SonicWall SSL VPN kredentzialekin), edo kalteberatasunen bidez; alboko mugimenduak egiten ditu, pribilegioen eskalada eta datuen esfiltrazioa. Gainera, segurtasun-kopiak ezabatzen ditu eta zerbitzu kritikoak geldiarazten ditu berreskuratzea eragozteko.


Sinobiren zifratze-prozesuak kriptografia modernoa aplikatzen du: artxiboak AES eta Curve25519 algoritmoen bidez zifratzen ditu, eta .sinobi luzapena gehitzen die.


### Ezaugarri tekniko nagusiak:

 **Ransomware-as-a-Service (RaaS)** gisa jarduten du: operadore zentralak, erasoak koordinatzen eta pertsonalizatzen dituzten afiliatuekin batera.

 **Hasierako sarbidearen bektoreak:** konprometitutako kredentzialak, esposiziopean jarritako VPNak, urruneko zerbitzuen ustiapena eta enpresa-aplikazioetako kalteberatasunak.

 **Fitxategiak zifratzea:** AES eta Curve25519 konbinatzen ditu eta .sinobi luzapena gehitzen die fitxategi zifratuei.

 **Ihes-teknikak:** segurtasun-kopiak ezabatzea, zerbitzu kritikoak amaitzea eta datuak esfiltratzeko tresna legitimoak erabiltzea.

 **Esfiltrazioa:** Rclone erabiltzea unitate mapatuetako edo partekatuetako fitxategiak erasotzaileak kontrolatutako kanpoko zerbitzarietara kopiatzeko.

## MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
<b>Initial Access</b>	T1190 – Exploitation of Public-Facing Application T1133 – External Remote Services
<b>Execution</b>	T1059.001 – Command and Scripting Interpreter: PowerShell T1203 – Exploitation for Client Execution T1059.003 – Command and Scripting Interpreter: Windows Command Shell
<b>Persistence</b>	T1136.001 – Create Account: Local Account T1543.003 – Create or Modify System Process: Windows Service
<b>Privilege Escalation</b>	T1055.001 – Process Injection: Dynamic-link Library Injection T1543.003 – Create or Modify System Process: Windows Service T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1548 – Abuse Elevation Control Mechanism
<b>Defense Evasion</b>	T1070 – Indicator Removal on Host T1027 – Obfuscated Files or Information T1140 – Deobfuscate/Decode Files or Information T1036.005 – Masquerading: Match Legitimate Name or Location T1222 – File and Directory Permissions Modification T1562.001 – Impair Defenses: Disable or Modify Tools
<b>Discovery</b>	T1007 – System Service Discovery T1012 – Query Registry T1057 – Process Discovery T1016 – System Network Configuration Discovery T1083 – File and Directory Discovery
<b>Lateral Movement</b>	T1021 – Remote Services T1091 – Replication Through Removable Media
<b>Command and Control</b>	T1071.001 – Application Layer Protocol: Web Protocols T1090.002 – Proxy: External Proxy T1095 – Non-Application Layer Protocol T1572 – Protocol Tunneling
<b>Impact</b>	T1486 – Data Encrypted for Impact T1485 – Data Destruction T1489 – Service Stop

## Arintze-neurriak

### Proaktiboak

- ❑ Softwarea eguneratuta mantentzea eta segurtasun-adabakiak aplikatzea. (T1190 – Exploitation of Public-Facing Application)
- ❑ Urruneko sarbideak mugatzea eta faktore anitzeko autentifikazioa aplikatzea. (T1133 / T1021 – External Remote Services / Remote Services)
- ❑ Sinatu gabeko scripten exekuzioa mugatzea eta interpreteen erabilera erregistratzea. (T1059.001 / T1059.003 – PowerShell / Windows Command Shell)
- ❑ EDR erabiltzea eta prozesu pribilegiatuen osotasuna babestea. (T1055.001 – Process Injection)
- ❑ Kontuen eta zerbitzuen sorrera auditatzea eta mugatzea. (T1136.001 / T1543.003 – Create Account / Create or Modify System Process)
- ❑ Hasiera automatikoko gakoak monitorizatzea eta babestea. (T1547.001 – Registry Run Keys / Startup Folder)
- ❑ Logak babestea eta prozesu lausotuak edo izena aldatutakoak monitorizatzea. (T1070 / T1027 / T1140 / T1036.005 – Indicator Removal / Obfuscation / Masquerading)

### Erreaktiboak

- ❑ USB gailuen erabilera blokeatzea edo kontrolatzea. (T1091 – Replication Through Removable Media)
- ❑ Ustiapen-fasean portaera anomaloa detektatzen duten segurtasun-aplikazioak (EMET edo WDEG) erabiltzea. (T1203 – Exploitation for Client Execution)

## Ondorioak eta gomendioak

Sinobi **2025aren erdialdean** sortu zen, eta berehala kokatu da **urteko ransomware-mehatxu** nagusien artean, hedapen azeleratuagatik eta erasoen irismenagatik nabarmenduz. Bi hilabete eskasetan, dozenaka erakunde konprometitu ditu (gehienak Estatu Batuetan), eta horrek ondo **antolatutako eta inpaktu globaleko** operazioa duela erakusten du.

Hasieran pentsatu zen Sinobi Lynx-en berragertzea izan zitekeela, antzeko kodea eta filtrazio-plataformak zituztelako. Hala ere, gaur egungo azterketek erakusten dute talde desberdinak direla, baina lotura dutela, seguruenik baliabideak edo azpiegitura partekatzen baitituzte. Lynx-ek, INC Ransom-ekin batera, aktibo jarraitzen du, eta horrek iradokitzen du **lankidetzan aritzen den edo tresnak trukutzen dituen ekosistema kriminal interkonektatu** bat dagoela.

**Sinobirekiko arriskua murrizteko**, gomendatzen da **urruneko sarbideak MFArekin babestea, segurtasun-kopia seguruak mantentzea, sarea segmentatzea eta erabiltzaile-pribilegioak mugatzea**. Gainera, funtsezkoa da **detekzio aurreratuko tresnak erabiltzea eta mehatxu aktiboak monitorizatzea**, balizko erasoeraz azkar erantzuteko.

