Ransomware-taldea: DeadLock

Laburpen exekutiboa

DeadLock ransomware-familia **informazioa zifratzera eta estortsio ekonomikora bideratuta dago**. Konprometitutako artxiboen izenak biktimaren identifikatzaile esklusibo batekin eta .dlock luzapenarekin aldatzen ditu. Malwareak **infekzio-bektore ugari** erabiltzen ditu –softwarearen legez kanpoko kopiak, infektatutako mezu kaltegarrien eranskinak eta deskarga engainagarriak barne–. Horrela, ekipo pertsonalak nahiz lan-estazio korporatiboak arriskuan jar ditzakete erasotzaileek. Biktima den sisteman exekutatzea lortu ondoren, DeadLock-ek erabiltzaile-fitxategiak zifratzen ditu, eta erreskate-ohar bat sortzen du kriptodiru bidez ordaintzeko jarraibideekin.

DeadLock **arrisku larria** da antolakundeentzat; izan ere, **etenaldi operatibo kritikoak** eragin ditzake, informazioaren galera jarraitua eragin, negozioaren jarraitutasuna arriskuan jarri eta antolakundearen ospeari kalte nabarmena eragin diezaioke. Horregatik, DeadLock **arrisku handiko mehatxutzat hartu behar da edozein antolakunderentzat**, bereziki segurtasun-kontrol ahulak, adabakiak kudeatzeko jardunbide ez-efizienteak, datu lokalen mendekotasun operatibo kritikoak edo heldu gabeko zibersegurtasun-kultura badituzte.

Arriskua arintzeko, funtsezkoak dira prebentzioa ardatz duen ikuspegia ezartzea, segurtasun-kopia sendo eta isolatuak egitea eta detekzio goiztiarra, portaeran oinarritutako segurtasun-konponbideen bidez.

Ransomware-taldea: DeadLock

DeadLock ransomwarea artxiboak zifratzean espezializatuta dago, **biktimak ekonomikoki estortsionatzeko helburuarekin**. Malwareak identifikatzaile esklusibo bat esleitzen dio biktima bakoitzari, eta identifikatzaile hori erabiltzen da artxibo zifratuen izenean eta erreskate-oharrean. Horrek aukera ematen die erasotzaileei estortsioak banaka kudeatzeko eta ordainketak deszifratze-gako espezifikoekin korrelazionatzeko.

DeadLock-ek hainbat **infekzio-bektore eta gizarte-ingeniaritzako teknika** erabiltzen ditu, eta horrek erakusten du gaitasuna duela zibersegurtasunaren arloan heldutasun eskaseko inguruneetan jarduteko. Exekutatu ondoren, ransomwareak **biktimaren artxiboak zifratzen** ditu (“.dlock” luzapenarekin eta dagokion identifikatzailearekin aldatzen ditu artxiboen izenak) ,eta kriptodirutan ordaintzea eskatzen duen **erreskate-ohar** bat zabaltzen du (Bitcoin edo Monero erabiliz, esate baterako) Gainera, komunikazio-kanal bat eskaintzen du, Session Messenger mezularitza anonimoko aplikazioaren bidez, erreskatea negoziatzeko.

DeadLock **konplexutasun tekniko baxuko edo ertaineko malware gisa posizionatzen da, baina eraginkortasun operatibo handikoa** aldi berean, bere banaketa-bektore zabala eta estortsio pertsonalizatuko eredua dela-eta.

Eragindako herrialdeak eta sektoreak

DeadLock **talde oportunistatzat eta nazioartekotzat** hartu daiteke, ez baitu bere jarduera herrialde edo sektore jakin batera mugatzen. Hala ere, ransomware honek sistemaren hizkuntza egiaztatzen du exekutatzen den bitartean, eta gelditu egiten da alfabeto zirilikoan oinarritutako konfigurazioak detektatzen baditu.

Portaera horrek malware batzuen praktika islatzen du: herrialde edo eskualde jakin batzuei erasotzea berariaz saihesten dute, tokiko agintarien arreta murrizteko edo beren jurisdikzioetan ondorioak saihesteko.

Analisi teknikoa

Ikuspegi teknikotik, DeadLock-en eraso-katea **erabiltzaileak** fitxategi kaltegarri bat **borondatez exekutatzen duenean hasten da**. Infektatutako **USB unitateen bidezko infekzioa ere aurreikusten da, eta euskarri tekniko faltsuko atarien** bidezko infekzioa ere bai; halako atariek “adabakiak” deskargatzera bultzatzen dute, baina benetan ransomwarea kargatzen dute.

Biktima den sisteman exekutatzea lortu ondoren, DeadLock-ek **erabiltzaile-fitxategiak zifratzen** ditu: fitxategi bakoitza .dlock luzapenarekin zifratzen du. Zifratzearen ondoren, malwareak erreskate-ohar bat sortzen du testu soilean, eta mahaigainaren atzeko planoa aldatzen du, konpromisoa bisualki berresteko.

Zifratze-fasearen ondorengo portaerari dagokionez, ransomwareak artxibo gehiago zifratzen jarraitu dezake, kredentzialak biltzen, atzeko ateak gaitzen edo sare lokaleko beste ekipo batzuetara edo baliabide partekatuetara alboko mugimenduak egiten saiatzen.

Ezaugarri tekniko nagusiak:

- **Zifratzea:** DeadLock-ek zifratu egiten ditu artxiboak, eta izena aldatzen die, biktima bakoitzari identifikatzaile esklusibo bat gehituz .dlock luzapenarekin batera.
- **Hasierako sarbidea:** Erabiltzaileek exekutatutako fitxategi kaltegarrien bidez, infektatutako USBen bidez eta euskarri-atari faltsuen bidez.
- **Operadorearen profila:** Alfabeto zirilikoarekin konfiguratutako sistemetan fitxategiak zifratzea saihesten du.
- **Living Off the Land erremintak erabiltzea:** Sistemaren erreminta legitimoak erabiltzea ekipoak eskaneatzeko edo aurkitzeko.

MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
Initial Access	**T1078** — Valid Accounts **T1133** — External Remote Services
Execution	**T1047** — Windows Management Instrumentation **T1059.003** — Command and Scripting Interpreter: Windows Command **T1106** — Native API
Persistence	**T1543.003** — Create or Modify System Process: Windows Service
Privilege Escalation	**T1055** — Process Injection
Defense Evasion	**T1006** — Direct Volume Access **T1027.013** — Encrypted/Encoded File **T1027.015** — Compression **T1497.001** — Virtualization/Sandbox Evasion: System Checks **T1562.001** — Impair Defenses: Disable or Modify Tools **T1622** — Debugger Evasion
Credential Access	**T1003** — OS Credential Dumping
Discovery	**T1046** — Network Service Discovery **T1082** — System Information Discovery **T1083** — File and Directory Discovery **T1135** — Network Share Discovery **T1614** — System Location Discovery
Lateral Movement	**T1021.001** — Remote Services
Collection	**T1039** — Data from Network Shared Drive
Command and Control	**T1219** — Remote Desktop Software
Impact	**T1486** — Data Encrypted for Impact **T1489** — Service Stop

Arintze-neurriak

Proaktiboak

- ❑ Faktore anitzeko autentifikazioa eta phishingaren aurkako prestakuntza inplementatzea. (T1078 – Valid Accounts)
- ❑ Sinatu gabeko scriptak eta makroak mugatzea eta PowerShell edo CMD bezalako interpreteen erabilera kontrolatzea. (T1059 – Command and Scripting Interpreter)
- ❑ Pribilegioak dituzten kontuak mugatzea. (T1562 – Impair Defenses)
- ❑ Pribilegio minimoaren printzipioa aplikatzea, sarea segmentatzea eta baliabide partekatuetarako sarbideak monitorizatzea. (T1083 – File and Directory Discovery, T1135 – Network Share Discovery)
- ❑ Offline segurtasun-kopiak mantentzea eta aldizkako leheneratzeak probatzea. (T1486 – Data Encrypted for Impact)
- ❑ Windowsen, eraso-azalera murrizteko arauak (ASR) gaitzea LSASS babesteko eta kredentzialak lapurtzea saihesteko. (T1003 - OS Credential Dumping)

Erreaktiboak

- ❑ Antibirusak AMSIrekin erabiltzea, ASR arauak aplikatzea eta erabiltzaileei prestakuntza ematea, artxibo lausotuak blokeatzeko. (T1027 - Obfuscated Files or Information)
- ❑ Kategorietan eta ospean oinarritutako web-iragazketako konponbideak erabiltzea. (T1133 – External Remote Services)

Ondorioak eta gomendioak

DeadLock **mehatxu nabarmena da gaur egungo ransomwarearen panoraman**, bere ikuspegi oportunistagatik, gizarte-ingeniaritzan oinarritutako sarrera-bektore ugari erabiltzen dituelako eta zifratzeko duen gaitasunagatik. Gainera, biktima bakoitzeko identifikatzaile indibiduala erabiltzeak, komunikazio-kanal anonimoekin batera, aukera ematen die operadoreei estortsio-prozesua zehaztasunez kudeatzeko, kobrantza-eredua deszifratze-gakoarekin indartuz. Hala ere, ordainketa horrek ez du bermatzen datuak berreskuratzea edo arriskua ezabatzea, taldeek sistema konprometituetarako sarbidea atxiki dezaketelako edo lortutako kredentzialak berrerabil ditzaketelako.

DeadLock ingurune korporatiboetarako eta antolakundeetarako inpaktu handiko arriskutzat hartu behar da. Horregatik, segurtasun-kopia fidagarriak, isolatuak eta probatuak egitea gomendatzen da; pribilegio minimoaren printzipioa eta makroen eta scripten kontrola zorrotz aplikatzea; baliabide erauzgarriak automatikoki exekutatzea desgaitzea; eta erabiltzaileentzat kontzientziazio-kanpainak egitea.

