Taldea: Arcus Media Ransomware

Laburpen exekutiboa

Arcus Media 2024aren erdialdean detektatu den eta 2025ean entzute handia lortu duen ransomware-talde bat da. **Ransomware-as-a-Service (RaaS)** ereduarekin jarduten du, eta horrek erraztu egiten du hainbat afiliatuk, sofistikazio-maila desberdinekin, eskala handiko erasoak egitea. Bere helburu nagusia manufaktura, osasuna, retail eta komunikabideak bezalako sektoreetako antolakundeak dira, eta Amerikan, Europan eta Asian erregistratutako biktimak ditu.

Maila operatiboan, Arcus Mediak profesionalizazio-maila handia erakusten du, **LockBit edo BlackCat bezalako familia sendotuek** erabiltzen dituztenen antzeko **ihes- eta iraunkortasun-taktikekin**. Taldeak segurtasun-kopiak (*shadow copies*) ezabatzen ditu, gertaeren erregistroak borratzen ditu, prozesu kritikoak amaitzen ditu eta segurtasun-zerbitzuak desaktibatzen ditu zifratu aurretik, eragindako sistemen ahalik eta disrupziorik handiena bermatuz.

Talde honek antolakundeentzat duen arrisku nagusia **negozioaren disrupziorako duen orientazioan** datza. Izan ere, berrikuntza teknikoan zentratuago dauden taldeek ez bezala, Arcus Mediak bere erasoen efizientzia optimizatzen du, erasoaren abiadura maximizatzeko fitxategi handiak partzialki zifratuz, sistema kritikoak seinalatuz (datu-baseak, posta, aplikazio korporatiboak...) eta leheneratze-mekanismoak nahita suntsituz. Gainera, erabiltzen duen estortsio bikoitzeko ereduak (sistemak zifratzea eta datu sentikorrak argitaratzearekin mehatxatzea) **ospe-kalteak eta finantza-eragina** sortu ditzake, batez ere datuak funtsezkoak diren sektoreetan edo oso araututa dauden sektoreetan (finantza-zerbitzuak, osasuna, teknologia edo manufaktura).

Ransomware-taldea: Arcus Media

Arcus Media ransomware-talde bat da, Ransomware-as-a-Service (RaaS) ereduarekin jarduten duena. Arcus Mediaren kanpainak **phishing** bidezko **hasierako sarbideetan**, **kredentzial konprometituetan** edo **esposiziopeko zerbitzuen ustiapenean** (RDP/VPN) oinarritzen dira. Behin sartutakoan, operadoreek **erreminta legitimoak** *(living-off-the-land*) eta **frameworkak erabiltzen dituzte (Cobalt Strike edo Mimikatz**, adibidez) alboko mugimendurako eta kredentzialak biltzeko.

Azkenik, **estortsio bikoitzeko** taktikak erabiltzen ditu, sistemen zifratzea eta datuen esfiltrazioa konbinatuz. Artxibo zifratuak luzapen espezifiko batekin markatuta geratzen dira, eta erreskate-ohar bat eransten da, harremanetarako jarraibideekin.

Eragindako herrialdeak eta sektoreak

Arcus Media ransomware-talde emergente bat da, eta jarduera areagotu egin du 2025ean. Eskuragarri dauden datuen arabera, jarduera gehien duten herrialdeen artean **Brasil, Estatu Batuak eta Europa** (Frantzia, Espainia...) daude.

Espainian, Arcus Media taldeak gutxienez **sei biktima berretsi** ditu, eta funtsezko hainbat sektore barne hartzen ditu, hala nola **teknologia, enpresa-zerbitzuak, aholkularitza eta hezkuntza.** Gainera, biktimen artean **zibersegurtasunean** espezializatutako enpresa bat ere badago.

Arcus Mediak **gehien erasotako sektoreak teknologia/IT eta enpresa-zerbitzuak** dira nagusiki, eta horien ondoren **nekazaritza eta elikagaien ekoizpena, garraioa eta logistika eta osasuna** daude. Horrek erakusten du taldeak mendekotasun teknologiko handia duten antolakundeetan zentratzen dituela bere erasoak, baina informazio kritikoa edo sentikorra duten sektoreei ere eragiten die.

Analisi teknikoa

Arcus Media ransomwareak RaaS gisa jarduten du, **kredentzial konprometituen edo esposiziopeko zerbitzuen** bidez sartuz sareetan. Sartutakoan, alboko mugimendua egiten du, datuak ateratzen ditu eta artxiboak zifratzen ditu, eta bere luzapen propioak uzten ditu. Gainera, segurtasun-kopiak ezabatzen ditu eta zerbitzu kritikoak geldiarazten ditu berreskuratzea eragozteko.

Ransomwareak **ChaCha20-n** oinarritutako **zifratze hibridoa** erabiltzen du, **RSA-2048** bidez **babestutako gakoekin**, eta artxibo handien zifratze partzialeko teknikak ere bai, operazioa bizkortzeko.

Ezaugarri tekniko nagusiak:

- **Hasierako sarbidearen bektoreak:** konprometitutako kredentzialak, esposiziopeko VPN/RDPak eta enpresa-aplikazioetako kalteberatasunen ustiapena.
- **Alboko mugimendua:** lapurtutako kredentzialak eta urruneko administrazioko erremintak erabiltzea sarearen barruan hedatzeko.
- **Esfiltrazioa:** zifratu aurretik datuak erauztea; gorabehera batzuetan, sinkronizazio- eta esfiltrazio-utilitateak ikusi dira (adib. Rclone edo beste batzuk) datuak urruneko helburuetara transferitzeko.
- **Zifratzea:** algoritmo hibridoa (artxiboetarako zifratze simetrikoa + gakoak kriptografia asimetrikoarekin babestea); fitxategi-luzapen/-izen propioak sortzen ditu biktimak identifikatzeko.
- **Ihes-teknikak:** *shadow copy*ak ezabatzea, logak garbitzea eta zerbitzuak/backupak amaitzea berreskuratzea eragozteko.

MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
Initial Access	**T1190** — Exploitation of Public-Facing Application **T1566** — Phishing **T1078** — Valid Accounts
Execution	**T1059.001** — Command and Scripting Interpreter: PowerShell **T1053** — Scheduled Task/Job
Persistence	**T1547.001** — Registry Run Keys / Startup Folder **T1543** — Service Installation
Privilege Escalation	**T1068** —Exploitation for Privilege Escalation **T1548** — Abuse Elevation Control Mechanism
Defense Evasion	**T1070** — Indicator Removal on Host **T1490** — Inhibit System Recovery **T1562.001** — Impair Defenses: Disable or Modify Tools
Discovery	**T1046** — Network Service Scanning **T1016** — System Network Configuration Discovery
Lateral Movement	**T1021** — Remote Services **T1078** — Use of Valid Accounts
Command and Control	**T1071.001** — Application Layer Protocol
Impact	**T1486** — Data Encrypted for Impact **T1485** — Data Destruction

Arintze-neurriak

Proaktiboak

- ❑ Erabiltzaileak gaitzea, mezu eta esteka susmagarriak iragaztea, MFA erabiltzea eta eranskinaren analisia. (T1566 – Phishing)
- ❑ Softwarea eguneratzea eta segurtasun-adabakiak aplikatzea. (T1190 – Exploitation of Public-Facing Application)
- ❑ Urruneko sarbideak mugatzea eta faktore anitzeko autentifikazioa erabiltzea. (T1078 – Valid Accounts, T1021 – Remote Services)
- ❑ Programatutako zereginen sorrera auditatzea eta pribilegioak murriztea. (T1053 – Scheduled Task / Job)
- ❑ Hasiera automatikoko gakoak babestea. (T1547 – Registry Run Keys / Startup Folder)
- ❑ Segurtasun-kopiak babestea eta horien ezabatzea monitorizatzea. (T1490 – Inhibit System Recovery)
- ❑ Segurtasun-kopia seguruak mantentzea eta leheneratzeak probatzea. (T1486 – Data Encrypted for Impact)

Erreaktiboak

- ❑ Sinatu gabeko scripten exekuzioa mugatzea eta haien erabilera erregistratzea. (T1059 – PowerShell / Command Shell)
- ❑ EDR erabiltzea eta memoriako kredentzialak babestea. (T1003 – OS Credential Dumping)

Ondorioak eta gomendioak

Arcus Media ransomware-talde aktiboenetako bat bihurtu da 2025ean, eta presentzia handia du Amerikan, Europan eta, bereziki, Espainian. Operadoreetan eta afiliatuetan oinarritutako **Ransomware-as-a-Service (RaaS)** ereduak aukera ematen dio erasoak eskalatzeko eta haien atribuzioa eragozteko. Bere antolamenduagatik, gaitasun teknikoagatik eta eragindako sektoreen aniztasunagatik nabarmentzen da.

Zantzu batzuen arabera Arcus Mediak azpiegitura edo metodologiak parteka baditzake ere beste talde batzuekin, duela gutxi egindako azterketek **entitate independente** gisa identifikatu dute **ransomwarearen ekosistemaren barruan**, estortsio bikoitzean eta urruneko sarbide kalteberen ustiapenean zentratutako entitate gisa, hain zuzen ere.

Arcus Mediaren aurreko arriskua arintzeko, **gomendatzen da kanpoko sarbideen segurtasuna indartzea faktore anitzeko autentifikazioaren bidez** (MFA), **segurtasun-kopiak** mantentzea, **sarearen segmentazioa** aplikatzea, **administrazio-pribilegioak mugatzea eta detekzio- eta erantzun-konponbideak** (EDR/XDR) **hedatzea**. Era berean, **mehatxuen eta kalteberatasunen etengabeko monitorizazioa** funtsezkoa da balizko intrusioei aurrea hartzeko eta haien inpaktua minimizatzeko.

