Ransomware-taldea: Clop

Laburpen exekutiboa

Clop (Cl0p ere esaten zaio) **ransomwarean eta datu-estortsioan espezializatutako talde zibergaizkile** bat da. 2019an agertu zenetik. berehala eboluzionatu du, gaur egun antolakunde publiko eta pribatuentzat dagoen zibermehatxu larrienetako bat bihurtu arte. Clop-ek kanpaina sofistikatuen bidez jarduten du. Kanpaina horiek sare korporatiboetan intrusioak, informazio kritikoa zifratzea eta datu konfidentzialak lapurtzea konbinatzen dituzte, biktimei presioa egiteko. Clop-en **eraso-ereduak estortsio bikoitza dakar**: sistemak artxiboak zifratuz deuseztatzeaz gain, informazio sentikorra esfiltratzen du antolakundeak mehatxatzeko. Horrek **inpaktu handiko mehatxu** bihurtzen du, xede-antolakundeen funtsezko eragiketak eteteko eta kalte ekonomiko nahiz ospe-kalte larriak eragiteko gai dena.

Clop-ek **arrisku handia dakar era guztietako antolakundeentzat**, bai sektore publikoarentzat bai pribatuarentzat. Izan ere, Clop-ek kalteberatasun ezezagunak ustiatzeko eta zuzendutako phishing-kanpainak egiteko duen gaitasunak aukera ematen dio zibersegurtasun-maila altua duten antolakundeei ere arrakastaz eraso egiteko. Behin biktimen sareetan sartutakoan, alboko mugimenduko taktikek pribilegioak eskalatzea eta sare korporatiboetan azkar hedatzea errazten diote, kaltearen irismena maximizatuz detektatu ahal izan aurretik. Gainera, **mehatxu horren inpaktuak berekin dakar eragindako sistemak desgaitzea eta datu sentikorrak zabaltzeko aukera**.

Horregatik guztiagatik, **zibersegurtasunaren ikuspegi integral eta proaktiboa** behar da mehatxua arintzeko. Horretarako, komeni da gorabeheren aurretik defentsak indartzea, hainbat neurri hartuta, hala nola sistemak etengabe eguneratzea, sareak segmentatzea, faktore anitzeko autentifikazioa ezartzea urruneko sarbideak babesteko eta langileak zibersegurtasunari buruz kontzientziatzea.

Ransomware-taldea: Clop

Ziberdelinkuentzia-talde antolatua da Clop, batez ere **irabazi-helburudun ransomware-erasoetara bideratua**. Hasieratik, Clop-ek **estortsio dualeko eredu** bat erakutsi du, informazio sentikorra zifratzearen eta informazioa filtratzeko mehatxuaren bidez. Taldea 2019ko otsailean sortu zen, CryptoMix ransomwarearen aldaera gisa, eta denborarekin **RaaS (Ransomware-as-a-Service) plataforma** bihurtu zen, afiliatuak errekrutatuz beren eragiketen irismena handitzeko. 2021ean zehar, hainbat segurtasun-agentziak esku-hartze batzuk egin zituzten Clop-en aurka, eta horrek taldearen jarduera tarte txiki batez etetea eragin zuen. Hala ere, 2022an berriro agertu zen, eta ordutik gaur egunera arte aktibo mantendu da.

Clop-en azpiegiturari eta modus operandiri dagokienez, **filtrazio-atari bat du Tor sarean**, “Clop Leaks” izenez ezagutzen dena, eta bertan biktimei lapurtutako informazioa jendaurrean azaltzen du. Gainera, biktimekiko komunikazioa **helbide elektroniko seguruen edo negoziazio-atarien bidez egin ohi da Tor-en**.

Eragindako herrialdeak eta sektoreak

Clop-en eragiketen **irismena globala** izan da, eta bere jardueraren zati handi bat **Ipar Amerikan eta Europan** kontzentratu da. Oro har, Clop-en helburuak dira **sistema digitalekiko eta datuekiko mendekotasun handia duten antolakundeak**.

Eragindako sektoreei dagokienez, **Clop-ek biktimen dibertsifikazio zabala** erakusten du. Gehien kaltetutako sektoreen artean, hauek nabarmentzen dira: **gobernua, osasuna, hezkuntza eta ikerketa, manufaktura eta industria, informazioaren teknologia, finantzak eta zerbitzu profesionalak, garraio-sektorea eta komunikabideak**.

Analisi teknikoa

Clop-ek **hasierako hainbat sarbide** erabiltzen ditu, hala nola **malwaredun phishing-kanpainak, esposiziopeko zerbitzu kalteberen zuzeneko ustiapena**, eta **konprometitutako kredentzialak erabiltzea**. Hasierako sarbidea lortu ondoren, ingurunearen gaineko kontrola zabaltzen du, konprometitutako **makinan pribilegioak** handituz. Aldi berean, Clop-eko operadoreek **ustiapenaren ondoko erremintak** zabaltzen dituzte, hala nola Cobalt Strike eta **barne-sarea mapatzeko** beste utilitate batzuk, sare-segmentuak zerrendatzeko eta zerbitzari kritikoak eta taldeak Active Directory-n identifikatzeko. Ondoren, **alboko mugimenduak** egiten ditu hasierako sarrera-puntutik balio handiagoko beste sistema batzuetara pasatzeko, kredentzialak eta exploitak erabiliz.

Gainera, dokumentu-bolumen handiak, datu-baseak eta barne-komunikazioak biltzen ditu, balio handienekoak lehenetsiz. **Datu horiek kanpo-zerbitzarietara bidaltzen dira**, normalean kanal zifratuen bidez. Azkenik, Clop-ek **zifratze hibridoko eskema** bat aplikatzen du, zifratze simetrikoko eta zifratze asimetrikoko algoritmoak konbinatuz gakoaren segurtasunerako.

Ezaugarri tekniko nagusiak:

- **Xede-plataformak:** Clop-ek, nagusiki, Windows, Linux eta VMware ESXi inguruneei eragiten die, plataforma anitzeko gaitasuna agerian utziz.
- **Bitar legitimoen erabilera (LOLBins):** Clop-ek sistema eragilearen jatorrizko erremintak eta utilitateak aprobetxatzen ditu ezkutuan geratzeko (Living off the Land). Adibidez, PowerShell eta utilitate administratibo estandarrak (wmic, net, schtasks, besteak beste).
- **Lotutako erreminta kaltegarriak:** Clop-en baliabideek malware-familia ugari eta intrusioan zehar hedatzen diren eraso-utilitate asko barne hartzen dituzte.

MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
Initial Access	**T1566** — Phishing **T1566.001** — Phishing: Spearphishing Attachment **T1190** — Exploit Public-Facing Application **T1078** — Valid Accounts
Execution	**T1059.001** — Command and Scripting Interpreter: PowerShell **T1059.003** — Command and Scripting Interpreter: Windows Command Shell **T1204** — User Execution
Persistence	**T1505.003** — Server Software Component: Web Shell **T1546.011** — Event Triggered Execution: Application Shimming **T1547** — Boot or Logon Autostart Execution **T1543** — Create or modify system process: Windows service
Privilege Escalation	**T1068** — Exploitation for Privilege Escalation
Defense Evasion	**T1055** — Process Injection **T1070** — Indicator Removal **T1574** — Hijack Execution Flow **T1036** — Masquerading **T1562** — Impair Defenses **T1140** — Deobfuscate/Decode Files or Information
Discovery	**T1018** — Remote System Discovery **T1083** — File and Directory Discovery
Lateral Movement	**T1021.002** — Remote Services: SMB/Windows Admin Shares
Collection	**T1005** — Data from Local System
Command and Control	**T1071** — Application Layer Protocol **T1105** — Ingress Tool Transfer
Exfiltration	**T1041** — Exfiltration Over C2 Channel
Impact	**T1486** — Data Encrypted for Impact

Arintze-neurriak

Proaktiboak

- ❑ Faktore anitzeko autentifikazioa (MFA) inplementatzea, baimendu gabeko sarbideak saihesteko. (T1078 – Valid Accounts)
- ❑ Segurtasun-kopia seguruak mantentzea eta aldizkako leheneratzeak probatzea. (T1486 – Data Encrypted for Impact)
- ❑ Sarea segmentatzea eta ostalarien arteko ikusgaitasuna mugatzea, prozesuen, sistemen eta direktorioen aurkikuntza murriztuz. (T1083 – File/Directory Discovery)
- ❑ RDP eta SSH erabiltzaileak auditatzea eta mugatzea; zerbitzuak desgaitzea ezinbestekoak ez badira. (T1021 – Remote Services)
- ❑ Softwarea aldian-aldian eguneratzea, adabakien kudeaketa egokia erabiliz. (T1190 – Exploit Public-Facing Application)

Erreaktiboak

- ❑ Irteerako trafikoa monitorizatzea eta baimendu gabeko SMTP/FTP/HTTP konexioak blokeatzea, esfiltraziorako erabiltzen baitira. (T1041 – Exfiltration Over C2 Channel)
- ❑ Antibirus bat erabiltzea artxibo susmagarriak automatikoki berrogeialdian jartzeko, PowerShell desaktibatzea beharrezkoa ez denean, edo "Constrained Language" modua erabiltzea sarbidea mugatzeko. (T1059.001 – Command and Scripting Interpreter: PowerShell)
- ❑ Intrusioak detektatzeko eta prebenitzeko sistemak inplementatzea, malwareari lotutako trafiko anomaloa edo sare-patroiak identifikatzeko aukera ematen dutenak. (T1071 – Application Layer Protocol)

Ondorioak eta gomendioak

Clop ransomware-taldea **mehatxu nabarmena** da, **tamaina eta sektore guztietako antolakundeetan inpaktu larria** eragiteko gaitasuna erakutsi duena. Horren arrazoia da Clop-ek ransomware-teknika aurreratuak eta estortsio erasokorreko estrategia bat konbinatzen dituela, kalteberatasunak eta giza erroreak ustiatuz sare korporatiboetan infiltratzeko. Behin sareetan sartutakoan, sistema kritikoen informazio- eta zifratze-lapurreta masiboak egiten ditu. Gainera, erasotzaile horren **estortsio bikoitzeko ereduak** bere gaitasuna handitu du, antolakundeentzako arriskua areagotuz, balizko ospe-kalteak eta legezko zehapenak eraginez eta konfiantza publikoa arriskuan jarriz.

Horregatik guztiagatik, gomendatzen da **sistemak eguneratuta eta behar diren adabakiak ezarrita mantentzea**, bereziki Interneten esposiziopean daudenak. Era berean, komeni da autentifikazioa eta urruneko sarbideak indartzea, **faktore anitzeko autentifikazioaren** bidez, kanpoko sarbide guztietan eta barneko kontu pribilegiatuetan. Horrez gain, nahitaezkoa da detekzio goiztiarra hobetzea, **EDR/XDR konponbideen** bidez, eta monitorizazio-sistemetan **mehatxuen adimena** integratzea. Azkenik, komenigarria da **sarea segmentatzea eta segurtasun-kopiak isolatzea**.

