Akira mehatxu-sortzailea

Laburpen exekutiboa

2023. urtearen hasieran agertu zenetik, **Akira ransomware** taldea mehatxu aktibo eta erasokorrenetako bat bihurtu da zerbitzu gisako ransomware ereduaren barruan **(RaaS)**. Haren jarduera azkar handitu da, eta mundu mailan ehundik gora biktima izan ditu. Geografikoki, Ameriketako Estatu Batuetan jarduten du nagusiki, hainbat sektore kritikotan; hain zuzen ere, osasun-sektorea da Akiraren jopuntuan dagoen industria nagusienetako bat.

Akira **gaitasun teknikoa eta ikuspegi selektiboa** izateagatik nabarmentzen da. Gai da kalteak eragiteko, bai **Windows** inguruneetan, bai **Linux** inguruneetan, eta horrek aukera ematen dio azpiegitura hibridoetan aritzeko. Batez ere kredentzial konprometituak erabiliz lortzen du biktimen sareetara hasierako sarbidea izatea. Behin barnean dela, **estortsio bikoitzaren** estrategia exekutatzen du: sistemak zifratzen ditu, eta biktimari diru-kopuru bat ordaintzea exijitzen dio, ez badu nahi lapurtutako informazioa filtrazioen atarian zabaltzea.

Lapurtutako kredentzialak eta VPN zerbitzu ahulak erabiliz, Akira ezkutuan sartzen da hasieran; defentsei ihes egiten die etapa goiztiarretan, eta ransomwarea hedatu bitartean sarbide iraunkorra izaten du. Gainera, legezko tresnak ere erabiltzen ditu, hala nola AnyDesk edo Remote Desktop Protocol (RDP) izeneko protokoloan oinarritutako beste batzuk, eta horrek zailagoa egiten du Akira detektatzea.

Mehatxu antolatua da Akira, eta ikuspuntu estrategiko argia du. Haren jarduera gero eta handiagoak ezinbestekoa egiten du antolakundeek haien defentsa goitik behera indartzea, urruneko sarbideen monitorizazioa lehenestea, albo-mugimenduak detektatzea, sarea segmentatzea eta erantzun azkarrak emateko gaitasuna handitzea, ziberinteligentzia-zerbitzuez lagunduta.

Mehatxu-sortzailea: Akira

Akira Ransomware-as-a-Service (RaaS) motako talde bat da, 2023ko martxoan agertu zena. Litekeena da Conti taldeko kide ohiekin lotura izatea, eta legatu tekniko hori aprobetxatzea ransomwareen munduan bizkor finkatzeko.

Sortu zenetik hona, taldeak bertsio aurreratuagoak abiarazi ditu, hala nola Akira_v2 eta Rust-en idatzitako tresnak; adibidez, Megazord. Horri guztiari esker, zifratze espezifikoagoak egin ditzake, eta artxibo kritikoei eta sistema birtualizatuei eraso egin; esaterako, VMware ESXi-ri.

Kaltetutako herrialde eta sektoreak

2024ko urtarrilera arte, Akirak 250 antolakundetik gora jarri zituen arriskuan, eta 42 milioi inguru dolar estatubatuar bildu zituen erreskate gisa. Batez ere Estatu Batuetan egiten ditu erasoak, eta Europako zenbait herrialdetan eta Australian ere bai.

Espainia da Akirak gehien kaltetu duen Europako herrialdeetako bat. 2025. urtean, taldeak Espainiako hainbat antolakunderi egin die eraso, hala nola Druni SA, Ste Group Key Corp eta GPS 909. Gertakari horiek agerian utzi dute antolakundeek ahulezia kritikoak dituztela urruneko sarbideak babesteko eta ahuleziak kudeatzeko, eta zibersegurtasun-arloko defentsak areagotzeko premia azpimarratu dute.

Kaltetutako sektoreei dagokienez, hezkuntza-, finantza-, manufaktura- eta osasun-sektoreetako enpresa handien kontra egin ohi du nagusiki, phishing-kanpainak eta ahuleziak baliatzekoak erabiliz. Lapurtutako datuak bere gunean argitaratzen ditu, Tor sarean, kontsola motako interfaze baten bidez, eta gune horixe erabiltzen du, orobat, biktimekin komunikatzeko.

Azterketa teknikoa

Akirak teknika sofistikatuak eta eredu operatibo profesionalizatua erabiltzen ditu, eta horrek askotariko inguruneetara azkar egokitzeko aukera ematen dio. Urruneko sarbideetako ahuleziak, albo-mugimenduak eta legezko tresnak erabiltzen ditu detektatua ez izateko, eta, beraz, zaila da Akira analizatzea eta haren ondorioak arintzea.

Ezaugarri tekniko nagusiak:

- Berriro hasi da erabiltzen **C++ lengoaiako zifratzailea Windows sistemetarako**, eta alde batera utzi du, aldi baterako, Rust-en zituen bertsioak Linuxerako. Aldaera berria 2023ko jatorrizko karga erabilgarriaren optimizazio bat da.

- **ChaCha20 eta RSA algoritmoak** konbinatzen dituen zifratze hibridoko eskema erabiltzen du, artxibo espezifikoen motetara eta tamainetara bideratuta.

- Hasierako sarbidea lortzeko, honelakoak erabiltzen ditu: **phishinga**, VPNetako **ahuleziak baliatzea** (adibidez, SonicWall eta Cisco) eta **kredentzial konprometituak** edo **kontu inaktiboak**.

- **Albo-mugimenduak** egiten ditu, **legezko tresnak** (LOLBAS) erabiliz, hala nola RClone, WinSCP eta Advanced IP Scanner.

- Akirak **estortsio bikoitzeko** eredu bat aplikatzen du: lehenik, sistema ukituak zifratzen ditu, eta, ondoren, erreskatea eskatzen du bitcoinetan. Biktimak ez badu ordaintzen, lapurtutako informazioa Tor sareko gunearen bidez zabaltzeko mehatxua egiten diote.

MITRE ATT&CK teknikak

Taktika	Teknika erabiliena
Initial Access	**T1078 –** Valid Accounts **T1133 –** External Remote Services
Execution	**T1059.001 –** Command and Scripting Interpreter: PowerShell
Persistence	**T1133** – External Remote Services **T1078 –** Valid Accounts
Privilege Escalation	**T1078 –** Valid Accounts
Defense Evasion	**T1562.001 –** Impair Defenses: Disable or Modify Tools **T1036.005 –** Masquerading: Match Legitimate Resource Name or Location **T1027.001 –** Obfuscated Files or Information: Binary Padding
Credential Access	**T1558 –** Steal or Forge Kerberos Tickets
Discovery	**T1482 –** Domain Trust Discovery **T1018 –** Remote System Discovery
Lateral Movement	**T1021.001 –** Remote Services: Remote Desktop Protocol
Collection	**T1560.001 –** Archive Collected Data: Archive via Utility **T1213.002 –** Data from Information Repositories: Sharepoint
Exfiltration	**T1567.001 –** Exfiltration to Cloud Storage
Command and Control	**T1219 –** Remote Access Tools
Impact	**T1486 –** Data Encrypted for Impact **T1531 –** Account Access Removal **T1657 –** Financial Theft

Arintzeko neurriak

Proaktiboak

- ❑ Faktore anitzeko autentifikazioa ezartzea (MFA), baimenik gabe inor ez sartzeko (T1078 - Valid Accounts) eta urruneko sarbideetarako (T1021.001 – Remote Services: RDP).

- ❑ Urruneko zerbitzuetarako sarbidea mugatzea, VPN gisa kudeatutako kontzentratzaileen eta urruneko beste sarbide-sistema batzuen bidez. (T1133 – External Remote Services).

- ❑ Segurtasun-tresnen aldaketak auditatzea eta aldaketen edo desaktibazioen alertak konfiguratzea jarduera kaltegarriak detektatu ahal izateko. (T1562.001 - Impair Defenses: Disable or Modify).

- ❑ Sharepoint-erako sarbidea mugatzea eta jarduera-erregistroa aktibatzea. (T1213.002 – Data from Information Repositories: Sharepoint).

- ❑ Sarea segmentatzea hautematea mugatzeko. (T1482 – Domain Trust Discovery).

Erreaktiboak

- ❑ Antibirusa 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).

- ❑ Betegarriak (padding) edo ezkutatze anomaloak dituzten bitarrak atzemateko tresnak erabiltzea. (T1027.001 – Obfuscated Files or Information: Binary Padding).

Ondorioak eta gomendioak

Akira mehatxu-sortzaile nagusietako bat da ransomwareen munduan; izan ere, teknika aurreratuak eta egitura profesionalizatua konbinatzen dituen eredu sofistikatu bat baliatzen du. Urruneko zerbitzuen ahuleziak aprobetxatzeko eta estortsio bikoitzeko taktikak erabiltzeko gaitasuna izanik, bereziki arriskutsua da, eta sektore eta eskualde askotako antolakunde handiak kaltetzeko gai.

Akirak eta haren gisako taldeek gero eta jarduera handiagoa dutenez eta bestelako ziberkriminal antolatuak ere badirenez, arrisku globalaren maila handitu egiten da, eta halako taldeen kanpainen eragina areagotzen da, azpiegitura kritikoetara eta enpresa estrategikoetara heltzeraino. Testuinguru horretan, funtsezkoa da defentsa-estrategiak zorrotz ezartzea eta zibersegurtasunari buruzko ikuspuntu proaktibo eta koordinatuari atxikitzea, ondorioak arintzeko eta aktibo sentikorrenak babesteko.

