

Laburpen exekutiboa

Rhysida **ransomware-motako talde** bat da; 2023tik, gaitasun handia erakutsi du intrusioak **motibazio ekonomikoarekin** egiteko, estortsio bikoitzaren bidez. Horretarako, negoziazio-prozesuak eta biktimaren gaineko presio operazionalako mekanismoak gauzatzen ditu TOR sareko atari batean oinarrituta.

Eraso-patroiak arriskua handitzen du antolakunde publiko eta pribatuentzat, **phishing bidezko hasierako sarbidea edo baliozko kredentzialen abusua** konbinatzen dituelako, ingurune korporatiboa menderatzera bideratutako ustiapenaren ondorengo fasearekin. Inpaktuari dagokionez, arriskua ez da soilik informazio sentikorra zifratzera mugatzen; datu-ihesak **ospeari kalte egiteko probabilitatea eta erregulazio-zehapenak** handitzen ditu, bai eta sistemak erantzuteko eta berreskuratzeko kostuak ere. Beraz, malware hori **arrisku handikotzat** hartu behar da antolakundeentzat, baldin eta urruneko sarbideak esposiziopean badituzte, kredentzial ahulak kudeatzen badituzte, segmentazio eskasa badute eta segurtasun-kopiarik egiten ez badute. Bereziki gobernuan, hezkuntzan, osasunean, manufaktura-industrietan eta teknologietan.

Horregatik guztiagatik, Rhysida mehatxua arintzeko funtsezko neurriak hauek izango lirake: hasierako sarbidea indartzea prestakuntzaren eta kontzientziazioaren bidez; sarbide perimetraleko zerbitzuetan (VPN/RDP) autentifikazio-faktore bikoitzak nahitaez erabiltzea; hedapena mugatzea sarearen segmentazioaren eta pribilegio minimoko politiken bidez; eta datuak babestea backup aldaezinen eta aldizkako leheneratze-proben bidez. Gainera, **deszifratze-erreminta publiko** bat dago, inplementazioan identifikatutako kalteberatasun batean oinarritua, baina **ransomwarearen aldaerak eta eragindako inguruneak** (batez ere Windows) **baldintzatzen dute** haren erabilera. Beraz, ez da konponbidetzat hartu behar, gorabeherei erantzuteko laguntza-neurritzat baizik, kasu bakoitzean alde aurretik haren aplikagarritasuna balidatuz.

Ransomware-taldea: Rhysida

Rhysida **motibazio nagusiki ekonomikoko** zibergaizkile-talde bat da, 2023ko martxotik gutxienez modu publikoan behatua. Bere iruzur-eredua **estortsio bikoitzean** oinarritzen da: sistemak eta datuak zifratzeaz gain, eragileak informazio sentikorra esfiltratzen du ordainketa behartzeko, eta mehatxua egiten du hori argitaratzearekin, biktimak ordaintzen ez badu. Horretarako, TOReko atari bat erabiltzen du, biktimekiko interakzioa eta datuen argitalpena zentralizatzeko.

Eragile horren ezaugarri bereizgarri bat da batzuetan ahultasunak nabarmentzen laguntzeko ustezko «zibersegurtasun-lantalde» baten itxura hartzea, nahiz eta bere helburua beti estortsioa eta onura ekonomikoa izan.

Gainera, **Ransomware-as-a-Service (RaaS) motako eragiketak** egiten ditu. Eredu horretan, afiliatuei malwarea eta azpiegitura eskaintzen zaizkie, intrusioak exekutatzeko eta erreskateak monetizatzeko.

Eragindako herrialdeak eta sektoreak

Rhysida ez da eremu geografiko jakin batera mugatzen; aitzitik, **modu globalean jarduten du**, Europan eta Ipar Amerikan eragin berezia izanik. Jarduera asoziatu gehien duten herrialdeen artean, Ameriketako Estatu Batuak, Erresuma Batua, Italia, Frantzia eta Alemania nabarmentzen dira.


Sektoreei dagokienez, Rhysidak biktimologia zabala erakusten du, inpaktu handiagoarekin **hezkuntzan, osasunean, administrazio publikoan, manufakturan eta informazioaren teknologietan**. Patroi hori bat dator estortsio bikoitzeko eragiketekin, zeinetan bilatzen den ordaintzeko presioa eta probabilitatea maximizatzea kritikotasun operatibo handiko eta datu sentikor ugariko inguruneetan.


Analisi teknikoa


Rhysidari lotutako intrusio-zikloa hasierako sarbidearekin hasten da normalean, phishing bidez edo VPN edo RDP zerbitzuen baliozko kontu konprometituen erabilerarekin. Hasierako sarbidea lortutakoan, operadoreek ustiapenaren ondorengo frameworkak erabiltzeko joera dute (hala nola Cobalt Strike), kontrol operatiboa ezartzeko, eta, aldi berean, iraunkortasuna eta hedapena ahalbidetzen duten urruneko administrazio-ahalmenak gaitzeko. Sarbidearen ondoren, jarduera ingurunea aurkitzera eta hedatzera bideratzen da, urruneko zerbitzuen bidezko alboko mugimenduak eta pribilegio-eskalatzea baliatuz. Horrez gain, Rhysidak defentsa-ebasioko teknikak erabiltzen ditu, segurtasun-zerbitzuak amaituz, backupak ezabatuz eta Direktorio Aktiboan aldaketak eginez.


Zifratze-fasea ransomware modernoetan ohikoa den eskema hibrido baten bidez gauzatzen da: 4096 biteko RSA zifratze asimetrikoa erabiltzen da gako pribatua babesteko, eta ChaCha20 zifratze simetrikoa fitxategien edukia zifratzeko. Azkenik, eskusio-zerrendak aplikatzen ditu fitxategiak zifratzean, sistemaren ezegonkortasuna saihesteko.

Ezaugarri tekniko nagusiak:

 **Plataformak:** Rhysidak Windows, Linux eta VMware ESXi inguruneen aurka operatzen du.

 **Hasierako sarbidea:** phishing eta VPN eta RDP zerbitzuetako baliozko kredentzialen abusua

 **Ustiatu ondorengo frameworkak eta lolbin-erremintak erabiltzea:** Cobalt Strike, DataGrabber.exe erreminta esfiltraziorako, PsExec, AnyDesk sarbide alternatibo gisa, WinRM scripten esparruan...

 **Defentsa-ebasioa:** PowerShell scriptak (SILENTKILL) erabiltzea malwarearen aurkako sistemak desaktibatzeke eta segurtasun-kopiak ezabatzeko.

MITRE ATT&CK teknikak

| Taktika | Teknika erabiliena |
|-----------------------------|--|
| Resource Development | T1587 – Develop Capabilities |
| Initial Access | T1078 – Valid Accounts T1566 – Phishing |
| Execution | T1059 – Command and Scripting Interpreter |
| Persistence | T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder |
| Privilege Escalation | T1055.002 – Process Injection: Portable Executable Injection |
| Defense Evasion | T1070 – Indicator Removal T1564.003 – Hide Artifacts: Hidden Window |
| Credential Access | T1003.003 – OS Credential Dumping: NTDS T1112 – Modify Registry |
| Discovery | T1016 – System Network Configuration Discovery T1018 – Remote System Discovery T1033 – System Owner/User Discovery T1069 – Permission Groups Discovery T1087.002 – Account Discovery: Domain Account T1482 – Domain Trust Discovery |
| Lateral Movement | T1021 – Remote Services |
| Collection | T1005 – Data from Local System T1119 – Automated Collection |
| Command and Control | T1219 – Remote Access Software |
| Exfiltration | T1041 – Exfiltration Over C2 Channel |
| Impact | T1486 – Data Encrypted for Impact T1657 – Financial Theft |

Arintze-neurriak

Proaktiboak

- ❑ Kontzientziarioari buruzko etengabeko prestakuntza, bereziki mezu eta eranskin susmagarriak detektatzeko. (T1566 - Phishing)
- ❑ Faktore anitzeko autentifikazioa (MFA) inplementatzea, baimendu gabeko sarbideak saihesteko. (T1078 - Valid Accounts)
- ❑ Sarea segmentatzea aurkikuntza mugatzeko. (T1482 – Domain Trust Discovery)
- ❑ Segurtasun-kopia seguruak mantentzea eta aldizkako leheneratzeak probatzea. (T1486 – Data Encrypted for Impact)
- ❑ Pribilegioak dituzten kontuak mugatzea eta sistemak eguneratuta mantentzea. (T1069 – Permission Groups Discovery, T1070 – Indicator Removal)
- ❑ RDP erabiltzaileak auditatzea eta mugatzea, eta zerbitzua desgaitzea ere bai, ezinbestekoa ez bada. (T1021 – Remote Services)
- ❑ Hasiera automatikoko gakoak monitorizatzea eta babestea. (T1547.001 – Registry Run Keys / Startup Folder)

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 - Command and Scripting Interpreter)

Ondorioak eta gomendioak

Rhysida **mehatxu global eta inpaktu handikotzat** hartu behar da sektore askotako antolakundeentzat, bereziki hezkuntza, osasuna, administrazio publikoa, manufaktura eta IT sektoreetan. Bere intrusio-zikloak hainbat elementu konbinatzen ditu: phishing bidezko hasierako sarbidea edo konprometitutako kredentzialen erabilera; erreminta arrunten bidezko hedapen azkarra; eta prestakuntza-fase bat berreskuratzea ahultzera eta defentsak desaktibatzerantz bideratuta. Konbinazio horrek nabarmen areagotzen du **zerbitzu kritikoaren erabilgarritasuna suntsitzeko, antolakundeak larriki konprometitzeko eta jarraitutasun operatiboa eteteko arriskua.**

Horrenbestez, arriskua murrizteko lehentasunezko neurriak honako hauetan oinarritu beharko lirateke: autentifikazio-faktore bikoitzak ezartzean urruneko sarbideetan eta kontu pribilegiatuetan; sarearen segmentazioan eta pribilegio minimoen politikak aplikatzean albo-mugimenduak mugatzeko; urruneko zerbitzuetan eta scriptetan ezohiko patroiak etengabe monitorizatzean; eta offline segurtasun-kopien kudeaketa egoki eta eraginkorrean. Gainera, **deszifratze-erreminta publiko** bat dago, baina ransomwarearen aldaerak eta eragindako inguruneak (batez ere Windows) baldintzatzen dute haren erabilera.

