ANDORRA DIGITAL

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciber-Intel·ligència

El Ransomware LockBit

TLP:WHITE

09/03/2023

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	20/03/2023	21/03/2023

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGÍA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). Es tracta d'un esquema creat per fomentar un millor intercanvi d'informació de caràcter delicat (però no classificada) en l'àmbit de la seguretat de la informació. A través d'aquest esquema, d'una forma àgil i senzilla, s'indica fins a on pot circular la informació més enllà del receptor en qüestió, i aquest ha de consultar a l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra) [https://www.anc.ad/] quan la informació necessiti ser distribuïda a tercers.

CODI	QUAN EMPRAR-LO	COM COMPARTIR-LO
TLP:RED	S'ha d'utilitzar TLP:RED quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, reputació o operacions si és mal utilitzada.	Els receptors no han de compartir informació designada com TLP:RED amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP:AMBER	S'ha d'usar TLP:AMBER quan la informació requereix ser distribuïda de manera limitada, però suposa un risc per a la privacitat, reputació o operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com TLP:AMBER únicament amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per a protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per a compartir aquesta informació.
TLP:GREEN	S'ha d'emprar TLP:GREEN quan la informació és útil per a totes les organitzacions que participen, així com amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com TLP:GREEN amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP:WHITE	S'ha d'utilitzar TLP:WHITE quan la informació no suposa cap risc de mal ús, dins de les regles i procediments establerts per a la seva difusió pública.	La informació TLP:WHITE pot ser distribuïda sense restriccions, únicament subjecta a controls de Copyright.

2. INTRODUCCIÓ

Aquest informe és un document d'anàlisi del *ransomware* LOCKBIT i té com a objectiu principal brindar informació rellevant que pugui ajudar a prendre les precaucions necessàries per protegir-vos enfront de possibles ciberatacs.

Els atacs de *ransomware* s'han convertit en un dels problemes de seguretat informàtica més preocupants de l'actualitat. De fet, la prevalença d'atacs de *ransomware* va aconseguir nivells sense precedents al llarg del 2022. En els últims anys, actors d'amenaces com ara LOCKBIT GROUP, RYUK, REVIL i SYNACK han guanyat milions de dòlars després d'infectar ordinadors en diferents parts del món.

El *ransomware* és un tipus de programari maliciós utilitzat per infectar els dispositius de les víctimes, bloquejant la seva funcionalitat. L'origen etimològic del mot «ransomware» prové de la paraula en anglès «ransom», que en català significa: «rescat».

El *ransomware* provoca un segrest virtual d'informació. Aquest concepte fa referència a quan es du a terme una extorsió cibernètica, la qual ocorre quan un programari maliciós s'infiltra en els sistemes informàtics i encripta les dades, mantenint-les com a ostatges fins que la víctima, en la majoria de casos es tracta d'organitzacions, pagui un rescat.

Descobert per MALWARE HUNTER TEAM, LOCKBIT és un programari maliciós que ha estat dissenyat per bloquejar l'accés dels usuaris als sistemes informàtics i exigeix un rescat per restablir-los. A diferència d'altres tipus de *ransomware*, LOCKBIT empra tècniques avançades d'ofuscació i d'evasió per tal d'evitar que els sistemes de seguretat el detecti.

Creiem que parlar sobre LOCKBIT és de summa importància donat que, aquest *ransomware* en qüestió, ha tingut darrerament un creixement exponencial i està orientat a atacar empreses i institucions.

Amb aquest informe, es pretén oferir un anàlisi que serveixi per adoptar les mesures preventives oportunes i/o elaborar els protocols d'actuació pertinents amb la finalitat d'evitar possibles atacs amb aquest *ransomware*.

3. ANÀLISI

A continuació, explicarem què és LOCKBIT, la seva evolució i com funciona.

3.1 Què és el ransomware LockBit?

Com ja hem esmentat, LOCKBIT és un programari maliciós utilitzat per bloquejar l'accés dels usuaris als sistemes informàtics i demanar, posteriorment, un rescat a canvi de desxifrar els arxius.

LOCKBIT funciona més de pressa que la majoria d'altres famílies de *ransomware* donat que és capaç de xifrar dotzenes de servidors i sistemes informàtics en poques hores.

Els atacants que empren LOCKBIT es caracteritzen per amenaçar a organitzacions d'arreu del món amb la interrupció de les operacions mitjançant la sobtada detenció de les funcions essencials, l'extorsió pel benefici financer de l'atacant, el furt de dades i la publicació il·legal d'aquestes com a forma de xantatge si la víctima no paga el rescat.

El *ransomware* LOCKBIT es va veure per primera vegada el setembre del 2019 amb l'extensió del nom d'arxiu següent: [.abcd].

Amb el temps, la capacitat i perillositat d'aquest tipus de *ransomware* ha anat en augment.

Altrament, podem esmentar que LOCKBIT forma part de la categoria RaaS (Ransomware as a Service), un model comercial basat en una subscripció la qual permet als ciberdelinqüents comprar *ransomware* estàndard dels mateixos desenvolupadors. El rescat obtingut pel segrest de dades es reparteix entre l'equip de LOCKBIT GROUP i els atacants afiliats, que reben fins a tres quartes parts dels fons aconseguits.

LOCKBIT GROUP és l'actor d'amenaces que està darrere del desenvolupament i distribució del *ransomware* LOCKBIT. Aquest grup és considerat un dels més perillosos i actius del moment i és per això que aprofundirem sobre ell més endavant.

3.2 Evolució de LockBit

El *ransomware* LOCKBIT ha evolucionat significativament des del seu llançament l'any 2019 per convertir-se en una eina d'atac més sofisticada i perillosa. En els seus inicis, el programari maliciós es distribuïa principalment a través de correus electrònics de phishing, però en l'actualitat està sent propagat a través d'altres tècniques, com ara l'aprofitament de vulnerabilitats i les eines d'automatització per a l'accés remot. Explicarem, a continuació, quines són les versions de LOCKBIT.

Extensió .abcd

La versió original de LOCKBIT canviava el nom dels arxius, suplantant la seva extensió per [.abcd]. A més, ho inseria a una carpeta on venia inclòs un arxiu amb el nom «Restore-My-Files.txt», que contenia la nota de rescat amb exigències i instruccions per la suposada restauració. Aquesta versió va començar a propagar-se al llarg del setembre de l'any 2019.

LockBit 2.0 (LockBit Red)

LockBit 2.0 va adoptar l'extensió d'arxiu [.LockBit]. També conegut com a LockBit Red, és una versió actualitzada, més perillosa i amb un xifratge més ràpid que l'anterior. Inclou nous mètodes d'emmagatzematge de dades robades, eines per a l'anàlisi d'infraestructura de xarxa, altres formes d'advertiment de recuperació de dades, entre altres.

LockBit 2.0 va ser identificat per primera vegada el 2021 i ha estat utilitzat en diversos atacs a empreses i organitzacions de tot el món. El 25 de juny del 2021, LOCKBIT GROUP va llançar el seu «Data Leak Site» (DLS) versió 2.0 amb la secció «Condicions per a socis». Aquesta secció probablement es va crear per reclutar nous afiliats després de la prohibició de l'activitat de *ransomware* en múltiples fòrums clandestins com EXPLOIT i XSS.

Davant la perillositat de LockBit 2.0, l'FBI va publicar, a principis del 2022, un document que adverteix sobre el potencial d'aquest *ransomware*:

"LockBit 2.0 es descriu millor com una aplicació de ransomware molt confusa que aprofita les operacions bit a bit per a descodificar cadenes i carregar mòduls necessaris per evadir la detecció. En iniciar-se, LockBit 2.0 descodifica les cadenes i el codi necessari per importar els mòduls requerits [...]. Al començament de la infecció, LockBit 2.0 elimina els arxius de registre i les instantànies que resideixen al disc."

El març del 2022, els investigadors de MICROSOFT van publicar un informe sobre errors crítics de LOCKBIT 2.0, la qual cosa va contribuir a l'aparició de la versió 3.0 del *ransomware*.

LockBit 3.0 (LockBit Black)

El 27 de juny del 2022, el grup d'amenaça LOCKBIT va revelar la versió 3.0 del seu *ransomware* sota l'eslògan «Make Ransomware Great Again». No obstant això, aquesta informació va ser descoberta i publicada algunes setmanes abans per investigadors de VX-UNDERGROUND, els qui es van referir a la versió 3.0 de LOCKBIT com LockBit Black.

LockBit 3.0 incloïa noves seccions, destacant «Seguretat web i recompensa per bugs», on l'actor d'amenaces exposava el següent missatge: *"Convidem a tots els investigadors de seguretat i pirates informàtics ètics i no ètics del planeta a participar en el nostre programa de recompenses*

per bugs. La suma de la remuneració varia de 10.000 a 1 milió de dòlars". Amb aquesta nova secció, LOCKBIT GROUP es convertia en el primer grup d'amenaça de *ransomware* a llançar un programa de recompenses per *bugs*. Aquest grup fomenta la cerca de vulnerabilitats en els seus ecosistemes i a més ha inclòs l'opció de sol·licitar noves idees per incloure en les seves activitats.

Una altra característica de Lockbit 3.0 era la possible inclusió de la criptomoneda «Zcash» a les ja utilitzades: «Monero» i «Bitcoin». Així mateix, encara que la nota del rescat es deia anteriorment [Restore-My-Files.txt], aquesta nova versió hauria canviat el nom de la nota al següent format: [[id].README.txt].

La versió 3.0 era coneguda per aprofitar-se tant de la vulnerabilitat [Log4j] així com d'un popular sistema antivirus per evadir la detecció. Recents informes assenyalen que els actors de LockBit 3.0 obtenien accés inicial a través de la vulnerabilitat [Log4j], emprant noves tàctiques per produir eines de seguretat legítimes que, sovint, operaven fora dels controls de seguretat instal·lats i evadien la detecció per EDR (Endpoint Detection and Response) i les eines d'antivirus tradicionals.

Un dels canvis més significatius va ser la introducció d'un codi d'accés únic per cada mostra de LockBit 3.0. Sense el codi d'accés, la mostra no s'executaria, de tal manera que no era possible analitzar el programari maliciós de manera dinàmica sense una contrasenya.

LOCKBIT treballa principalment a través del seu propi DLS (Data Leak Site), el qual gestiona i tracta les operacions amb les seves víctimes. Abans, a les víctimes se'ls donava un període de temps definit per a pagar el rescat. La versió 3.0 de LOCKBIT incloïa noves possibilitats de negociació. En pagar una tarifa específica, la víctima tindria la possibilitat d'estendre el temporitzador 24 hores i destruir totes les dades o descarregar-les immediatament. D'aquesta manera no es faria públic el preu real del rescat i, bàsicament, estarien maximitzant els diners que podrien obtenir de cada víctima.

LockBit Green

El gener del 2023, l'actor d'amenaces LOCKBIT GROUP va informar als investigadors de VX-UNDERGROUND sobre el llançament de LockBit Green, una nova variant del seu *ransomware*. Investigadors de seguretat han analitzat aquesta variant i han confirmat que es basa en el codi font filtrat de Conti v3. La nota de rescat per aquesta variant es va modificar per incloure la informació de la nota de rescat de LockBit 3.0, però l'extensió agregada als arxius xifrats va canviar de [.lockbit] a un aleatori. Juntament amb aquest nou llançament, el grup també hauria modificat la seva variant de *ransomware* ESXI.

3.3 Com funciona el ransomware LockBit?

Els atacants solen propagar LOCKBIT mitjançant correus electrònics de *phishing* i altres tècniques, per exemple, explotant vulnerabilitats del programari del sistema objectiu.

Una vegada que LOCKBIT s'instal·la, encripta els arxius de l'usuari i deixa notes de rescat dels directoris afectats. Els atacants exigeixen un pagament en criptomonedes a canvi de proporcionar una eina de desxifrat. No obstant això, pagar el rescat no garanteix la recuperació dels arxius afectats i pot animar als atacants a continuar les seves activitats delictives.

Aquest *ransomware* s'utilitza per llançar atacs selectius contra empreses i altres organitzacions. Els grups que empren LOCKBIT es caracteritzen per amenaçar a organitzacions de tot el món amb la interrupció de les operacions per la detenció sobtada de les funcions essencials; l'extorsió per al benefici financer del ciberdelinqüent; el robatori de dades i la publicació il·legal d'aquests com a xantatge en cas que la víctima decideixi no pagar el rescat.

A continuació explicarem amb més detall com funciona el *ransomware* en qüestió, a través de tres etapes:

Etapa 1: Explotar

En primer lloc, s'exploten les febleses d'una xarxa. Com ja hem esmentat, una organització pot ser explotada mitjançant diferents tàctiques, per exemple, l'enginyeria social com ara el *phishing* o l'ús d'atacs de força bruta contra els servidors de la intranet i els sistemes de xarxa d'una organització. Si la xarxa manca d'una configuració adequada, les sondes d'atac poden trigar només uns dies a fer el seu treball.

Una vegada que LOCKBIT entra en la xarxa, el *ransomware* prepara el sistema per a alliberar la seva càrrega útil de xifratge en tots els dispositius possibles. No obstant això, és possible que un atacant hagi d'assegurar-se que es realitzin alguns passos addicionals previs.

Etapa 2: Infiltrar-se

Si és necessari, s'infiltra més profundament per completar la configuració de l'atac. A partir d'aquí, el programari LOCKBIT realitza tota l'activitat per si mateix. Està programat per emprar eines de postexplotació per escalar privilegis i aconseguir el nivell d'accés necessari per llançar els atacs. També és present a través d'un accés ja disponible mitjançant un moviment lateral per examinar la viabilitat de l'objectiu.

En aquesta etapa LOCKBIT presa les mesures de preparació necessàries abans d'implementar el xifratge del *ransomware*. Això inclou la desactivació dels programes de seguretat i de qualsevol altra infraestructura que pogués permetre la recuperació del sistema.

L'objectiu de la infiltració és impossibilitar la recuperació sense ajuda o, també, fer que sigui molt lenta, a fi que la víctima decideixi pagar el rescat exigit per l'atacant.

Etapa 3: Implementar

En aquesta etapa s'implementa la càrrega de xifratge. Una vegada que la xarxa està llesta perquè LOCKBIT es mobilitzi per complet, el *ransomware* començarà a propagar-se a través de qualsevol

màquina a la qual pugui accedir. LOCKBIT no necessita molt per completar aquesta etapa. Una sola unitat de sistema amb alt nivell d'accés pot emetre ordres a altres unitats de la xarxa per descarregar LOCKBIT i executar-lo.

L'etapa del xifratge posarà una espècie de cadenat en tots els arxius del sistema. Les víctimes només podran desbloquejar els seus sistemes amb una clau personalitzada creada per l'eina de desxifrat de LOCKBIT. També deixa còpies d'un arxiu de text de notes de rescat en cada carpeta del sistema. Aquest proporciona a la víctima instruccions per restaurar el seu sistema i fins i tot inclou l'amenaça de xantatge en algunes versions de LOCKBIT.

Una vegada completades totes les etapes, els següents passos queden a càrrec de la víctima. Pot decidir comunicar-se amb el servei d'assistència tècnica de LOCKBIT i pagar el rescat. No obstant això, s'aconsella no cedir a les seves demandes, ja que les víctimes no tenen garanties que els atacants vagin a complir amb la seva part del tracte.

4. ACTORS D'AMENAÇA

LOCKBIT és utilitzat per grups de ciberdelinqüents per a atacar a empreses i organitzacions. Aquests grups empren el *ransomware* en qüestió per xifrar els arxius de les víctimes i exigir un rescat a canvi de la clau de desxifrat.

Alguns dels grups de cibercriminals que se sap que han utilitzat LockBit inclouen: LOCKBIT GROUP, DRIDEX GROUP, DEV-0504 i BASSTELORD.

4.1 LockBit Group

Com ja hem esmentat, l'actor d'amenaces LOCKBIT GROUP està darrere del desenvolupament i distribució del *ransomware* LOCKBIT. El grup també manté comptes als fòrums en rus XSS (anteriorment DAMAGELAB) i EXPLOIT.

LOCKBIT GROUP ha anunciat la seva intenció d'adherir-se a la tècnica de la triple extorsió (xifrat + fugida de dades + ddos).

Si bé LOCKBIT GROUP opera des de setembre del 2019, aquest actor d'amenaces va passar pràcticament desapercebut fins que van llançar un lloc de filtracions per publicar les dades ex-filtrades de les víctimes el setembre del 2020, seguint una tendència marcada mesos abans per la banda de *ransomware* MAZE.

Alies

LOCKBIT, LOCKBIT GANG, LOCKBIT GROUP, LOCKBI, LOCKBIT BLACK, LOCKBITSUPP, GOLD MYSTIC, LEGASOV, UNC2758, WATER SELKIE, BITWISE SPIDER.

Objectiu

Obtenció de guanys econòmics.

Descripció

LOCKBIT GROUP ha dirigit el negoci de LOCKBIT com «Ransomware as a Service» (RaaS) des de setembre de 2019. Els desenvolupadors de LOCKBIT guanyen al voltant del 25-40% del pagament dels rescats, mentre que els afiliats reben el 60-75% restant pel seu paper en la realització dels atacs. A l'agost de 2021, LOCKBIT GROUP va començar a reclutar persones amb accés a informació privilegiada amb el següent missatge publicat al fons de pantalla de Windows col·locat en els dispositius xifrats:

"Li agradaria guanyar milions de dòlars? La nostra empresa obté accés a les xarxes de diverses empreses, així com informació privilegiada que pot ajudar-lo a robar les dades més valuoses de qualsevol empresa. Vostè pot proporcionar-nos les dades comptables per a l'accés a qualsevol empresa, per exemple, nom d'usuari i contrasenya per a RDP, VPN, correu electrònic corporatiu, etc. Obri la nostra carta en el seu correu electrònic. Llanci el virus proporcionat en qualsevol ordinador de la seva empresa. Les empreses ens paguen el rescat per al desxifrat d'arxius i la prevenció de fugida de dades."

Modus Operandi

Com s'ha explicat prèviament, el *modus operandi* de LOCKBIT GROUP consisteix a infiltrar-se als sistemes de les víctimes, xifrar les dades i exigir un rescat a canvi de la clau de desxifrat. A més, el grup amenaça amb filtrar les dades robades de les víctimes si no es paga el rescat.

4.2 Dridex Group

DRIDEX GROUP és un grup de ciberdelinqüents centrat a desenvolupar, distribuir i beneficiar-se de troians i *ransomware*. Es presumeix que DRIDEX GROUP és una branca de la colla darrere de GAMEOVER ZEUS (també conegut com el 'CLUB DELS NEGOCIS'). En els últims anys, les TTP (Tàctiques, tècniques i procediments) de DRIDEX GROUP semblen estar canviant, implementant *ransomware* en sistemes infectats i centrant-se a comprometre objectius d'alt valor.

Alies

DRIDEX GROUP, EVIL CORP, INDRIK SPIDER, GOLD DRAKE, EVILCORP, SILVERFISH, DEV-0243, UNC2165, MX1R.

Objectiu

Benefici econòmic mitjançant l'adquisició de credencials bancàries d'usuaris o prenent el control del navegador web de l'usuari i exigint el pagament dels rescats.

Descripció

DRIDEX GROUP està centrat a desenvolupar, distribuir i beneficiar-se de troians bancaris i *ransomware*. Aquest actor d'amenaça s'ha vinculat a DRIDEX (un successor de BUGAT, CRIDEX i FEODO) i LOCKY; i, més recentment, al *ransomware* BITPAYMER (també

conegut com FRIEDEX). El grup està compost principalment per ciberdelinqüents d'Europa de l'Est (moldaus, romanesos i russos).

DRIDEX va aparèixer per primera vegada el juny de 2014, només un mes després del desmantellament de GAMEOVER ZEUS per part de les forces de l'ordre el maig de 2014, durant l'OPERACIÓ TOVAR. A causa d'aquesta i altres raons, com les similituds de codi entre GAMEOVER ZEUS i DRIDEX, es presumeix, com ja havíem avançat, que DRIDEX GROUP és una branca de la colla darrere de GAMEOVER ZEUS. Un dels supòsits líders de DRIDEX GROUP, Andrey Ghinkul, va ser arrestat l'octubre de 2015. Si bé l'arrest de Ghinkul va conduir a una caiguda dels atacs de DRIDEX a curt termini, el grup ha demostrat ser resistent malgrat l'arrest d'alt perfil.

Aquest actor d'amenaces ha estat canviant d'eina des de principis de 2020, amb motiu d'una acció de l'Oficina de Control d'Actius Estrangers (OFAC) del Departament del Tresor dels Estats Units contra el grup. La sanció de l'OFAC contra la banda criminal va plantejar un desafiament per al grup, que ara intenta evadir les sancions imposades canviant les eines utilitzades, com el *ransomware* HADES, PHOENIX CRYPTOLOCKER i MACAW.

Per a evitar sancions han usat el *ransomware* LOCKBIT. En aquest atac en particular, pel que sembla Dridex Group va emprar el *ransomware* LOCKBIT per a xifrar els arxius de la víctima i exigir el pagament a canvi de la clau de desxifrat.

Modus Operandi

Realitzen campanyes d'*spam* malicioses que contenen URL no de confiança, documents de Microsoft Office, arxius ZIP o qualsevol altre arxiu adjunt amb una càrrega maliciosa en el seu interior. Mantenen una arquitectura complexa composta per múltiples servidors C&C i de ex-filtració, i capes d'anonimització.

Accedeixen a una xarxa a través d'una màquina considerada com a feble (servidors RDP de força bruta, instal·lar actualitzacions falses, etc.). Una altra forma d'accés és utilitzar infeccions DRIDEX existents i després aplicar tècniques de reconeixement de xarxa i moviment lateral per a continuar comprometent els sistemes. Posteriorment, quan es troben les màquines crítiques, les infecten amb *ransomware*.

4.3 DEV-504

DEV-504 ha desplegat *ransomware* contra organitzacions d'alt perfil com a afiliat de molts esquemes de Ransomware-as-a-Service (RaaS).

Alies

DEV-0504.

Objectiu

Guanys econòmics.

Descripció

DEV-0504 ha estat un afiliat de moltes operacions diferents de Ransomware-as-a-Service (RaaS) des de 2020. DEV-0504 va començar inicialment desplegant el *ransomware* RYUK fins al maig de 2021 per després canviar a REVIL i, més tard, a LOCKBIT 2.0, BLACKMATTER, CONTI i BLACKCAT. La decisió de canviar d'una operació RaaS a una altra pot deure's a múltiples motius, com una operació policial en el cas de REVIL, o passar a un altre projecte amb millors marges de benefici.

Segons els investigadors de Microsoft, DEV-0504 aparentment es basa en la compra d'accés a la xarxa dels intermediaris d'accés inicial per entrar en una organització objectiu, a continuació, utilitzen PSEXEC per a moure's lateralment, intentar desactivar el programari antivirus i desplegar programari maliciós.

Modus Operandi

Unir-se com a afiliat a operacions de Ransomware-as-a-Service (RaaS) per a desplegar *ransomware* amb finalitats lucratives.

4.4 Bassterlord

L'actor d'amenaces BASSTERLORD afirma que en 2019 va ser contractat per un mentor per a desenvolupar campanyes de correu brossa dirigides a bancs i oficines financeres estrangeres. Aquest mentor, que va brindar assessorament, suposadament és un afiliat de SODINOKIBI. A partir d'aquest any, BASSTERLORD es va especialitzar a vendre accés a escriptori remot, principalment, mitjançant força bruta.

BASSTERLORD té accés a quatre eines: REVIL, LOCKBIT, RANSOMEX I ABBADON. L'actor d'amenaces també ofereix formació i tutoria com a servei.

Alies

BASSTERLORD, BASTERLORD, FISHEYE.

Objectiu

Obtenció de guanys financers.

Descripció

Bassterlord és un petit equip de pirates informàtics que afirma estar en l'escena clandestina des de 2016, treballant en una varietat d'activitats delictives.

En el seu perfil del fòrum XSS, BLASTERLORD indica que el seu origen és moldau. Altres fonts afirmen que BLASTERLORD és ucraïnès. No obstant això, en una publicació de l'actor, esmenten que el salari a la seva ciutat era en rubles, moneda oficial de Rússia. Com a tal, és clar que l'actor d'amenaces és d'un país d'Europa de l'Est o Àsia Central, però la seva procedència no és clara, ja que no se sap si és de Rússia, Ucraïna o Moldàvia.

Bassterlord ha comunicat que té accés a quatre eines: REVIL, LOCKBIT, RANSOMEX i ABBADON però en 2021, per exemple, només van usar LOCKBIT i ABADDON.

Modus Operandi

A través d'atacs de força bruta, Bassterlord obté accés a escriptoris remots de diferents empreses i després embeni aquests accessos.

5. CAMPANYES RELLEVANTS

El *ransomware* LOCKBIT ha estat utilitzat en diversos atacs a empreses i organitzacions de tot el món. A continuació, es presenten algunes de les campanyes més rellevants de LOCKBIT:

Empresa municipal Aguas do Porto, Portugal

VIST PRIMER	**08/02/2023**
VIST ÚLTIM	**18/02/2023**

El 8 de febrer del 2023, l'empresa d'aigua municipal portuguesa ÁGUAS DO PORTO va anunciar que havia estat objecte d'un ciberatac encara que aquest no va interrompre l'accés als serveis públics de proveïment d'aigua i sanejament. Aquesta entitat va treballar en estreta col·laboració amb el Centre Nacional de Ciberseguretat i la Policia Judicial per restablir les condicions normals d'operació.

L'actor d'amenaça LOCKBIT GROUP es va atribuir l'autoria de l'atac i va amenaçar de fer pública la informació. CNN Portugal va informar que LOCKBIT havia apuntat prèviament al proveïdor portuguès de serveis informàtics DIVULTEC i, entre la informació filtrada pels adversaris, hi havia contrasenyes de ÁGUAS DO PORTO.

Ajuntament de Medellín, Colòmbia

VIST PRIMER	**01/02/2023**
VIST ÚLTIM	**07/02/2023**

El 2 de febrer del 2023, l'Alcaldia de Medellín va anunciar a través de TWITTER, que un ciberatac d'origen desconegut va afectar els servidors del seu sistema d'emergència i seguretat denominat «Sistema Integrat d'Emergències i Seguretat» (SIES-M).

El 6 de febrer, l'actor d'amenaces LOCKBIT va incloure en l'entitat governamental en la seva DATA LEAK SITE (DLS), i va amenaçar de publicar documents confidencials si la suma del rescat sol·licitat no es pagava abans del 27 de febrer. Les captures de pantalla publicades com a mostra inclouen informació d'identificació personal dels empleats i bases de dades relacionades amb delictes, homicidis i trucades d'emergència per suïcidi.

Royal Mail, Regne Unit

VIST PRIMER	**11/01/2023**
VIST ÚLTIM	**07/02/2023**

L'11 de gener del 2023, el servei de correus britànic ROYAL MAIL va publicar un comunicat en el qual anunciava que, a causa d'un incident cibernètic, havia interromput els enviaments internacionals. Segons aquest comunicat, els sistemes informàtics per l'enviament de cartes i paquets a l'estranger s'havien vist greument aturats i, com a resultat, demanaven als clients que deixessin d'enviar temporalment qualsevol article d'exportació a la xarxa mentre es resolia el problema.

Mitjans de comunicació britànics com ara la BBC i THE TELEGRAPH, van confirmar l'endemà que la causa de la interrupció seria un atac de *ransomware* dut a terme per LOCKBIT GROUP. No obstant això, el 13 de febrer LOCKBIT GROUP va publicar un missatge en el fòrum de parla russa XSS afirmant que no tenien relació amb l'atac. Però també va confirmar en el mateix fòrum que, efectivament, un afiliat va ser el responsable de l'atac.

SickKids, Hospital infantil de Toronto, Canadà

VIST PRIMER	**18/12/2022**
VIST ÚLTIM	**05/01/2023**

El 18 de desembre del 2022, l'HOSPITAL FOR SICK CHILDREN DE TORONTO (SICKKIDS) va sofrir un atac de *ransomware* que va deixar molts dels seus sistemes inaccessibles, la qual cosa va afectar directament les operacions de l'hospital.

Després d'aquest anunci, l'hospital va publicar un comunicat confirmant que des de la nit del 18 de desembre havien estat treballant amb experts externs per a implementar solucions alternatives i restaurar l'accés al sistema una vegada que fos segur fer-lo. Van afirmar conèixer el desxifrador gratuït, però van confirmar que, fins al moment, no l'havien usat per a restaurar els seus sistemes i que no s'havia efectuat cap pagament de rescat. La possibilitat d'emprar o no el desxifrador gratuït es va deixar d'avaluar pels experts externs que havien estat treballant en l'incident.

El 31 de desembre, tretze dies després de l'incident, LOCKBIT GROUP va publicar un anunci en la seva DATA LEAK SITE (DLS), web en la qual publiquen les dades que comprometen, en el qual es disculpa formalment per l'atac i oferia a l'hospital un desxifrador gratis. Segons la seva declaració, l'atac va ser comès per un afiliat que va violar les seves regles i, com a resultat, va ser bloquejat.

Per al 5 de gener de 2023, des de l'hospital van afirmar que es va poder restaurar aproximadament el 80% dels sistemes prioritaris, aquells que tenen un impacte directe

en les operacions de l'hospital. En aquest últim comunicat, la institució no brinda detalls addicionals sobre si la restauració s'ha dut a terme o no amb l'ús del desxifrador gratuït.

L'incident ha tingut un ampli impacte no sols en els mitjans de comunicació, sinó també en els fòrums clandestins, on el grup ha estat criticat per les seves accions malgrat haver-se disculpat públicament i haver facilitat el desxifrador gratuït.

Centre Hospitalier Sud Francilien, França

VIST PRIMER	**21/08/2022**
VIST ÚLTIM	**23/09/2022**

Segons un comunicat publicat pel CENTRE HOSPITALIER SUD FRANCILIEN (CHSF), el 21 d'agost del 2022, el centre va sofrir un atac informàtic a la xarxa a la 1:00 h, que va fer inaccessibles el programari comercial de l'hospital, els sistemes d'emmagatzematge i el sistema d'informació relacionat amb les admissions de pacients. Aquest atac va arribar a interrompre els serveis d'emergència i les cirurgies. En primer lloc, es van adoptar les mesures pertinents per a garantir la seguretat dels pacients i, seguidament, la unitat de crisi va contactar a l'AGÈNCIA NACIONAL DE SEGURETAT DELS SISTEMES D'INFORMACIÓ (ANSSI). Segons la recerca tècnica realitzada per ANSSI, l'atacant ja estava accedint al sistema d'informació de la CHSF de Corbeil-Essonnes, a través d'un accés VPN, deu dies abans d'activar el *ransomware*.

El 7 de setembre de 2022, LOCKBIT GROUP va amenaçar de divulgar les dades robades de l'hospital el 22 de setembre. L'actor d'amenaces va afirmar tenir informació personal confidencial de clients, acords d'associació i correspondència confidencial amb les autoritats; i va oferir la descàrrega completa o la destrucció de les dades robades a canvi d'1 milió de dòlars. L'hospital es va negar a pagar el rescat i, finalment, les dades robades es van publicar el 23 de setembre. Es tractaria d'informació especialment confidencial, procedent dels historials mèdics de pacients de l'hospital, segons una recerca de FRANCE INFO.

Accenture

VIST PRIMER	**30/07/2021**
VIST ÚLTIM	**23/08/2021**

ACCENTURE va patir un ciberatac el 30 de juliol del 2021 que va comprometre 2.500 ordinadors d'empleats i socis. LOCKBIT GROUP va exigir un rescat de 50 milions de dòlars per recuperar 6 TB de dades ex-filtrades. Es va col·locar un temporitzador de compte

regressiu al DATA LEAK SITE (DLS) per marcar el final del període en el qual es pot efectuar el pagament abans que el grup de *ransomware* publiqui les dades en línia.

L'empresa va emetre un comunicat intern en el qual afirmava que, si bé els ciberdelinqüents van poder adquirir uns certs documents que feien referència a un petit nombre de clients i uns certs materials de treball que havien preparat per als clients, cap de la informació era de naturalesa altament confidencial. Així mateix, segons ACCENTURE, no va haver-hi impacte en les operacions ni en els sistemes dels seus clients.

Xarxa ferroviària de Merseyrail, Regne Unit

VIST PRIMER	**30/07/2021**
VIST ÚLTIM	**23/08/2021**

L'abril del 2021, LOCKBIT GROUP va xifrar la xarxa ferroviària MERSEYRAIL del Regne Unit amb el seu *ransomware* personalitzat. LOCKBIT GROUP va revelar aquest ciberatac tant a empleats com a la premsa, a través de l'accés que van obtenir al correu electrònic corporatiu. El correu, amb l'assumpte, "Atac de ransomware LOCKBIT i furt de dades" va ser enviat des del compte d'Andy Heath, director de MERSEYRAIL. El missatge venia acompanyat d'una imatge adjunta on es mostrava informació delicada d'un empleat de la companyia.

6. RECOMANACIONS

Tal com hem explicat, el *ransomware* LOCKBIT representa una amenaça per les empreses i entitats en general. Per tant, s'han d'establir mesures de protecció per garantir que les organitzacions resisteixin qualsevol mena de *ransomware* o atac maliciós que exigeixi una compensació. Cada versió és una oportunitat per canviar el joc, tal com s'ha vist en LOCKBIT 3.0, i els ciberdelinqüents de *ransomware* continuaran evolucionant en els seus enfocaments i els seus atacs.
Una protecció eficaç contra el *ransomware* implica bloquejar l'*endpoint* i evitar que el programari maliciós continuï expandint-se a cada pas en la cadena d'atac, però mai a costa de l'usuari final. És important adoptar una defensa de múltiples capes, inclosos els controls de seguretat d'*endpoints*. Això ajudarà a aconseguir un equilibri entre la seguretat i la productivitat. D'una banda, es protegeixen els *endpoints* i, per un altre, s'automatitzen les elevacions de privilegis per als usuaris finals, de manera transparent, amb la finalitat de desmantellar la cadena d'atac.

A continuació, esmentem algunes mesures concretes que poden dur-se a terme:

- **Implementar contrasenyes segures.** Moltes vulneracions de comptes ocorren a causa de l'ús de contrasenyes fàcils d'endevinar o que són tan simples que una eina d'algorismes les descobreix ràpidament. Triar contrasenyes segures és clau, per la qual cosa aquestes han de ser llargues i amb variacions de caràcters.
- **Activar l'autenticació multifactor.** Els atacs de força bruta es poden detenir agregant capes addicionals de protecció en els inicis de sessió amb contrasenya. Es poden incloure mesures com la biometria o els autenticadors de claus de dispositius USB físics en tots els teus sistemes quan sigui possible.
- **Limitar permisos d'usuari.** Els permisos han d'avaluar-se, simplificar-se i ser molt estrictes amb els permisos dels comptes d'usuari. Cal prestar especial atenció als permisos assignats als usuaris dels *endpoints* i els comptes de TI amb permisos de nivell d'administrador. Així mateix, els dominis web, les plataformes de col·laboració, els serveis de reunions en la web i les bases de dades de les empreses han d'estar protegits.
- **Eliminar els comptes d'usuari des-actualitzats i no utilitzar-les.** És possible que alguns sistemes més antics tinguin comptes d'empleats anteriors que mai es van desactivar ni van tancar. L'últim pas d'una revisió dels sistemes hauria d'incloure l'eliminació d'aquests possibles punts febles.
- **Assegurar-se que les configuracions del sistema segueixin tots els procediments de seguretat.** Això pot portar un temps, però revisar les configuracions existents pot revelar nous problemes i directives obsoletes que

poden posar a la teva organització sota risc d'atac. Els procediments operatius estàndard s'han de tornar a avaluar periòdicament per a mantenir-los actualitzats contra les noves amenaces cibernètiques.

- **Realitzar còpies de seguretat de tot el sistema i imatges netes dels equips locals.** Les organitzacions han de crear còpies de seguretat periòdicament per a estar al dia de qualsevol canvi important en els sistemes. És important mantenir còpies de seguretat dels arxius crítics i assegurar-se que els sistemes estiguin actualitzats i protegits contra les vulnerabilitats conegudes per a evitar el risc d'infecció per *ransomware*. L'única protecció real contra la pèrdua permanent de les dades és una còpia sense connexió. S'ha de considerar la possibilitat de tenir diversos punts de còpia de seguretat rotatius per si ocorregués que una còpia de seguretat es contamini amb una infecció de *malware*.

7. GLOSSARI

Bug

És un error de codi en un programa informàtic. El procés de trobar errors abans que ho facin els usuaris del programa es diu depuració (debugging).

Ciberatac

Intent deliberat d'un ciberdelinqüent d'obtenir accés a un sistema informàtic sense autorització servint-se de diferents tècniques i vulnerabilitats per la realització d'activitats amb finalitats malicioses, com ara el robatori d'informació, extorsió del propietari o simplement danys al sistema.

Data Leak

Una fuga de dades o Data Leak és la pèrdua de confidencialitat de la informació d'una organització, empresa o individu, mitjançant l'obtenció d'aquesta o el coneixement del contingut d'aquesta per part de persones no autoritzades per a això.

EDR

Endpoint Detection and Response (EDR) és un enfocament integrat en capes per a la protecció de *endpoints* que combina el monitoratge constant en temps real i l'anàlisi de dades de *endpoints* amb una resposta automatitzada basada en regles.

Enginyeria Social

És un conjunt de tècniques que usen els ciberdelinqüents per a enganyar els usuaris i aquests els enviïn dades confidencials, infectin els seus ordinadors amb programari maliciós o obrin enllaços a llocs infectats.

Malware

És un tipus de programari que té com a objectiu danyar o infiltrar-se sense el consentiment del seu propietari en un sistema d'informació. El mot neix de la unió dels termes en anglès de programari maliciós: *malicious software*. Dins d'aquesta definició té cabuda un ampli ventall de programes maliciosos: virus, cucs, troians, *backdoors*, *spyware*, etc. La part que comparteixen tots aquests programes és el seu caràcter nociu o lesiu.

Phishing

El *phishing* fa referència a l'enviament de correus electrònics que semblen ser de fonts de confiança (com ara bancs, companyies d'energia etc.) però que en realitat pretenen manipular al receptor per robar informació confidencial.

Ransomware

El *ransomware* és un tipus de programari maliciós que bloqueja les dades o el dispositiu informàtic d'una víctima i amenaça de mantenir-lo bloquejat, o alguna cosa pitjor, tret que la víctima pagui un rescat a l'atacant.

Ransomware-as-a-Service (RaaS)

El *Ransomware-as-a-Service* (RaaS) que en català seria: «*ransomware* com a servei» és un model de negoci en el qual actors maliciosos contracten els serveis d'un *ransomware* a través d'un programa d'afiliats i s'encarreguen de portar endavant els atacs.

CLÀUSULA DE CONFIDENCIALITAT