ANDORRA DIGITAL

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

Informe de ciberintel·ligència

RansomHouse

TLP:WHITE

24/05/2023

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	30/05/2023	30/05/2023

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

El present informe té com a objectiu proporcionar un anàlisi de RansomHouse. L'actor d'amenaça en qüestió ha demostrat activitats malicioses i representa un risc significatiu per qualsevol mena d'organització.

RansomHouse és un actor d'amenaça amb una trajectòria bastant curta, ja que va aparèixer en escena a les acaballes de l'any 2021 amb un ciberatac a la seva primera víctima: la SLGA (Saskatchewan Liquor and Gaming Authority), regulador d'alcohol, cànnabis i jocs d'atzar de la província de Saskatchewan, el Canadà.

Fins al març d'enguany era considerat com un grup d'extorsió perquè es dedicaven al furt de dades i demanar un rescat per ells, sense arribar a xifrar els arxius dels equips i els sistemes compromesos. No obstant això, a partir del ciberatac a l'Hospital Clínic de Barcelona canvia el seu modus operandi en utilitzar el ransomware com a part del seu modus operandi.

Al llarg d'aquest informe, es proporcionarà informació sobre les característiques de RansomHouse, el seu modus operandi, els canals de comunicació que empra i les seves principals campanyes. A més, es presentaran recomanacions per mitigar els riscs associats.

Cal destacar que la identificació i el monitoratge continu dels actors d'amenaça és essencial per mitigar els riscs associats amb les activitats cibernètiques malicioses. Aquest informe es presenta com una eina per informar els professionals de la seguretat i als responsables de la presa de decisions sobre les mesures necessàries per salvaguardar els actius digitals i protegir-se de les amenaces plantejades per aquest actor en particular.

Finalment, per una major comprensió del document, es proporciona un conjunt de vocables útils desglossats en un glossari.

3. PERFIL D'ACTOR D'AMENAÇA

A continuació, explicarem qui és l'actor d'amenaça RansomHouse, el seu origen, els seus objectius i motivacions principals.

3.1 Qui és RansomHouse

Tal com hem esmentat, RansomHouse (també conegut com Ransom House) és un actor d'amenaça relativament recent. De fet, el primer atac que se li atribueix va ocórrer al desembre del 2021. No obstant això, aquest grup ha suscitat molt d'interès des de la seva aparició en el panorama de la ciberdelinqüència pel fet que el seu modus operandi és ben particular

Objectiu

Guanys econòmics.

Països Objectiu

Austràlia, el Canadà, Alemanya, Espanya, Indonèsia, Suècia, els Estats Units, Vanuatu, Sud-àfrica.

	**ORÍGEN**	Desconegut		**ESTAT**	Actiu
	**VIST PER PRIMER COP**	10/12/2021		**TIPUS**	Sindicat del Crim
	**VIST PER DARRERA VEGADA**	07/03/2023		**SOFISTICACIÓ**	Avançada

Com hem esmentat, RansomHouse no era considerat com un grup de ransomware pròpiament dit. És a dir, en els seus atacs no utilitzaven aquest tipus de malware. Aquest grup ingressava a les xarxes de les víctimes per explotar vulnerabilitats i així poder prendre dades. D'aquesta manera, obligaven a pagar a les víctimes perquè aquests no poguessin vendre's al millor postor.

Podem dir, que més que un grup de ransomware, es definia com un grup d'extorsió que sempre anaven un pas més enllà degut que publica al seu web tots els furts que comet. D'aquesta manera, si no s'arribava a un acord de rescat amb l'organització compromesa, venen les dades. Amb això, altres grups de cibercriminals podien anar consultant la informació que necessitaven adquirir de les diferents entitats afectades.

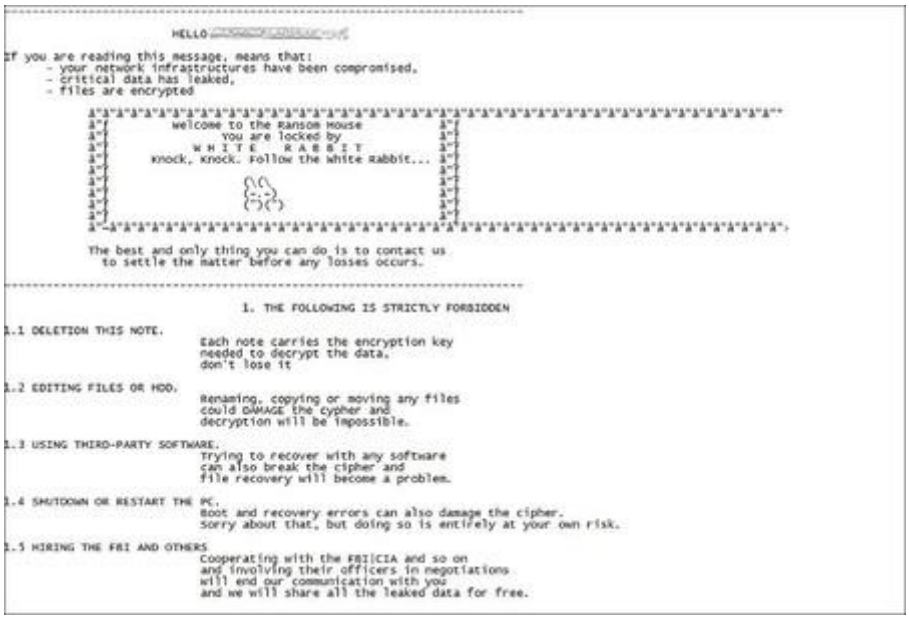
No obstant això, com veurem més endavant, en el ciberatac a l'Hospital Clínic de Barcelona canvien el seu modus operandi donat que van realitzar un segrest d'informació. Per la qual cosa, va passar a ser considerat com un grup de ransomware.

A diferència de la majoria d'altres actors d'amenaça, RansomHouse no sol reivindicar l'autoria dels seus atacs. Aquest grup s'encarrega d'assenyalar i culpabilitzar a les víctimes del ciberatac per no haver pres les mesures pertinents per prevenir-lo i evitar-lo.

En el seu espai de comunicació d'Onion, es defineixen a ells mateixos com "una comunitat de mediadors professionals". I en la secció "sobre" comparteixen un manifest en el qual declara que les organitzacions, i no els ciberdelinqüents que busquen les seves dades, són els veritables "culpables" dels ciberatacs. També mostren el seu descontentament per la falta de reconeixement a l'esforç i temps que dediquen els *bugs bounty* a trobar errors en sistemes i xarxes corporatives. A més, critiquen que, en molts casos, no existeixin programes de recompenses acord amb la seva labor.

Investigadors de seguretat com CYBERINT, han assenyalat que el grup podria estar compost per experts en ciberseguretat cansats d'intentar obtenir recompenses per detectar errors de seguretat en empreses i entitats. En alguns fòrums, s'assegura que aquests antics tècnics estaven frustrats amb les organitzacions per la poca importància que se'ls hi donava a les seves tasques en l'àmbit de la ciberseguretat i, com a conseqüència, van decidir unir-se per castigar a les empreses per la seva inoperància i falta de diligència.

Cal destacar que RansomHouse té una història d'origen una mica estranya, perquè van ser esmentats per primera vegada dins les notes de rescat del ransomware denominat White Rabbit. Pel que sembla, RansomHouse va ajudar al desenvolupament d'aquest malware, però indicant que ells no l'usaven en els seus atacs.



Notes de publicació del ransomware White Rabbit en què, s'esmenta per primera vegada, RansomHouse. Font: BleepingComputer.

3.2 Modus operandi

El modus operandi de RansomHouse ha canviat, segons veurem a continuació:

Abans de l'atac a l'Hospital Clínic de Barcelona

La seva activitat era més simple perquè invertien els seus recursos en la investigació de vulnerabilitats i l'ex-filtració de dades. Es presumeix que RansomHouse operava manualment i s'enfocava solament en una víctima.

Les campanyes de RansomHouse se centraven únicament en l'ex-filtració de dades. La característica particular és que en comptes de xifrar les dades sostretes i fer servir un programa de ransomware, aquest actor d'amenaça es saltava la fase del xifrat i passava directament a exigir diners a canvi de la informació presa. És a dir, extreia dades confidencials a través de l'explotació de vulnerabilitats i després demanava el pagament d'un rescat per no filtrar arxius en línia. No posseïen ni desenvolupaven cap mòdul d'encriptació.

La posició en què el grup extorsionador posava a la víctima era pagar el rescat per no filtrar els arxius aconseguits en el furt. Si la víctima no volia pagar el rescat, seria avergonyida en el seu blog per no haver-se preocupat a pagar per protegir la informació dels seus clients, cosa que podria mostrar una imatge negativa sobre l'entitat davant dels seus clients i accionistes, per exemple. RansomHouse intentava vendre aquests arxius en línia; si els arxius no es compraven, el grup d'amenaces simplement els publicava en un lloc de filtració de dades.

Durant l'atac a l'Hospital Clínic de Barcelona

Tot i haver afirmat que el seu model de negoci no implica xifrar les dades segrestades, en el ciberatac a l'Hospital Clínic de Barcelona van dur a terme un atac més complex en què segresten els arxius del seu target i inhabiliten el seu sistema informàtic. Amb aquesta acció, el grup hauria passat de no paralitzar mai els sistemes de les seves víctimes a tombar una infraestructura crítica com la d'un hospital. Comentarem això més en detall en l'apartat "Campanyes".

3.3 Canals de comunicació

RansomHouse té dos canals de comunicació: Telegram i Onion.

Telegram

Actualment, operen tres canals de Telegram. El primer l'han utilitzat per anunciar cadascuna de les nou accions que han comès, així com les reaccions de les respectives víctimes. A més, també l'han fet servir per compartir com ha estat el procés de negociació amb les diferents organitzacions, donant visibilitat a aquelles que van col·laborar de manera "solidària i responsable", i quines no.

El segon canal de Telegram és un xat en què els seguidors poden comunicar-se amb els administradors del grup i parlar entre ells. Pel que sembla, aquest canal no sol tenir gaire trànsit.

També han obert un nou canal el qual està dirigit a periodistes. L'actor d'amenaça es promociona a si mateix com un gran soci amb el qual treballar, tal com es pot apreciar en el següent missatge:

Do you have special offers for journalists or reporters?

We highly respect the work of journalists and consider information accessibility to be our priority. We have a special program for journalists which includes sharing information a few hours or even days before it is officially published on our news website and Telegram channel: you would need to go through a KYC procedure to apply. Journalists and reporters can contact us via our PR Telegram channel with any questions.

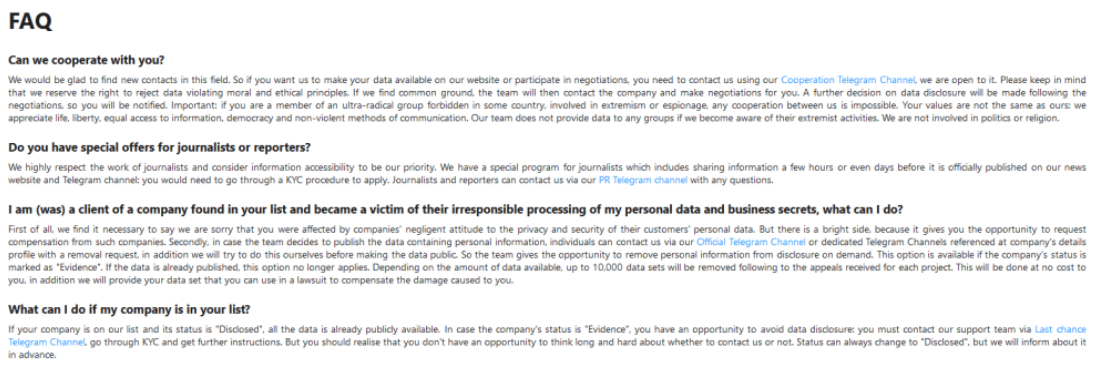
Onion

El segon canal de comunicació és la pàgina d'Onion del grup, que és on s'anuncia la seva llista actual de víctimes juntament amb algunes seccions que expliquen les intencions del grup, etc.

3.4 Regles de joc

RansomHouse té una "ètica" molt marcada que ha seguit en els atacs perpetrats a les seves víctimes. Sempre ho han manifestat en les seves comunicacions i regles que es poden trobar al seu lloc web, la qual cosa, és poc comuna en aquests grups de ciberdelinqüents. Per exemple, a la seva web podem trobar com expliquen que un usuari pot demanar el seu esborrat de dades si apareix en un *leak* fins a un màxim de 10.000 línies.

També manifesten estar en contra de grups ultres o terroristes. Endemés, estan oberts a la captació de possibles nous col·laboradors que comparteixin claus d'accessos o altres dades. Això, es fa a través dels grups de contacte que faciliten a l'apartat de preguntes freqüents.



FAQ

Can we cooperate with you?

We would be glad to find new contacts in this field. So if you want us to make your data available on our website or participate in negotiations, you need to contact us using our Cooperation Telegram Channel, we are open to it. Please keep in mind that we reserve the right to reject data violating moral and ethical principles. If we find common ground, the team will then contact the company and make negotiations for you. A further decision on data disclosure will be made following the negotiations, so you will be notified. Important: if you are a member of an ultra-radical group forbidden in some country, involved in extremism or espionage, any cooperation between us is impossible. Your values are not the same as ours: we appreciate life, liberty, equal access to information, democracy and non-violent methods of communication. Our team does not provide data to any groups if we become aware of their extremist activities. We are not involved in politics or religion.

Do you have special offers for journalists or reporters?

We highly respect the work of journalists and consider information accessibility to be our priority. We have a special program for journalists which includes sharing information a few hours or even days before it is officially published on our news website and Telegram channel: you would need to go through a KYC procedure to apply. Journalists and reporters can contact us via our PR Telegram channel with any questions.

I am (was) a client of a company found in your list and became a victim of their irresponsible processing of my personal data and business secrets, what can I do?

First of all, we find it necessary to say we are sorry that you were affected by companies' negligent attitude to the privacy and security of their customers' personal data. But there is a bright side, because it gives you the opportunity to request compensation from such companies. Secondly, in case the team decides to publish the data containing personal information, individuals can contact us via our Official Telegram Channel or dedicated Telegram Channels referenced at company's details profile with a removal request, in addition we will try to do this ourselves before making the data public. So the team gives the opportunity to remove personal information from disclosure on demand. This option is available if the company's status is marked as "Evidence". If the data is already published, this option no longer applies. Depending on the amount of data available, up to 10,000 data sets will be removed following to the appeals received for each project. This will be done at no cost to you, in addition we will provide your data set that you can use in a lawsuit to compensate the damage caused to you.

What can I do if my company is in your list?

If your company is on our list and its status is "Disclosed", all the data is already publicly available. In case the company's status is "Evidence", you have an opportunity to avoid data disclosure: you must contact our support team via Last chance Telegram Channel, go through KYC and get further instructions. But you should realise that you don't have an opportunity to think long and hard about whether to contact us or not. Status can always change to "Disclosed", but we will inform about it in advance.

4. CAMPANYES RELLEVANTS

Des de la seva aparició en escena a les acaballes del 2021 amb l'atac dirigit a la SASKATCHEWAN LIQUOR AND GAMING AUTHORITY (SLGA) del Canadà, a RansomHouse se li atribueixen més 30 atacs. Amb això, es considera que és un dels grups de ciberdelinqüents més actius dels últims mesos. En el seu punt de mira hi han empreses de Suècia, Canadà, Estats Units, Alemanya, diversos països africans, Colòmbia i Espanya.

La companyia ferroviària sueca DELLNER COUPLERS, el proveïdor de serveis de suport a aerolínies alemanyes AHS Group, el banc JEFFERSON CREDIT UNION (Alabama, Estats Units), ADVANCED MICRO DEVICES (AMD), la multinacional d'atenció sanitària KERALTY, el govern de Vanuatu i SHOPRITE GROUP (una de les cadenes de supermercats més grans del sud d'Àfrica), l'HOSPITAL CLÍNIC DE BARCELONA, són alguns dels exemples més representatius de les 30 víctimes del grup RansomHouse.

A continuació, comentarem cinc de les seves campanyes més rellevants.

Hospital Clínic de Barcelona

VIST PER PRIMER COP	05/03/2023
VIST PER DARRERA VEGADA	07/03/2023

Tal com hem esmentat prèviament, amb aquest atac RansomHouse, el grup canvia el seu modus operandi. En l'atac contra el Clínic recorren al segrest d'informació i a un mètode de doble extorsió, segons van confirmar els Mossos.

Primer, van infectar el sistema informàtic de l'hospital amb un virus que bloqueja l'accés a la informació i exigeixen el pagament d'un rescat per desbloquejar-los. Si la víctima decideix no pagar, els atacants roben les dades i amenacen de vendre'ls a tercers. Si ningú s'interessa a comprar-los, RansomHouse sol fer-los públics a la seva pàgina web o al seu canal de Telegram.

El 5 de març de 2023 l'Hospital Clínic, un dels principals hospitals públics més importants de Catalunya, va patir un atac de ransomware que va afectar greument el laboratori, farmàcia i serveis d'urgències. A més, l'atemptat va afectar també el centre de recerca associat IDIBAPS i tres centres de salut locals dependents del CAPSBE (Consorci d'Atenció Primària de Salut de l'Eixample), en concret el CAP Casanova, CAP Borrell i CAP Les Corts. L'Hospital va patir el robatori i el xifrat de més de 4,5 terabytes de dades personals de pacients i empleats.

Després de l'atac, l'hospital es va posar en contacte amb l'Agència de Ciberseguretat de Catalunya i, de manera coordinada amb la Secretaria de Telecomunicacions i Transformació Digital de la Generalitat, es va activar el protocol d'actuació per mirar de contenir-lo.

L'atac va aconseguir tombar des del primer moment gran part del sistema informàtic del Clínic i, com a conseqüència, la seva operativa es va veure seriosament afectada. Com a resultat, el centre va haver de suspendre 150 intervencions quirúrgiques no urgents i entre el 2000 i el 3000 visites de consultes externes, a més de 400 o 500 extraccions. Segons les notes de premsa de la Generalitat de Catalunya, l'hospital va haver de cancel·lar les cites relacionades amb les cirurgies electives, el centre d'extracció i les consultes externes, posposar la radioteràpia oncològica i redirigir els pacients amb codi urgent (infart, ictus, etc.) a altres centres sanitaris.

Una anàlisi de la firma QuantiKa14 revela importants bretxes de seguretat. L'accés no autoritzat, robatori i segrest de les dades que ha impedit el funcionament habitual de l'hospital s'ha pogut produir per una vulnerabilitat en els sistemes informàtics. Concretament, l'hospital disposava - actualment apagat o fora de servei - d'una intranet connectada a Internet possiblement vulnerable a "Drupalgeddon". I en les dades que aporta es pot comprovar que aquesta intranet estava desenvolupada mitjançant el cms Drupal, però amb una versió desactualitzada, concretament es tractava de la 7. A més, també demostrava que es va trobar més de 600 correus electrònics exposats a internet amb les seves respectives contrasenyes.

El grup RansomHouse li va sol·licitar a la Generalitat el pagament de 4.5 milions de dòlars per poder recuperar tota la informació segrestada. No obstant, la Generalitat es va negar a pagar.

Advanced Micro Devices, Inc. (AMD)

VIST PER PRIMER COP	27/06/2022
VIST PER DARRERA VEGADA	28/06/2022

El ciberatac contra Advanced Micro Devices, Inc (AMD) va ser un dels més sonats, ja que es tracta d'una tecnològica d'alt perfil. RansomHouse va afirmar tenir al seu poder més de 450 GB de dades que haurien estat robats d'AMD el gener del 2022.

El 20 de juny del 2022, el grup va anunciar a través de Telegram que havia hackejat una important empresa i després va dur a terme un concurs per veure si algú podia endevinar de quina empresa es tractava. RansomHouse va proporcionar una endevinalla perquè les persones endevinessin qui era la víctima.

El grup va afirmar a la seva pàgina que havia piratejat la seguretat d'AMD el 5 de gener i va obtenir les dades gràcies a l'ús de contrasenyes febles en tota l'organització. RansomHouse la va criticar després que perpetrés l'atac i la va culpar per haver permès que els seus empleats utilitzessin contrasenyes febles. Aquest actor d'amenaça va afirmar el següent:

> *"Es tractava de tecnologia de punta, de progrés i de màxima seguretat... hi ha molt en aquestes paraules per les multituds. No obstant, sembla que continuen sent simplement paraules embellides i buides de valor quan fins i tot els gegants tecnològics com AMD usen contrasenyes simples com ara 'contrasenya', ' P@ssw0rd', '123456', '123qwe-',*

> *'Contraseña0', 'amd!23', '12345a.' i '12345qert' per protegir les seves xarxes d'intrusions. És una pena que siguin contrasenyes reals utilitzades pels empleats d'AMD, però és una vergonya major pel Departament de Seguretat d'AMD, que obté un finançament significatiu d'acord amb els documents que tenim a les nostres mans, tot gràcies a aquestes contrasenyes".*

RansomHouse afirma no haver-se posat en contacte amb AMD per exigir un rescat, ja que el grup creu que és més interessant i rendible vendre directament les dades extretes a altres actors d'amenaces.

Sofrit Holdings, Africa

VIST PER PRIMER COP	10/06/2023
VIST PER DARRERA VEGADA	14/06/2023

Una altra de les víctimes de RansomHouse fou Shoprite Holdings, la cadena de supermercats més gran d'Àfrica. L'empresa té la seva seu a Sud-àfrica, però té presència en molts més països de l'Àfrica subsahariana, com ara Ghana, Nigèria, Namíbia, Botswana, etc.

L'atac va ser revelat per l'empresa el 10 de juny del 2022, afirmant que les dades dels clients podrien haver-se vist compromeses. Segons el comunicat de premsa que van realitzar, l'atac va poder afectar alguns clients que efectuesisn transferències de diners cap a i dins d'Eswatini, de Namíbia així com de Zàmbia, però va assegurar que no es va veure afectada la informació financera ni els nombres de comptes bancaris.

El 14 de juny de 2022, RansomHouse va revelar l'atac contra Shoprite i va declarar el següent al seu canal de Telegram:

> *"ha passat bastant temps des que ens trobem amb una cosa TAN escandalosa: el seu personal guardava enormes quantitats de dades personals en text sense format o imatges sense processar. Ambdós empacats en arxius arxivats, completament desprotegits [...] Ens vam posar en contacte amb la gerència de Shoprite i els vam convidar a negociar, però l'única cosa que van fer va ser canviar les seves contrasenyes com si així es solucionés tot. Si la seva posició no canvia, la majoria d'aquestes dades es vendrà per ser divulgat al públic. A més de les dades KYC, també vam obtenir moltes altres coses interessants de la companyia. Sí, sembla que els agrada mantenir moltes coses sense protecció".*

Keralty, Colòmbia

A finals de novembre del 2022 el grup va atacar el sistema informàtic de l'empresa Keralty, que opera serveis de salut a 11 països. A Colòmbia és propietària de la EPS Sanitas i de l'empresa Colsanitas Medicina Prepagada, que administren la salut a més de cinc milions de colombians.

A conseqüència de l'atac, els ciutadans no podien programar o accedir digitalment a cites mèdiques, exàmens, o realitzar tràmits administratius. El 19 de desembre RansomHouse va fer públic, a través de Telegram que ells n'eren els responables.

Saskatchewan Liquo rand Gaming Authority (SLGA)

Tal com s'ha esmentat prèviament, la primera víctima de RansomHouse va ser la Saskatchewan Liquor and Gaming Authority (SLGA), com reflectia la llista d'empreses i entitats extorquides en el lloc web de RansomHouse, al qual es pot accedir des de la Dark Web. Allí es publiquen els enllaços URL de les víctimes atacades i extorquides, augmentant l'exposició d'aquestes empreses i usant la informació com un mètode addicional d'extorsió.

5. RECOMANACIONS

Qualsevol organització està exposada a patir un ciberatac, ja que és impossible estar totalment protegit, però sí que es poden prendre algunes mesures per tal d'evitar el furt d'informació. Aquestes mesures podrien ser, per exemple, tenir credencials complexes i diferents entre les diferents plataformes i aplicacions.

Tal com hem explicat, RansomHouse 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 d'atac per part d'aquest o un altre actor similar.

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

- És important adoptar una defensa de múltiples capes, inclosos els controls de seguretat d'*endpoints*.

- Una altra mesura que ha de tenir en compte qualsevol companyia és activar processos de doble verificació en tots els comptes que es pugui. Aquests processos consisteixen en introduir dues claus per entrar a un compte, i la contrasenya, per exemple, és un SMS que s'envia al moment.

- Implementar credencials 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 múltiples variacions de caràcters.

- Activar l'autenticació multifactor. Els atacs de força bruta es poden aturar afegint capes addicionals de protecció als inicis de sessió amb contrasenya. Es poden incloure mesures com la biometria o els autenticadors de claus de dispositius USB físics en tots els vostres 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 a la web i les bases de dades de les empreses han d'estar protegits.

- Utilitzar l'escaneig/filtrat de contingut als servidors de correu. Fent servir aquesta eina s'evita que el ransomware accedeixi als nostres dispositius per una de les principals rutes d'infecció.

- Esborrar els comptes d'usuari desactualitzats o que ja no s'utilitzen. És possible que alguns sistemes més antics tinguin comptes d'empleats anteriors que mai es van desactivar o no es

van arribar a tancar. L'últim pas d'una revisió dels sistemes hauria d'incloure l'eliminació d'aquests possibles punts febles.

- Mantenir els sistemes i programari actualitzats. Endarrerir l'actualització d'un programari pot obrir una porta d'accés als dispositius de l'empresa pels fabricants de ransomware.

- Realitzar còpies de seguretat de tot el sistema i tenir imatges netes dels equips locals. Les organitzacions han de crear còpies de seguretat periòdicament per estar al dia de qualsevol canvi important en els sistemes. És important mantenir còpies de seguretat dels arxius més crítics. 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 còpies de seguretat rotatius per si ocorregués que una còpia de seguretat es contamini amb una infecció de programari maliciós.

- Així mateix, per evitar ser víctima de ransomware és crucial evitar descarregar arxius de fonts desconegudes.

- Formar als empleats perquè reconeguin els signes de phishing als seus correus electrònics.

6. 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).

Bug Bounty

El Bug Bounty es pot definir com una modalitat de seguretat ofensiva en el qual una organització ofereix recompensa a aquells hackers que trobin diferents vulnerabilitats de la seva infraestructura.

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, l'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 això.

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.

Ransomware

El ransomware és un tipus de malware, o 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.

White Hat

El terme barret blanc a Internet es refereix a un hacker ètic, o un expert de seguretat informàtica que s'especialitza en proves de penetració i en altres metodologies per detectar vulnerabilitats i millorar la seguretat dels sistemes de comunicació i informació d'una organització.

CLÀUSULA DE CONFIDENCIALITAT