ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

BreachForums: una plataforma crítica per a l'ecosistema de la ciberdelinqüència

TLP: WHITE

SETEMBRE 2024

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	19/09/2024	23/09/2024

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a 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

La proliferació de fòrums clandestins al web fosc, com ara BreachForums, ha transformat la manera en la qual els actors maliciosos operen a l'ecosistema digital. **BreachForums s'ha consolidat com una plataforma clau per a la compra i venda de dades robades, vulnerabilitats i eines de pirateig**. No només facilita el comerç de la informació compromesa, sinó que també actua com a **punt de trobada per als ciberdelinqüents** que busquen intercanviar tècniques, tàctiques i procediments per dur a terme atacs més sofisticats i perjudicials.

En aquest context, el monitoratge actiu de fòrums com ara BreachForums és fonamental per a la defensa de les organitzacions públiques i privades. Mitjançant la identificació primerenca de les filtracions de dades i la vigilància de les activitats dels ciberdelinqüents, les organitzacions poden anticipar-se a possibles atacs, o, atès el cas, millorar la capacitat de resposta davant d'incidents, a més d'enfortir la infraestructura de seguretat.

L'objectiu d'aquest informe és analitzar de manera exhaustiva BreachForums, i proporcionar **informació detallada sobre el funcionament, la rellevància dins de l'ecosistema de la cibercriminalitat, i la seva implicació en els ciberincidents recents**. També s'abordarà com va sorgir aquest fòrum, i es farà un repàs d'aquells llocs web amb finalitats similars que el van precedir, i s'explicarà el paper que juga actualment en la facilitació d'activitats il·lícites. Aquesta anàlisi no només busca descriure la naturalesa i l'impacte de BreachForums, sinó també subratllar la importància de vigilar activament aquest tipus de plataformes com a part d'una estratègia integral de ciberseguretat.

En un entorn digital on les amenaces són cada vegada més complexes i persistents, **la intel·ligència d'amenaces basada en el monitoratge de fòrums clandestins ha esdevingut una acció crítica.** Aquesta intel·ligència permet a les organitzacions adoptar mesures proactives que limitin els danys potencials. L'informe també destacarà les tècniques i estratègies que les empreses han d'implementar per millorar-ne la resiliència davant dels riscos que representen aquests espais del web fosc, com ara BreachForums.

3. BREACHFORUMS: HISTÒRIA I PREDECESSORS

BreachForums és una plataforma clandestina del web fosc que ha guanyat notorietat com a espai on els ciberdelinqüents poden bescanviar i vendre dades obtingudes de bretxes de seguretat, com també eines per dur a terme atacs cibernètics.

Aquest fòrum actua com un mercat en el qual es transaccionen bases de dades robades, explotadors, credencials filtrades i una gran varietat d'informació delicada. **La naturalesa de la plataforma atrau actors maliciosos de diversos nivells, des de ciberdelinqüents novells fins a actors d'amenaça professionals i reconeguts** que fan servir la informació disponible per impulsar accions a gran escala i d'un impacte potencial molt alt.

3.1. Evolució i predecessors

BreachForums no és un fenomen aïllat, sinó que **és el resultat de l'evolució d'una llarga cadena de fòrums clandestins dedicats a activitats cibercriminals**. Alguns dels seus predecessors més notables van ser RaidForums o Darkode, i van assentar les bases de la popularitat que ha adquirit fins al dia d'avui.

- **RaidForums**: va ser un dels fòrums més rellevants en la venda i distribució de dades compromeses abans de l'aparició de BreachForums. Fundat l'any 2015, RaidForums es va convertir en un mercat de bases de dades filtrades, credencials robades i un altre tipus d'informació delicada. Després de diversos anys operant al web fosc, va ser clausurat el 2022 per les autoritats, cosa que va deixar un buit a la comunitat cibercriminal que BreachForums va ocupar ràpidament.

- **Darkode**: va sorgir abans que RaidForums, i va néixer com un fòrum on es compartien eines de pirateig i s'organitzaven atacs cibernètics en col·laboració entre diferents actors maliciosos. El seu desmantellament l'any 2015, liderat per l'FBI i l'Europol, va ser un cop significatiu per a la comunitat de ciberdelinqüents, tot i que aquesta va migrar ràpidament a altres espais.

- **AlphaBay i Hansa Market**: tot i que aquests fòrums estaven més orientats al comerç de béns il·lícits en general (com ara drogues o armes), també jugaven un paper rellevant en la venda d'explotadors i eines per fer atacs cibernètics. Els seus tancaments el 2017 van marcar un punt d'inflexió en la migració dels ciberdelinqüents cap a fòrums més especialitzats com ara BreachForums.

3.2. Creació de BreachForums

Després de la captura de RaidForums, BreachForums va emergir com l'hereu natural d'aquesta mena de plataformes. **Fundat el 2022, es va posicionar ràpidament com el principal fòrum del web fosc per a la compra i venda de bases de dades robades i altres béns relacionats amb la cibercriminalitat**. Aquesta nova plataforma va absorbir molts dels usuaris i venedors que operaven a RaidForums, i va consolidar la seva posició com un espai clau dintre de l'ecosistema criminal digital.

El fòrum **està dissenyat per facilitar transaccions en criptomonedes com ara el bitcoin i el monero, cosa que garanteix un alt grau d'anonimat** tant per a compradors com per a venedors. A més a més, la seva estructura és similar a la dels seus predecessors: els venedors ofereixen fragments de bases de dades com a mostra per atraure els compradors, i els moderadors del fòrum faciliten les interaccions i garanteixen la credibilitat de les transaccions.

4. ACTIVITAT I MODUS OPERANDI A BREACHFORUMS

BreachForums, com molts altres fòrums del web fosc dedicats a la cibercriminalitat, segueix un conjunt de pràctiques i estratègies ben definides per facilitar l'intercanvi d'informació, dades robades i eines de pirateig entre actors maliciosos.

En aquest apartat, es desglossen en detall les **activitats principals que es duen a terme al fòrum, com també les tècniques emprades pels seus usuaris per maximitzar l'efectivitat de les seves operacions** mentre mantenen l'anonimat.

4.1. Publicació i venda de bases de dades robades

Un dels pilars principals de BreachForums és l'intercanvi de BBDD compromeses. Aquestes solen provenir de bretxes de seguretat que han pogut afectar des d'empreses privades fins a entitats governamentals. Les dades publicades i venudes a BreachForums abasten gran varietat d'informació, entre la qual caldria destacar:

- **Credencials d'accés** (noms d'usuari, contrasenyes, adreces de correu electrònic).
- **Dades personals** (noms complets, adreces, números de telèfons, dates de naixement).
- **Informació financera** (targetes de crèdit, números de compte bancari, historials financers).
- **Dades mèdiques** (informació de pacients, historials clínics, assegurances de salut).
- **Documentació confidencial** (contractes, informes interns, estratègies de negocis).

Procés de venda:

Els actors maliciosos solen seguir un **procés estructurat per vendre aquestes dades**:

- **Mostres de dades**: els venedors generalment comparteixen una **petita porció de les dades robades com a prova de la seva autenticitat**. Aquest és un pas clau per convèncer els possibles compradors que el lot complet d'informació és real i valuós.
- **Preus variables**: el cost de les bases de dades pot variar **en funció de la quantitat i qualitat de les dades, la reputació del venedor, com és de delicada la informació, i el valor d'ús potencial per part d'altres ciberdelinqüents.** Per exemple, les bases de dades que contenen informació bancària o credencials d'accés a xarxes corporatives solen ser més valuoses que aquelles que només contenen informació personal bàsica.
- **Mètodes de pagament**: les transaccions **generalment es fan a través de criptomonedes com ara el bitcoin i el monero, que són difícils de rastrejar** i garanteixen l'anonimat tant del comprador com del venedor. El monero, en particular, és preferit per molts ateses les seves característiques avançades de privacitat.

4.2. Validació i reputació dels venedors

Com en altres mercats clandestins, la reputació és fonamental per establir la confiança entre els usuaris. Atès que moltes transaccions involucren grans quantitats de diners o l'adquisició d'informació valuosa, **el fòrum implementa diversos mecanismes per protegir els compradors** i assegura que les transaccions es facin de manera legítima:

- **Sistemes de reputació**: els venedors poden rebre **qualificacions i comentaris d'altres usuaris que hagin comprat prèviament els seus productes**. Com millor sigui la reputació del venedor, més confiança genera en futurs compradors. Les ressenyes inclouen la qualitat de les dades, l'exactitud de la informació i la rapidesa en el procés de lliurament.

- **Moderació del fòrum**: hi ha moderadors que ajuden a mediar en les disputes i, en alguns casos, **actuen com a intermediaris per verificar l'autenticitat de les dades ofertes pels venedors**. Això protegeix els compradors de ser estafats per venedors que intentin vendre informació falsa o duplicada.

- **Sistemes d'*Escrow***: alguns fòrums, inclòs el BreachForums, poden fer servir un sistema d'«escrow» o fideïcomís, en el qual **el pagament del comprador queda en mans d'un tercer neutral fins que es confirma el lliurament satisfactori** de les dades o serveis oferts.

4.3. Col·laboració entre ciberdelinqüents

BreachForums no només és un mercat per a la venda de dades robades; **també és un lloc on els ciberdelinqüents col·laboren i comparteixen informació** sobre noves tècniques d'atac, eines i vulnerabilitats. Aquest intercanvi de coneixements i recursos és una de les característiques més perilloses del fòrum perquè **permet que actors maliciosos menys experimentats puguin accedir a eines sofisticades que faciliten la seva participació en activitats delictives**.

- **Explotadors i vulnerabilitats**: els usuaris comparteixen vulnerabilitats descobertes en sistemes operatius, aplicacions, dispositius IoT i xarxes corporatives. Aquests explotadors permeten que altres ciberdelinqüents executin atacs sense necessitats de tenir coneixements tècnics avançats.
- **Eines de pirateig i scripts automatitzats**: es venen eines de pirateig que faciliten l'explotació de vulnerabilitats i la intrusió a xarxes i sistemes. Aquestes eines inclouen programari de pesca, kits d'explotació de vulnerabilitats, i scripts automatitzats per escanejar i atacar llocs web.
- **Tutorials i guies**: també és habitual trobar tutorials detallats i guies pas a pas **sobre com dur a terme ciberatacs**, com el desplegament de programari de segrest, atacs DDoS, pesca dirigida, i com evadir sistemes de detecció o anàlisi forense.

4.4. Intercanvi d'informació estratègica

BreachForums també actua com un fòrum de discussió on els membres intercanvien informació i estratègies per millorar les seves capacitats d'atac. Aquests intercanvis inclouen:

- **Tècniques d'anonimització:** es comparteixen tècniques avançades per ocultar registres d'activitat maliciosa com l'ús de servidors intermediaris, VPN, xarxes TOR, i altres maneres de xifratge i emmascarament.

- **Estafes i fraus**: es discuteixen tàctiques per dur a terme fraus financers, com la clonació de targetes de crèdit, el robatori d'identitat i fraus fiscals. Aquests intercanvis solen ser valuosos per als ciberdelinqüents interessats en la monetització directa de la informació robada.

- **Blanqueig de criptomonedes**: a mesura que les criptomonedes es converteixen en el principal mitjà de transacció per a activitats il·lícites, també es comparteixen guies sobre com "netejar" o blanquejar criptomonedes, i fer-les més difícils de rastrejar.

4.5. Atacs coordinats

En alguns casos, BreachForums serveix com a lloc de trobada per coordinar atacs cibernètics organitzats. Hi ha grups de ciberdelinqüents que poden **planejar i executar atacs massius a partir d'informació compartida en el fòrum**, especialment en relació amb les vulnerabilitats crítiques o grans filtracions de dades. Aquests atacs poden ser coordinats contra empreses, governs o infraestructures crítiques, cosa que incrementa el nivell de risc i el dany potencial.

4.6. Interaccions amb grups de programari de segrest

BreachForums també té vincles estrets amb grups de programari de segrest, que fan servir el fòrum per **compartir informació sobre les xarxes compromeses, a més de filtrar dades robades com a part de les seves tàctiques d'extorsió**. Sovint, els actors de programari de segrest publiquen mostres de dades de les víctimes al fòrum, per tal de pressionar les organitzacions perquè paguin el rescat exigit a canvi de no fer pública la informació completa.

5. CASOS D'ESTUDI

5.1. Bretxa de seguretat d'Uber (2022)

5.1.1 Context de l'incident

El setembre del 2022, Uber va patir una bretxa de seguretat important quan **un actor maliciós va aconseguir obtenir accés a una sèrie de sistemes interns de l'empresa**, incloses eines internes, el panell d'administració de G Suite i dades crítiques relacionades amb la infraestructura d'Uber.

Aquesta violació va permetre que l'atacant tingués accés a:

- Sistemes de pagament i facturació.
- Documentació interna.
- Eines de control d'accés.
- Informes de seguretat i vulnerabilitats internes.

L'atacant **va fer servir enginyeria social per comprometre el compte d'un empleat** a través de pesca dirigida, cosa que li va permetre saltar-se les mesures d'autenticació multifactor (MFA) i aconseguir accés a la xarxa interna d'Uber.

5.1.2 BreachForums i la publicació de l'atac

L'autoria de l'atac se la va atribuir Lapsus$, un actor d'amenaça reconegut per altres incidents de perfil alt. Va fer ús de BreachForums com una de les plataformes principals per donar a conèixer i filtrar informació de l'atac.

El rol de BreachForums en aquest cas inclou:

1. **Divulgació inicial de l'atac**: a través de BreachForums, van començar a aparèixer discussions i publicacions en les quals es detallaven els mètodes fets servir per l'atacant per comprometre la xarxa d'Uber. Això va incloure l'explicació detallada de com es va fer servir l'enginyeria social per enredar els controls de seguretat d'Uber, i proporcionar a altres ciberdelinqüents informació valuosa sobre tàctiques i procediments efectius.

2. **Distribució de proves de l'atac**: com és comú en aquests fòrums, l'atacant va publicar captures de pantalla i fragments de dades robades per demostrar que havia aconseguit accedir als sistemes d'Uber. Aquesta pràctica és utilitzada per guanyar credibilitat dins del fòrum i per atraure possibles compradors interessats en dades addicionals que encara no podrien haver estat exposades.

3. **Venda de dades compromeses**: encara que no tota la informació robada va ser publicada de manera lliure, a BreachForums es va començar a discutir sobre la possibilitat de vendre accés a algunes dades o fer servir l'accés compromès per a futurs atacs. Això demostra el valor que fòrums com ara BreachForums proporcionen com a mercats il·legals per a la compra i venda d'accés a sistemes compromesos.

4. **Anàlisi de vulnerabilitats**: BreachForums també va ser un lloc on altres ciberdelinqüents i experts en pirateig van discutir les possibles vulnerabilitats que Uber havia deixat exposades, i van assenyalar els punts dèbils en els seus sistemes de seguretat. Això no només va amplificar la reputació de l'atacant, sinó que també va proporcionar a altres actors maliciosos informació sobre com atacar sistemes corporatius similars.

5.1.3 Impacte de l'incident

L'atac a Uber va tenir una sèrie de conseqüències importants, tant per a l'empresa com per a l'ecosistema de ciberseguretat en general:

- **Reputació i confiança**: Uber es va haver d'enfrontar a una crisi de confiança entre els seus clients i empleats a causa de l'exposició dels seus sistemes interns i d'informació crítica. La divulgació en fòrums com ara BreachForums va augmentar la visibilitat de l'incident, i va amplificar el dany a la seva reputació.

- **Dany financer**: tot i que els detalls financers no es van fer públics, els costos associats amb la resposta a l'incident, les recerques i les millores en la ciberseguretat van representar una càrrega significativa per a l'empresa.

- **Creixement de l'amenaça d'enginyeria social**: va posar en relleu l'efectivitat dels atacs d'enginyeria social, en particular quan es combinen amb tècniques avançades de manipulació humana per superar les barreres d'autenticació multifactor. La discussió d'aquests mètodes a BreachForums va augmentar l'interès en aquesta mena de tàctiques dins de la comunitat cibercriminal.

5.1.4 Rellevància de BreachForums a l'ecosistema criminal

L'atac a Uber és un exemple clar de com BreachForums s'ha convertit en una plataforma clau per a la divulgació, discussió i comercialització de dades compromeses en incidents de perfil alt, i oferir als ciberdelinqüents:

- **Anonimat i confiança**: l'estructura del fòrum i la seva política de moderació permeten que els atacants operin de manera anònima mentre guanyen credibilitat entre els seus iguals mitjançant la publicació de dades robades o proves d'accés compromès.

- **Intercanvi de coneixements**: a més d'actuar com un mercat negre de dades, BreachForums també és un espai perquè els actors maliciosos comparteixin coneixements, estratègies i eines. L'anàlisi d'atacs amb èxit com el d'Uber es fa servir per millorar les tàctiques d'altres atacants.

- **Plataforma per al cibercrim**: com en altres fòrums clandestins, BreachForums funciona com una plataforma on es pot comerciar amb l'accés a sistemes compromesos, informació robada i eines de pirateig. Això facilita el creixement i l'evolució de la ciberdelinqüència, perquè els actors menys experimentats poden aprendre i participar en aquests mercats il·lícits.

5.1.5 Conclusió

L'atac a Uber el 2022 és un exemple clar de com BreachForums l'han feta servir com una plataforma de divulgació i comercialització d'informació compromesa en grans incidents de ciberseguretat. Aquesta mena de fòrums no només juguen un paper central en l'exposició de les vulnerabilitats de grans organitzacions, sinó que també serveixen com a hubs per a la col·laboració entre ciberdelinqüents, i amplificar l'impacte dels atacs.

El cas d'Uber posa en relleu la importància del monitoratge de fòrums clandestins com ara BreachForums dintre d'una estratègia integral de ciberintel·ligència. La capacitat d'identificar i actuar ràpidament quan les dades es fan públiques en aquests espais és crucial per mitigar el dany potencial i comprendre més bé les tàctiques que fan servir els actors maliciosos per comprometre les xarxes corporatives.

6. CIBERINTEL·LIGÈNCIA: LA CLAU PER PROTEGIR-SE DE BREACHFORUMS

Per combatre amenaces com les que emergeixen de llocs com ara BreachForums, la ciberintel·ligència s'erigeix en una eina indispensable, perquè dona visibilitat al moviment que es registra en aquests espais opacs i facilita la presa de decisions basades en dades, amb un enfocament proactiu i preventiu.

Permet recopilar, analitzar i fer servir informació relacionada amb amenaces cibernètiques per anticipar-se a atacs, enfortir la seguretat i reduir l'impacte de possibles incidents. En el context de fòrums com ara BreachForums, la ciberintel·ligència es fa servir per:

- Fer un monitoratge continuat d'activitats al web fosc i fòrums clandestins, permetre que les organitzacions identifiquin aviat bretxes de seguretat i la venda d'informació delicada robada.
- Analitzar patrons de comportament d'actors maliciosos, cosa que facilita la identificació d'amenaces emergents, grups de ciberdelinqüents organitzats i noves tàctiques d'atac.
- Detectar vulnerabilitats compartides i discutides en aquests fòrums abans que siguin explotades massivament pels ciberdelinqüents.
- Dotar de capacitat d'anticipació. En lloc de reaccionar només després de l'incident, la ciberintel·ligència permet anticipar amenaces abans que es materialitzin, cosa que és vital per evitar el dany abans que succeeixi.
- Reduir i minimitzar els riscos derivats de dades delicades que s'estan compartint, que es poden haver vist compromeses. També permet conèixer noves tàctiques que estan fent servir els ciberdelinqüents. Així, les organitzacions poden implementar mesures específiques per tancar les bretxes de seguretat abans no siguin explotades.
- Resposta ràpida en cas que es produeixi un incident, perquè permet identificar amb precisió l'abast de l'atac.

7. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.