

UNIVERSIDAD CENTROAMERICANA “JOSÉ SIMEÓN CAÑAS”



TRABAJO DE INVESTIGACIÓN SED

ALUMNO:

MENDOZA YANES, VÍCTOR ENRIQUE – 00046517

ASIGNATURA:

SEGURIDAD EN ENTORNOS DE DESARROLLO

DOCENTE:

ELISA ALDANA CRISTINA CALDERÓN

ANTIGUO CUSCATLÁN, 26 DE SEPTIEMBRE DE 2019

Descripción de la empresa

Nombre: Bethesda.

Descripción:

Bethesda está formada principalmente por 2 sub-divisiones: Bethesda Softworks y Bethesda Game Studios. La primera es una distribuidora de videojuegos lo que significa que se encarga de la manufactura y comercialización de videojuegos, pero no son ellos los encargados del diseño y desarrollo de estos, similar al trabajo realizado por una editorial. Por otro lado Bethesda Game Studios se dedica al desarrollo y creación de videojuegos.

Estas 2 divisiones de Bethesda trabajan juntas para sacar al mercado varios juegos al año, algunos de ellos muy portentosos y afamados por la comunidad lo que ha convertido a Bethesda en una de las compañías de videojuegos más grandes en el mercado actual siendo una de las pocas (junto con Microsoft, Sony, Nintendo y otras) en tener su propia conferencia en el E3, evento en el que se reúnen las mayores compañías relacionadas a videojuegos y presentan trailers y noticias sobre sus próximos lanzamientos.

Ataques sufridos

Robo de información de usuarios, Junio 2011.

En Junio de 2011 un grupo llamado *LulzSec* se declaró responsable de haber forzado su entrada en la red de Bethesda. Dicho grupo ha sido culpable de otros tantos ataques a diferentes empresas, entre ellas Sony, de la cual robaron la información de 1 millón de usuarios aproximadamente, esto sucedió poco antes del ataque a Bethesda.

El ataque se concentró en el sitio web de uno de los videojuegos de la empresa, llamado Brink. Los hackers aseguraron haber entrado a la red y obtenido la información de los usuarios desde dos meses antes de hacer público el ataque y le pedían a la compañía que por favor “arreglara su basura”, citando sus palabras.

Bethesda confirmó que un grupo de hackers había logrado acceder a sus servidores pero que datos valiosos como la información financiera de sus usuarios o tarjetas de crédito no había sido comprometida, sin embargo, el grupo de hackers posiblemente tuvo acceso a información de sus usuarios como nombres, contraseñas y correos electrónicos. La empresa rápidamente sacó un comunicado

en el que expresaban que el problema había sido resuelto pero recomendaba a sus usuarios cambiar inmediatamente su contraseña.

Afortunadamente para Bethesda, el modo de trabajar de los hackers es el de entrar a las redes inseguras para exponer posibles fallos en la seguridad para que estos puedan ser corregidos y, según ellos, no robaron ninguna información de sus servidores.

```
Some weeks ago, we smashed into Brink with our heavy artillery Lulz  
Cannons and decided to switch to ninja mode. From our LFI entry point,  
we acquired command execution via local file inclusion of enemy fleet  
Apache vessel. We then found that the HTTPD had SSH auth keys, which  
let our ship SSH into other servers. See where this is going?
```

```
We then switched to root ammunition rounds.  
And we rooted... and rooted... and rooted...
```

```
After mapping their internal network and thoroughly pillaging all of  
their servers, we grabbed all their source code and database passwords,  
which we proceeded to shift silently back to our storage deck.
```

```
Please find enclosed everything we took, excluding one thing -  
200,000+ Brink users. We actually like this company and would  
like for them to speed up the production of Skyrim, so we'll  
give them one less thing to worry about. You're welcome! :D
```

```
Please keep making awesome games, guys, and you should  
totally add an official LulzSec top hat to new releases.
```

```
But anyway, bwahahaha... >:]
```

```
LINKS:
```

```
http://thepiratebay.org/torrent/6467131/Bethesda\_internal\_data
```

Imagen 1. Parte del comunicado publicado por LulzSec donde anuncian haber hackeado Bethesda.

Fallo en el sistema de soporte al cliente, Mayo 2018.

Junto con el lanzamiento de uno de sus títulos más esperados: Fallout 76, Bethesda estaba regalando una bolsa en una edición especial del juego mucho más cara. El problema resultó ser que aparentemente la compañía había dicho que la bolsa estaría hecha de lona y cuando empezaron a llegar a las casas de las personas que la habían comprado, se dieron cuenta que, en realidad, estaba hecha de nylon.

Lo anterior llevó a que muchos usuarios se sintieran estafados por el producto entregado y decidieran acudir al soporte de la empresa para pedir un reembolso, sin embargo, cuando estos empezaron a mandar “tickets” con su caso se dieron cuenta que tenían acceso a los tickets de otros usuarios, así como a la información personal de estos y la posibilidad de cerrar y dar por concluido el ticket de un usuario.

Al parecer existía un error de software en la página web de Bethesda por el que los usuarios tenían acceso al módulo de administrador pudiendo así ver información que solo debería estar disponible para empleados de la compañía. Dicho error provocó la filtración de información personal de los usuarios como el correo electrónico, dirección y hasta la tarjeta de crédito con la cual se compró el juego. Los usuarios, ya molestos por la calidad del producto entregado sumado a la posibilidad de que su información haya sido filtrada, hicieron todo lo posible por hacer conocer sus casos y finalmente el juego vendió muy por debajo de lo esperado.

Inmediatamente se supo del error Bethesda cortó toda conexión a la página web mientras solucionaban el problema. En la explicación oficial dada por la empresa esta afirma que ninguna contraseña o números de tarjeta completos fueron revelados y pedía perdón a todos los usuarios afectados. En un segundo comunicado que publicó Bethesda poco después dio más detalles acerca del suceso ocurrido.

La información comprometida fue la de usuarios que mandaron tickets durante un período de 45 minutos el 5 de Diciembre de 2018 y que, según ellos, menos de 123 tickets fueron los afectados en este lapso. De estos 123 tickets no más de 65 fueron los comprometidos y recalcaron que información clave como contraseñas, o números completos de tarjetas de crédito fueron filtrados.

Subject	ID	Description	Status	Time
Power Armor Edition Bag Replacement Request Form	181205-005058	Power Armor Edition Bag Replacement Request Form	Waiting on agent	Moments Ago
Power Armor Edition Bag Replacement Request Form	181204-009158	Power Armor Edition Bag Replacement Request Form	Closed by Customer	Moments Ago
Power Armor Edition Bag Replacement Request Form	181205-005051	Power Armor Edition Bag Replacement Request Form	Waiting on agent	Moments Ago
I linked the wrong Xbox account to my Bethesda account and would ...	181205-005036	I can't unlink my account	Closed by Customer	Moments Ago
Power Armor Edition Bag Replacement Request Form	181205-005045	Power Armor Edition Bag Replacement Request Form	Waiting on agent	Moments Ago
Power Armor Edition Bag Replacement Request Form	181205-005031	Power Armor Edition Bag Replacement Request Form	Waiting on agent	3 Minutes Ago
Power Armor Edition Bag Replacement Request Form	181205-005026	Power Armor Edition Bag Replacement Request Form	Waiting on agent	4 Minutes Ago
It says my budget is full even though there is nothing in my camp ...	181205-005015	Item Reset	Investigation Ongoing	5 Minutes Ago
Bethesda Customer Support: Login			Customer	1 Day

Imagen 2. Información confidencial a la que los usuarios tenían acceso.

Referencias

- Constantin, L. (14 de Junio de 2011). *LulzSec Hacks Bethesda Softworks and Dumps Private Data*. Obtenido de Softpedia News: <https://news.softpedia.com/news/LulzSec-Hacks-Bethesda-Softworks-and-Dumps-Private-Data-205898.shtml>
- Dissent. (13 de Junio de 2011). *Bethesda Softworks hacked, personal data 'stolen'*. Obtenido de DataBreaches: <https://www.databreaches.net/bethesda-softworks-hacked-personal-data-stolen/>
- Gault, M. (6 de Diciembre de 2018). *Bethesda Accidentally Leaked Personal Data of 'Fallout 76' Customers Looking for Help*. Obtenido de Vice: https://www.vice.com/en_us/article/59vywz/these-lawyers-want-to-sue-bethesda-over-fallout-76-refunds
- Lynley, M. (13 de Junio de 2011). *LulzSec: "You're welcome!" for hacking Bethesda, not stealing anything*. Obtenido de VentureBeat: <https://venturebeat.com/2011/06/13/lulzsec-bethesda-hack/>
- Plunkett, L. (12 de Mayo de 2018). *Bethesda Support Leaks Fallout 76 Customer Names, Addresses & Phone Numbers*. Obtenido de Kotaku: <https://kotaku.com/bethesda-support-leaks-fallout-76-customer-names-addre-1830892930>
- Valentine, R. (06 de Diciembre de 2018). *Bethesda's support ticket system leaked personal information*. Obtenido de game industry: <https://www.gamesindustry.biz/articles/2018-12-06-bethesas-support-ticket-system-reportedly-leaked-personal-information>