

# **Gestión de incidentes de seguridad**

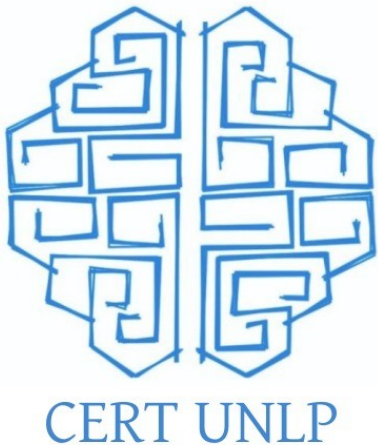


# Gestión de incidentes

- La gestión de incidentes de seguridad implica:
  - Recepción de incidentes
  - Evaluar su pertinencia
  - Clasificación / Priorización
  - Gestión del incidente
    - Realizar distintos tipos de notificaciones
    - Coordinar acciones



# Consideremos que trabajamos en el CSIRT académico CERTUNLP



- **Comunidad objetivo:**  
Usuarios y servicios de la UNLP.
- **Bloque IPV4 163.10.0.0/16**
- **Dominio: unlp.edu.ar**



# Recepción

- Los reportes pueden provenir de:
  - Un usuario de nuestra comunidad objetivo
  - Un usuario externos
    - WHOIS / RDAP
  - Herramientas que podemos tener realizando distintos tipos de funciones:
    - Monitoreo de seguridad de la red
    - Análisis de vulnerabilidades



# Pertinencia

- No todo lo que nos reportan es un incidente
- Para determinar si lo que nos reportan:
  - ¿es un incidente de seguridad?
  - En caso afirmativo,
    - ¿afecta a alguien de nuestra comunidad objetivo?
    - ¿es ocasionado por un recurso de nuestra comunidad objetivo?



# Evaluar su pertinencia

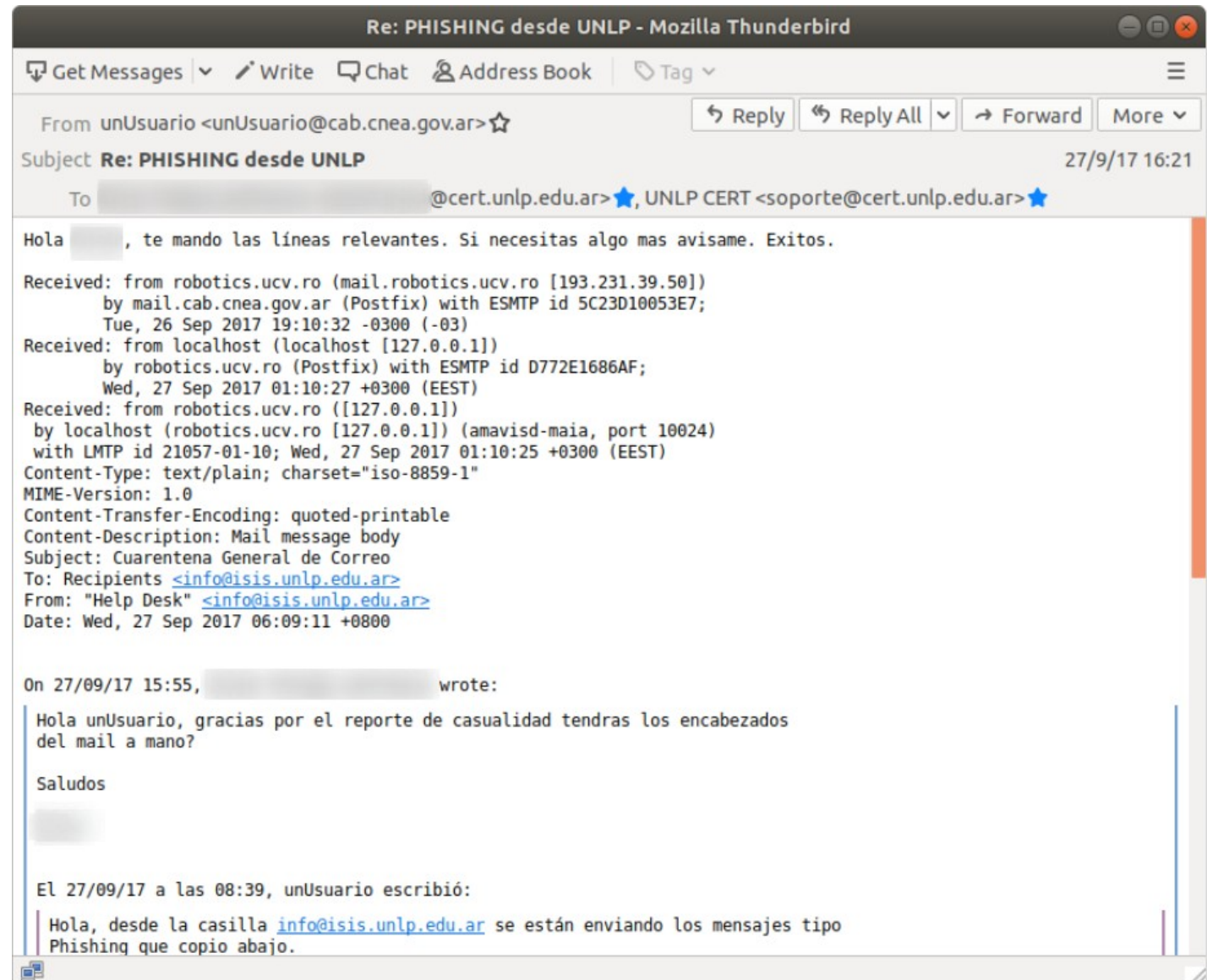
## Ejemplo 3- parte 1

¿Es pertinente?



# Evaluar su pertinencia

## Ejemplo 3- parte 2



¿Es pertinente?



# Clasificación / Priorización

- Los incidentes se clasifican y priorizan en función de su criticidad.
- En caso de tener muchas cosas para gestionar, conviene dirigir los esfuerzos a los incidentes más importantes.
- La criticidad puede ser estimada a partir de:
  - El tipo de incidente
  - los recursos afectados por el incidente y
  - el impacto que podría tener en actividades críticas de la organización





# Clasificación de incidentes

🔗 Incident Types (7/54)			
Name			
cryptojacking	Scan	DOS SNMP	Open VNC
Undefined	Shellshock	Open DNS	Cisco Smart Install
Open LDAP	SSL Poodle	Open Elasticsearch	Data Breach
Open MongoDB	Suspicious Behavior	Open IPMI	Open MDNS
Open SNMP	Phishing Mail	Open NTP monitor	Bruteforce
Phishing Web	RPZ Botnet	Open SSDP	Copyright
RPZ DBL	RPZ Malware Aggressive	Open Telnet	Drupal Remote Code Execution
RPZ Drop	DOS NTP	Botnet	Heartbleed
RPZ Malware	Open Chargen	Deface	Malware
Poodle	Open MSSQL	DNS zone transfer	Open memcached
Spam	Open SMB	Information Leakage	Open QOTD
SQL Injection	Open TFTP	Open ISAKMP	Open RDP
Open NTP version	Blacklist	Open NetBios	
Open Portmap	DOS chargen	Open Redis	



# Ejemplo priorización

Una buena práctica para priorizar eventos es, por ejemplo, utilizar niveles de prioridad.

Por ejemplo:

- **Nivel 1:** incidentes con bajo impacto para la institución. Por ejemplo, un incidente que afecta a un equipo de trabajo (desktop):
  - Envío de spam
  - Malware en PC de usuario



# Ejemplo priorización (cont)

- **Nivel 2:** incidentes con alto impacto a terceros que no comprometen los datos de la organización.

Por ejemplo:

- Un conjunto de estaciones de trabajo infectadas con algún malware y realizando un ataque de DOS a un servidor externo;



# Ejemplo priorización (cont)

- **Nivel 3:** incidentes con alto impacto sobre la organización. Son eventos que requieren una rápida intervención.

Por ejemplo:

- Un sistema crítico de la organización comprometido.
- Un defacement en un sistema con información sensible de la organización



# Notificación

- La notificación de un incidente de seguridad es un aspecto clave en el proceso de resolución del mismo.
  - En esta etapa se contacta y comunica al responsable de un determinado recurso, los hechos relevantes que ayuden en la resolución del incidente.
  - Se debe proporcionar evidencia para que las partes implicadas puedan investigar el incidente y actuar en consecuencia.



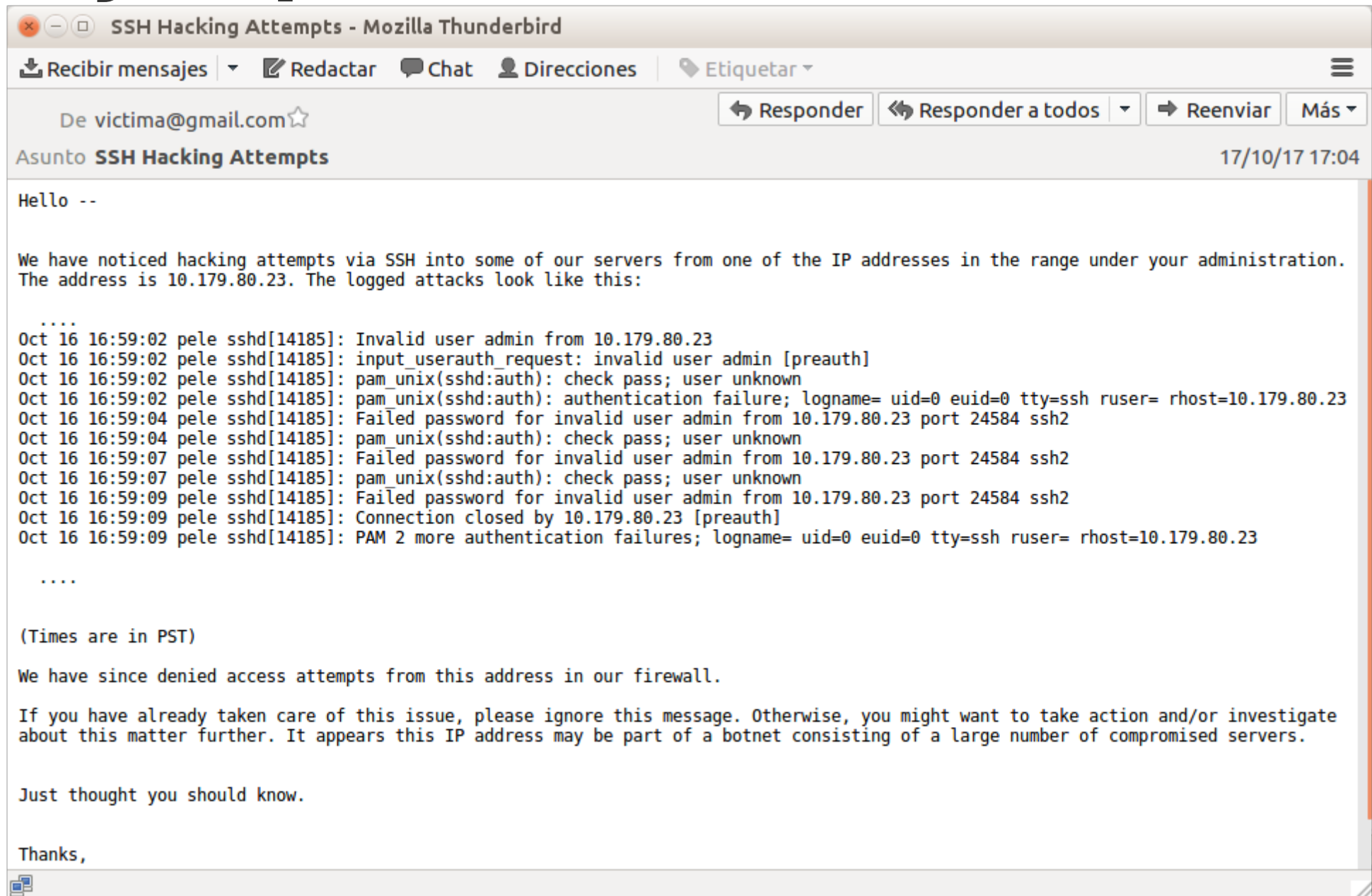
# Notificación

Datos fundamentales que deben estar presentes en una notificación:

- Contacto de quien reportó el problema;
- Incidente de seguridad:
  - Tipo de incidente
  - Descripción del ataque
  - Dirección IP de origen del ataque
  - Dirección IP o red de destino del ataque
- Evidencia (preferentemente en formato texto):
  - Registros asociados con el ataque
  - Los registros deben proveer información de tiempo. Debe ser clara la zona horaria utilizada



# Ejemplo notificación

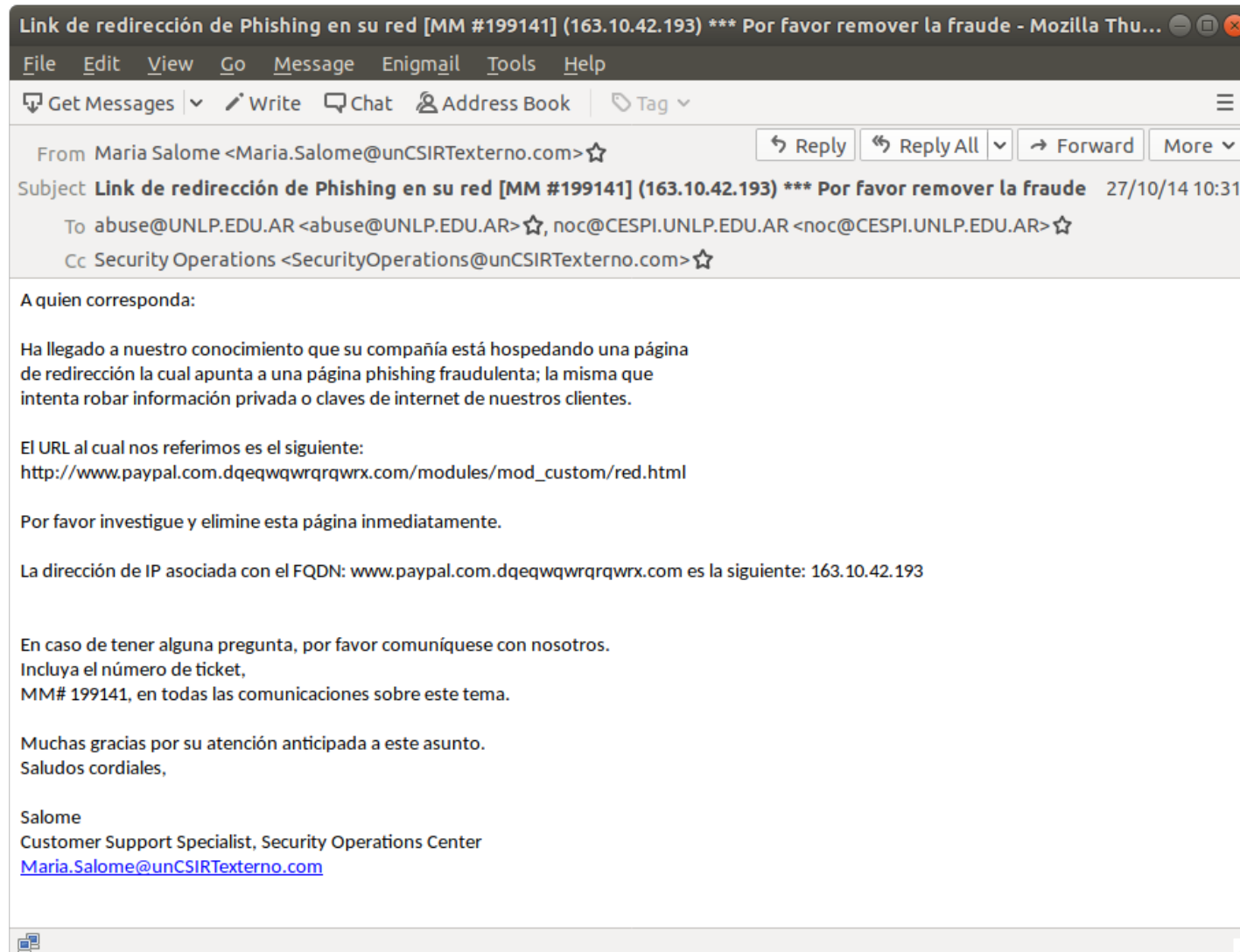


# **Gestión de incidentes análisis de casos basados en la realidad**





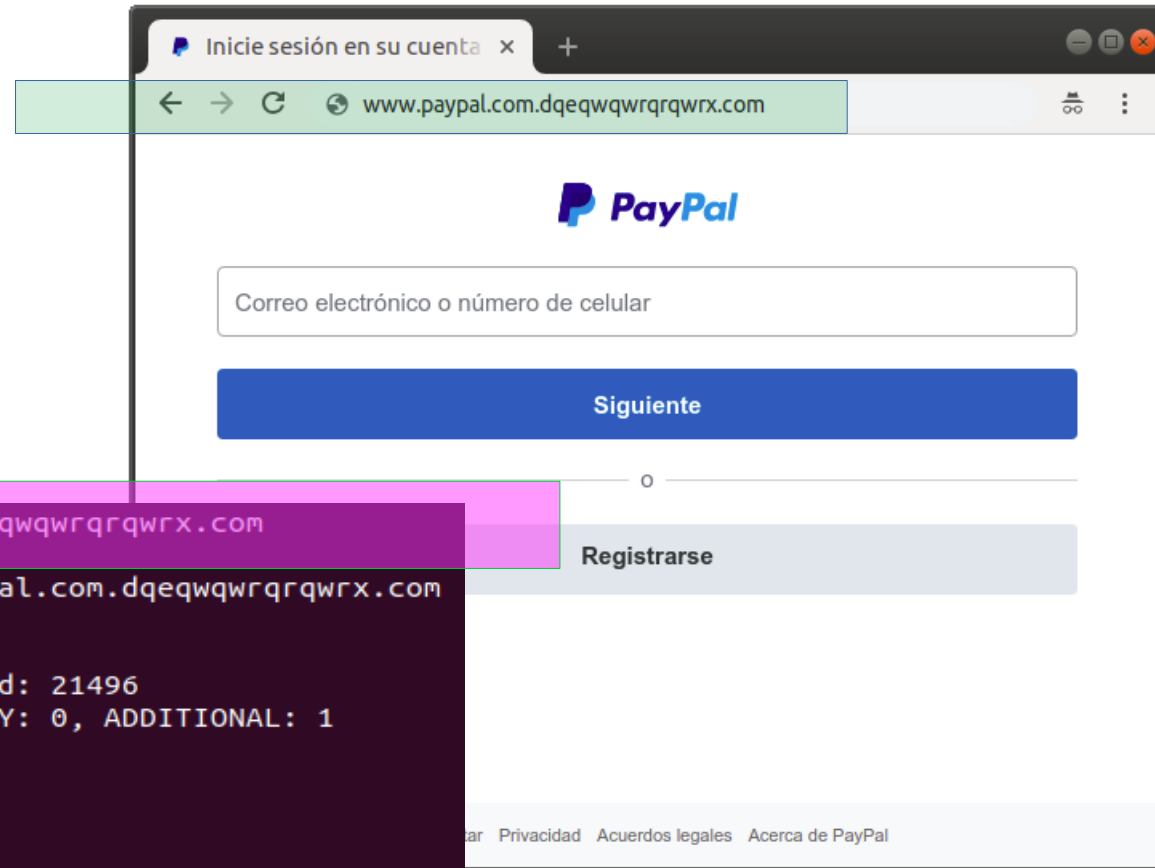
# Caso 1 - Recepción



¿Es pertinente?



# Es pertinente



```
nico@nico-PORTEGE-Z30-B:~$ dig www.paypal.com.dqeqwqwrqrqwr.com
```

```
;; <<>> DiG 9.11.3-1ubuntu1.5-Ubuntu <<>> www.paypal.com.dqeqwqwrqrqwr.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21496
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.paypal.com.dqeqwqwrqrqwr.com. IN A
```

```
;; ANSWER SECTION:
www.paypal.com.dqeqwqwrqrqwr.com. 0 IN A      163.10.42.193
```

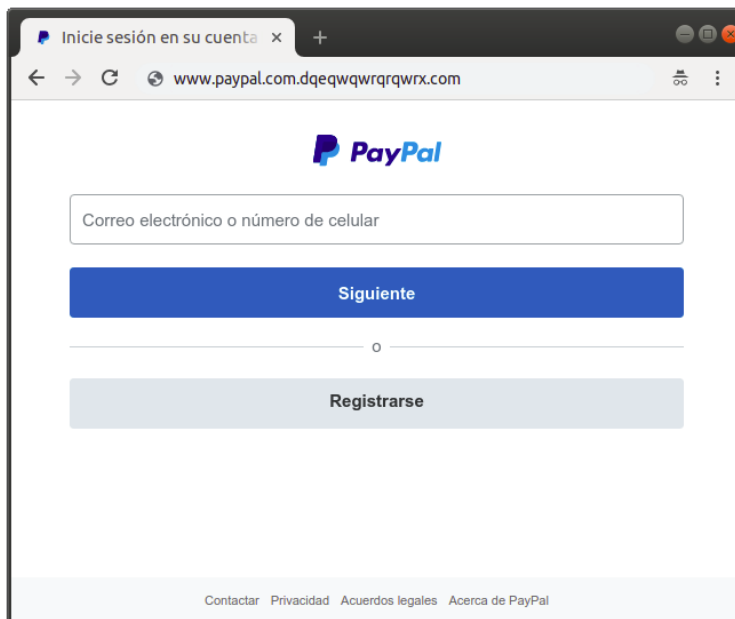
```
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue May 21 15:37:58 -03 2019
;; MSG SIZE rcvd: 78
```

```
nico@nico-PORTEGE-Z30-B:~$
```



# ¿Es un incidente? ¿Tipo?

- A la hora de evaluar un incidente, puede ser necesario tomar precauciones....
  - Descargar la página con herramientas desde la línea de comando (curl / wget)
  - Utilizar el modo incógnito de los navegadores.



# Situación hipotética:

El responsable del Servidor donde se aloja el phishing, nos comentó luego de que le informamos sobre el incidente, que encontró que la página de phishing hace por atrás varias cosas cada vez que una víctima cae en el engaño:

- 1) Registra las credenciales en un archivo TXT en dicho servidor
- 2) Envía las credenciales a `dqeqwqwrqrqwrwx@gmail.com`
- 3) Hace un POST a:

`http://130.206.13.20/index.php?id=$USUARIO&c=$PASSWORD`



# Gestión y notificación

1) Registra las credenciales en un archivo TXT en dicho servidor  
**Informar a Paypal de las credenciales comprometidas**

2) Envía las credenciales a dgeqwqwrqwrqx@gmail.com  
**Notificar a gmail de la cuenta utilizada para leakear información**

3) Hace un POST a:  
[http://130.206.13.20/index.php?id=\\$USUARIO&c=\\$PASSWORD](http://130.206.13.20/index.php?id=$USUARIO&c=$PASSWORD)  
**Notificar al contacto de abuse de 130.206.13.20 sobre el compromiso de dicho servidor para ataques**



# Contención y erradicación

## Contención:

- Eliminar las páginas del servidor vulnerable

## Erradicación

- Encontrar la vulnerabilidad que permitió el defacement:
  - Evaluar otros recursos que pudieron ser afectados.
  - ¿posibilidad de escalamiento?
  - ¿Movimiento lateral?
  - Parchear o reinstalar el sistema



# Gestión de incidentes

## Escenario 2



# Caso 2 - Recepción





# Evaluar su pertinencia



# ¿Es un incidente? ¿Tipo?

- Minería de criptomonedas ...
  - ¿Para beneficio personal?
  - ¿Para beneficio de un tercero?
    - Malware
    - Explotación de alguna vulnerabilidad con posterior ejecución de código.



# Notificación

[TLP:AMBER][CERTUNLP] Incidente de tipo "miner" en 163.10.42.193 [ID:146317] - Mozilla Thun...

Get Messages | Write | Chat | Address Book | Tag

From alertas@cert.unlp.edu.ar★

Reply | Reply All | Forward | More

Subject [TLP:AMBER][CERTUNLP] Incidente de tipo "miner" en 163.10.42.193 [ID:146317] 21/5/19 09:58

To alertas@cert.unlp.edu.ar★, admin\_red\_42@unlp.edu.ar☆

**CERTunlp** **TLP:AMBER**

Estimado Administrador de la red 42,

Lo contactamos porque hemos detectado que el host/servidor 163.10.42.193 está realizando minería de criptomonedas. Si bien esto puede deberse a un proceso que usted haya ejecutado, es muy probable que alguien haya logrado acceder al mismo y programar la ejecución de dicha tarea.

**Problemas derivados**

La PC podría estar infectada o haber sido comprometida de alguna forma para que un tercero ejecute comandos.

**Cómo verificar el problema**

Verificar los procesos que se están ejecutando en el host.

**Mas información**

<https://www.csoonline.com/article/3267572/encryption/how-to-detect-and-prevent-crypto-mining-malware.html>

1 attachment: \_75286ef51d375554052491df10865d1cc77c92e7.txt 444 bytes Save

\_75286ef51d375554052491df10865d1cc77c92e7.txt 444 bytes



# Gestión de incidentes

## Escenario 3



# Caso 3 - Recepción

From [pepe@unlp.edu.ar](mailto:pepe@unlp.edu.ar) ☆

Subject **password (abc123) for [pepe@unlp.edu.ar](mailto:pepe@unlp.edu.ar) is compromised**

23/10/18 13:10

To [abc123 <pepe@unlp.edu.ar>](mailto:abc123@unlp.edu.ar) ☆

Hello!

I'm a hacker who cracked your email and device a few months ago.  
You entered a password on one of the sites you visited, and I intercepted it.

This is your password from [pepe@unlp.edu.ar](mailto:pepe@unlp.edu.ar) on moment of hack: abc123

Of course you can will change it, or already changed it.  
But it doesn't matter, my malware updated it every time.



# Contención

- El servidor de correo estaba mal configurado
  - El registro SPF no estaba configurado
  - No pide autenticación cuando el que recibe es un usuario propio:
    - El que envía es un usuario propio. Si se hubiese pedido autenticación, un tercero no podría haber mandado este mail.



# Notificación del incidente

- El SPAM/PHISHING fue recibido desde 184.22.82.123
- El contacto de abuso es: abuseIPv4@ais.co.th

```
Tue, 23 Oct 2018 06:20:09 -0300 (ART)
Received: by mail.unlp.edu.ar (Postfix, from userid 999)
      id AC1D61FF58; Tue, 23 Oct 2018 06:20:09 -0300 (ART)
X-Greylist: delayed 133 seconds by postgrey-1.34 at amavis; Tue, 23 Oct 2018 06:20:08 ART
Received: from 184-22-82-0.24.nat.tls1b-cgn03.myaisfibre.com (unknown [184.22.82.123])
      by mail.unlp.edu.ar (Postfix) with ESMTTP id B53A71FF58
      for <pepe@unlp.edu.ar>; Tue, 23 Oct 2018 06:20:08 -0300 (ART)
Message-ID: <FBB7A22BEBEE3E622E3BB27277A7FBB7@FJY3I0E0BYJ>
From: <pepe@unlp.edu.ar>
To: "abc123" <pepe@unlp.edu.ar>
```

## [ IP NETWORK ]

```
Handle: 184.22.64.0 - 184.22.127.255
Start Address: 184.22.64.0
End Address: 184.22.127.255
CIDRs: 184.22.64.0/18
IP Version: v4
Country: TH
Type: ALLOCATED NON-PORTABLE
Last Changed: Sat, 16 Jan 2016 07:09:53 -0000
Remarks: -- description --
1: AIS Fibre
```

## [ ENTITY ]

```
Handle: IRT-AWN-CO-LTD-TH
Common Name: IRT-AWN-CO-LTD-TH
Email: abuseIPv4@ais.co.th
Email: abuseIPv4@ais.co.th
Roles: Abuse
Last Changed: Fri, 22 May 2015 09:43:10 -0000
```



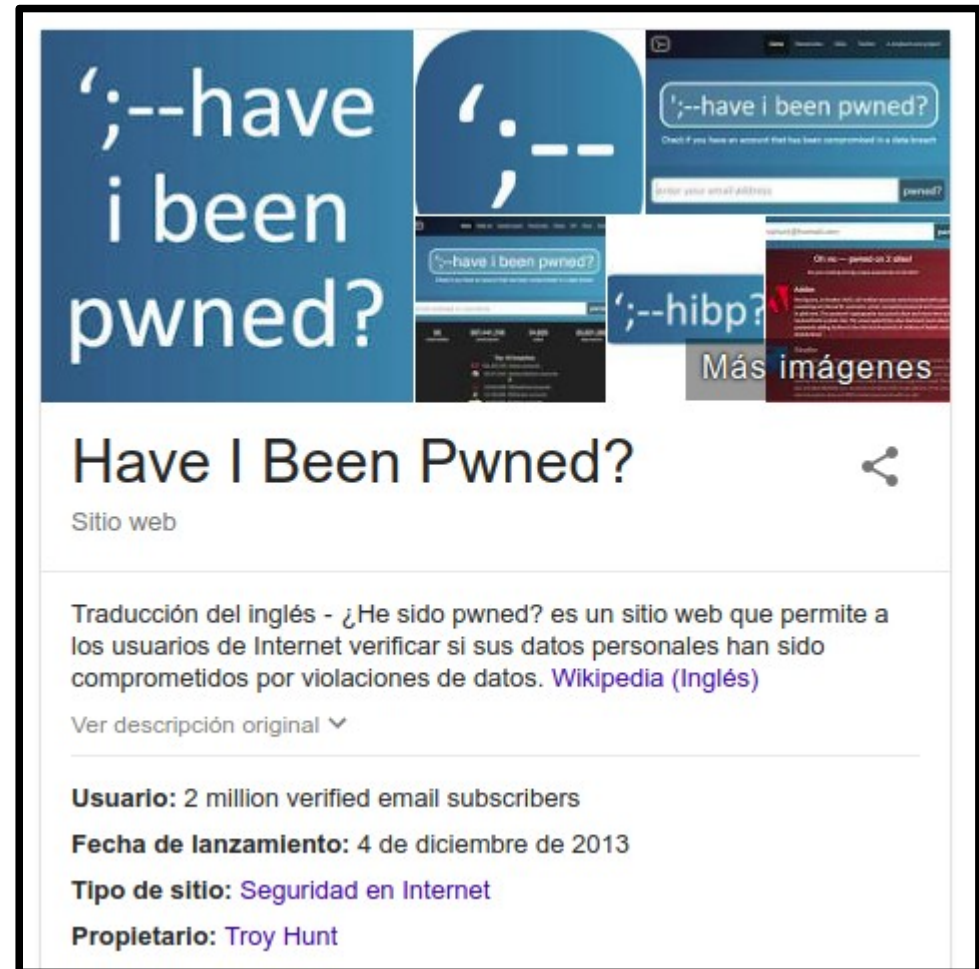
# Lecciones aprendidas

- Para entender el incidente, es necesario analizar:
  - ¿Qué datos sensibles fueron expuestos?
  - ¿De dónde salió esa información?
- Lo siguiente es adecuado ser informado a la comunidad objetivo para que estén informados de la amenaza y no sean víctimas de este tipo de engaños.





<https://haveibeenpwned.com/>



## Have I Been Pwned?

From Wikipedia, the free encyclopedia

**Have I Been Pwned?** (**HIBP**) is a website that allows internet users to check if their personal data has been compromised by [data breaches](#). The service collects and analyzes hundreds of [database dumps](#) and [pastes](#) containing information about billions of leaked accounts, and allows users to search for their own information by entering their username or email address. Users can also sign up to be notified if their email address appears in future dumps. The site has been widely touted as a valuable resource for internet users wishing to protect their own security and privacy.<sup>[2][3]</sup> Have I Been Pwned? was created by security expert [Troy Hunt](#) on 4 December 2013.





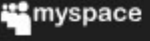



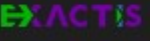
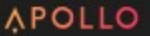


# ';--have i been pwned?


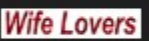

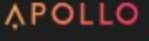


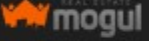



Check if you have an account that has been compromised in a data breach



## Largest breaches

	711,477,622 <a href="#">Onliner Spambot accounts</a>
	593,427,119 <a href="#">Exploit.In accounts</a>
	457,962,538 <a href="#">Anti Public Combo List accounts</a>
	393,430,309 <a href="#">River City Media Spam List accounts</a>
	359,420,698 <a href="#">MySpace accounts</a>
	234,842,089 <a href="#">NetEase accounts</a>
	164,611,595 <a href="#">LinkedIn accounts</a>
	152,445,165 <a href="#">Adobe accounts</a>
	131,577,763 <a href="#">Exactis accounts</a>
	125,929,660 <a href="#">Apollo accounts</a>

## Recently added breaches

	846,742 <a href="#">Baby Names accounts</a>
	1,274,051 <a href="#">Wife Lovers accounts</a>
	342,913 <a href="#">Facepunch accounts</a>
	125,929,660 <a href="#">Apollo accounts</a>
	7,687,679 <a href="#">Digimon accounts</a>
	2,457,420 <a href="#">SaverSpy accounts</a>
	307,768 <a href="#">Real Estate Mogul accounts</a>
	3,472,916 <a href="#">NemoWeb accounts</a>
	41,826,763 <a href="#">Kayo.moe Credential Stuffing List accounts</a>
	182,717 <a href="#">Russian America accounts</a>



## Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

last.fm

**Last.fm:** In March 2012, the music website [Last.fm](#) was hacked and 43 million user accounts were exposed. Whilst [Last.fm](#) knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.

**Compromised data:** Email addresses, Passwords, Usernames, Website activity



**LinkedIn:** In May 2016, [LinkedIn](#) had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

**Compromised data:** Email addresses, Passwords





# Bilhões de senhas vazadas estão disponíveis na web. Você está na lista?

**Verifique se o seu e-mail ou senha foram comprometidos em um vazamento**

digite seu e-mail

verificar

## Qual é o tamanho do problema?

Sempre que um site é invadido, o login e a senha de milhões de usuários são disponibilizados na internet. Nós coletamos essas bases para que você seja informado se for atingido e possa trocar sua senha a tempo.

**224**

sites estrangeiros que vazaram senhas

**85**

sites brasileiros que vazaram senhas

**1.425.135**

de posts analisados no pastebin

**187.931**

páginas monitoradas na deep web





From contato@minhasenha.com ☆

↩ Reply

↩ Reply All ▼

➦ Forward

📁 Archive

🔥 Junk

🗑 Delete

More ▼

Subject MinhaSenha.com - Nova base de senhas vazadas

21/12/17 17:56

To [REDACTED]

Prezado(a),

Você deve ter [lido na mídia](#) sobre um novo vazamento de senhas na web. São 1.4 bilhões e-mails e senhas supostamente de empresas como Netflix, Uber e dezenas de outros serviços digitais. Esse vazamento foi noticiado no dia 13 de dezembro.

Como você acessou o site [minhasenha.com](#) e solicitou que fosse notificado a cada novo vazamento, **estamos enviando essa mensagem para dizer que o seu email não consta nessa nova base.**

Por outro lado, identificamos 1 novo(s) vazamento(s) relacionado(s) ao nome da sua empresa @ [REDACTED]. Repasse essa mensagem para o responsável, que pode entrar em contato com a nossa equipe pelo email [contato@axur.com](mailto:contato@axur.com)

Atenciosamente,

Time MinhaSenha

[contato@minhasenha.com](mailto:contato@minhasenha.com)

