CSIRT -PONAL

Equipo de Respuesta a Incidentes de Seguridad Informática

No. 009/18-02-2016

"ALERTA DE MALWARE CIRCULANDO EN LA RED"

De: first-teams-request@sympa.first.org [mailto:first-teams-request@sympa.first.org]
Enviado el: miércoles, 17 de febrero de 2016 08:46 p.m.
Para: first-teams@first.org
Asunto: [1st-t] Intimacao de n. 7743872. O MINISTERIO PUBLICO FEDERAL

Ministério Público Federal

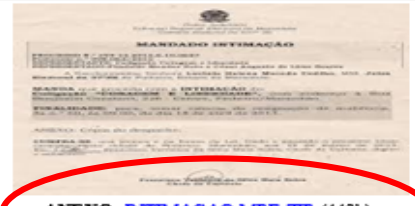
PROCEDIMENTO INVESTIGATÓRIO N.º 34662561M

Intimacao de n. 7743872. O MINISTERIO PUBLICO FEDERAL, no desempenho de suas atribuicoes institucionais, com fundamento nos artigos 229 e 241, inciso VI da constituicao Federal e artigo 61 , inciso VII da lei complementar n, 676, de 28 de Maio de 1998, INTIMA Vossa Senhoria a comparecer nessa procuradoria Regional da Republica ---

Data do comparecimento 26/02/2016 (Sexta feira) as 9:00 AM

: INTIMAÇÃO ID: - Atuelizado.
: PROCESSO Nº : - 90761782SM.
: PRECENÇA IT : - Desabilitado.

ANEXO INTIMAÇÃO-MPF (342K)



ANEXO: INTIMACAO-MPF.ZIP (442k)

```
http://cotrantos.bitnamiapp.com/index.php
```

Al realizar el análisis detallado del archivo adjunto de puede evidenciar que se trata de un malware que puede afectar su información personal guardada en el equipo de cómputo o en su dispositivo móvil.

COMANDO Y CONTROL DEL MALWARE

DNS

Name	Response	Post-Analysis Lookup
cotrantos.bitnamiapp.com	A 54.173.219.125	54.173.219.125
dns.msftncsi.com	A 131.107.255.255	131.107.255.255
dns.msftncsi.com	AAAA fd3e:4f5a:5b81::1	131.107.255.255
teredo.ipv6.microsoft.com	CNAME teredo.ipv6.microsoft.com.nsatc.net	

Hosts

IP
4.2.2.3
54.173.219.125

Analizador	Resultado
ESET	Malware site
Fortinet	Malware site
Kaspersky	Malware site

CSIRT -PONAL

Equipo de Respuesta a Incidentes de Seguridad Informática

No. 009/18-02-2016

RECOMENDACIONES

- Nunca haga clic en enlaces dentro de un e-mail y siempre ignore los e-mails que solicitan estas acciones.

- No responda mensajes que le pidan información personal o financiera.

- No abra mensajes ni archivos adjuntos de remitentes desconocidos.

- Use programas que verifiquen automáticamente si una URL es legítima antes de que se acceda al sitio (Virustotal.com)

- Identifique los correos que le son enviados por remitentes desconocidos, en los cuales le solicitan información personal y financiera.

- Mantenga actualizado el sistema operativos y el software antivirus de su equipo.

CUALQUIER DUDA O INQUIETUD COMUNICARSE CON EL CSIRT-PONAL (EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA POLICÍA NACIONAL) AL TELEFONO 3159090 O AL CORREO ELECTRÓNICO
ponal.csirt@policia.gov.co

Coordinador CSIRT-PONAL