



DNS malicioso é usado para roubar dados dos voluntários na Venezuela

13 de fevereiro de 2019

Fonte: **Kaspersky Lab**

ESTADO ACTUAL

¿CÓMO AYUDAR?



DESCARGAR EL KIT

REGÍSTRATE

La red de voluntarios de la AYUDA HUMANITARIA

ÚNETE AL VOLUNTARIADO
INFÓRMATE E INFORMA
SUMEMOS A PROFESIONALES DE LA SALUD

SABER MÁS

SÉ VOLUNTARIO

Nombre



Apellido

Cédula de Identidad

Teléfono celular

Correo electrónico

Profesional de la salud ▼

Tiene teléfono inteligente ▼

Tiene vehículo ▼

País ▼

Estado ▼

Municipio ▼



I'm not a robot



reCAPTCHA
Privacy - Terms

REGISTRAR



O site oficial dos voluntáriosxvenezuela

- Primeiro dia online, 6 de fevereiro de 2019
- Registrado em nome de Sigerist Rodriguez, em 4 de fevereiro de 2019
- Hospedado no Amazon Web Services

Site Falso

- Primeiro dia online, 11 de fevereiro de 2019
- Registrado pelo GoDaddy, usando a função de Proteção de Privacidade em 11 de fevereiro de 2019
- Hospedado primeiro no GoDaddy e depois no DigitalOcean

C:\WINDOWS\system32\cmd.exe - nslookup

(c) 2013 Microsoft Corporation. Todos los derechos reservados

C:\>nslookup
Servidor predeterminado: UnKnown
Address: 192.168.1.1

> voluntariosxvenezuela.com
Servidor: UnKnown
Address: 192.168.1.1

Respuesta no autoritativa:
Nombre: voluntariosxvenezuela.com
Address: 159.65.65.194

> volunta zuela.com
Servidor: UnKnown
Address: 192.168.1.1

Respuesta no autoritativa:
DNS request timed out.
timeout was 2 seconds.
Nombre: volunta zuela.com
Address: 159.65.65.194



Como se prevenir ...

- Uso de servidores DNS públicos, como os servidores do Google (8.8.8.8 e 8.8.4.4) ou os servidores do CloudFlare e do APNIC (1.1.1.1 e 1.0.0.1).
- Utilizar conexões VPN sem um DNS de terceiros.



Nova praga rouba caixa eletrônicos no México e Colômbia

2 de julho de 2019

Fonte: **Kaspersky Lab**



Como foi efetuado

ATMJaDi, Malware

Objetivo do grupo de cibercriminoso é sacar todo o dinheiro disponível nos caixas, através de um arquivo .jar para acessar o ATM para controlá-lo e assim infectar o dispositivo por meio de processos legítimos.

O grupo deve ter invadido com sucesso a infraestrutura bancária para obter acesso à rede no qual os caixas eletrônicos estão conectados.



Como se prevenir ...

As ações necessárias para evitar um ataque direcionado como este são simples: basta que a rede dos caixas eletrônicos esteja isolada da rede corporativa e que seu acesso seja restrito, isso já impediria o golpe.

Em segundo lugar é essencial que uma instituição financeira tenha soluções avançadas para monitorar possíveis atividades maliciosas, o que permitiria detectar a atividade do malware, mesmo este usando processos legítimos do software de controle do ATM.