Dirección Cibernética Naval

MINISTERIO DE DEFENSA / ARMADA NACIONAL / JEFATURA DE INTELIGENCIA NAVAL

BOLETÍN N°001

Bogotá, febrero 2020

CAMPAÑA CORONAVIRUS, USADO PARA DIFUNDIR MALWARE

Ante la expansión geográfica del coronavirus, la industria del cibercrimen está aprovechando el miedo de la sociedad para difundir a través de internet archivos maliciosos camuflados en mensajes de prevención del **coronavirus**.

Los ciberdelincuentes suplantan los mensajes de las entidades de salud publica con campañas de prevención del **coronavirus**, realizando ataques como **Spear Phishing**[1] y **Watering Holes**[2] por medio del correo electrónico, adjuntando supuestos documentos de Microsoft Word infectados con cargas maliciosas vinculadas con el malware **Emotet**.

Este tipo de malware **Emotet** es capaz de destruir, bloquear, modificar o copiar datos, así como también interferir con el funcionamiento de los computadores o red de datos .

- Archivos infectados con malware.
- No hacer clic para descargar.

Las firmas del antivirus Kaspersky detectaron malware identificados con los siguientes nombres:

- **Worm.VBS.Dinihou.r**
- **Worm.Python.Agent.c**
- **UDS:DangerousObject.Multi.Generic**
- **Trojan.WinLNK.Agent.gg**
- **Trojan.WinLNK.Agent.ew**
- **HEUR:Trojan.WinLNK.Agent.gen**
- **HEUR:Trojan.PDF.Badur.b**

Relacionados con la campaña expansiva de coronavirus:

Recomendaciones

- ❖ Identificar que la fuente del correo sea legítimo y confiable.
- ❖ No hacer clic en los hipervínculos o enlaces que estén adjuntados en el mensaje de correo, podría ser redirigido a un sitio web malicioso.
- ❖ No descargue los archivos adjuntos de estos correos sospechosos, pueden tener malware embebido en los archivos.

FUENTE

a) https://www.infosecurity-magazine.com/news/coronavirus-attacks-malware/
b) **https://www.muyseguridad.net/2020/02/03/coronavirus-de-china-malware/**

1. **Spear phishing:** Es una estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas.
2. **Watering holes:** Estrategia de ataque dirigido a un grupo particular (organización, industria o región). En este ataque, el atacante adivina u observa qué sitios web usa el grupo a menudo e infecta a uno o más de ellos con malware