Ciberseguridad
UV-CSIRT

Guía de respuesta a incidentes en caso de Malware

1.- Identificación de los equipos infectados y desconectarlos de la red (cableada ó inalámbrica)

2.- Tomar una muestra del malware y enviarla al proveedor de antivirus:

a. Contacto directo con proveedor de antivirus

b. Ejecutar en Sandbox local o remoto

c. Recaudar y evaluar información y alertas en internet acerca del este malware.

d. Activar el servicio de respuesta a incidentes del proveedor

3.- En conjunto con el proveedor tecnológico evaluar métodos para su contención

a. Entorno Citrix

b. Entorno Local

c. Servidores

d. Red

4.- Conjuntar evidencias (logs, registros, configuraciones, archivos dañados, archivos prefetch, procesos, temporales, etc.)

5.- Revisar los datos del correlacionador de eventos.

6.- Emitir comunicado/boletín interno, informando de la situación.

7.- Vigilar continuamente el impacto, y evaluar la necesidad de disparar el plan de continuidad previamente escalando el incidente a la gerencia de riesgos.

8.- Verificar el flujo de correo mediante las herramientas Antispam, Sandbox Antivirus, etc.

9. Analizar los encabezados del correo electrónico.

10. Analizar IPs y URLs

11. Analizar tráfico de red (proxy web, gateway de correo electrónico o antispam, firewall, IPS).

12. Identificar ataque y su impacto.

13. Identificar vulnerabilidades existentes, principalmente las explotadas el malware en cuestión.

14. Remediar vulnerabilidades

15. Efectuar recuperación desde respaldos de ser necesario.

16. Evaluar la situación y de ser necesario reportarla a la justicia

17. Emitir comunicado con la solución de la problemática a los usuarios