BetaBot y Fleercivet, dos nuevos informes de código dañino del CCN-CERT

ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/6087-betabot-y-fleercivet-dos-nuevos-informes-de-codigo-danino-del-ccn-cert.html

- **Los ID-07/18 e ID-08/18 están disponibles en la parte privada de su portal.**
- **Ambos código dañinos están diseñados para infectar sistemas, tomar su control y extraer información sensible perteneciente a los usuarios del sistema infectado.**
- **El CERT Gubernamental Nacional publica este informe con sus reglas YARA e IOCs correspondientes.**

El CCN-CERT ha publicado en la parte privada de su portal los Informes de Código Dañino **CCN-CERT_ID-07-18_BetaBot** y **CCN-CERT_ ID-8-18_Fleercivet** en los que se recoge un análisis de ambos malware. El primero de ellos, el BetaBot está diseñado para infectar sistemas, tomar su control y extraer información sensible perteneciente a los usuarios del sistema infectado. Utiliza multitud de métodos destinados a dificultar su análisis, ya que se ha hecho mucho hincapié en proteger el código original. Además, inyecta código tras las funciones del sistema para pasar inadvertido, utilizando técnicas de *API Hooking* a nivel de aplicación.

El código **Fleercivet,** por su parte, es una familia de troyanos que ha sido diseñada para infectar sistemas, tomar su control y realizar las consultas de manera oculta a páginas publicitarias. El código dañino utiliza multitud de métodos destinados a dificultar su análisis. Despliega un entramado de procesos ocultos, utilizando técnicas de suplantación de binarios en memoria. Además, lanza instancias pertenecientes al navegador de Google Chrome o Internet Explorer desde las que realiza las peticiones, con objetivo de conseguir ganancias monetarias mediante clic.

Como es habitual en este tipo de Informes, el CERT Gubernamental Nacional incluye las siguientes secciones:

- Información y características del código dañino
- Procedimiento de infección
- Cifrado y ofuscación
- Persistencia en el sistema
- Conexiones de red
- Archivos relacionados
- Detección y desinfección
- Información del atacante

Además, se incluyen diversos Anexos con reglas de detección (Snort y Yara) e Indicadores de Compropiso (IoC).

Pueden acceder a los informes en la sección de Informes de Código Dañino del portal del CCN-CERT.
CCN-CERT (11/04/2018)