El ID-03/16 y el ID-05/16 están disponibles en la parte pública de su portal web

Informes del CCN-CERT sobre código dañino diseñados para formar parte de una botnet y comprometer equipos

- **Una variante del código dañino "Ponmocup" cuya botnet está considerada como una de las mayores descubiertas hasta el momento y otra de "Gamarue" diseñada para formar parte de una botnet y dificultar su detección, protagonistas de sendos informes.**

- **El CERT Gubernamental Nacional publica estos documentos con sus reglas SNORT, YARA e IOCs correspondientes.**

Madrid, 24 de febrero de 2016.- El CCN-CERT ha publicado en la parte pública del portal dos nuevos Informes de Código Dañino:

- **CCN-CERT ID-03/16 Ponmocup**: recoge el análisis de una variante de este código dañino con capacidad para comprometer y controlar equipos, de forma que pasan a ser nuevos nodos de una red botnet. Además, es capaz de detectar cómo y dónde está siendo ejecutado, cambiando su comportamiento y actuando como un simple dropper o descargando y ejecutando otros códigos dañinos.

Ponmocup utiliza diversas técnicas para garantizar con éxito su persistencia en los sistemas ya comprometidos y la botnet a la que pertenece está considerada como una de las mayores descubiertas hasta el momento.

- **CCN-CERT ID-05/16 "Gamarue":** una variante diseñada para formar una botnet, conectada a su servidor de Mando y Control (C2), desde donde es capaz de robar información y distribuirse. Se trata de una botnet modular que puede añadir nuevas características maliciosas, propias o externas, por medio de módulos o librerías (vendidas por separado).

Los informes, recogidos en la parte pública del portal del CCN-CERT, recogen las siguientes secciones:

- Características del código dañino
- Detalles generales
- Procedimiento de infección
- Características técnicas
- Persistencia en el sistema
- Conexiones de red

25 de febrero de 2016

- Archivos relacionados
- Detección
- Desinfección

Además, se incluyen diversos Anexos con regla SNORT, Indicadores de Compromiso (IOC) y Regla Yara.

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/
@CCNCERT

http://youtu.be/5XxS9mZZfKs