IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

CARMEN un caso práctico

CENTRO CRIPTOLÓGICO NACIONAL

- Roberto Amado
- S2 Grupo
- ramado@s2grupo.es

Índice

Conocimiento

61 Analizadores

32 Indicadores

47 IOC

Adquisición

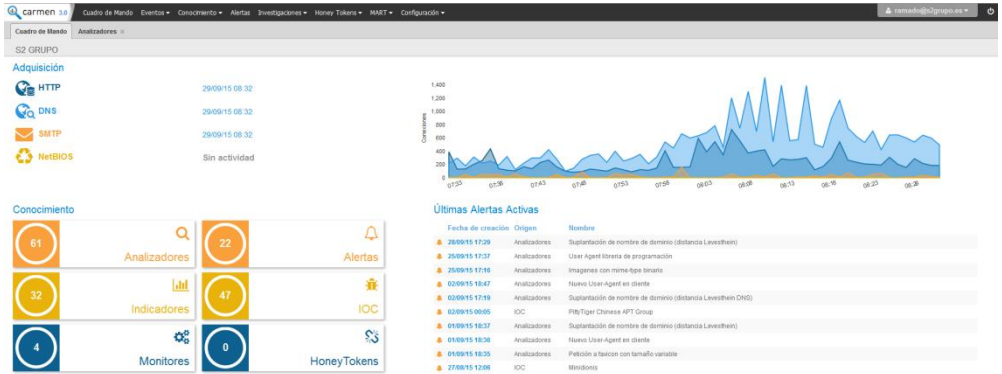
carmen 3.0
Centro de Análisis de Registros y Minería de eventos

HTTP

DNS

SMTP

NetBIOS



Análisis HTTP

- Patrones de comportamiento auto.
- Series temporales
- Anomalías en el uso del protocolo
- Actividad maliciosa

Detección de DNSs maliciosos

Campañas de phising dirigido

Exfiltración por SMTP

Named pipes

TAIDOOR APT

USA

TAIWAN

VECTOR DE INTRUSIÓN

Hasta 7 tipos diferentes de adjuntos por correo electrónico

CARACTERISTICAS

cve.mitre.org

HASTA 9 VULNERABILIDADES

14 VERSIONES IDENTIFICADAS DESDE 2008

CARACTERÍSTICAS

TRABAJA SOLO CUANDO EL USUARIO TRABAJA

Dropper

+

Malware

IDENTIFICACION

HTTP requests

URL: http://61.67.151.166/akkvj.php?id=02806019113804EF8B
TYPE: GET
USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

URL: http://61.67.151.166/akkvj.php?id=024231191
TYPE: GET
USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; \

virustotal

SHA256: 32662ffd294f62174425902a03c4bc5e3882a7a37e90c124ce7aa94ee8080112

Nombre: vt-upload-EE9Za

Detecciones: 40 / 57

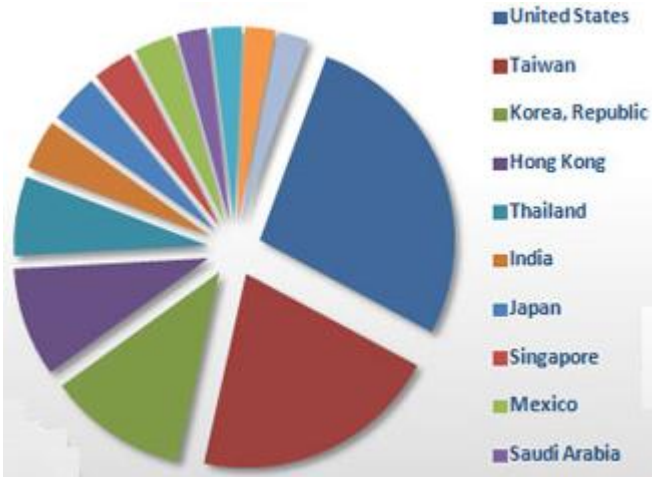
Fecha de análisis: 2015-03-19 14:01:18 UTC (hace 8 meses, 3 semanas)

0 0

Análisis | Detalles | Información adicional | Comentarios 0 | Votos | Información de comportamiento

Antivirus	Resultado	Actualización
ALYac	Generic.Malware.SFdld!.2F292D27	20150319
AVG	Downloader.Generic13.YXG	20150319
AVware	Trojan.Win32.Generic!BT	20150319
Ad-Aware	Generic.Malware.SFdld!.2F292D27	20150319
AhnLab-V3	Trojan/Win32.Taidoor	20150319

CARACTERÍSTICAS



C&C repartidos por más de 9 países

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en Linked in