



**▣ CYBER EVENTO**

**COBERTURA DE EVENTOS DEL DIA:**

**ESET Latinoamérica and ZMA - Zampatti – Maida y Asoc. – (\* mostrando chiches nuevos... ¡hasta la conferencia! \*)**: Y sí, aunque ya por estos lares desde el 2004 con oficinas propias (\* empezando con una o dos personas, ya siendo actualmente unas 20, and desde donde se maneja todo LA – “desde Tijuana hasta Ushuaia”, como le gusta decir a Ignacio Sbampato, VP pa’todo LA \*)-, la muchachada y sus soluciones de seguridad (\* acompañados siempre por la people de ZMA como distribuidor exclusivo en Argentina \*)-, en realidad una conferencia específica pa’ prensa argenta nunca habían hecho. Sip nos habían invitado a algunas reuniones con clientes y canal. Pero algo para nos solamente, nada. Y el hacerlo, denota por un lado una mayor apertura, una decisión de – por más de su participación en un montón de eventos, congresos y demás -, asomar un poco más la cabeza, y dejar de lado una cierta especia de low-profile mediático; y por el otro, que en una época como la que se vive, se demuestran ganas de ganar posiciones, aprovechar y sacarle el jugo a la situación. Bien por ello...

Así pues, todo bien armadito en el Hotel Continental 725 - que es un place que me gusta -, aprovechando la visita por estos lares de Richard Marko, CTO de ESET (\* que por su puesto, aparte de seguro venir a revisar las cuentas, je, planes y demás, va a participar en SegurInfo de hoy \*)-, Ignacio Sbampato y Juan Carlos Zampatti. ¿La razón?: hablar un poco de la evolución de las amenazas, el negocio que involucra, así como el mercado – y su propio business -, tendencias, y, por supu, las nuevas versiones de sus solutions, el ESET NOD32 Antivirus 4 y el ESET Smart Security 4 - este último incorporando anti-spam y firewall -, que fueran liberadas a nivel mundial a principios de mes -, tanto para usuarios hogareños como para corporativos – las Business Edition para estos últimos – (\* y sí, tienen más, pero estas son las más nuevas \*)...

A ver, comencemos con las tendencias. Para ellos son: encriptación, polimorfismo, mutaciones internamente y distribuidas – como el Virtumonde o el ZLOB -, y mutaciones generadas en el servidor – como el Swizzor -. A lo que hay que sumar lo de siempre de ingeniería social, phishing, man-in-the-middle, etc. (\* estas últimas donde no básicamente no importa la tecnología, ya que si el usuario no está medianamente instruido – en todas las variantes que se les ocurra, no sólo en tec. -, hmmm, sonamos, algo le va a pasar, igual va a caer \*)-. Todo complejo, y los bichos y malware también cada vez más complejo y mutable, con el objetivo de siempre – bueno, principalmente de los últimos años – de sacarnos plata, robarnos la identidad – para sacarles datos y plata a otros, y continuar -, etc... Ergo, la solución y la protección tampoco puede ser simple (\* sí, ya sé, parece verso como para vendermos cada vez más cosas... pero es cierto, la complejidad conlleva complejidad \*), y la acumulación de firmas por la simple acumulación, va desapareciendo, tomando cada vez más preponderancia las tecnologías de heurística y firmas inteligentes. Que again, sí, ya sé que no es nada completamente nuevo, pero que cada vez se irá viendo más – aunque aún conviviendo con la vieja metodología -, cuanto más performantes se hacen las soluciones – el soft -, y más rápidas son las máquinas que se tengan (\* porque este tipo de procesos más pro-activos, con inteligencia y demás, también requieren de más procesamiento... bastante procesamiento – no por nada corporativamente tuvieron bastante éxito los appliances dedicados a esto específicamente, como una desktop en relación a una consola, haciendo la comparación del mundo de los games - \*). Aparte que va a llegar n momento que tener todas las firmas de todos los bichos que anden dando vueltas, va a ser un devorador de espacio y storage, peor que un SO (\* si durante el 2009 esperan que lleguen a 3 millones la cantidad de muestras intercambiadas entre las empresas de antivirus, bueno, es como mucho \*). Y ah, dicen que con esta metodología heurística ellos detectan el 70 % del malware que detectan – valga la redundancia -...

Yendo a los products, citan que estas últimas versiones tienen más de 20 nuevas características. Que Tecnología de Autodefensa – contra cambios en procesos o en el registro de Win -, mejoras en la interfaz – aseguran que es más amigable – (\* ¿te saluda?, ¿te dice cosas lindas?... ehm, sí, ya sé, chiste malo, pero daba \*)-, Menores consumos de energía – vía minimizar el consumo de recursos utilizados -, Control de Acceso a medios removibles – sippi, CDs, USBs y todo eso -, categorización avanzada de infiltraciones – en 3 niveles -, o Compatibilidad con CISCO Network Admission Control, Protección de Parámetros – cambios de configuración, o instalación y desinstalación de programas -, integración con su SysInspector – por rootkits por ejemplo - etc., hasta algunas específicas para el Smart Security, como un motor anti-spam optimizado, el control de acceso, o soporte para IMAP...

Pasando a los negocios – manejados 100 % vía canal -, citan clientes como Telefónica de Argentina, Asociat S.A. ART, Car One, Cervecería Quilmes, Hospital Italiano, Metrovías, Moño Azul, Personal, SanCor, Reginald Lee-Coca Cola, Medicus, Banco De Formosa, Tecnovoz, Banco Industrial, Vía Bariloche, etc... Una facturación mundial de 140 palitogreenmorlacos – en los que LA representa el 5,2 % -, y un crecimiento de entre el 100 y 150% anual desde que están por estos lares...

Por la conferencia en si misma, el principio estuvo bien (\* le puso ganas Don Marko en hablar en castellano – bastante bien -, aunque eso too hizo que la presentación fuera un tanto lenta \*). Es que no nos pudimos quedar a todo, porque teníamos que ir a otro lado. Y con detalles interesantes. Como que hasta a las empresas de seguridad le hacen la gran ingeniería social, mandando “empresas” cartas documento para que saquen de sus definiciones de malware a sus desarrollos, porque son “legítimos” y las condiciones de licencia no les permiten – a los antivirus y demás – hacerlo. ¡Meu Deus!, hasta a esto han llegado, ¡y a tener abogados! (\* Dios los cría... jajajaja... auch, eso dolió... ¡que era un chiste Monastersky!, jejeje \*). Aunque claro, no le dan bolilla a los que son más obviamente bichos malos, pero en este mundo no es todo o negro o blanco, y hay zonas grises, sobre todo cuando de ingresos por publicidad o datos para estudiar comportamientos y demás se trata – hay formas y formas de hacerlo, todos los sabemos -, así que algunas cosas que la solution detecta, deja que uno manualmente decida si la deja correr o no...

¿Me queda algo?... Sip, un par de cosas... Por ejemplo, me interesa saber mas sobre esto del concurso- en su cuarta edición - al Mejor Trabajo de Investigación en Seguridad Antivirus entre estudiantes universitarios y terciarios. ¿Cómo se participa?, ¿dónde están las bases?, ¿hasta cuándo hay time?, ¿nos llevan al Virus Bulletin 2009 en Ginebra para cubrirlo periódicamente? (\* ehm, estem, sorry, la última se me chispoteó, jajaja \*)... Por el otro, simpático un regalito que nos dieron. Que cuando lo tuve en mis manos, aún envuelto, por la forma, ehm, miré al robot que aparece en sus cajas y afiches y me dije “estem, me da miedo pensar en que parte tuya es”. Es un device de forma ovalada – je, ya saben que me imaginaba que era -, un juego de adivine en 20 preguntas, donde es el aparatito el que tiene que adivinar lo que vos estás pensando, y te va haciendo las questions. La mayoría me las adivinó – como cigarrillo, mousse, o televisor -. Realmente un simpático chiche (\* ni hablar del CD de música hecho por el capo de MKT mundial, con temas como The NOD Song, Infected o Tommy Trojan’s Lament... ehmmmm, me da miedito hasta el sacarle el envoltorio de plástico, jajaja \*)... Y che, ¿quieren saber que significa NOD32?. Remember que el origen de la empresa es eslovaco, and quiere decir: “Nemocnica na Okraji Disku 32”, que dicen que se traduciría como “Hospital al Borde del Disco”, para plataformas 32 bits. Ehm, lo comento por si lo quiere sacar a colación durante la sobremesa de algún almuerzo – sobre todo hoy en el Sheraton -. Van a quedar como unos dandys...



**▣ CREDITOS**

**Idea, Producción Gral. y Redacción (and Errores Too)** : Fabián García  
**Producción Técnico Periodística** : Fernando Juliá

**Soporte Periodístico** : Enrique Garabetyan

**Producción Administrativa-Comercial** : Jorge García

**FG y Asoc. Offices - Center of Operations** : Salguero 1575 - 7mo. - Cap. Fed. - Bs. As. Argentina Tel. : (5411) 4829- 0298

**Contacto Operacion & Comercial** : {15} 4413-2325 / {15} 4447-9578

**Producción** : {15} 5327-3185 / {15} 4447-9578