

*Underground*

## **El retorno de Mister Sandman**

MrSandman es un conocido programador de virus de la escena underground. Fue un antiguo integrante del conocido grupo 29A ahora ha comenzado su carrera en solitario por lo que le hemos entrevistado para conocer un poco más de él y de su nueva andadura.

\* Desde que dejaste 29A hemos tenido pocas noticias tuyas. ¿Qué ha sido de Mister Sandman en todo este tiempo?

*Apenas unos meses después de dejar el grupo me ofrecieron una beca en la universidad. Como primer destino escogí Atenas, pero ya no había plazas, de manera que he ido a parar a Malta, un sitio que ya conocía anteriormente y que siempre me ha gustado mucho. Desde entonces me paso en Madrid desde finales de agosto hasta finales de octubre, y desde mediados de diciembre hasta finales de febrero, más alguna escapadilla esporádica y los primeros días del verano.*

*El resto del año me lo paso en Malta, y de esta manera es como me las voy apañando para estudiar simultáneamente dos carreras, aunque mi trabajo también me hace viajar bastante.*

\* ¿Cuáles son esas carreras? ¿en qué trabajas?

*Las carreras son de letras, es lo único que no me importa que se sepa. Trabajo como traductor semifreelance. Estoy ligado a una firma maltesa, pero soy yo quien decide cuánto quiero hacer cada mes, siempre en función del dinero que quiera ganar, claro. Los trabajos van desde traducir un manual o un libro hasta acudir a una conferencia en calidad de traductor simultáneo. Es un curro muy específico y, por tanto, muy bien remunerado... los únicos problemas llegan cuando alguna oferta interesante se me junta con exámenes, pero nada es perfecto.*

\* A pesar de todo hemos comprobado que sigues activo, y de hecho desde finales de diciembre es posible visitar tu nuevo website, el "Virus Café". ¿Por qué ese nombre? ¿qué pretende ofrecer?

*Bueno... Stallone, Willis y compañía tienen el Planet Hollywood, McPherson, Schiffer y Crawford tenían el Fashion Café... yo como soy muy chulo quería tener también mi Virus Café, heheh.*

*Lo cierto es que estaba cansado de lo de "Labs". Desde que se me ocurrió bautizar el website de 29A como "29A Labs" hace ya más de dos años, todo el mundo ha ido copiando la modita, hasta Eugene Kaspersky... todo es "Labs". Lo único que espero es no tener que decir lo mismo de "Café" dentro de otros dos años.*

*En mi website pretendo ofrecer una especie de "book" de mi carrera en la escena, poniendo todos mis trabajos publicados a disposición de quien los quiera.*

*Por otra parte, me interesa también que el Virus Café preste un servicio más genérico, y por ahora lo que he hecho ha sido inaugurar el "Museo de virus", por medio del que la*

*gente puede votar por sus favoritos en tres categorías distintas, que van cambiando cada mes*

\* ¿Y ahora qué... cuáles son las metas en esta tu nueva etapa como creador independiente?

*Sencillamente, escribir virus a mi bola: cuando me apetece y como me apetece, sin ceñirme a calendarios ni a presiones externas. Ahora me divierto más, y me puedo permitir "lujos" como escribir virus "a pachas" con amigos como Spanska.*

\* Un poco de historia... tus comienzos y tu nick ¿cuando nace mrsandman?

*En realidad llevo merodeando la escena desde mediados del 95. He llegado a usar cuatro apodos distintos, hasta que al final me decanté por "Mister Sandman", que es con el que me di a conocer finalmente allá por noviembre o diciembre del mismo año.*

*Los primeros contactos con el mundo VX a nivel internacional los tuve por medio de la legendaria BBS "WCIVR", de Estados Unidos, que era un foro de reunión al que acudían los escritores de virus más importantes de aquella época. Además de algún ex-miembro de Phalcon/SKISM, estaban las plantillas de VLAD y NuKE casi al completo... fue una experiencia interesante.*

*En cualquier caso, todo esto corresponde a una etapa de rodaje. Las cosas empezaron a tomar un cariz realmente definitivo a partir de mis primeras entradas al canal #virus de EFnet como "Mister Sandman". Allí me empecé a encontrar con casi todos los de WCIVR, pagando una décima parte por conectarme... heheh.*

\* Una pregunta cañera... ¿por qué no dedicar tu creatividad, técnica y dedicación en fines más provechosos para la comunidad?

*Un error muy común de los programadores de antivirus es hacerse (o hacernos) la misma pregunta. ¿Por qué todo el mundo da por hecho que nuestra vida se limita a sentarnos en frente de un monitor y escribir virus? no digo que no haya gente así, pero lo que sí que puedo asegurar, tras haber conocido a decenas de VXers en persona, es que no es lo habitual, ni mucho menos.*

*Yo por ejemplo he estado trabajando durante unos meses en la industria del cine, y he aprovechado ese tiempo para dirigir mi propio largometraje, que se suma a una lista de cortos que ya había dirigido previamente. Actualmente trabajo en calidad de traductor y estudio dos carreras.*

\* Detrás de mrsandman a quien podemos encontrar? edad, hobby, música, cine.

*Edad incógnita... nacido en 197X. Hobbies tengo muchos, quizás demasiados... pero digamos que me gusta viajar siempre que mi trabajo me lo permite, salir a pasear, ver una buena película, tener buena música siempre sonando en casa... etc,etc.*

*¿Qué es para mí una buena película? me gustan de casi todos los géneros, y a ser posible, en versión original. En mi casa tengo una videoteca en la que abarco desde películas de Fritz , Lang, Mankiewicz o Wenders hasta cintas de Ren y Stimpy... eso sí... si tuviese que elegir a un director que me ha impactado en los últimos años, ése es*

Quentin Tarantino, sobre todo en "Jackie Brown". En cuanto al cine español, Amenábar y Médem me parecen muy buenos.

En cuanto a la música, tres cuartas partes de lo mismo... toco casi todos los palos, pero siempre de heavy metal para abajo. En general todo lo que sea de los 70 me apasiona... desde canciones como "Machine Gun" o "Jungle Boogie" hasta otras tipo "Strawberry Letter 23". Además, siempre que viajo me traigo música de cada país... tengo decenas de CDs de música turca, árabe, hindú... y también me apasionan.

\* Haznos una breve descripción de tus creaciones (nombre, fecha, características básicas, alguna anécdota sobre alguno de ellos)..

Los virus que he distribuido hasta el momento son AntiCARO, Torero, Esperanto, Hong Kong, Gibraltar Monkey y Girigat.

Los dos primeros fueron escritos en 1996... son virus de DOS, que destacan por alguna particularidad técnica en concreto. El primero fuerza al AVP 2.2 a detectar al virus Bizatch como "Bizatch\_:P", y no como "Win95.Boza", y el segundo demuestra cómo se pueden usar las entradas de directorio para almacenar la cabecera original de los ficheros infectados, así como el octavo bit de atributo, para diferenciar a dichos ficheros.

Esperanto es un punto y aparte... meses de trabajo con un PC y un Mac al lado, todo tipo de emuladores, horas debuggeando kernels, y finalmente lo conseguí: el primer (y por ahora único) virus multiprocesador del mundo, capaz de funcionar en PCs (bajo DOS, Win 3.1x y Win32) y Macs (Mac OS).

Hong Kong es un virus de circo, como los llamo yo... funciona en Win32 y es capaz de infectar todo tipo de EXEs, ocupando un total de 58 bytes. Lo escribí para un concurso de virus enanos, en el que acabé tercero, a un voto del segundo.

Gibraltar Monkey fue mi último virus de DOS y el primero como escritor independiente... un bicho intencionadamente raro, desconcertante, una especie de homenaje estilístico a "Q", uno de los mejores VXers.

Por último, Girigat es mi primer virus "puro" de Win32, y creo que me quedó bastante curioso... en cuanto llega a un ordenador nuevo cambia por completo sus características, pudiendo ser en uno un simple infector runtime de EXEs y en otro, un infector de EXE, CPL y SCR por acción directa y residencia por proceso. En total hay 52 virus posibles distintos, que, a su vez, disponen de cuatro posibles payloads: uno que marea el cursor, otro que abre y cierra la bandeja del CD, otro que cambia el diseño del escritorio, y otro que saca un mensaje de información del sistema ligeramente modificado.

Probablemente para cuando la gente esté leyendo esto ya habré terminado mi última creación, un i-worm del que no tardaréis en tener detalles.

\* ¿Qué represento el nacimiento de 29A para la scene y para ti en particular? mucha gente se pregunta como está/ba organizado un grupo como 29A, había reuniones periódicas, proyectos en común, estaba jerarquizado?

*De 29A sólo puedo hablar como hablarían un padre o una madre de un hijo enclenque que llegó a ganar una medalla en los Juegos Olímpicos. La genética era buena, sólo hacía falta canalizarla e ir haciendo algunos aportes extra, que en el caso de 29A fueron los fichajes que se iban llevando a cabo.*

*En cuanto ese hijo empezó a valerse por sí solo, a su padre le llegó la hora de descansar un poco y empezar a disfrutar de la vida por su cuenta... no sé si me explico.*

\* cuanto hay de leyenda negra y cuanto de verdad en las relaciones entre los creadores de virus y las casas antivirus

*Mucha gente me pregunta si los propios programadores de antivirus se dedican a escribir virus... quizás eso llegó a suceder en el pasado, cuando había más escasez... pero ahora la escena vírica se mueve por inercia, y los AVers trabajan más bien poco.*

*Ciñéndome más a tu pregunta... en mi caso particular te puedo comentar que en los últimos tres años he recibido más de una oferta de trabajo en una compañía antivirus, como "Mister Sandman", y que conozco también a más de un escritor de virus con pluriempleo. A nadie le amarga un dulce (y esto va para ambos bandos).*

*Yo personalmente me niego a cobrar menos de la mitad de lo que cobro actualmente en mi trabajo para dedicarme a desvirgar virus sentado en una mesa de oficina.*

\* Da rienda suelta... ¿qué echas en falta/crítica a los antivirus actuales: demasiado marketing y pocos desarrollos nuevos?

*¿Qué echo de menos? trabajo y seriedad. Si eso que nos contaban de pequeños de que si mentimos nos convertiremos en una estatua de piedra fuese cierto, apuesto a que la Gran Muralla China no sería la única construcción humana visible desde el espacio.*

\* saca tu bola mágica... que nos depara el futuro en cuanto a creaciones víricas?

*Si te lo dijera no tendría tanta gracia. ¿Qué sería de la vida sin emociones ni intrigas?*

## Los virus de MrSandman

En VirusCafe, la propia web de MrSandman podemos encontrar las creaciones de este prolífico coder, así como algunos datos interesantes sobre dichos virus.

Los virus de Mister Sandman de los que se pueden encontrar información en su web son los siguientes AntiCARO.1235, Torero.1427, MP.Esperanto, Win32.HongKong, Gibraltar Monkey.2256, Girigat y i-worm.Ix-xitan.

Así por ejemplo, de torero MrSandman explica que se trata de un virus DOS, que ataca ficheros COM, su payload hace creer al usuario que intenta ejecutar una aplicación de Windows bajo DOS. Este virus destaca por utilizar el octavo bit de atributo para marcar y distinguir los ficheros infectados, y almacenar la cabecera original de dichos programas en su entrada de directorio correspondiente. También contiene instrucciones reales del kernel del DOS en su handler de memoria para confundir a usuarios avanzados

Esperanto es un virus que realmente merece una mención especial, este virus ya fue analizado en profundidad en nuestra revista en febrero de 1998, su principal característica es su capacidad multiplataforma, ya que infecta indiferentemente sistemas operativos DOS/Windows 3.1x, Windows 32 bits y MacOS. Según su propio autor: "Se trata del primer virus multiprocesador y multiplataforma, capaz de funcionar en PCs y Macs, en modo lineal y protegido, y de infectar diversos tipos de ficheros, por medio de rutinas de 16 bits y de 32 bits."

Otro virus que aparece dentro de «Virus Café» es Gibraltar Monkey un infector DOS cuya primera activación es lanzada por ficheros SYS, desde los cuales muestra un mensaje y cuelga el ordenador. La segunda activación sobrescribe todos los ficheros GIF que encuentra con una imagen de la bandera de Gibraltar.

Uno de los últimos virus de MrSandman es Win32.Girigat, cuando se activa su payload varía dependiendo de la vez en que dicha acción ocurre. En su primera activación sustituye el diseño del escritorio por el nombre del virus escrito en alfabeto hindú. La segunda cambia la ubicación del cursor a posiciones aleatorias por medio de un bucle infinito. La tercera activación muestra un cuadro de diálogo con información del sistema y del virus. Y la cuarta activación abre y cierra la bandeja del CD en un bucle infinito. Una de las particularidades de este virus es su capacidad de mutación, cada vez que salta a un nuevo ordenador varía su forma de infección y de actuación, con un total de 52 combinaciones diferentes.