

## *Underground*

### **GriYo, un creador de virus**

Este mes hemos estado conversando con GriYo uno de los escritores de virus de más relevancia en la actualidad. Este integrante del grupo 29A, famoso en la actualidad por la gran difusión de una de sus últimas creaciones.

GriYo (<http://www.geocities.com/Area51/Corridor/2618/>) es un joven normal y corriente, de 26 años, estudió la carrera de informática, aunque lleva trabajando como programador desde los ocho. Pero tiene un «hobby» que muchos no considerarían normal, entre sus aficiones se cuenta el escribir virus.

Cuando hablamos con él nos confesó que siempre había estado interesado en el tema vírico, pero nunca había tenido ningún contacto directo con él hasta que un día un virus entro en su ordenador. Al arrancar el viejo PC en el que iba a trabajar algo le sorprendió, durante el arranque apareció en la pantalla un mensaje que decía «Your Pc is now stoned». Durante unos minutos se quedó mirando el monitor sin llegar a creer lo que estaba pasando. La idea de un programa escrito por alguien en otra parte del mundo llegara hasta su ordenador le fascinó.

GriYo forma parte del grupo de creadores de virus 29A (<http://sourceofkaos.com/homes/29a/>). Publican un ezine que se distribuye por Internet, en el que dan a conocer los últimos avances en el tema. Este grupo nació a partir de una conocida BBS underground llamada Dark Node. En ella se daban cita varios autores que decidieron unir fuerzas para publicar un e-zine. En cuanto al significado, 29A es un numero en hexadecimal, probar a convertirlo a decimal.

La organización de 29A cuenta con una lista de correo interna, además de un canal irc en el que los integrantes se reúnen para charlar de todo tipo de temas. Los proyectos son tanto individuales como en grupo. Cuando GriYo entró en 29A y empezó a conocer a otros autores le llamó la atención lo diferentes que eran unos de otros en cuanto a aficiones al margen del mundo de los virus, en algunos casos los gustos sólo coincidían en un punto: los virus informáticos.

Aunque dentro del underground GriYo su interés se centra en el virii, no niega que ha hecho también «sus pinitos» en otros campos, como el hacking y el phreaking. Entrando también en la «demo scene».

A GriYo le gusta que el payload de sus creaciones dejen al usuario estupefacto ante algún efecto gráfico inesperado. Según nos cuenta resulta más divertido cuando se habla del virus «que te da la vuelta a la pantalla» en lugar del virus que «te borra el disco duro».

## Sus creaciones

GriYo nos confiesa que ha escrito muchos virus, de los cuales, al día de hoy, sólo seis han salido a la luz.

«Cricri», un virus polimórfico y full-stealth que fue ampliamente distribuido en China, al infectar el disquete de instalación de los controladores para Windows de la tarjeta de vídeo S3Triop64.

«Sucksexee» fue dotado de polimorfismo y full-stealth, pero ampliando sus posibilidades. «Gollum» era un «espécimen de laboratorio», un bicho raro, el propio GriYo se sorprendió al verlo recientemente en la lista de virus más reportados de Virus Bulletin.

«AntiEta» es otro ejemplar de laboratorio, su nombre es en protesta por el asesinato de Miguel Angel Blanco. Como payload el virus muestra una imagen de una mano blanca. Con él, 29A pretendía que la gente de fuera de España supiese del problema que tenemos aquí con ETA.

«Marburg» es el primer virus polimórfico de 32bits. Pese a ser un runtime infectador (es decir, no residente en memoria) el virus se ha propagado por el mundo a gran velocidad, protagonizando diversos incidentes. Las revistas PcGamer y Pc Power Play contenían varios programas infectados en los CD Rom que las acompañaban. El CDROM del juego MGM/Wargames salía al mercado infectado. Como activación este virus llena el escritorio de iconos de error crítico de Windows, un círculo rojo con un aspa blanca.

El virus «HPS» levantó polémica por ser el primer virus polimórfico diseñado para Windows98. La CNN dijo de él «Un virus se adelanta a la salida del sistema operativo». Eso fue el detonante de una explosión de noticias en periódicos y revistas locales (DerSpiegel, LeMonde...) acerca de éste virus. Como activación, el virus giraba todos los archivos gráficos a los que Windows accedía.

## El virus Marbug

En Octubre de 1997 GriYo estaba dando los últimos retoques al virus Marburg. Al hacer pruebas de los paquetes antivirus existentes por aquel entonces ninguno era capaz de detectar la presencia del virus, ni tan siquiera con el motor de polimorfismo desactivado. Varios miembros de 29A enviaron mensajes al grupo de news alt.comp.virus (punto de reunión de los desarrolladores de antivirus como AVP, DrSolomon's, FProt, etc...) contando sus descubrimientos y protestando ante la falsa sensación de seguridad que el software antivirus ofrecía a sus usuarios. Ya que algunos productos aun se vendían bajo el eslogan publicitario «Detecta el 100% de los virus conocidos y desconocidos». Como respuesta, en el mejor de los casos obtuvieron burlas, alguno llegó a decir que estaban ocupados con cosas más importantes.

En noviembre de 1997 «Marburg» aparece «in-the-wild» como el primer virus polimórfico para Windows. Todos los antivirus existentes no solo son incapaces de detectarlo sino que además, aun en el caso de disponer del virus para su análisis, sería necesario actualizar la versión existente del producto para poder afrontar este nuevo tipo de virus. La primera vacuna apareció nueve meses después, cuando el virus ya ha tenido tiempo de propagarse por miles de ordenadores. A diferencia de los expertos en seguridad informática, los desarrolladores de antivirus no admiten que un escritor de virus burle su software. Y esto les costó la credibilidad entre otras cosas.

### Casas antivirus

Ya hemos comentado su experiencia con las casas antivirus y el virus «Marbug», a pesar de ello, como creador de virus, GriYo no puede pasar alto la existencia de antivirus. Aunque él sólo utiliza los antivirus como herramientas de desarrollo, no para protegerse de los virus. Cuando desarrollo un nuevo virus no lo doy por terminado hasta que escapa a la detección de todos los antivirus.»

Según él <|>«si se siguen ciertas normas uno puede estar a salvo de ellos». Sus consejos son <|>«no ejecutar nada de dudoso origen, desactivar el arranque desde disquetes y no usar el Office de Microsoft.». Tampoco nos sorprende cuando le preguntamos por el mejor antivirus: «cual es el mejor es algo que desconozco. Personalmente prefiero el Antiviral Toolkit Pro, por la regularidad con que se actualiza. No obstante hay algunos antivirus que nunca utilizaría: Aquellos para los que no es necesario añadir ninguna característica especial a mis virus, el antivirus es incapaz de detectarlos. En este grupo se encuentran productos muy populares, como Norton Antivirus, Panda Antivirus, el conocidísimo y ampliamente extendido SCAN de McAfee, etc...»

Se habla mucho del contacto y de las relaciones entre creadores de virus y firmas antivirus, ante esto GriYo afirma que hay de todo, que tiene amigos y enemigos en ellas. También confirma que ha tenido contactos con firmas antivirus, muchas propuestas, e incluso algunas ofertas de trabajo, y de colaboración. «A pesar de ello ninguna lo suficientemente atractiva. Son mucho más atractivas las proposiciones del «lado oscuro», ¿me sigues?»

Al preguntarle por su opinión acerca las dos casas de antivirus españolas, Panda y Anyware, sonrío y nos responde que «las dos entran dentro del grupo "antivirus que nunca utilizo y que jamás compraría". Panda, no obstante, está evolucionando muy deprisa; si siguen trabajando tan duro pronto pueden convertirse en un número uno (eso si quitan la foto de Diana de Gales de su home page).»

## Entrevista con GriYo

GriYo es un personaje de la escena underground española bastante peculiar, nuestra entrevista con él permite conocerlo un poco mejor.

\* ¿Por qué «Griyo»?

*Fue una idea de un compañero de trabajo, penso que me parecía a Pepito Grillo y empezó a llamarme así. Finalmente me quede con el mote. Lo de escribir GriYo con «Y» es una cuestión de optimización ;)*

\* ¿Qué te motiva para estar durante horas y horas creando un virus?

*Por un lado está mi afición por la programación a nivel del sistema, por los lenguajes de bajo nivel, mi interés por los temas relacionados con la seguridad informática o acerca de la «vida artificial». Por otro lado está la curiosidad, las ganas de hacer cosas difíciles, quizás para demostrarme a mí mismo que soy capaz de hacer eso que tanto me fascina. Y lejos de cansarme, cuanto más profundizo en el mundo de la programación de virus, más me entusiasma.*

\* Música, películas favoritas, deportes, novia?,

*La música electrónica es mi favorita. En cuanto a películas, me gustan las de ciencia ficción. Practico muchos deportes, sobre todo deportes de alto riesgo... Y novia, sí, salgo con una chica rusa, nos queremos mucho y tenemos un perro que se llama Gollum x'D*

\* ¿Cómo ves la «scene vírica» a escala mundial, y especialmente en España?.

*En el ámbito mundial hay grupos muy buenos, y una gran rivalidad entre los autores. Esto favorece el desarrollo de nuevas técnicas, cada vez más complejas y avanzadas. En España tenemos gran cantidad de autores destacados; parece que España se ha convertido en una potencia mundial en el desarrollo y la investigación de los virus informáticos.*

\* Describe el virus perfecto.

*En mi opinión un virus perfecto sería aquel que estuviese diseñado para atacar un sistema en concreto, es decir, un virus a medida. Los virus se encuentran con multitud de configuraciones diferentes que en ocasiones dan lugar a incompatibilidades. Esto no sucede con un virus a medida, puesto que se puede alterar artificialmente el proceso de replica para evitar que escapen al exterior.*

\* ¿Cuál es el futuro de los virus?

*Las nuevas plataformas son cada día más potentes, pero a la vez más complejas. Desarrollar virus será cada vez una labor más complicada, y requerirá más tiempo y más recursos. Los virus, tal y como ahora los conocemos, desaparecerán, para dar lugar a sofisticados hackers electrónicos desarrollados al amparo de instituciones gubernamentales. Toma ya! ;)*

\* Proyectos actuales y metas a medio plazo.

*Pronto tendré acabado un virus nuevo, me gusta llamarlo "virus de nueva generación", puesto que aplica conceptos nuevos que pronto serán muy comunes. Te puedo avanzar que Internet es tan importante para este virus como los ficheros .EXE lo han sido para los virus tradicionales.*

\* ¿Qué consejos darías a aquellas personas que se quieran introducir en la creación de virus.?

*Consejo: Dejalo. Si no quieres dedicarse al 100% lo mejor será que lo dejes. La programación de virus requiere cada vez más esfuerzo, y sin dedicación no se llega a ningún lado. Si pese a esto quieres introducirte en este mundo, adelante, sorpréndenos haciendo posible lo imposible.*

\* ¿Algo más para terminar?

*Un saludo a mi novia, a la gente de #hack y de #virus y especialmente a todo el equipo de desarrollo de 29A.*