

Perfil de un analista de códigos maliciosos

Prefacio

Vlad Borisenko, un analista de códigos maliciosos en Agnitum, comparte con nosotros los pormenores de su profesión.

Cuéntenos un poco acerca de usted, su educación, qué es lo que hace cuando no está trabajando, etc.

Bueno, creo que soy una persona bastante común, con la diferencia que sé un poco acerca de ordenadores y de las amenazas que complican nuestra vida en el mundo digital.

Me gradué en la Universidad Politécnica de San Petersburgo, con un título en matemáticas, y desde entonces estuve involucrado con la seguridad informática.

Hace tres años que estoy trabajando en Agnitum, donde comencé supervisando la expansión de la base de firmas para Tauscan, una aplicación contra troyanos.

Cuando posteriormente pasamos a trabajar en la detección de programas espía, me convertí en un analista superior de códigos maliciosos.

Hoy día, mi responsabilidad es asegurar que nuestros clientes tengan las últimas definiciones de códigos maliciosos tan rápido como sea posible. También trabajo en el emprendimiento [ImproveNet](#), que ayuda a los usuarios a obtener el conjunto de reglas automatizadas más recientes para el cortafuegos.

Cuando no estoy trabajando, soy un fanático de los nuevos dispositivos tecnológicos (creo que esto no es sorprendente).

También soy un gran aficionado a los deportes motorizados y a la lectura.

Cuando puedo escaparme por un tiempo de las amenazas de los códigos maliciosos me gusta viajar, hecho que despertó en mí un profundo interés por cuestiones medioambientales.

No entiendo cómo algunas personas pueden tener aviones privados, mientras que en África hay millones padeciendo hambre y enfermedades.

Tal vez en el futuro participe en algún programa de las Naciones Unidas para ayudar a los necesitados.

La gran pregunta es si lograremos vencer a los códigos maliciosos a tiempo como para que yo pueda hacer eso.

¿Cómo es que encuentra tiempo para hacer todo esto, si trabaja día y noche analizando los códigos maliciosos?

Todos necesitan tener algo de equilibrio en sus vidas.

En este negocio es necesario estar siempre alerta y en actividad, para adelantarse a "los malos".

Y aun cuando nuestro equipo trabaja las 24 horas, los 7 días de la semana, intento dedicar mi tiempo libre a mis intereses personales y mi familia.

Esto es siempre un desafío, ya que las amenazas tienden a propagarse durante los fines de semana, cuando por lo general el nivel de vigilancia es menor, pero me motiva saber que estoy ayudando a los usuarios a mantenerse a salvo cuando están en línea.

Hay un programa de televisión muy interesante llamado "Cómo está hecho", que describe cómo evolucionan los productos desde una idea hasta su resultado final. ¿Podría darnos una aproximación al negocio de las aplicaciones contra códigos maliciosos, con el estilo de "Cómo está hecho"?

Bueno, como se imaginará, podría extenderme mucho con respecto a esto.

Pero en honor a la simplicidad, intentaré hacer una revisión rápida del proceso, sin meterme mucho en detalles técnicos... ¡y sin revelar los secretos comerciales de Agnitum, por supuesto!

El primer paso es la recolección de muestras, que son códigos sospechados de ser maliciosos, para su análisis y posible inclusión en nuestra base de datos de firmas.

Obtenemos las muestras de una variedad de fuentes: de asociados; de usuarios, que las envían a través de nuestra página web; y de otros desarrolladores de aplicaciones contra códigos maliciosos.


Cuando existe un brote, todos trabajamos juntos para asegurarnos que los usuarios obtengan las herramientas de detección tan rápido como sea posible.

Además de esto, usamos un programa de búsqueda automatizado, que examina la red buscando rastros de códigos maliciosos y exploits [*] embebidos.

Una vez encontrados, cada aplicación o elemento dañino detectado, es enviado a nuestros ingenieros de laboratorio para una evaluación interna más rigurosa.

Si eso no es suficiente, también comprobamos nuestros servidores de correo electrónico en busca de amenazas entrantes dentro los mensajes no solicitados.

Cada elemento del código sospechoso es sometido a procedimientos automatizados de análisis y evaluación, que nos permiten verificar cuanto antes las amenazas desconocidas, en este proceso tan complejo que es la investigación de amenazas informáticas.

[*]  Un *exploit* es un código escrito con el fin de aprovechar un error de programación y otras vulnerabilidades del sistema, para obtener diversos privilegios y realizar actividades maliciosas.

Después de completar esta primera etapa, el código sospechoso se revisa para confirmar actividades dañinas o comportamiento peligroso, usando máquinas virtuales.

Estas son copias del sistema operativo Windows, ubicadas en ordenadores exclusivamente destinados a realizar este tipo de pruebas.

En ellos se utilizan aplicaciones especiales, que permiten revertir instantáneamente los cambios realizados desde la ejecución del código.

Es entonces cuando el investigador rastrea las alteraciones en el sistema y, si encuentra algún impacto dañino, la muestra analizada se marca inmediatamente como código malicioso.

Los autores más sofisticados de códigos maliciosos han perfeccionado su técnica para “percibir” los entornos virtuales y reaccionar de acuerdo a esto, suprimiendo las intenciones dañinas para no ser detectados de inmediato.

En estos casos, nosotros también recurrimos a nuestras herramientas más sofisticadas para descubrirlos.

A continuación; el investigador necesita observar el código original completo, y así descubrir la porción que constituye la carga peligrosa del código malicioso.

Para lograrlo, se convierte el archivo a un formato que pueda ser analizado por humanos, utilizando uno de los siguientes métodos:

- **Descompresión**

El código puede llegar bajo la forma de un archivo comprimido, que necesitará del uso de una utilidad especial para descomprimirlo y así revelar su contenido.

- **Descifrado**

Si el archivo está cifrado, es necesario encontrar y aplicar la clave para descifrarlo. Una vez hecho esto, será posible para el investigador acceder a su contenido.

- **Desempaquetado / desensamblado**

Desempaquetar significa llegar hasta el código fuente de un archivo ejecutable, el cual puede estar escrito en cualquier lenguaje de programación de alto nivel, como Delphi, C o C++. Desensamblar significa traducir el archivo ejecutable a un lenguaje ensamblador de menor nivel.

Esto le permite al investigador ver el código en bruto, y analizarlo manualmente.

Una vez que el código malicioso fue identificado definitivamente, la base de firmas debe ser actualizada.

Utilizamos nuestro propio editor registrado para manejar firmas de amenazas y, en algunos casos, preparamos un módulo de análisis heurístico dedicado, que detecta las amenazas por su comportamiento más que por el código en sí.

Después de compilar las definiciones, estas se prueban con la ayuda de máquinas que ejecutan diferentes ediciones de Windows, distintas versiones de Outpost y una gran variedad de aplicaciones de otras compañías, con el fin de asegurar que los usuarios no tendrán problemas cuando actualicen las firmas.

Finalmente, las definiciones nuevas se suben a nuestros servidores para su distribución.

Fascinante. ¿Y qué herramientas utilizan para hacer todo esto?

Más allá de las aplicaciones de virtualización, la mayoría de los programas que utilizamos fueron desarrollados en Agnitum, por nuestros propios ingenieros e investigadores.

¿En qué dirección cree usted que evolucionará la industria de la seguridad informática?

Estamos encontrando un volumen cada vez mayor de amenazas ocultas, como por ejemplo troyanos y registradores de pulsaciones de teclas, encubiertos por las poderosas técnicas de los *rootkits*, que les permiten mantenerse escondidos dentro del sistema.

También estamos viendo códigos maliciosos que atacan aplicaciones específicas, en especial productos de seguridad, con el propósito de desactivarlos y así abrirse camino hacia el ordenador del usuario.

Todo esto es un desafío constante, tanto desde el punto de vista de la investigación, como de la atención al cliente.

La única forma que tenemos de aumentar nuestra eficiencia es, antes que nada, hacer más para evitar que los códigos maliciosos se introduzcan en los ordenadores de los usuarios.

Es por eso que trabajamos en conjunto con el equipo de ingenieros de Agnitum, enfocándonos particularmente en el desarrollo de técnicas para monitorizar y bloquear el comportamiento sospechoso de las aplicaciones.

¿Se refiere a alguna forma de Sistema de prevención de intrusos en el equipo anfitrión (HIPS, *Host Intrusion Prevention System*)?

Exactamente. Es el tipo de protección que monitoriza el comportamiento de los programas, verificando que las aplicaciones no se comporten de forma dañina dentro del sistema.
Los usuarios verán un énfasis cada vez mayor en este tipo de protección en las próximas versiones de Outpost.

Ese es un buen dato para tener en cuenta. A modo de conclusión, ¿tiene algún consejo final para nuestros lectores?

Les agradezco que me den la oportunidad de hablar directamente con nuestros usuarios.
Les deseo que tengan viajes seguros a través de Internet, siempre recordando que la mejor defensa es una combinación de conocimientos, prácticas seguras de navegación y un sistema de seguridad potente.