Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1126

(03/2017)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios con seguridad – Seguridad en las redes móviles

Directrices para la mitigación de los efectos negativos de los terminales infectados en las redes móviles

Recomendación UIT-T X.1126

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	**X.1120–X.1139**
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistema de transporte inteligente (ITS)	X.1370–X.1379
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1126

Directrices para la mitigación de los efectos negativos de los terminales infectados en las redes móviles

Resumen

La Recomendación UIT-T X.1126 proporciona directrices a los operadores móviles para limitar el número de terminales infectados en las redes móviles mediante la utilización de tecnologías que protejan tanto a los abonados como a los operadores móviles. Del mismo modo, describe las características y las repercusiones del software malicioso en los ecosistemas nocivos del entorno móvil. La presente Recomendación se basa en las tecnologías del lado de red y se centra en la mitigación de los efectos perniciosos de los terminales infectados. Por último, define y organiza medidas de mitigación y tecnologías pertinentes.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1126	2017-03-30	17	11.1002/1000/13194

Palabras clave

Infección, red móvil, software malicioso, terminal

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

La rapidez con que se han expandido y desarrollado los sistemas operativos para dispositivos móviles ha abierto las puertas de un vasto y vibrante mercado para la industria móvil. Alrededor de este valioso epicentro han florecido numerosos ecosistemas que tratan de aprovechar las ventajas conexas. No obstante, el software malicioso también puede abusar de las poderosas capacidades de las actuales esferas móviles para explotar las vulnerabilidades de los terminales, las redes y los servicios, lo que podría entrañar graves daños.

Cabe señalar que los ecosistemas saludables deberían primar sobre los "jardines vallados" en los sistemas móviles existentes, a fin de proteger el mercado móvil y salvaguardar los beneficios de todos los asociados pertinentes. Estos ecosistemas saludables se han desarrollado con éxito en algunos países.

En otros países, los ecosistemas del mercado móvil se han diversificado profusamente dando lugar, en algunos casos, a entornos irresponsables, nocivos o incluso peligrosos. Los efectos negativos de los ecosistemas irresponsables y el software malicioso móvil pueden causar graves daños a los abonados y las redes móviles. En ocasiones, los terminales infectados pueden perjudicar a los abonados y las redes móviles incluso en ecosistemas saludables, puesto que muchos de los actuales servicios de Internet móvil revisten un carácter mundial.

A continuación se citan los posibles riesgos del software malicioso que se propaga esencialmente en ecosistemas irresponsables.

Para los abonados:

- atentados contra la privacidad, véanse la escucha y el seguimiento de la posición;
- pérdida de activos, véanse la disfunción del sistema o la destrucción de datos;
- transacción y consumo maliciosos, véanse el envío de mensajes caros y la marcación de números de centros de llamadas internacionales;
- propagación de software malicioso para atacar a otros terminales;
- envío de correo no deseado para molestar a otros abonados;
- fraude y chantaje.

Para los operadores, los ataques a entidades de red, servicios móviles y otros terminales incluyen:

- ocupación de ingentes recursos de redes y servicios móviles, lo que podría comprometerlos y suscitar quejas relativas a la calidad de servicio entre los abonados; y
- secuestro de anfitriones de servicio e incluso de entidades de red.

Los efectos del software malicioso son más nocivos para la Internet móvil que para la alámbrica tradicional debido a los siguientes motivos:

- la Internet móvil integra un mercado emergente, cuyos mecanismos de seguridad se están desarrollando con relativa lentitud;
- los terminales móviles suelen ser portadores de negocios privados y confidenciales, altamente atractivos para los piratas informáticos;
- las redes móviles tienen menos recursos y un ataque de tipo inundación los consume con mayor facilidad e intensidad;
- muchos terminales móviles están estrechamente asociados a sus redes; los servicios maliciosos y los atentados contra la privacidad podrían dar lugar a la reducción de los ingresos de los operadores y el aumento de las quejas de los abonados y los problemas jurídicos;
- los sistemas operativos móviles abiertos/vulnerados son un caldo de cultivo para el software malicioso, que escapa al control del operador;

- los terminales móviles suelen tener numerosas interfaces de intercambio de datos, incluidos bus serial universal (USB), ranura para tarjeta Secure Digital (SD) y Bluetooth, que no todos los operadores pueden proteger.

Con objeto de mitigar los daños del software malicioso y localizar las fuentes de las amenazas, los operadores tienen la obligación y la responsabilidad cruciales de gestionar los terminales infectados en el lado de red.

Recomendación UIT-T X.1126

Directrices para la mitigación de los efectos negativos de los terminales infectados en las redes móviles

1 Alcance

En la presente Recomendación se facilitan directrices para la mitigación de los efectos negativos de los terminales infectados en el lado de red de las redes móviles. Además, se establece un marco que articula las directrices en torno a varios procesos, y se examinan los principios, políticas y tecnologías atinentes a dichos procesos.

El cumplimiento de la presente Recomendación no se considerará, ni podrá ser utilizado, como prueba del cumplimiento de ningún reglamento, ley o política nacional o regional. Los medios técnicos, organizativos y de procedimiento descritos en la presente Recomendación no garantizan en modo alguno el nivel de seguridad que un reglamento, ley o política en concreto, nacional o regional, pudiera exigir para una determinada correspondencia.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 lista negra (*blacklist*) [b-UIT-T X.1245]: Lista identificativa de personas o fuentes vinculadas a servicios de comunicación, cuando a las identificaciones de la lista se les deniega el acceso a determinados recursos de comunicación.

3.1.2 malware [b-UIT-T X.1211]: Software maligno diseñado específicamente para dañar o interrumpir un sistema atacando su confidencialidad, integridad y/o disponibilidad.

NOTA – Por ejemplo: virus, programas de secuestro, programas espía, programas con publicidad y falsos programas de seguridad.

3.1.3 red móvil [b-UIT-T X.1121]: Red que proporciona puntos de acceso de red inalámbrica a terminales móviles.

3.1.4 terminal móvil [b-UIT-T X.1121]: Entidad que cuenta con una función de acceso a una red inalámbrica y conecta a una red móvil de comunicación de datos con servidores de aplicaciones u otros terminales móviles.

3.1.5 spammings [b-UIT-T X.1244]: Cadena de actividades que realizan los spammers para enviar el spam, como elaboración de lista de objetivos, creación del spam, entrega del spam, etc.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se define el siguiente término:

3.2.1 red robot: Grupo de sistemas informáticos infectados con software malicioso y conectados de manera coordinada, con fines maliciosos y sin el conocimiento del propietario, por ejemplo, para transmitir software malicioso o correo basura, o para lanzar ataques.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

API Interfaz de programación de aplicaciones (*application programming interface*)

App Aplicaciones que se ejecutan en terminales móviles (*application running in mobile terminals*)

C&C Mando y control (*command and control*)

DDoS Ataque de denegación de servicio distribuido (*distributed denial of service*)

GGSN Nodo de soporte de la pasarela del servicio general de radiocomunicaciones por paquetes (*gateway general packet radio service support node*)

IP Protocolo de Internet (*internet protocol*)

MMS Servicio de mensajería multimedios (*multimedia messaging service*)

MMSC Centro de servicios de mensajería multimedios (*multimedia messaging service centre*)

SD *Secure Digital*

SIM Módulo de identidad del abonado (*subscriber identity module*)

SMS Servicio de mensajes cortos (*short message service*)

SMSC Centro de servicios de mensajes cortos (*short message service centre*)

URL Identificador uniforme de recursos (*uniform resource locator*)

USB Bus serial universal (*universal serial bus*)

VAS Servicio de valor añadido (*value-added service*)

WAP Protocolo de aplicación inalámbrica (*wireless application protocol*)

5 Convenios

Ninguno.

6 Marco y procesos

En la mayor parte de los casos, después de haber sido infectados por software malicioso, muchos terminales móviles pueden seguir accediendo a la red y utilizando como de costumbre todo tipo de servicios; la diferencia radica en que desencadenan una serie de efectos negativos sobre los servicios y redes que los abonados pueden ignorar. El operador móvil debe ser consciente de la infección y contener el terminal infectado adecuadamente, con objeto de conservar sus capacidades de red y servicio en condiciones estables y mantener intacta su credibilidad mediante la protección de los beneficios de los abonados. La Figura 1 ilustra un marco de mitigación de los efectos negativos de los terminales infectados que comprende tres tipos de funciones: las de los operadores, las de los abonados y las de otros organismos. Los operadores desempeñan el papel principal y su labor puede articularse en torno a tres procesos: descubrimiento, gestión e intercambio de información. Con el fin de respaldar dichos procesos, la figura comprende bases de datos de fuentes y software maliciosos. Los operadores emprenden los procesos incluidos en este marco teniendo en cuenta las obligaciones jurídicas y reglamentarias vigentes en los Estados Miembros en que operan.

Los tres procesos se relacionan como sigue: los operadores descubren y gestionan las anomalías de los terminales de los abonados en el lado de red y, a continuación, les comunican las amenazas que entrañan dichas anomalías. Los operadores también pueden compartir la información relativa al software malicioso con otros operadores y organismos asociados.

En el proceso de descubrimiento, se pueden recopilar y analizar muestras de aplicaciones para terminales móviles (apps) e informes de ataques, con miras al descubrimiento de anomalías en la red móvil. Las anomalías y los terminales afectados son objeto de informe durante el proceso de gestión. En el marco de dicho proceso, se verifican las anomalías y se adoptan medidas específicas a fin de mitigar los efectos negativos para los abonados y los operadores. Con objeto de proporcionar información oportuna para contrarrestar o gestionar el software malicioso móvil, cabe establecer un proceso de intercambio de información. En el marco de dicho proceso, la información relativa al software malicioso se comparte con otros operadores y organismos asociados para mejorar la seguridad en todo el sector.

Base de datos de fuentes y software maliciosos: Existe una base de datos de fuentes y software maliciosos común a todos estos procesos, cuyo objetivo es almacenar y proporcionar datos relativos a dicho código, incluidas sus fuentes y pautas de comportamiento. Estos datos facilitan la identificación de anomalías, el control de los terminales infectados y la publicación de información sobre software malicioso en los tres procesos. Además, si se obtienen nuevos datos atinentes al software malicioso durante los procesos de descubrimiento e intercambio de información, cabe la posibilidad de introducirlos en la base de datos para garantizar una protección "siempre actualizada".

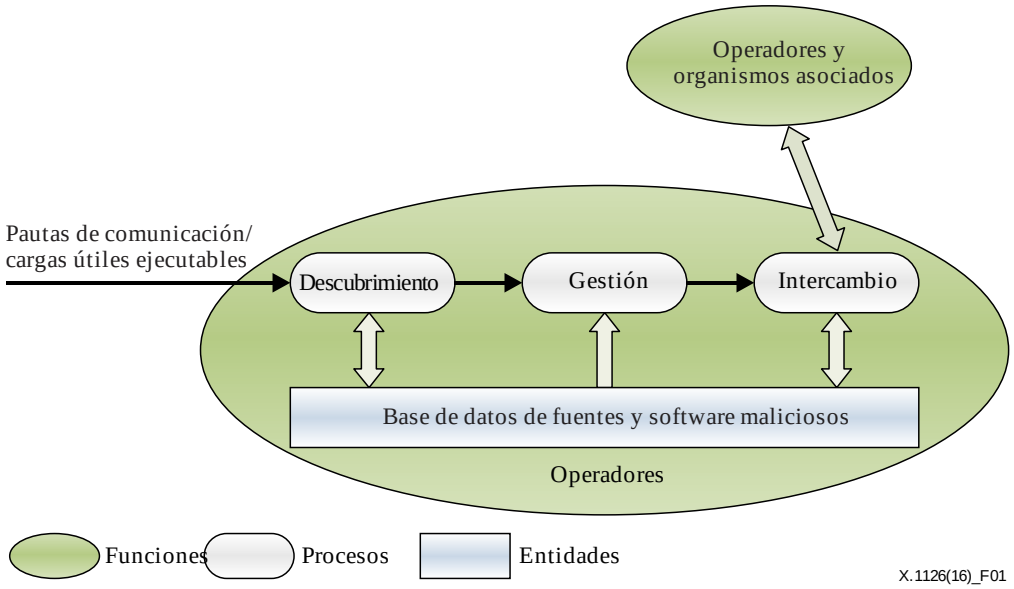

Figura 1 – Marco de mitigación de los efectos negativos de los terminales infectados

7 Descubrimiento

En el proceso de descubrimiento, se recopilan muestras de aplicaciones de tiendas de aplicaciones e informes de ataques consumados por terminales y elementos de red, a fin de analizar anomalías en la red móvil que puedan indicar o sugerir la presencia de terminales infectados y fuentes maliciosas. La Figura 2 ilustra el flujo de trabajo del proceso de descubrimiento.

Todos los datos utilizados del presente apartado en adelante pueden extraerse de muestras de aplicaciones de tiendas de aplicaciones e informes de ataques consumados por terminales de abonados o elementos de red. En el proceso de descubrimiento, la utilización de datos vinculados a la privacidad del abonado puede requerir el consentimiento o la autorización del mismo, de conformidad con legislación local, y debe limitarse estrictamente a fines relacionados con el análisis del software malicioso y otras actividades conexas.

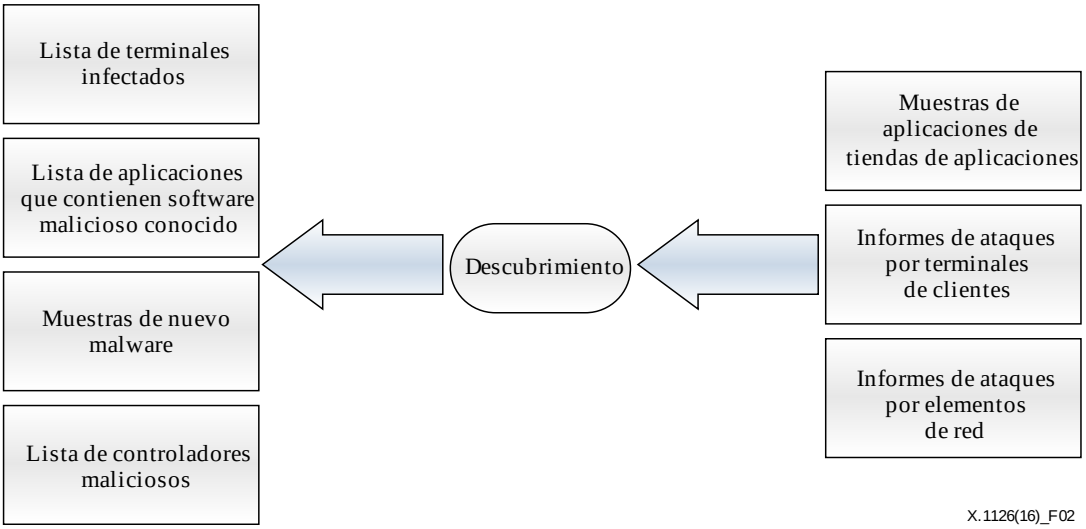

Figura 2 – Relaciones interactivas del proceso de descubrimiento

7.1 Recopilación de aplicaciones e informes de ataques

En el proceso de descubrimiento, pueden recopilarse dos tipos de datos para determinar las características de las anomalías de la red:

- informes de ataques de terminales de abonados y elementos de red; y
- muestras de aplicaciones de tiendas o mercados de aplicaciones.

7.2 Análisis de terminales infectados y software malicioso conocido

Algunos de los terminales infectados pueden identificarse gracias a los informes de ataques. La correspondencia de firmas adicional puede facilitar la localización de nuevas aplicaciones que contengan software malicioso conocido.

El análisis de terminales infectados y software malicioso conocido tiene por objeto la ubicación de los controladores maliciosos que se esconden en la red.

Cabe analizar las direcciones de protocolo de Internet (IP) de los paquetes de control de los terminales infectados, con miras a descubrir las fuentes IP desde las que se controlan los terminales infectados o se recopila la información relativa al estado de dichos terminales.

El software malicioso conocido en el ámbito de las aplicaciones deberá ser objeto de un análisis dinámico, que permita comprobar si los controladores maliciosos han introducido actualizaciones.

7.3 Análisis del nuevo software malicioso

Cabe la posibilidad de descubrir nuevo software malicioso mediante el análisis conductual, estático y dinámico de las aplicaciones obtenidas de las tiendas de aplicaciones.

7.3.1 Análisis de programas ejecutables y códigos maliciosos

El objetivo del análisis estático consiste en desentrañar el plano sintáctico del software malicioso bajo sospecha. Por ejemplo, una aplicación móvil puede desarticularse utilizando técnicas de ingeniería inversa para obtener su archivo de manifiesto (que contiene información acerca de los permisos a los que accede la aplicación) y sus códigos fuente. Al examinar el archivo de manifiesto y explorar las características que se alega posee la interfaz de programación de aplicaciones (API), pueden reconocerse determinados intentos maliciosos gracias a una serie de políticas de detección típicas. En ese sentido, cabe verificar:

- si se permiten privilegios de acceso innecesarios y delicados;
- si se invoca la API de red para acceder a fuentes de Internet maliciosas;

- si se invoca la API de procesos para cerrar una aplicación;
- si se invoca la API de procesos para exportar información de contacto a una ubicación específica;
- si el comportamiento de la tarjeta (de memoria) Secure Digital (SD) o la tarjeta de módulo de identidad de abonado (SIM) es anómalo;
- si se produce un intercambio de datos con identificadores uniformes de recursos (URL) maliciosos conocidos;
- si existe una suscripción a un servicio de mensajes cortos (SMS) que no haya sido solicitada por el abonado;
- si existen instrucciones para controlar el terminal móvil a distancia.

El objetivo del análisis dinámico consiste en ejecutar y supervisar software malicioso móvil en un entorno (por ejemplo, un ambiente aislado o *sandbox*) controlado (e incluso virtualizado). A continuación se citan algunas de las políticas de detección típicas.

a) Comunicación de las redes robot:

   i) Descripción: Para poder unirse a una de estas redes, el robot ha de comunicar su existencia a un servidor de mando y control (C&C), encargado de ordenar a dicha red la realización de actividades maliciosas. El servidor C&C puede ser un servidor web o un terminal de la red móvil, y puede transmitir sus órdenes a través de servicios de Internet, mensajes cortos (SMS) y mensajería multimedios (MMS).

   ii) Políticas de detección:

      1) un gran número de terminales se conecta a un anfitrión malicioso conocido;
      2) un terminal se conecta a un anfitrión malicioso conocido regularmente durante un largo periodo de tiempo;
      3) un terminal envía mensajes SMS binarios a un gran número de terminales.

b) Propagación y correo basura:

   i) Descripción: El software malicioso se propaga a sí mismo o envía correos basura a otros abonados a través de diversos servicios (Internet, MMS, SMS, etc.) de la manera más amplia posible.

   ii) Políticas de detección:

      1) un gran número de terminales envía los mismos MMS o SMS (los mensajes se cotejan mediante una comprobación aleatoria unidireccional), cuya distribución geográfica es arbitraria;
      2) el volumen de un servicio aumenta vertiginosamente en momentos de inactividad;
      3) se realizan llamadas triples;
      4) se envían mensajes SMS;
      5) se envían mensajes MMS;
      6) si el software invoca una llamada falsificada;
      7) si el software exporta la información de la tarjeta SIM a un servidor;
      8) si el software invoca una llamada maliciosa después de un corto intervalo;
      9) si se inducen descargas adicionales de forma innecesaria;
      10) si se accede a controladores maliciosos conocidos.

c) Suscripción y consumo maliciosos:

i) Descripción: Los terminales infectados se suscribirán a servicios de valor añadido (VAS) o de llamadas triples, realizarán llamadas sobretasadas o internacionales, y enviarán un elevado número de mensajes. El abonado ignorará estos cargos.

ii) Políticas de detección:

1) la factura del abonado aumenta inexplicablemente;

2) el terminal infectado realiza con frecuencia llamadas sobretasadas o internacionales en periodos de tiempo específicos;

3) numerosos terminales envían constantemente los mismos mensajes en repetidas ocasiones y en periodos de tiempo específicos;

4) el terminal se suscribe a servicios de llamadas triples y los utiliza con frecuencia e incluso todo el tiempo.

d) Ataque de denegación de servicio distribuido (DDoS):

i) Descripción: Una multitud de terminales inunda los recursos de radiocomunicaciones y otros recursos de la red móvil a fin de comprometer la calidad de servicio.

ii) Políticas de detección:

1) el tráfico en el nodo de soporte de la pasarela del servicio general de radiocomunicaciones por paquetes (GGSN) u otras entidades de red aumenta vertiginosamente y la mayor parte del tráfico se dirige al mismo destino.

El análisis estático no es adecuado para el software malicioso sospechoso que se oculta o camufla, y el análisis dinámico no abarca todo el código de programa. Por consiguiente, deben llevarse a cabo ambos análisis para obtener una visión más completa del funcionamiento del software malicioso en cuestión.

Los intentos o comportamientos anómalos aislados y reconocidos mediante los análisis estático y dinámico resultan de utilidad para actualizar las políticas en materia de análisis conductual que se aplican a los últimos casos de anomalías. Por otra parte, estas características reconocidas pueden ayudar a los operadores a localizar direcciones IP o URL maliciosas desconocidas.

7.3.2 Enfoque combinado

En consecuencia, se sugiere combinar ambos planteamientos analíticos para mejorar los resultados y reducir el número de falsos positivos en el proceso de descubrimiento.

En dicho proceso, pueden generarse diversos resultados con miras a facilitar el proceso de gestión sucesivo. Entre los resultados del proceso de descubrimiento deben figurar:

- una lista de terminales infectados;
- muestras de aplicaciones que contengan software malicioso conocido;
- muestras de software malicioso nuevo; y
- una lista de controladores maliciosos.

La información que antecede reviste una importancia crucial para que los operadores puedan adoptar las medidas adecuadas en los procesos descritos en los apartados 8 y 9.

8 Gestión

En el proceso de gestión, los resultados del proceso de descubrimiento se analizan y validan de manera automática o semiautomática. A continuación, se aplican medidas de gestión conformes a la gravedad de las anomalías. La Figura 3 ilustra las relaciones interactivas entre el proceso de gestión y otras entidades de red y servicio.

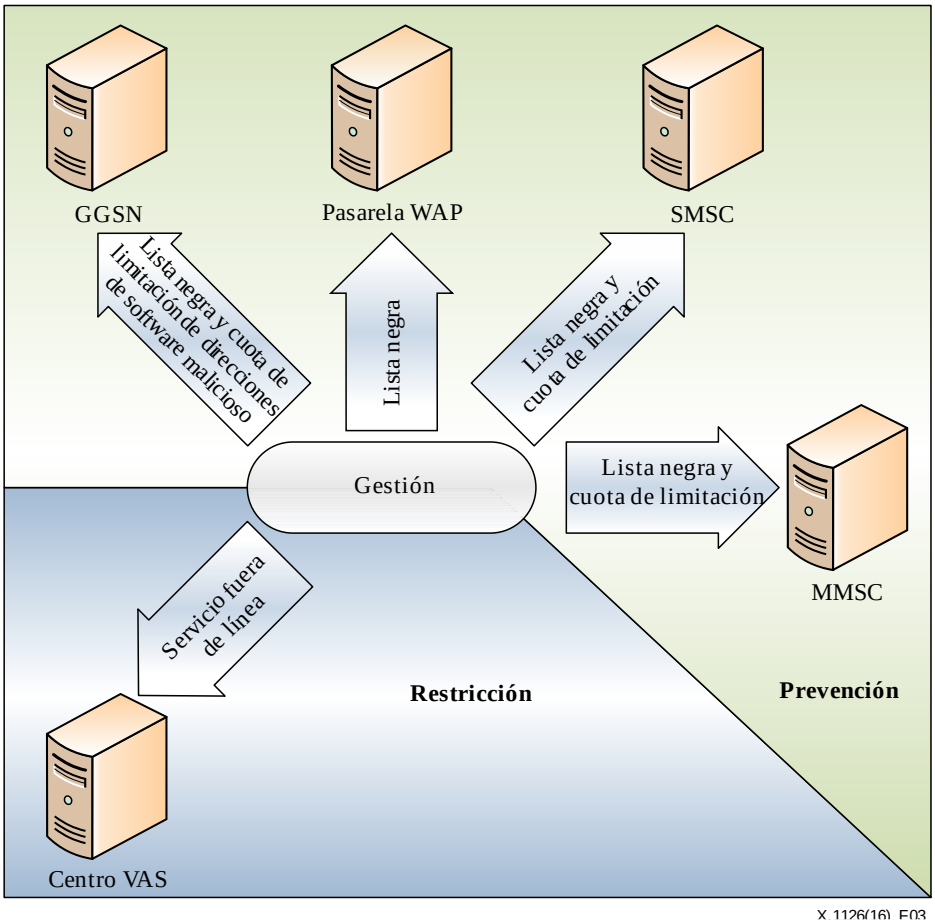

Figura 3 – Relaciones interactivas del proceso de gestión

8.1 Medidas de gestión

En función de la gravedad de la anomalía, pueden aplicarse dos tipos de medidas: las de prevención y las de restricción. En ambos casos, se utilizarán únicamente las capacidades de las entidades de red y las plataformas que dan soporte al servicio.

- Prevención: Si la anomalía es moderada y puede controlarse sin interrumpir los servicios ofrecidos a los abonados, cabe adoptar el método de prevención para gestionar el problema.
- Restricción: Si las medidas preventivas no resultan eficaces y el abonado ya ha sufrido una gran pérdida de dinero, se emplearán medidas restrictivas para suspender el servicio afectado de forma selectiva o integral.

8.2 Prevención

8.2.1 Lista negra

Cuando un controlador malicioso desencadena una anomalía, sus datos pueden añadirse a una lista negra. A continuación, se bloquean el envío y la recepción de solicitudes vinculadas a dicho controlador. Numerosas entidades de red, tales como los GGSN, las pasarelas de protocolo de aplicaciones inalámbricas (WAP) y los centros de servicios de mensajería multimedios (MMSC), respaldan la función de las listas negras. Pueden mantenerse múltiples listas negras con miras a bloquear diferentes tipos de controladores maliciosos, incluidos nombres de dominio de sitios web maliciosos y direcciones IP de servidores C&C. Cabe tener en cuenta que las fuentes de las listas negras se verifican y actualizan periódicamente, a fin de evitar el bloqueo de fuentes legítimas.

El GGSN puede bloquear todas las direcciones encaminadas a la descarga de aplicaciones que contengan software malicioso.

8.2.2 Cuota de limitación

Cuando el correo basura constituye la principal causa de una anomalía en la red (véanse los ataques DDoS), pueden aplicarse cuotas de limitación para disminuir la velocidad de propagación. La cuota de limitación define el número máximo de mensajes que puede enviarse en un periodo de tiempo determinado (por ejemplo, un mes), garantizando plenamente las capacidades de comunicación básica o de emergencia de los terminales. Una vez que se excede dicho umbral, no se permite el envío de más mensajes.

8.3 Restricción

8.3.1 Servicios del operador fuera de línea

Si un controlador malicioso accede al servicio de un operador, por ejemplo, utilizando técnicas de piratería informática, el operador puede ejercer su derecho y obligación de desconectar su propio servicio de forma temporal y utilizar un servicio secundario, en caso de necesidad, para proporcionar comunicaciones de emergencia.

9 Intercambio de información

La gestión del problema no puede constituir el objetivo final, ya que dicho proceso no procura sino minimizar las repercusiones negativas sobre los abonados y las redes. En ese sentido, el objetivo final debe consistir en recuperar la normalidad y tratar de prevenir infecciones más amplias. Por consiguiente, el proceso de intercambio de información es importante para perfeccionar el marco.

En aras del bienestar de la industria, los operadores solo deberían compartir muestras de software malicioso.

Téngase en cuenta que el proceso de intercambio de información debe ajustarse a la legislación local y a los contratos de suscripción.

Bibliografía

[b-UIT-T X.1121] Recomendación UIT-T X.1121 (2004), *Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo*.

[b-UIT-T X.1211] Recomendación UIT-T X.1211 (2014), *Técnicas para prevenir ataques en la web*.

[b-UIT-T X.1244] Recomendación UIT-T X.1244 (2008), *Características generales de la lucha contra el correo basura (spam) en aplicaciones multimedios basadas en IP*.

[b-UIT-T X.1245] Recomendación UIT-T X.1245 (2010), *Marco para la lucha contra el correo basura en aplicaciones multimedios IP*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017