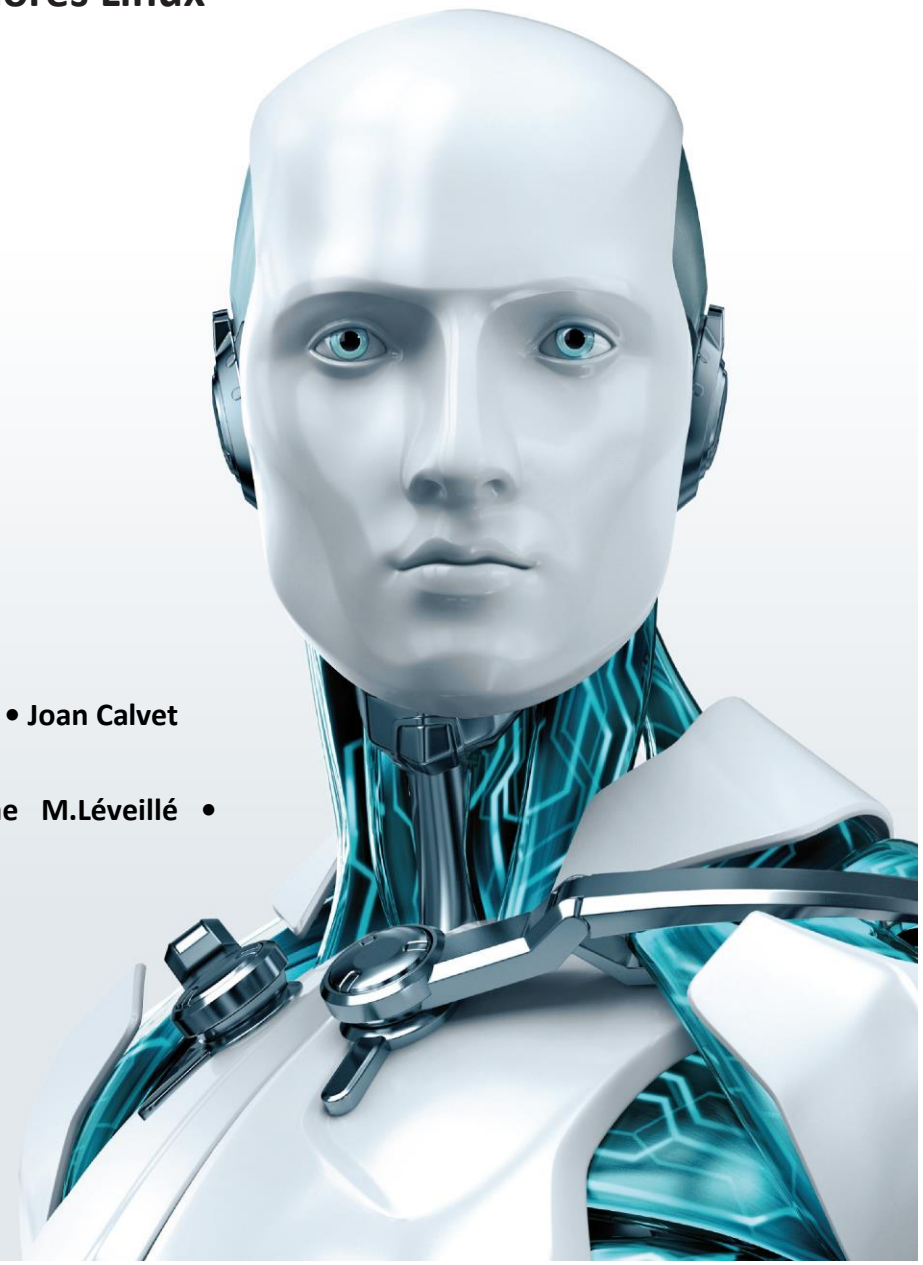
Operación Windigo

Análisis de una gran campaña de malware que roba credenciales desde servidores Linux



Olivier Bilodeau • Pierre-Marc Bureau • Joan Calvet

Alexis Dorais-Joncas • Marc-Étienne M.Léveillé • Benjamin Vanheuverzwijn

Marzo, 2014

ESET
ENJOY SAFER TECHNOLOGY™

Contenido

RESUMEN EJECUTIVO

El presente documento aporta detalles sobre una sofisticada operación de gran magnitud, cuyo nombre en código es "Windigo", y mediante la cual un grupo malicioso afectó miles de servidores Linux y Unix. Los servidores comprometidos se usan para robar credenciales SSH, para redirigir a quienes visitan los sitios Web a contenido malicioso y para enviar spam.

Esta operación ha estado activa desde al menos 2011 y afectó servidores y empresas de alto perfil, entre las que se incluyen cPanel (la empresa tras el famoso panel de control de hosting de sitios Web) y kernel.org de la Fundación Linux (el repositorio principal de código fuente para el núcleo de Linux. No obstante, el objetivo de esta operación no es robar recursos corporativos ni alterar el código fuente de Linux, como revelaremos a lo largo del informe.

La complejidad de los backdoors (programas de puerta trasera) desplegados por los agentes maliciosos demuestra que tienen un conocimiento fuera de lo común sobre sistemas operativos y programación. Además, se tuvo un cuidado especial para asegurar la portabilidad, es decir que las diversas amenazas maliciosas cuentan con la capacidad de ejecutarse en una amplia gama de sistemas operativos de servidores y de una manera extremadamente furtiva.

El presente informe incluye una descripción minuciosa de nuestra investigación aún en curso sobre la operación Windigo. Suministramos detalles de la cantidad de usuarios que resultaron víctimas y el tipo exacto de recursos que ahora están bajo el control de la banda criminal. Lo que es más, proveemos un análisis detallado de los tres componentes maliciosos principales de esta operación.

• Linux/Ebury: un backdoor OpenSSH utilizado para controlar los servidores y robar credenciales

• Linux/Cdorked: un backdoor HTTP utilizado para redirigir el tráfico Web. También brindamos detalles de la infraestructura desplegada para redirigir el tráfico, incluyendo un servidor DNS modificado usado para resolver direcciones IP arbitrarias con la etiqueta Linux/Onimiki

• Perl/Calfbot: un script en Perl utilizado para enviar spam

La operación Windigo no aprovecha ninguna vulnerabilidad nueva de los sistemas Linux o Unix. Los agentes maliciosos explotaron las deficiencias sistémicas conocidas para crear y mantener su botnet.

Descubrimientos principales

• La operación Windigo ha estado activa desde al menos 2011

• Más de 25.000 servidores únicos se vieron comprometidos en los últimos dos años

• Los atacantes afectaron una amplia gama de sistemas operativos: Apple OS X, OpenBSD, FreeBSD, Microsoft Windows (a través de Cygwin) y Linux, incluyendo Linux en la arquitectura ARM

• Los módulos maliciosos utilizados en la Operación Windigo se diseñaron para ser portables. Se pudo observar que el módulo de envío de spam estuvo activo en todos los tipos de sistemas operativos, mientras que el backdoor SSH se vio tanto en servidores Linux como en FreeBSD

• Organizaciones reconocidas, incluyendo cPanel y la Fundación Linux, resultaron víctimas de esta operación

• Windigo es responsable de enviar un promedio de 35 millones de mensajes de spam diarios

• Actualmente hay más de 700 servidores que están redirigiendo a sus visitantes a contenido malicioso

• Cada día, más de medio millón de visitantes de sitios web legítimos alojados en servidores afectados por Windigo son redirigidos a un paquete de exploits

• La tasa de éxito del aprovechamiento de los equipos visitantes es de aproximadamente 1%

• El grupo malicioso prefiere detener la actividad maliciosa antes que ser descubierto

• La calidad de las diversas amenazas maliciosas es elevada: furtivas, portables, con cifrado sólido (claves de sesión y códigos de un solo uso) y demuestran un conocimiento profundo del ecosistema Linux

• El backdoor HTTP es portable para httpd de Apache , Nginx y lighttpd

• La banda criminal maximiza los recursos disponibles del servidor mediante la ejecución de distintos códigos maliciosos y actividades según el nivel de acceso que posea

• No se aprovecharon vulnerabilidades en los servidores Linux; solo se sacó provecho de las credenciales robadas. Llegamos a la conclusión de que la autenticación por contraseña en servidores ya debería haber quedado en el pasado.

Los apéndices del presente documento incluyen información sobre la desinfección y la prevención de estas amenazas.

INTRODUCCIÓN

Este artículo contiene la explicación de las principales características de la Operación Windigo y hace parte del análisis completo de todas las amenazas involucradas y que se pueden encontrar en el artículo "Operation Windigo: The vivisection of a large Linux server-side credential stealing malware campaign"

Los Algonquinos son una de las primeras naciones de los Estados Unidos de América. En su idioma, la palabra Windigo hace referencia a una criatura demoníaca. En muchas leyendas, el Windigo es un ser malévolo mitad bestia que se transformó dejando su figura humana para convertirse en monstruo porque se alimentaba de carne humana. Al igual que el Windigo, actualmente hay un agente malicioso alimentándose como un caníbal de miles de servidores y convirtiendo recursos legítimos en una amplia infraestructura utilizada con propósitos nefastos.

A principios de 2012, ESET comenzó a investigar un grupo de software malicioso dirigido a servidores Linux. Desde entonces, nos percatamos de que dichos componentes en realidad estaban interconectados entre sí. Pronto descubrimos que, de hecho, un grupo malicioso tiene el control de más de diez mil servidores. Actualmente están utilizando dichos recursos para redirigir tráfico Web desde sitios Web legítimos a contenido malicioso, enviar mensajes de spam y robar más credenciales de usuarios que inician la sesión en esos servidores.

La investigación de ESET con respecto a la Operación Windigo forma parte de un esfuerzo de investigación conjunto con CERT-Bund, la Organización Nacional Sueca de Informática (SNIC), la Organización Europea para la Investigación Nuclear (CERN) y otras organizaciones que conforman un Grupo de trabajo a nivel internacional.

La cantidad de sistemas afectados por la Operación Windigo puede parecer pequeña al compararla con brotes recientes de malware donde se infectan millones de equipos de escritorio. En este caso, es importante recordar que cada sistema infectado es un servidor. Los servidores normalmente ofrecen servicios a una numerosa cantidad de usuarios y están equipados con muchos más recursos en lo que respecta a ancho de banda, almacenamiento y poder informático que los equipos personales normales. Un ataque de denegación de servicio o una operación de envío de spam que use mil servidores van a ser mucho más efectivos que las mismas operaciones efectuadas en la misma cantidad de equipos de escritorio.

En este informe presentamos información general global sobre la Operación Windigo y mostramos un análisis de los datos que pudimos recopilar provenientes de diversas fuentes, incluyendo la captura de tráfico de servidores de comando y control. Esta información general muestra la forma en que se conectan todos los componentes diferentes de la operación y estima el tamaño de la misma.

Luego hacemos una descripción detallada de los tres módulos principales utilizados en la operación Windigo. El primer módulo constituye el eje central de la operación: un backdoor OpenSSH etiquetado Linux/Ebury. Este programa de puerta trasera se discutió por primera vez en público en el año 2011, cuando se lo llamó "Ebury".

A continuación, examinamos el componente utilizado para redirigir el tráfico Web, y que se denomina Linux/Cdorked. Luego analizamos Perl/Calfbot, un script en Perl utilizado para enviar mensajes de spam.

Finalmente suministramos información detallada para los administradores de sistemas sobre cómo pueden detectar si sus sistemas fueron afectados y cómo deben desinfectar las infecciones de los diversos módulos.

Por qué estamos publicando este informe

Decidimos publicar el presente informe para concientizar a las personas sobre esta operación maliciosa. Muchos proveedores de servicios de hosting quedaron completamente afectados, incluyendo sus sistemas de facturación. Creemos que el mejor modo de proceder para mitigar esta amenaza es suministrar un análisis en profundidad de los diversos componentes maliciosos utilizados en el ataque. Por esta misma razón estamos publicando instrucciones minuciosas para detectar hosts infectados por los distintos módulos (en la sección "Indicadores de sistemas comprometidos" de este documento).

En el transcurso de nuestra investigación, prestamos una estricta atención a la notificación de las víctimas y ayudamos a quienes nos respondían y se preocupaban por desinfectarse. El presente documento constituye otro paso en el proceso de proteger los servidores infectados y concientizar sobre la gran amenaza que constituye la Operación Windigo.

OPERACIÓN WINDIGO

Panorama global

La operación Windigo ha estado activa durante años. Creemos que el propósito principal de este esfuerzo significativo es el rédito económico a través de las siguientes acciones:

- Spam
- Infección de los equipos de los usuarios Web mediante descargas desde las páginas Web visitadas
- Redirección del tráfico Web a redes publicitarias

En esta sección presentaremos información general sobre la operación Windigo y su evolución con el paso del tiempo. Además, analizaremos diversas fuentes de datos a las que pudimos acceder durante el curso de la investigación.

La siguiente imagen muestra una perspectiva de alto nivel sobre la operación Windigo.

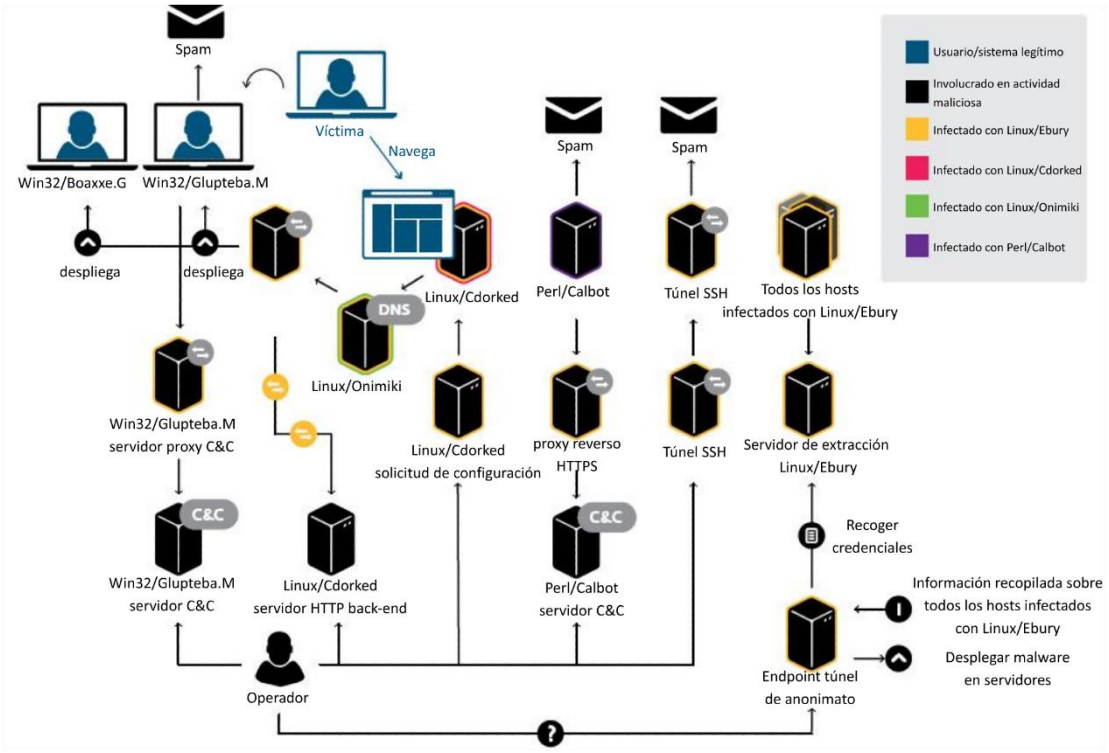


Imagen 1. Perspectiva de alto nivel sobre los componentes de Windigo y cómo se relacionan

Como se muestra en la Imagen 1, son varios los componentes de software malicioso que conforman la operación Windigo:

• Linux/Ebury se ejecuta mayormente en servidores Linux. Proporciona un shell de puerta trasera con privilegios de raíz y tiene la habilidad de robar credenciales SSH.

• Linux/Cdorked se ejecuta mayormente en servidores Web de Linux. Proporciona un shell de puerta trasera y distribuye malware para Windows a usuarios finales mediante infecciones por páginas Web.

• Linux/Onimiki se ejecuta mayormente en servidores DNS de Linux. Resuelve nombres de dominio con un patrón particular para *cualquier dirección IP*, sin necesidad de cambiar la configuración del lado del servidor.

• Perl/Calfbot se ejecuta en la mayoría de las plataformas compatibles con Perl. Es un bot liviano para enviar spam escrito en Perl.

• Win32/Boaxxe.G, un programa malicioso basado en el fraude de clic, y Win32/Glubteta.M, un proxy genérico, se ejecutan en equipos Windows. Estas son las dos amenazas que se distribuyen mediante las infecciones por páginas Web.

En resumen, los operadores de Windigo realizan varias actividades a través de las siguientes familias de malware:

Actividad maliciosa	Componente de malware
Spam	Win32/Glupteba.M, Perl/Calfbot, Linux/Ebury
Infección por páginas Web	Linux/Cdorked
Estafa de avisos publicitarios	Linux/Cdorked, Win32/Boaxxe.G
Robo de credenciales	Linux/Ebury

Tabla 1. Relación entre los componentes de malware y sus actividades

Una característica extraordinaria de esta operación es la vasta cantidad de servidores infectados que soportan las actividades maliciosas mencionadas arriba. En otras palabras, aquí hay dos clases de víctimas: los usuarios finales de Windows que visitan sitios Web legítimos alojados en servidores comprometidos y los operadores de servidores Linux/Unix cuyos servidores se vieron afectados a través de la extensa red de robo de credenciales del lado del servidor. Los agentes maliciosos están usando estos servidores comprometidos para ejecutar uno o más servicios maliciosos, necesarios para administrar la operación completa. A continuación se muestran los tipos de servicios y el componente de malware con el que se relacionan:

Servicio de infraestructura maliciosa	Componente de malware involucrado
Servicios DNS relacionados con spam	Linux/Ebury con TinyDNS
Servicios DNS Cdorked	Linux/Ebury con Linux/Onimiki
Servicio de robo de credenciales	Linux/Ebury con un componente binario adicional
Servicio de configuración	Linux/Ebury
Túnel SSH	Todos infectados con Linux/Ebury
Servicio de poxy reverso	Todos infectados con Linux/Ebury
Túnel de anonimato	Linux/Ebury

Tabla 2. Relación entre los componentes de malware y su utilización en la infraestructura

Cronología de sucesos

En esta sección se detalla la línea de tiempo de los sucesos relacionados con la operación Windigo, como lo observaron los investigadores de ESET.

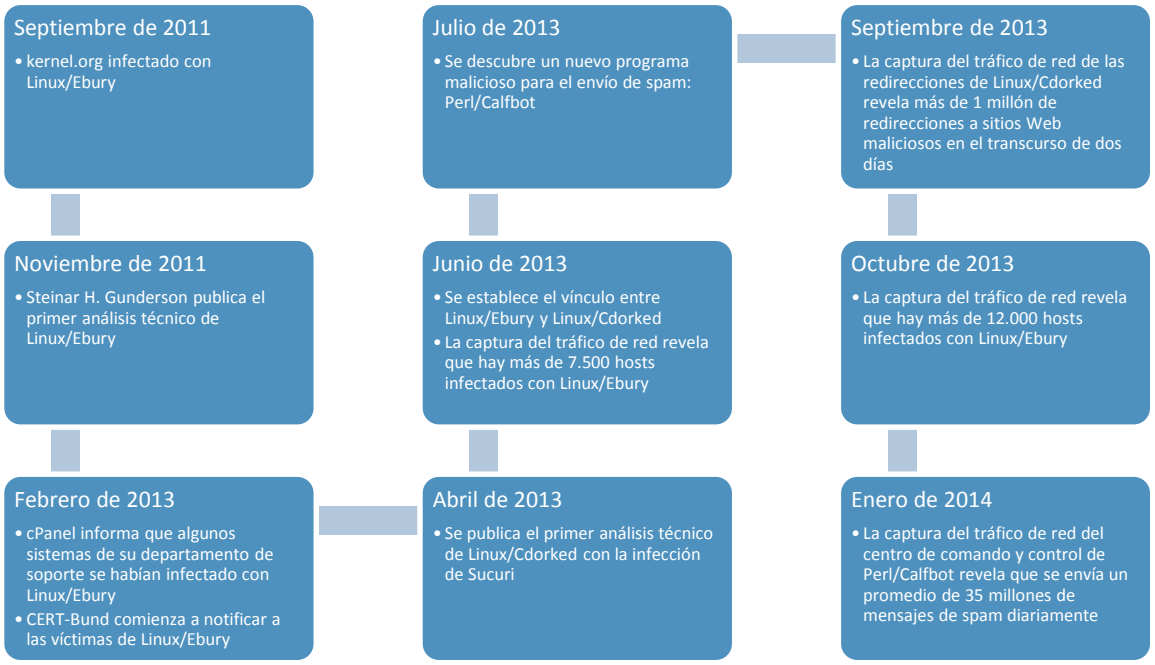


Imagen 2. Cronología de sucesos

2011

- Septiembre: La Fundación Linux anuncia en forma interna la infección de varios de sus servidores back-end así como de 448 usuarios de kernel.org. A pesar de que hasta el momento no se publicó ningún informe donde se explique qué ocurrió en la Fundación Linux, varios artículos de prensa así como otras fuentes de confianza indican que se emplearon dos tipos de malware sofisticados para atacar la Fundación Linux. Mientras que el primer programa malicioso es el conocido rootkit Phalanx2, pruebas contundentes indican que el segundo, distribuido como archivos OpenSSH modificados, constituye en realidad la versión inicial de Linux/Ebury. La línea de tiempo también es interesante: a pesar de que Phalanx2 ya se había utilizado antes en varias infecciones, por lo que sabemos, nunca se volvió a ver *in-the-wild* luego de la infección de la Fundación Linux. Es interesante señalar que éste fue el primer caso conocido que involucraba Linux/Ebury.
- Noviembre: Primer publicación en blog sobre Ebury escrita por Steinar H. Gunderson. La descripción técnica de este programa de puerta trasera coincide exactamente con los resultados de nuestro análisis sobre Linux/Ebury.

2012

- Noviembre: Primera observación de los patrones de redirección URL de Linux/Cdorked.

2013

- Febrero: cPanel anuncia que uno de sus servidores de soporte se infectó con el troyano Linux/Ebury. Es probable que esta infección haya contribuido a la propagación del código malicioso a varias organizaciones.

- Febrero: CERT-Bund identifica que hay más de 11.000 servidores infectados con Linux/Ebury. Se envían notificaciones sobre los servidores comprometidos a los proveedores de servicios de hosting y a los CERT nacionales.
- Marzo: ESET recibe la primera muestra de Linux/Cdorked de la empresa de seguridad Sucuri.
- Abril: El grupo malicioso responde a las notificaciones de las víctimas mediante la actualización de la mayoría de los servidores infectados a una nueva versión de Linux/Ebury. Esta versión usa un nuevo algoritmo que genera nombres de dominio utilizados para el robo de datos.
- Abril: Sucuri y ESET publican un análisis detallado del programa de malware Linux/Cdorked que afectó al servidor Web Apache. También se publican herramientas autosostenibles con las que los administradores de sistemas pueden detectar el malware en servidores de producción y volcar la información de configuración almacenada solo en memoria RAM.
- Mayo: ESET recibe muestras adicionales de malware provenientes de administradores de sistemas que están desinfectando sus servidores. Se publica un segundo blog donde se confirma que otros servidores Web como lighttpd y nginx también pueden estar infectados con Linux/Cdorked.
- Mayo: ESET comienza un monitoreo extensivo de los sitios Web infectados con Linux/Cdorked y descubre que varios cientos de miles de nuestros clientes navegan en estos sitios todos los meses.
- Junio: Los operadores de Windigo lanzan una nueva versión de su programa de puerta trasera DNS (denominado Linux/Onimiki) y cambian el patrón de nombres de host utilizados por la operación. Los operadores también lanzan una nueva versión del backdoor HTTP Linux/Cdorked para evadir la herramienta de detección lanzada en abril.
- Junio: ESET recibe la primera muestra del backdoor OpenSSH Linux/Ebury.
- Junio: El acceso a uno de los servidores utilizados para extraer credenciales robadas por Linux/Ebury revela que más de 7.000 hosts están infectados con el malware.
- Julio: Se encuentra el módulo de envío de spam Perl/Calfbot en un host infectado con Linux/Ebury.
- Julio: El descubrimiento de un archivo de configuración TinyDNS revela que hay 62.186 nombres de dominio únicos que unen varias piezas del rompecabezas. Demuestra que el mismo grupo es responsable de enviar spam, redirigir a los usuarios a paquetes de exploits y otras actividades maliciosas.
- Septiembre: ESET captura tráfico de red de un servidor infectado con Linux/Ebury que ejecuta un servicio de proxy reverso utilizado como el objetivo de las redirecciones de Linux/Cdorked, y revela que se realizan más de 1.000.000 de redirecciones de sitios Web en 48 horas.
- Octubre: ESET captura 72 horas de tráfico de red y se revela que existen más de 12.000 servidores infectados con Linux/Ebury.

2014

- January: CERT-Bund publica un artículo de Preguntas frecuentes sobre Ebury luego de recibir muchas preguntas en relación con las notificaciones de los infectados.
- Enero: ESET captura tráfico de red durante tres períodos distintivos de 24 horas de un servidor donde se ejecutaban tanto un servicio de extracción de datos Linux/Ebury y un proxy reverso de comando y control Perl/Calfbot, y reveló que cada día se enviaba un promedio de 35 millones de mensajes de spam.
- Febrero: Primera referencia pública de una conexión entre Linux/Ebury y Linux/Cdorked.

Uniendo los cabos sueltos

Esta sección proporciona evidencia que nos conduce a la conclusión de que los componentes de la Operación Windigo son desarrollados y operados por un mismo grupo.

Infraestructura en común

Al correlacionar los datos del servidor de extracción de Linux/Ebury con los de Linux/Cdorked, notamos que la mayoría de los hosts infectados con Linux/Cdorked también estaban infectados con Linux/Ebury. Se puede decir lo mismo de los demás componentes maliciosos. El servidor de comando y control de Win32/Glupteba.M se encuentra alojado en un host infectado con Linux/Ebury; el caso de Perl/Calfbot es el mismo.

Finalmente, Win32/Glupteba.M, un proxy genérico, se usa únicamente para retransmitir spam. Cuando investigamos sus mensajes de spam, encontramos que contienen las mismas URL que las de los mensajes de spam de Perl/Calfbot.

Código en común

Durante el análisis de Linux/Cdorked y Linux/Ebury, nos dimos cuenta de que un algoritmo de descifrado hecho a medida manifestaba características muy similares. Este algoritmo usa la dirección IP del cliente como una clave seed para descifrar los datos subyacentes.

Linux/Cdorked

```
push    rbp
mov     rbp, rsp
push    rbx
sub     rsp, 48h
mov     [rbp+crypted_string_arg1], rdi
mov     [rbp+decrypted_string_arg2], rsi
mov     [rbp+key_int_arg3], edx
mov     eax, [rbp+key_int_arg3]
cdqe
and     eax, 0FF000000h
sar     rax, 0Ah
add     eax, 5
mov     [rbp+key_from_arg3], al
mov     eax, [rbp+key_int_arg3]
cdqe
and     eax, 0FF0000h
sar     rax, 10h
add     eax, 33
mov     [rbp+key_from_arg3+1], al
mov     eax, [rbp+key_int_arg3]
cdqe
and     eax, 0FF00h
sar     rax, 8
add     eax, 55
mov     [rbp+key_from_arg3+2], al
mov     eax, [rbp+key_int_arg3]
add     eax, 78
mov     [rbp+key_from_arg3+3], al
mov     [rbp+var_2E], 0
mov     [rbp+i], 0
```

Linux/Ebury

```
push    r15
movsxd  rax, edx
add     edx, 78
mov     rcx, rax
push    r14
shr     rcx, 24
mov     r14, rsi
add     ecx, 5
push    r13
push    r12
mov     r12, rdi
push    rbp
xor     ebp, ebp
push    rbx
sub     rsp, 38h
mov     [rsp+68h+xorkey], cl
mov     rcx, rax
movzx   eax, ah
shr     rcx, 16
add     eax, 55
mov     [rsp+68h+xorkey+3], dl
add     ecx, 33
mov     [rsp+68h+xorkey+2], al
mov     [rsp+68h+var_46], 0
mov     [rsp+68h+xorkey+1], cl
lea     r13, [rsp+68h+str]
lea     r15, [rsp+68h+var_5C]
jmp     short loc_36E7003390
```

Imagen 3. Comparación del cifrado hecho a medida de Linux/Cdorked y Linux/Ebury

A pesar de que el código está organizado en forma diferente debido al comportamiento distinto de otro programa de compilación, efectivamente se trata del mismo código y muestra las mismas constantes: 5, 33, 55 y 78.

Luego, al observar el código de Perl/Calfbot, algo curiosamente familiar nos llama la atención:

```
...
    my @h7fk;
    $h7fk[0] = ( ( ( $key & 0xFF000000 ) >> 24 ) + 15 ) % 256;
    $h7fk[1] = ( ( ( $key & 0x00FF0000 ) >> 16 ) + 13 ) % 256;
    $h7fk[2] = ( ( ( $key & 0x0000FF00 ) >> 8 ) + 52 ) % 256;
    $h7fk[3] = ( ( ( $key & 0x000000FF ) ) + 71 ) % 256;
    my $apjn;
    for ( my $i = 0 ; $i < length($encrypted_string) / 2 ; $i++ ) {
       my $id5b = hex( substr( $encrypted_string, $i * 2, 2 ) );
       $h7fk[ ( $i + 1 ) % 4 ] = ( $h7fk[ ( $i + 1 ) % 4 ] + $id5b )
% 256;
       $apjn .= chr( $id5b ^ $h7fk[ $i % 4 ] );
    }
    return $apjn;
}
```

Imagen 4. Código de descifrado de la cadena de Perl/Calfbot descifrada

Modus operandi del robo de credenciales

El robo de credenciales SSH de usuario es la única técnica que observamos de expansión de la operación Windigo. Existen dos escenarios típicos de robo de credenciales SSH. El primer caso es cuando un usuario inicia la sesión correctamente en un servidor infectado. El segundo caso es cuando un usuario usa un servidor comprometido para iniciar la sesión en cualquier otro sistema.

El backdoor Linux/Ebury es el módulo responsable del robo de la credencial y constituye el eje central de la operación Windigo. Podrá encontrar una descripción técnica de esta amenaza en la sección Linux/Ebury del presente documento.

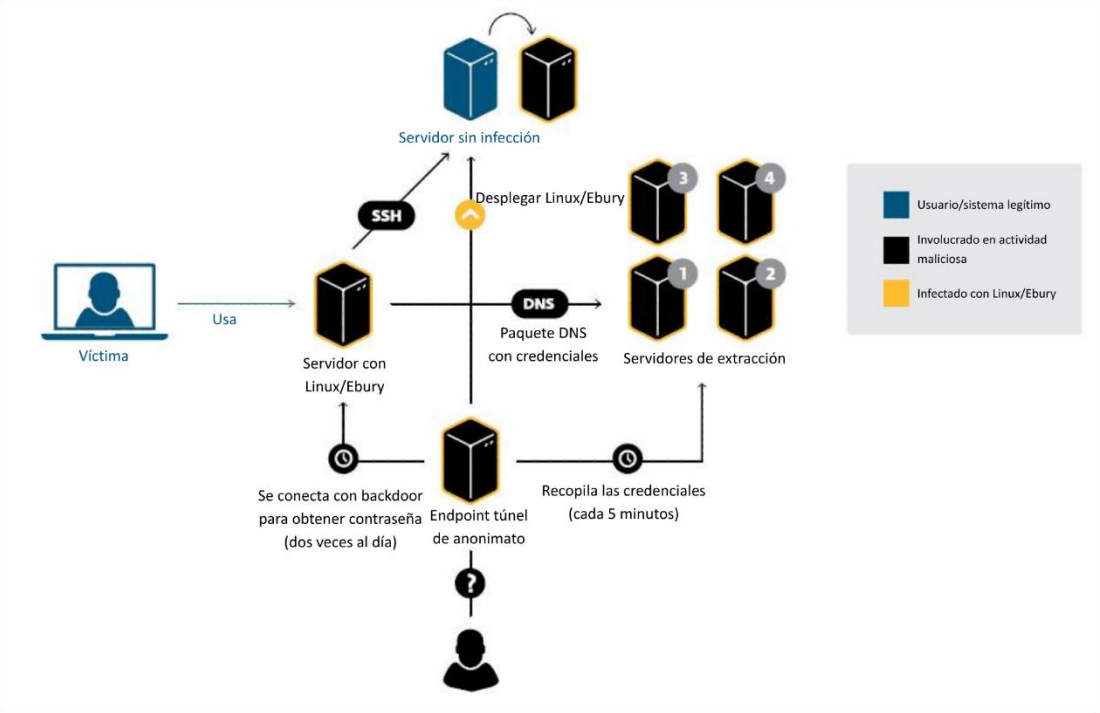


Imagen 5. Infraestructura detallada del robo de credenciales por Linux/Ebury

Arriba se encuentran representados los diversos componentes relacionados con la amenaza Linux/Ebury. Las credenciales interceptadas por Linux/Ebury se envían a los servidores de extracción a través de solicitudes DNS personalizadas. Dichas credenciales luego se usan para seguir propagando la infección, como se detalla en la próxima sección.

La banda criminal emplea buenas prácticas de seguridad operativa. Nunca se conectan en forma directa a ninguno de los servidores comprometidos para realizar sus operaciones. Utilizan uno de los servicios de túneles de anonimato que se ejecuta en otra parte del servidor comprometido, dentro la infraestructura maliciosa.

Este túnel normalmente se usa para recuperar las credenciales robadas que se almacenan en diversos servidores infectados.

Escenarios de infección

La siguiente imagen muestra un escenario típico de un servidor con sus credenciales comprometidas. Según el nivel de privilegios que obtuvo el atacante, usará el servidor de distintas maneras.

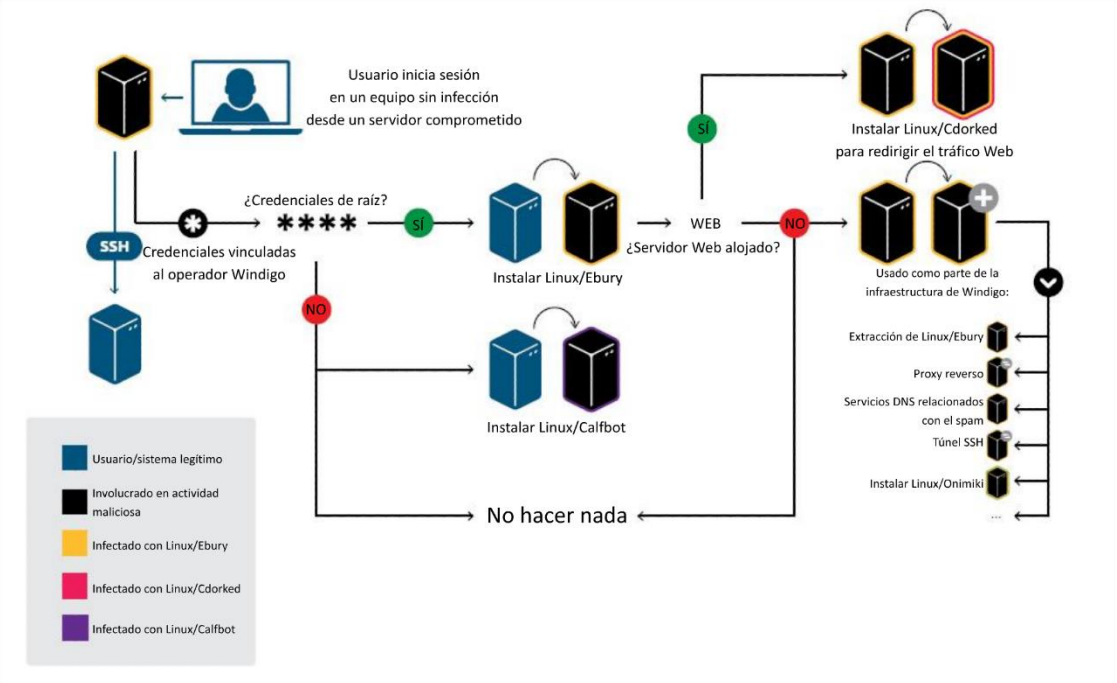


Imagen 6. Organigrama del escenario de robo de credenciales de Windigo

Una vez que se extrajeron las credenciales y se encuentran en manos de los operadores de Windigo, se evalúan para determinar el nivel de privilegios obtenido. En el caso de que no se haya obtenido el acceso a la raíz, el servidor se deja intacto o se le instala el módulo Perl/Calfbot.

Si se obtuvo acceso a la raíz, el backdoor Linux/Ebury se instala en todos los casos para mantener el acceso al servidor incluso aunque el administrador del sistema modifique las credenciales posteriormente. En algunos casos poco frecuentes, se instala Perl/Calfbot como raíz, pero constituye algo secundario, como se podrá observar en el análisis de metadatos de comando y control de Perl/Calfbot más adelante.

Si el servidor comprometido opera un sitio Web legítimo o más, es probable que se siga propagando la infección con Linux/Cdorked. Adicionalmente, se pueden desplegar cero o más servicios maliciosos de la lista de infraestructura de malware previamente mencionada. Por ejemplo, si se puede acceder al puerto HTTPS (443) del servidor desde Internet, entonces se podría desplegar una instancia de proxy reverso nginx para que actúe como la primera capa de direccionamiento indirecto entre los hosts infectados con Perl/Calfbot y el verdadero servidor de comando y control.[1]

Esto demuestra que los operadores están maximizando lo que pueden obtener de los servidores a los que tienen acceso. Se usan diversos elementos maliciosos y una variedad de servicios, pero el malware que une todas las piezas definitivamente es Linux/Ebury.

[1] Es posible que se usen varias capas de direccionamiento indirecto para ocultar aún más el verdadero comando y control.

Hosts infectados con Linux/Ebury

Esta sección brinda información general sobre la cantidad de hosts infectados con Linux/Ebury y su ubicación geográfica. Los datos utilizados para generar estas estadísticas provienen de las distintas capturas de tráfico de red indicadas en la sección sobre cronología de sucesos en el presente documento.

La siguiente tabla muestra la cantidad de direcciones IP únicas infectadas para cada captura:

Fecha de la captura	Recuento de direcciones IP únicas infectadas
Junio de 2013	7.707
Octubre de 2013	12.326
Enero de 2014	11.110

Imagen 7. Recuento de infecciones con Linux/Ebury en diferentes capturas

Desde que comenzamos a monitorear la operación, observamos 26.024 direcciones IP únicas infectadas con Linux/Ebury. Nuestra última captura de enero de 2014 muestra que se infectaron 3.794 direcciones IP nuevas desde nuestra captura de octubre. Esto demuestra que durante dicho período se produjo un promedio de 38 nuevas infecciones diarias. Además de los infectados de Linux, observamos un total de 147 hosts de FreeBSD.

> *Dato curioso: Encontramos un mirror oficial de paquetes CentOS infectados con Linux/Ebury. Afortunadamente, al parecer, los archivos del paquete no fueron alterados por los operadores maliciosos. No obstante, al saber que los paquetes RPM de Linux cuentan con firmas cifradas, dicha manipulación indebida probablemente sea impracticable.*

El tamaño de esta botnet y su curva de crecimiento son mucho más pequeños que las botnets dirigidas a los típicos sistemas operativos de usuarios finales, como Microsoft Windows. Sin embargo, recuerde que cada uno de los hosts comprometidos tiene el potencial de exponer a cada usuario final que visite el sitio Web, así como de facilitar el robo de más credenciales del servidor. El impacto de una infección de Windigo es de varias veces la magnitud de una sola estación de trabajo de usuario final infectada.

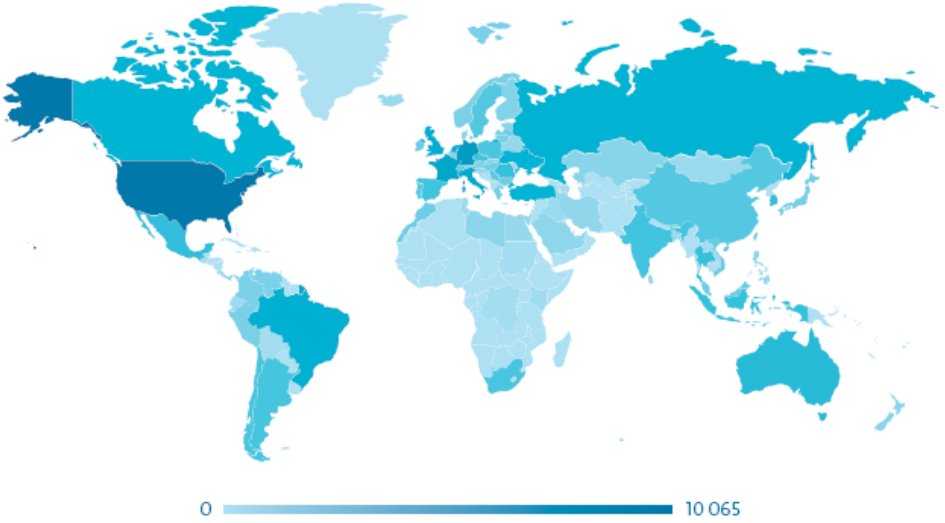


Imagen 8. Distribución geográfica de hosts infectados con Linux/Ebury

Un total de 110 países se vieron afectados por Linux/Ebury, donde los 5 principales son los siguientes:

Posición	País	Cantidad
1	Estados Unidos	10.065
2	Alemania	2.489
3	Francia	1.431
4	Italia	1.169
5	Reino Unido	993
	Otros	9.877
Total		26.024

Tabla 3. Los 5 países principales con infecciones Linux/Ebury

Modus operandi de la redirección del tráfico Web

Los servidores Web infectados con Linux/Cdorked redirigen a sus usuarios a servidores con paquetes de exploits, que a su vez intentan infectar a los usuarios con malware. Esta sección proporciona información general de alto nivel sobre este mecanismo de redirección y las estadísticas relacionadas a la población de servidores Web infectados. Más adelante en este documento se presenta un análisis minucioso de Linux/Cdorked.

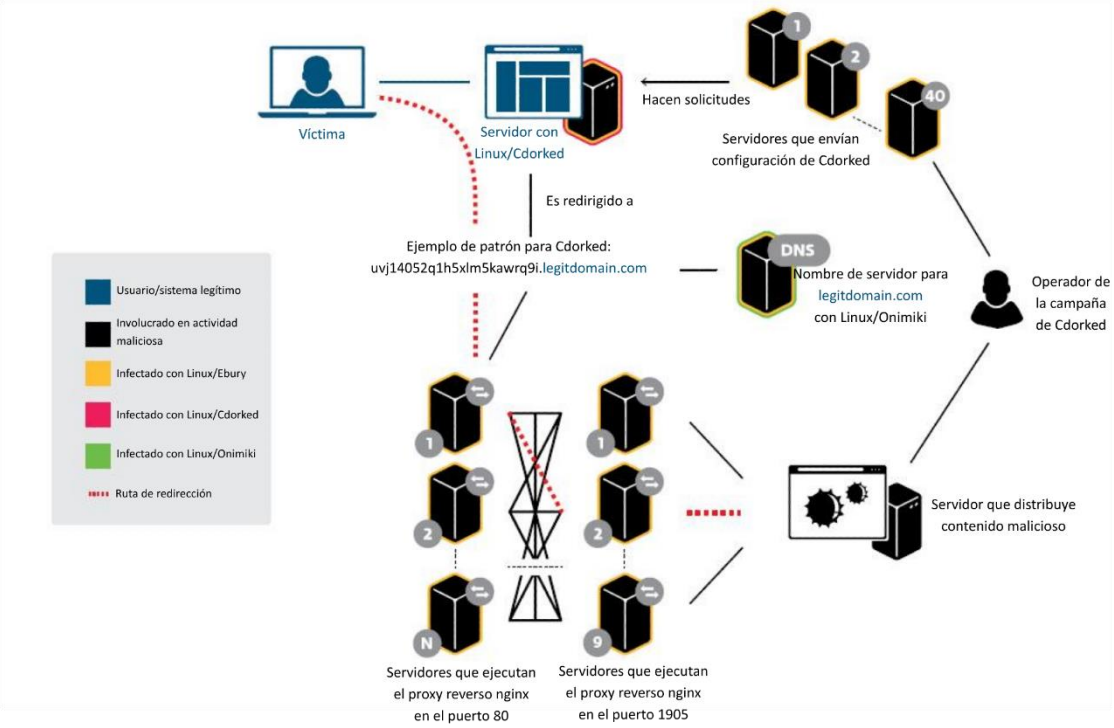


Imagen 9. Infraestructura de malware tras la redirección de tráfico Web.

La lógica de la redirección puede resumirse en los siguientes tres pasos:

1 Las víctimas visitan un sitio Web legítimo alojado en un servidor infectado con Linux/Cdorked, que luego las redirige a un subdominio creado específicamente para un nombre de dominio legítimo. Esta redirección no es automática y depende de ciertas condiciones establecidas por los operadores mediante una serie de servidores infectados con Linux/Ebury.

2 El servidor de nombres autoritario para el nombre de dominio legítimo, infectado con otro componente de la operación Windigo llamado Linux/Onimiki, devuelve una dirección IP codificada en el subdominio mismo. Esto le permite a la operación Windigo basarse en servidores de nombres legítimos, lo que dificulta la detección basada en la red, como explicaremos con mayor detalle en la sección sobre Linux/Onimiki. La dirección IP pertenece a un servidor proxy reverso.

3 Este servidor es el punto de entrada de una cadena de servidores proxy reversos que termina en una máquina que entrega exploits (se explica más adelante). Luego de varios intercambios de red, los operadores maliciosos hacen el intento de aprovecharse del usuario: si el intento es acertado, llevan a cabo alguna tarea maliciosa, mientras que si fracasan, redirigen a los usuarios a avisos publicitarios.

En algunos casos, los agentes de usuario de iPhone eran redirigidos a contenido pornográfico en vez de a un paquete de exploits.

Mediante nuestros sistemas de telemetría, podemos monitorear los accesos a los proxies reversos. Un campo presente en las URL de redirección contiene el nombre de dominio visitado por el usuario víctima de la redirección, lo que nos permite enumerar todos los dominios infectados visitados por los usuarios de ESET.

La siguiente tabla muestra el recuento de direcciones IP de servidores Web infectados durante los últimos tres meses al momento en que se escribe este documento, es decir: noviembre de 2013, diciembre de 2013 y enero de 2014. Las direcciones IP se obtuvieron a través de bases de datos con los registros de DNS de los dominios infectados.

Fecha de recopilación	Direcciones IP únicas infectadas
Noviembre de 2013	1.593
Diciembre de 2013	831
Enero de 2014	771

Tabla 4. Recuento de direcciones IP de servidores Web infectados

En estos tres meses, se observaron 2.183 direcciones IP únicas que distribuían contenido malicioso asociado con Linux/Cdorked. De estas direcciones IP, solo se observaron 221 durante los tres meses, lo que indica una rotación bastante intensa.

El siguiente mapa muestra la distribución geográfica de los servidores infectados:

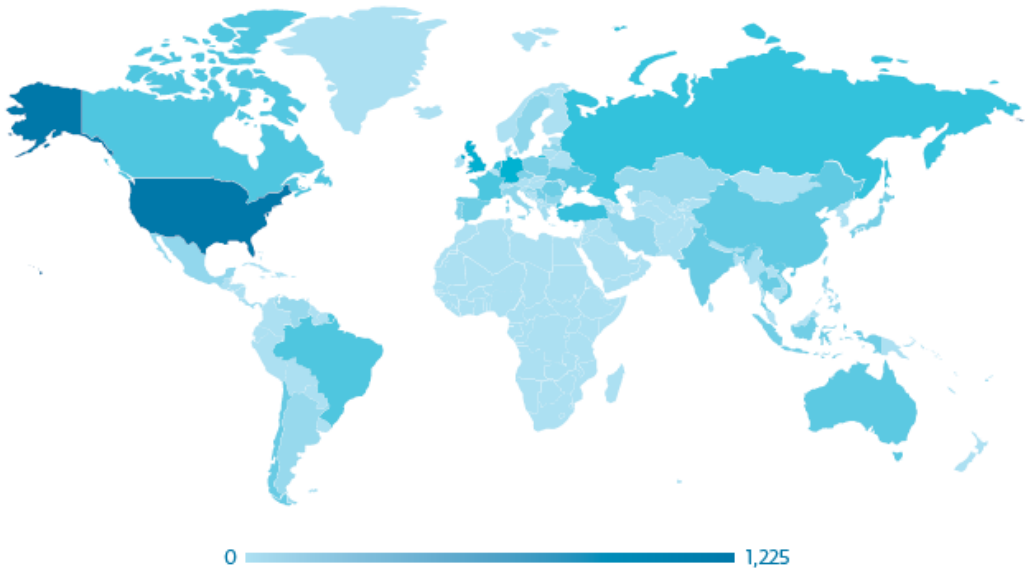


Imagen 10. Distribución geográfica de infecciones con Linux/Cdorked.

En el transcurso de los tres meses, se vieron afectados 63 países distintos, y los 5 países principales con su cantidad de servidores infectados son los siguientes:

Posición	País	Cantidad
1	Estados Unidos	1.225
2	Reino Unido	151
3	Alemania	129
4	Holanda	65
5	Turquía	61
	Otros	552
Total		2.183

Tabla 5. Los 5 países principales con infecciones Linux/Cdorked

Creemos que el claro dominio de los Estados Unidos de América en este ranking de los 5 principales, así como el segundo y tercer lugar, ocupados por Reino Unido y Alemania, es el simple reflejo de la cantidad de empresas de hosting existentes en dichos países y no una estrategia deliberada de los operadores de Windigo.

Análisis de contraseñas SSH robadas

A lo largo de esta investigación, logramos monitorear los datos enviados a los servidores de extracción. Durante un lapso de cinco días, grabamos las credenciales que se usaban exitosamente para iniciar la sesión en servidores. Grabamos un total de 5.362 inicios de sesión exitosos únicos provenientes de 2.840 direcciones IP diferentes y correspondientes a 2.145 contraseñas únicas.

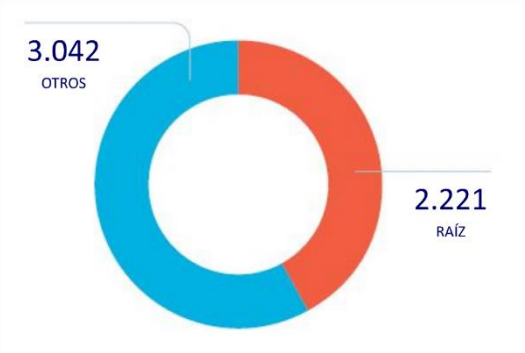


Imagen 11. Distribución de los nombres de usuario de las credenciales robadas

No es sorprendente observar una gran proporción de credenciales raíz robadas por Linux/Ebury si consideramos que los operadores de Windigo deben instalar el malware en la raíz. Cuanto más alta es la cantidad de contraseñas raíz, mayor es el número de infecciones que a su vez se convierten en más posibilidades de robar otras credenciales raíz.

Seguimos analizando las credenciales con mayor detalle; a continuación les mostramos algunas estadísticas de alto nivel sobre las contraseñas:

Cantidad de contraseñas únicas	2145
Cantidad de contraseñas que contienen solo caracteres del alfabeto	190
Cantidad de contraseñas que contienen solo caracteres numéricos	36
Cantidad de contraseñas que contienen solo caracteres alfanuméricos	1.422
Cantidad de contraseñas con caracteres especiales (no alfanuméricos)	723
Longitud mínima de la contraseña	3
Longitud máxima de la contraseña	50
Longitud media de la contraseña	10

Cantidad promedio de caracteres en una contraseña	11,1

Tabla 6. Estadísticas de alto nivel sobre las contraseñas SSH

Lo primero que llama la atención al ver estos datos es la longitud promedio, que resulta mucho más extensa que la esperada. La longitud promedio es de 11,09 caracteres, mucho mayor que el promedio de 7,63 caracteres encontrado en la fuga de LulzSec, analizada en 2011. Seguramente refleja el hecho de que los administradores de sistemas son más conscientes de la importancia de contar con contraseñas fuertes que el usuario promedio de Internet.

El siguiente histograma muestra la distribución de la longitud de las contraseñas:

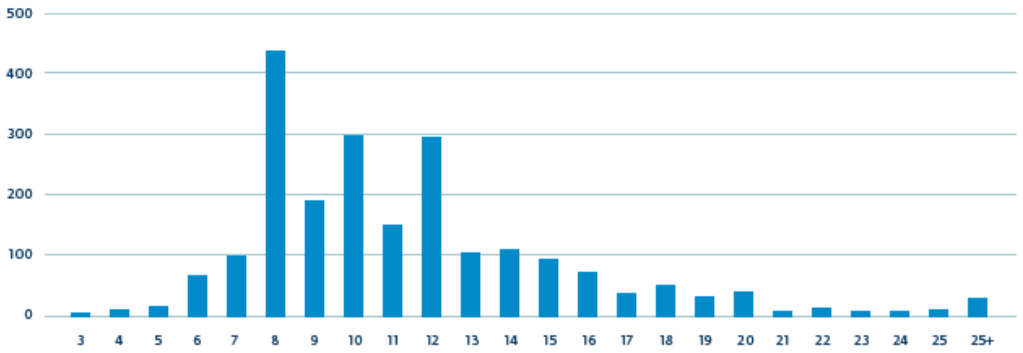


Imagen 12. Distribución de la longitud de las contraseñas

Las contraseñas más utilizadas están bien elegidas y no contienen patrones repetidos. Algunas de las contraseñas aparecieron varias veces; sospechamos que algunos administradores de red reutilizan la misma contraseña en distintos servidores. Por ejemplo, observamos inicios de sesión exitosos desde un mismo sistema a 10 direcciones IP diferentes, todas ubicadas secuencialmente en la misma subred con las mismas credenciales.

Con 33% de las contraseñas que contienen al menos un carácter especial y un promedio de longitud de más de 11 caracteres, se puede considerar que las contraseñas están protegidas contra ataques de fuerza bruta.

Análisis de spam

Uno de los elementos principales a través del cual los operadores de Windigo están obteniendo dinero gracias a las infecciones es el envío de mensajes de spam por correo electrónico. El spam se envía mediante dos métodos diferentes: servidores infectados con Perl/Calfbot y estaciones de trabajo de usuarios finales infectadas con el malware Win32/Glupteba.M. Esta sección presenta únicamente el análisis del spam enviado con instancias de Perl/Calfbot.

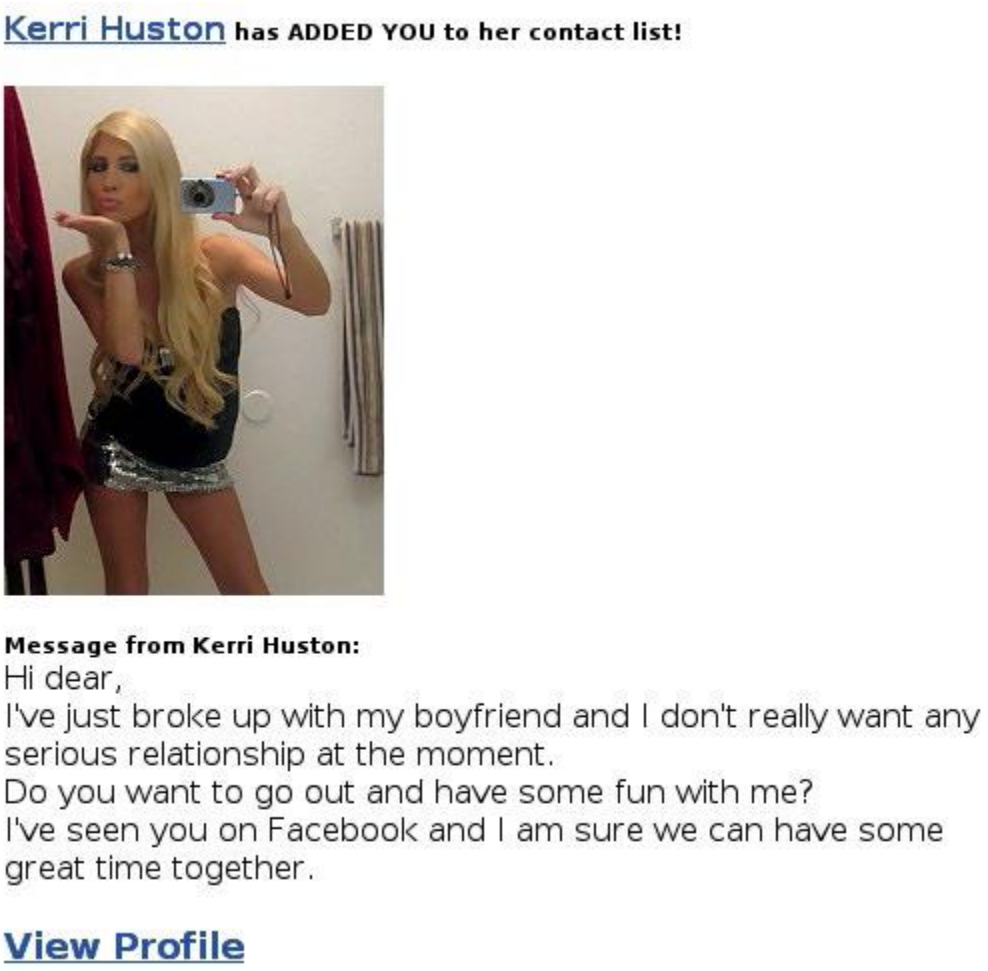


Imagen 13. Ejemplo de un spam del tipo 'MeetMe' (conóceme)

Utilizamos dos enfoques diferentes para entender el volumen y el tipo de spam enviado a través de la infraestructura Perl/Calfbot. El primero consiste en crear un bot falso para implementar el protocolo de red de comando y control apropiado. El segundo enfoque es procesar la captura del tráfico de red obtenido en enero de 2014 en el servidor de proxi reverso de comando y control de Perl/Calfbot y extrapolar los resultados.

Bot falso

El cliente falso se programó tomando como base el código descrito en la sección sobre Perl/Calfbot. Este cliente tiene la función de recuperar trabajos de spam desde el servidor de comando y control. Los trabajos de spam están conformados por una serie de plantillas de correo electrónico y una lista de direcciones de correo electrónico de los destinatarios.

Analizamos los datos desde agosto de 2013 hasta febrero de 2014. Durante dicho período, nuestro bot falso recuperó 13.422 trabajos de spam diferentes dirigidos a 20.683.814 direcciones de correo electrónico únicas. El siguiente histograma muestra los 10 dominios más afectados.

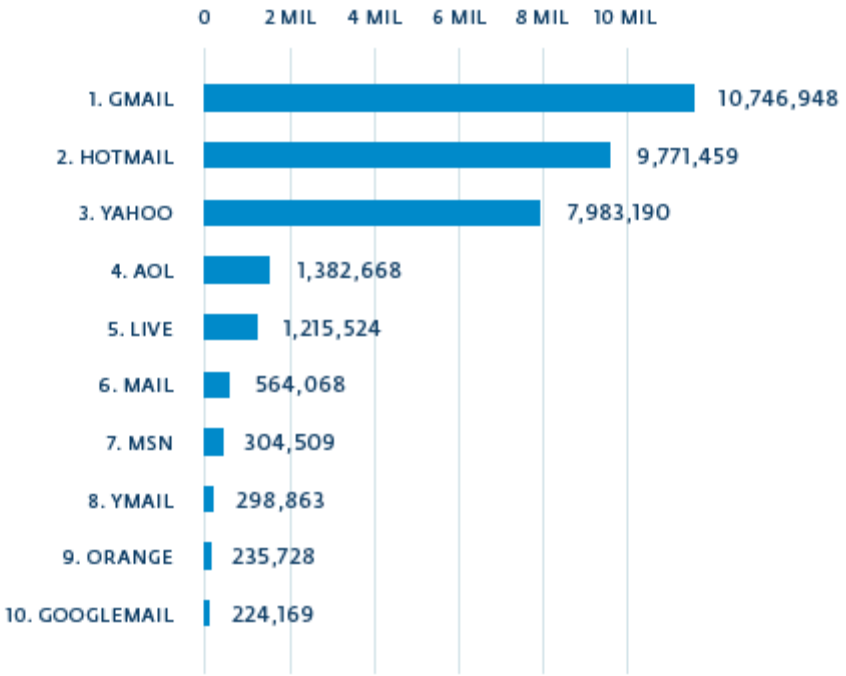


Imagen 14. Volumen de spam recibido por países (dominios de primer nivel)

El siguiente mapa muestra la distribución de los dominios de primer nivel que recibieron la mayor cantidad de mensajes de spam de la operación Windigo. Podemos observar que los países cuyos dominios de primer nivel recibieron la mayor cantidad de mensajes de spam son Francia, Reino Unido y Rusia.

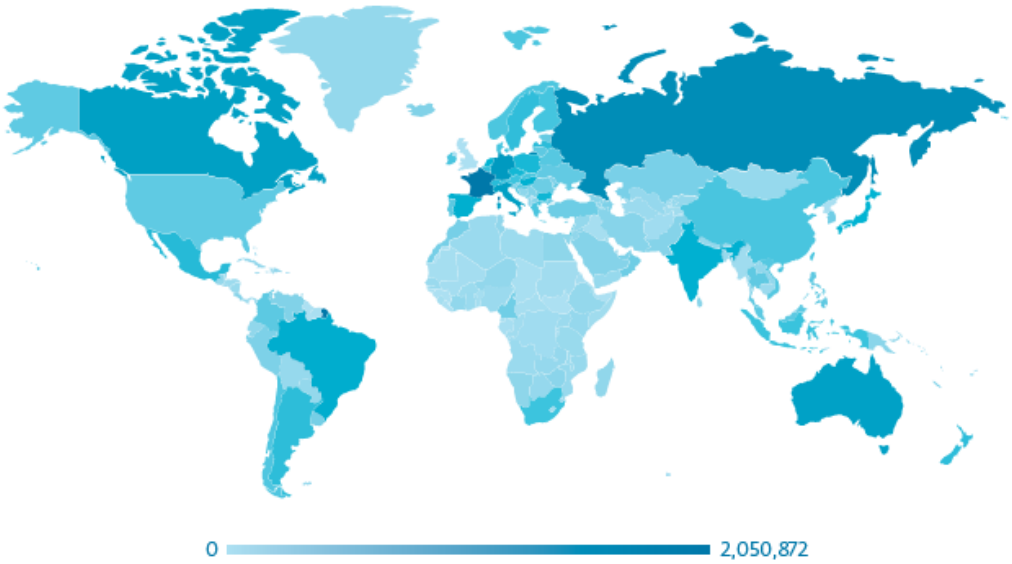


Imagen 15. Volumen de spam recibido por países (dominios de primer nivel)

Posición	País	Cantidad
1	Francia	2.050.872
2	Reino Unido	1.483.725
3	Rusia	854.580
4	Alemania	458.041
5	Italia	333.204
	Otros	2.271.782
Total		7.452.204

Imagen 16. Los 5 países más vistos en las listas de correo electrónico de dominios de primer nivel

Al analizar el contenido de los mensajes de spam, encontramos algunos temas recurrentes. La mayoría de las plantillas de spam contienen referencias a casinos, bonificaciones y citas en línea. La mayoría de los mensajes de spam también contienen palabras como "darse de baja" e "informar", probablemente en un intento de evadir la detección de spam. Al seguir dichos vínculos, se llega a un mensaje correcto de notificación o de baja. Sin embargo, seguramente etiqueten las direcciones de quienes envíen notificaciones y solicitudes de baja como direcciones válidas.

Imagen 17. Darse de baja de la lista de correo

El típico trabajo de spam llega a alrededor de 3.000 direcciones de correo electrónico y utiliza plantillas escritas en idioma inglés, aunque también encontramos francés, alemán, español y ruso. Todas las plantillas de spam contienen URL que conducen a dominios alojados en la infraestructura de TinyDNS detallada más abajo.

Imagen 18. Ejemplo de un spam del tipo 'casino'

Análisis del tráfico de comando y control

La segunda técnica empleada para evaluar el volumen de spam enviado era analizar el tráfico de red capturado en uno de los servidores de comando y control durante el mes de enero de 2014. Capturamos períodos de 24 horas con intervalos semanales durante tres semanas.

Gracias al hecho de que Perl/Calfbot registra la cantidad de mensajes de spam enviados con éxito, pudimos

observar que los servidores infectados informaron un promedio diario de 35 millones de mensajes de spam enviados correctamente; el servidor más prolífico llegó a más de un millón de mensajes de spam en un solo día.

La siguiente tabla resume algunas estadísticas que extrajimos de esos datos. Abajo se resalta la noción de una dirección IP activa, es decir, un servidor infectado que al menos una vez le informó al centro de comando y control que envió spam con éxito.

Fecha	Direcciones IP	Direcciones IP activas (% del total)	Spam enviado (promedio por cada IP activa)
7 de enero	1.442	244 (17 %)	27.713.339 (113.579)
14 de enero	483	300 (62 %)	32.793.722 (109.312)
24 de enero	877	490 (56 %)	46.402.673 (94.699)

Imagen 19. Eficiencia del spam

El porcentaje de direcciones IP activas es en cierto modo bajo, pero existen muchos factores que pueden explicarlo: el servidor podría no tener instalado un agente de envío de correo (MSA), podría tener su puerto saliente 25 bloqueado o podría figurar en la lista negra por bloqueo de spam, como la lista Spamhaus (un resultado probable dado que el servidor realmente está enviando spam).

Esta captura de tráfico de red también nos permitió acceder al número de servidores infectados con Perl/Calfbot. El siguiente mapa muestra la cantidad de direcciones IP que se observaron contactando a la primera capa del servidor proxy reverso del centro de comando y control de Perl/Calfbot. Durante nuestros períodos de observación, 2.215 direcciones IP únicas se conectaron al servidor proxy. Desde estas direcciones IP, solo 735 informaron haber tenido éxito al enviar spam. En la siguiente imagen podemos ver que la mayoría de los servidores están ubicados en los Estados Unidos de América, Alemania y Rusia.

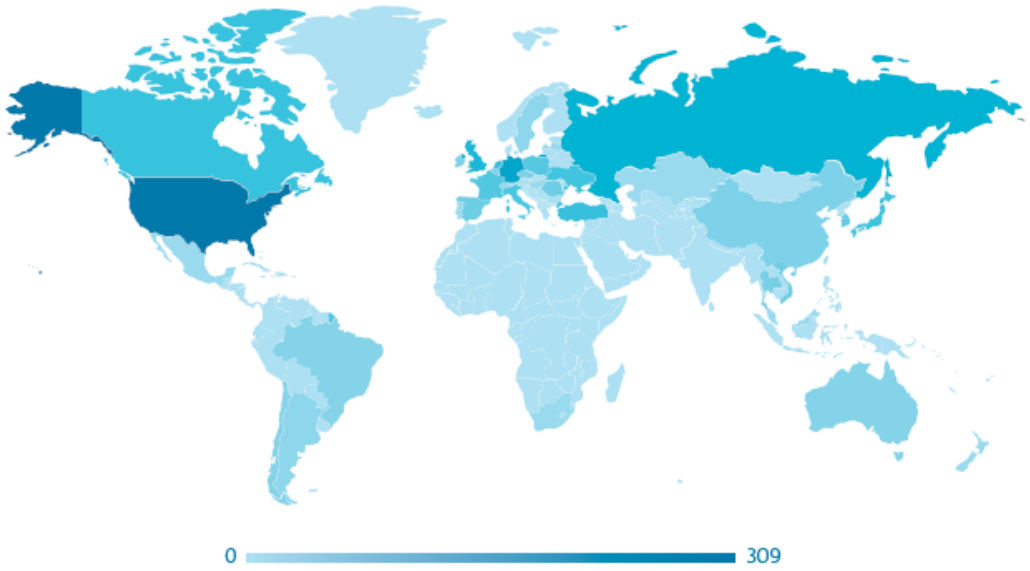


Imagen 20. Distribución del sistema operativo Perl/Calfbot

Posición	País	Cantidad
1	Estados Unidos	309
2	Alemania	72
3	Rusia	41
4	Reino Unido	32
5	Turquía	23
	Otros	258
Total		735

Tabla 7. Los 5 países principales que envían spam a través de servidores infectados con Perl/Calfbot

Cada semana, cambiaron alrededor de la mitad de las direcciones IP que informaron haber enviado spam exitosamente. Tanto cambio seguramente pueda explicarse por la existencia de las listas negras con direcciones IP de spam confeccionadas por los servicios antispam y el hecho de que los centros de comando y control hacen a un lado los bots de spam que no enviaron ningún mensaje de spam con éxito (como ya se mencionó).

La primera semana observamos 244 direcciones IP activas únicas; la segunda, 300 direcciones; y la tercera semana, 490. Entre la primera y la segunda semana, solo 123 direcciones IP eran las mismas. Entre la primera y la tercera semana, tan solo 89. Esta es una tasa de cambio de direcciones IP extremadamente elevada, lo que

significa que Perl/Calfbot podría haber estado ejecutándose en varios miles de servidores diferentes durante el último año.

Metadatos de comando y control

El tráfico de los hosts infectados por Perl/Calfbot arroja otros datos interesantes. Por ejemplo, el protocolo de comando y control se envía a través de HTTP[2], lo que nos permite observar la variada información de los encabezados HTTP además de información sobre el protocolo específica del malware.

Información del agente de usuario

Al analizar la información del agente de usuario, descubrimos que las cadenas más prevalentes son, como era de esperar, de sistemas Linux x86 y x64. También observamos cadenas de agente de usuario de OpenBSD, FreeBSD, Apple Mac y Cygwin.

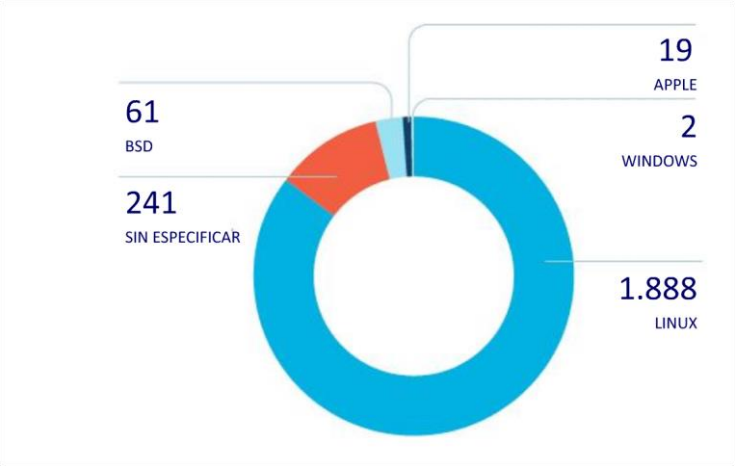


Imagen 21. Distribución del nombre de usuario de Perl/Calfbot

Vale la pena mencionar que al menos dos sistemas que le informan al servidor de comando y control estaban ejecutando la versión gnueabi de la herramienta wget. Esto significa que dichos sistemas están usando la interfaz binaria de la aplicación integrada GNU, utilizada comúnmente en arquitectura ARM.

> *Los sistemas ARM están infectados con Perl/Calfbot. Como Raspberry Pi es el sistema integrado más popular para consumidores, nos gusta pensar que algunos de ellos están enviando "deliciosos" mensajes de spam.*

[2] En realidad, está en HTTPS, pero logramos descifrarla.

La siguiente lista contiene las cadenas de agentes de usuario encontradas mientras monitoreábamos el servidor de comando y control de Perl/Calfbot.

```
curl/7.21.4 (universal-apple-darwin11.0) libcurl/7.21.4
OpenSSL/0.9.8y zlib/1.2.5
curl/7.24.0 (x86_64-apple-darwin12.0) libcurl/7.24.0 OpenSSL/0.9.8y
zlib/1.2.5
curl/7.19.7 (universal-apple-darwin10.0) libcurl/7.19.7
OpenSSL/0.9.8l zlib/1.2.3
curl/7.19.7 (universal-apple-darwin10.0) libcurl/7.19.7
OpenSSL/0.9.8r zlib/1.2.3
curl/7.19.7 (universal-apple-darwin10.0) libcurl/7.19.7
OpenSSL/0.9.8y zlib/1.2.3
Wget/1.12 (cygwin)
Wget/1.12 (freebsd7.2)
Wget/1.12 (freebsd7.4)
Wget/1.12 (freebsd8.2)
Wget/1.12 (linux-gnu)
Wget/1.12 (linux-gnueabi)
Wget/1.13.4 (cygwin)
Wget/1.13.4 (darwin10.7.0)
Wget/1.13.4 (freebsd8.1)
Wget/1.13.4 (freebsd8.2)
Wget/1.13.4 (freebsd8.3)
Wget/1.13.4 (freebsd9.0)
Wget/1.13.4 (linux-gnu)
Wget/1.13.4 (openbsd5.2)
Wget/1.14 (freebsd9.1)
Wget/1.14 (linux-gnueabi)
Wget/1.12 (linux-gnueabi)
```

Información de nombre de usuario

Perl/Calfbot le informa al comando y control el nombre de usuario bajo el cual se ejecuta el malware. Abajo mostramos los nombres de usuario utilizados con mayor frecuencia.

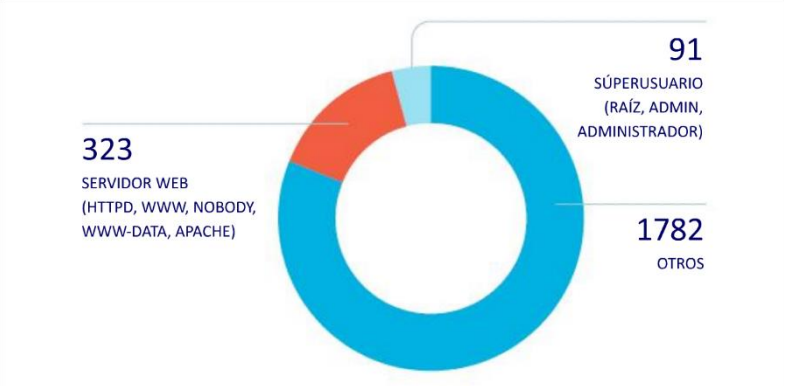


Imagen 22. Cantidades de infecciones únicas

Las cuentas de servidores Web (httpd, www, nobody, www-data y apache) son, con gran ventaja, el tipo de cuenta más frecuente que ejecuta Perl/Calfbot. No obstante, es solo una fracción de la población completa de nombres de usuario que encontramos, como se ve claramente en la extensa sección denominada "otros". Esto puede explicarse por la gran variedad de nombres de usuario que se vio comprometida con la operación de robo de credenciales. Como creíamos inicialmente, solo una pequeña fracción del malware se está ejecutando

con privilegios de raíz. Consideramos que esto fortalece la hipótesis de que Perl/Calfbot se utiliza para aprovechar las credenciales robadas con cuentas que no tienen privilegios elevados, maximizando la utilidad de cualquier credencial (de raíz o no) que posean los operadores.

Infraestructura de alojamiento de DNS

La operación Windigo emplea nombres de dominio en varios lugares, por ejemplo, en campañas de spam o como puntos de contacto de los servidores de comando y control. Descubrimos que los servidores de nombres autoritarios para estos dominios están alojados en servidores infectados con Linux/Ebury y que se ejecutan con TinyDNS.

En julio de 2013 logramos recuperar el archivo de al base de datos de un servidor TinyDNS que contenía detalles de configuración para 62.186 nombres de dominio únicos. Tan extensa cantidad de nombres de dominio (todos registrados y pagados) puede explicarse por el hecho de que se usan en correos electrónicos de spam, tanto en las direcciones del remitente como en la misma URL del spam. Por lo tanto, un bajo nivel de reutilización permite que estos nombres de dominio mantengan una reputación entre media y buena, con lo que evitan efectivamente las listas negras de spam.

Al correlacionar nuestros datos, encontramos que el spam no era la única parte de la operación Windigo basada en este servidor TinyDNS, ya que éste también alojaba:

- Los nombres de dominio generados en forma dinámica por Perl/Calfbot para llegar a sus servidores de comando y control
- Los nombres de dominio generados en forma dinámica por Linux/Ebury para extraer las credenciales (solo en la versión 1.2.1 y anteriores)
- Los nombres de dominio de las múltiples capas de redirección ubicadas para resguardar las URL de spam
- Los registros MX del Marco de directivas de remitente (SPF) y los registros A del DNS (probablemente usados para evadir la detección del spam)

De esta forma, la base de datos TinyDNS une diversas partes de Windigo, y demuestra una vez más que las personas tras la operación seguramente sean las mismas.

> *Los administradores de sistemas encontraron algunos binarios y datos de TinyDNS en /home/./root (yes, / home/<space><dot>/root).*

Usuarios finales infectados

Un fin de semana de septiembre de 2013, capturamos el tráfico de red de un proxy reverso front-end de Linux/Cdorked. A pesar de que esta captura se realizó solamente con un solo servidor proxy (de entre todos los

utilizados), su análisis nos permitió llegar a comprender con mayor profundidad la cantidad y el perfil de los usuarios que resultaban víctimas de las redirecciones maliciosas.

Durante un único fin de semana observamos más de 1,1 millón de direcciones IP diferentes que iban pasando por este servidor antes de ser redirigidas a servidores de paquetes de exploits. Como explicaremos luego, solo una fracción de estos usuarios terminó infectada.

Para tener una idea del perfil de estos usuarios, extrajimos del campo HTTP del agente de usuario (siempre que fuera posible) el nombre de su sistema operativo, lo que nos condujo a la siguiente distribución:

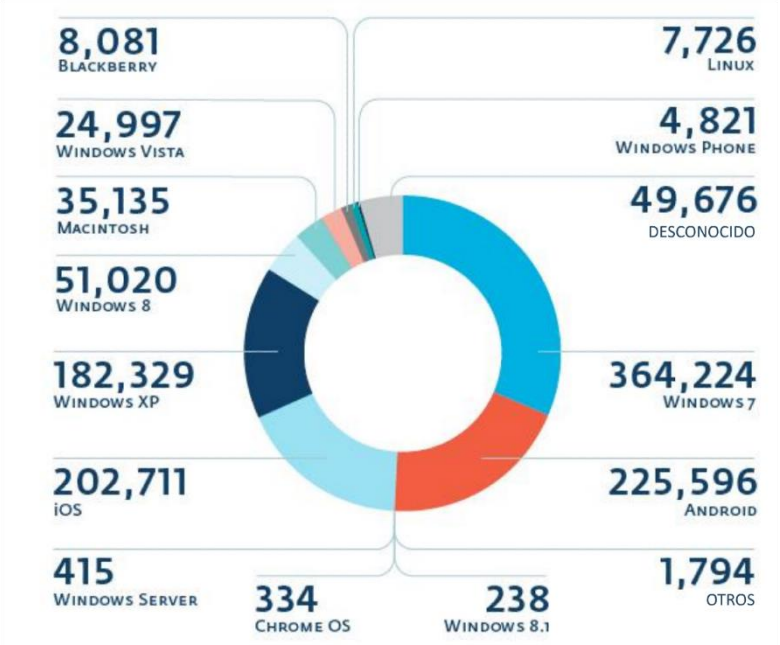


Imagen 23. Víctimas de redirección de Linux/Cdorked por sistema operativo

La categoría "otros" incluye varias versiones secundarias de los sistemas operativos principales, mientras que la categoría "desconocido" contiene las direcciones IP para las cuales no se pudo extraer el sistema operativo, sobre todo porque no estaba declarado.

> *Es increíble encontrar que 23 personas aparentemente siguen navegando en Internet con Windows 98 y una incluso todavía usa Windows 95.*

Además, extrajimos los nombres de los navegadores del mismo campo de agente de usuario:

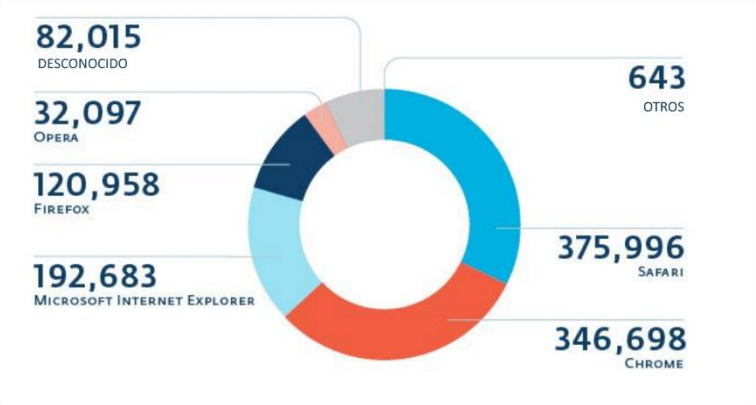


Imagen 24. Víctimas de redirección de Linux/Cdorked por navegador

La interpretación de los campos HTTP del agente de usuario debe hacerse cuidadosamente, ya que una dirección IP puede asociarse con valores diferentes del agente de usuario, por ejemplo, debido a la Traducción de direcciones de red, pero también porque el campo HTTP del agente de usuario tiene un formato libre, lo que hace que su procesamiento no sea para nada insignificante.

Cuando se redirige el equipo de un usuario a un proxy reverso front-end, se da inicio a una serie de comunicaciones con el servidor del paquete de exploits, que permanece cómodamente oculto tras la cadena de proxies reversos. Al final de este diálogo, el equipo del usuario se infectará con malware si es vulnerable a uno de los exploits incluidos en el paquete.

En el momento de nuestra captura, los operadores de Windigo usaron el infame paquete Blackhole, que les permitió atacar a usuarios de Windows. En noviembre de 2013, los operadores cambiaron al paquete de exploits Neutrino luego del arresto del supuesto autor de Blackhole. Ya está disponible un análisis técnico detallado del funcionamiento interno del paquete Blackhole en la literatura exitente, así como de Neutrino.

Como se descifró la carga maliciosa final distribuida por Blackhole, pudimos hacer un recuento de la cantidad de usuarios alcanzados con éxito por la amenaza, los que en realidad recibieron un ejecutable binario malicioso. Del total de 1,1 millón de visitantes, 11.108 fueron afectados exitosamente, lo que da un índice de infección de 1%. Aunque el índice puede parecer bajo, 10.000 es un número significativo de infecciones nuevas, en especial si se considera que este valor proviene de un único servidor front-end en solo dos días.

Observamos dos familias distintivas de malware distribuidas por el paquete de exploits. Los usuarios provenientes de Estados Unidos de América, Reino Unido, Canadá y Australia se infectaron con Win32/Boaxxe.G, mientras que los demás se infectaron con Win32/Leechole, un simple dropper que luego instalaba Win32/Glupteba.M. La distribución específica de malware se mantuvo constante desde que comenzamos a rastrear la operación Windigo. Discutiremos el caso de Win32/Boaxxe.G (un infame malware

basado en el fraude de clic) con más detalle aquí, y el de Win32/Glupteba.M (un proxy de spam) aquí.

Algunas empresas de seguridad usaron en forma reiterada los espacios de direcciones IP corporativas para visitar el servidor front-end que estábamos monitoreando. No recibieron ningún recurso, probablemente porque los operadores de Windigo ya habrían bloqueado sus direcciones IP.

CONCLUSIÓN

La operación Windigo es un esfuerzo a gran escala que actualmente involucra a más de diez mil servidores infectados en todo el mundo. El propósito de la operación parece ser el rédito económico. La ganancia se obtiene con diversos métodos, incluyendo la redirección de usuarios Web a contenido malicioso y el envío de correos electrónicos no solicitados.

En este informe detallamos los tres componentes principales de la operación Windigo: un backdoor OpenSSH, un módulo de redirección Web y un programa de envío de spam. Explicamos por qué creemos que estos tres componentes están relacionados y de qué forma se utilizaron durante los dos últimos años para redirigir a millones de usuarios de Internet y para enviar aún más mensajes de spam. La escala de esta operación solo se equipara con su sofisticación y complejidad.

Al leer el presente informe, uno podría preguntarse por qué ESET, una empresa de seguridad que se enfoca principalmente en el mercado de los equipos de escritorio, invierte tiempo y energía en comprender y documentar complejas amenazas para Linux. La primera razón es que, al reunir información sobre los servidores comprometidos y ver cómo los utilizan los agentes maliciosos, podemos proteger mejor a nuestros usuarios. Realizar el seguimiento de la redirección de sitios Web y las páginas de destino del contenido malicioso nos permitió evitar que cientos de miles de nuestros usuarios accedieran a contenido malicioso. La descarga proactiva y el análisis de las plantillas de spam también garantizaron el correcto etiquetado de los mensajes de spam antes de que llegaran a nuestros clientes.

La comprensión de las amenazas emergentes en sistemas operativos alternativos que normalmente son menos atacados por malware también nos permite encauzar mejor nuestros mecanismos de detección para dichas plataformas.

Nuestro objetivo al generar este informe es ayudar al público general, a la comunidad de investigadores y a los administradores de sistemas a entender que cambiaron las reglas del juego en lo que respecta a la gestión de los servidores en Internet. El inicio de sesión a servidores basado en contraseñas ya debería haber quedado en el pasado. Debemos considerar seriamente la autenticación en dos fases o, al menos, el uso seguro de claves SSH como se describe en el apéndice de prevención. El impacto de la operación Windigo habría sido mucho

más reducido si se hubieran empleado estas precauciones.

Finalmente, al suministrar los indicadores de sistemas comprometidos y las instrucciones sobre cómo desinfectar los servidores, esperamos que más administradores de sistemas puedan desinfectar con rapidez sus equipos y que los proveedores de servicios de hosting sean más proactivos al notificar a sus clientes, de modo que se reduzcan los recursos disponibles para la banda criminal tras la operación Windigo.

APÉNDICE 1: DESINFECCIÓN

Linux/Ebury

Para instalar Linux/Ebury en un sistema, los operadores de malware necesitan acceso de raíz. Con este nivel de acceso, todo es posible. Por esa razón aconsejamos a todos los que estén infectados borrar sus servidores por completo y reconstruirlos desde cero usando una fuente verificada. Es la única forma de asegurarse de que se quitará esta amenaza.

Lo que es más importante aún, es necesario hacerse la idea de que las credenciales de administrador y de usuario también están comprometidas. Por eso aconsejamos a todo el que se haya infectado a restablecer todas las credenciales de usuario y administrador de los equipos no infectados y poner en vigencia una medida para evitar que los usuarios puedan volver a cambiar las nuevas contraseñas por las originales[3].

Es importante notar que Linux/Ebury robó las credenciales de todos los intentos de inicio de sesión realizados en un servidor infectado (tanto de los que ingresaron con éxito como los que no). Además, también roba las credenciales de las conexiones que se originan en ese servidor mediante un binario SSH troyano, lo que significa que todo el que use el servidor como un retransmisor de SSH también será víctima del robo de credenciales de otros servidores. Asimismo, ssh y ssh-add[4] robarán frases de contraseñas para abrir las llaves SSH y guardarán en memoria las llaves SSH descifradas para que los operadores de malware puedan recuperarlas más tarde. Esta infraestructura de robo de credenciales es muy completa y detallada, por lo que recomendamos que las organizaciones infectadas se lo tomen muy en serio y reconsideren sus mecanismos de autenticación de servidores. Daremos más consejos en el apéndice de prevención.

Linux/Cdorked

ADVERTENCIA Asegúrese de no tener Linux/Ebury en el sistema. De ser así, consulte la sección de desinfección de Linux/Ebury.

Debido a la presencia de un backdoor interactivo en el nivel de permisos del servidor Web, también aconsejamos llevar a cabo la reinstalación completa del servidor comprometido desde fuentes verificadas.

Linux/Onimiki

[3] Los módulos de autenticación PAM cracklib o passwdqc son un buen lugar para comenzar

[4] Un auxiliar para el agente de autenticación OpenSSH

ADVERTENCIA Asegúrese de no tener Linux/Ebury en el sistema. De ser así, consulte la sección de desinfección de Linux/Ebury.

Aconsejamos llevar a cabo la reinstalación completa del servidor comprometido desde fuentes verificadas. En caso de que no esté dispuesto a hacerlo, hay ciertos pasos discutibles que serán mejor que no hacer nada:

- Asegúrese de que el usuario relacionado con la instalación de named no tenga acceso a shell (/etc/passwd)
- Reinstale el binario named principal (normalmente en /usr/sbin/named) y hágalo preferentemente a través de su administrador de paquetes
- Reinicie named

Perl/Calfbot

ADVERTENCIA Asegúrese de no tener Linux/Ebury en el sistema. De ser así, consulte la sección de desinfección de Linux/Ebury.

Aconsejamos llevar a cabo la reinstalación completa del servidor comprometido desde fuentes verificadas. En caso de que no esté dispuesto a hacerlo, hay ciertos pasos discutibles que serán mejor que no hacer nada:

- Lea la sección sobre Indicadores de sistemas comprometidos conPerl/Calfbot para comprender cómo encontrar el id de usuario y el id de proceso de Perl/Calfbot
- Cambie todas las credenciales de usuario comprometidas (bajo la cual se está ejecutando Perl/Calfbot)
- Cierre el proceso Perl asociado con Perl/Calfbot

APÉNDICE 2: PREVENCIÓN

Aquí encontrará unas recomendaciones sencillas para protegerse ante este grupo de amenazas:

- Deshabilite el inicio de sesión de raíz directo en el daemon de OpenSSH (PermitRootLogin no in /etc/ssh/sshd_config)
- Deshabilite los inicios de sesión basados en contraseñas y utilice una llave SSH
- Use el Agente de reenvío de SSH de servidores a servidores en lugar de copiar sus claves privadas de SSH en los servidores. En GNU/Linux use el agente SSH o GnomeKeyring con ForwardAgent yes bajo una entrada de Host confiable en su archivo .ssh/config5. En Windows, el Agente de clave PuTTY es compatible con el Agente de reenvío de SSH

Use la doble autenticación en sus servidores. Hay soluciones gratuitas disponibles, como la integración de Google Authenticator.

[5] Este tutorial continúa con más detalle en: https://help.github.com/articles/using-ssh-agent-forwarding