Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Boletin de Seguridad UNAM-CERT-2014-007 Backoff - Software malicioso para sistemas Punto de Venta

Este boletín fue preparado en colaboración con el Centro de Integración de Comunicaciones y Ciberseguridad Nacional (NCCIC), el Servicio Secreto de los Estados Unidos (USSS), el Centro de Análisis e Intercambio de Información del Sector Financiero (FS-ISAC) y Trustwave Spiderlabs, un socio de confianza bajo contrato con el Servicio Secreto de los Estados Unidos. El propósito de este comunicado es proporcionar indicadores técnicos relevantes y aplicables para proteger la red.

Investigaciones recientes revelaron que atacantes maliciosos utilizan herramientas disponibles públicamente para localizar negocios que utilizan aplicaciones de Escritorio Remoto. Soluciones de Escritorio Remoto como Remote Desktop de Microsoft [1], Apple Remote Desktop [2], Chrome Remote Desktop [3], Splashtop 2 [4], Pulseway [5] y Join.Me de LogMeIn [6], ofrecen comodidad y eficiencia para conectarse a computadoras desde una ubicación remota. Una vez que estas aplicaciones son localizadas, los atacantes intentan iniciar sesión mediante fuerza bruta. Después de ganar acceso, a lo que frecuentemente son cuentas de administrador o usuarios con privilegios, los atacantes distribuyen software malicioso al Punto de Venta (PoS) y posteriormente extraen datos de pago de los consumidores a través de peticiones POST cifradas.

El Servicio Secreto de los Estados Unidos junto con NCCIC/US-CERT y Trustwave SpiderLabs trabajan para caracterizar el software malicioso identificado recientemente, denominado "Backoff", asociado con varias investigaciones de extracción de datos en Puntos de Venta. Para el momento del descubrimiento y análisis, las variantes del software malicioso tenían tasa de detección de baja a 0%, lo que significa que los motores antivirus actualizados con todos los parches no pudieron identificar la pieza como maliciosa.

Ataques similares se han observado en campañas previas de software malicioso orientado a Puntos de Venta [7] y algunos estudios indican que los ataques de fuerza bruta dirigidos al protocolo de Escritorio Remoto van en aumento [8]. En el artículo se incluye una sección de mitigación y estrategias de prevención que ofrecen opciones que los administradores de red podrían considerar.

- **Fecha de Liberación:** 31-Jul-2014
- **Ultima Revisión:** 3-Nov-2014
- **Fuente:** us-cert.gov
- **Problema de Vulnerabilidad** Local y remoto

1. Descripción

"Backoff" es una familia de software malicioso para Puntos de Venta que fue descubierta recientemente. La familia de software malicioso ha sido objeto de por lo menos tres investigaciones forenses independientes. Los investigadores identificaron tres variantes principales para el software malicioso "Backoff", incluyendo: 1.4, 1.55 ("backoff", "goo", "MAY", "net") y 1.56 ("LAST").

Estas variantes se observaron en octubre de 2013 y continúan operando. En general, el software malicioso consiste de las siguientes 4 capacidades:

- Búsqueda de datos sensibles en la memoria.
- Registro de las pulsaciones del teclado.
- Comunicación Command & Control.

- Inyección de código malicioso en el proceso explorer.exe.

Algunas excepciones son la variante más antigua (1.4) que no incluye la funcionalidad de keylogger y la variante 1.55 'net' que elimina el componente de inyección en el proceso explorer.exe.

El código malicioso que se inyecta en el proceso explorer.exe es responsable de la persistencia en caso de que el ejecutable malicioso sea interrumpido o forzado a terminar su ejecución. El software malicioso es responsable de explorar la memoria de los procesos que se están ejecutando en la máquina de la víctima y buscar datos sensibles. La funcionalidad de registrar las pulsaciones del teclado también está presente en las variantes más recientes de "Backoff". Adicionalmente, el software malicioso tiene un componente C&C que es responsable de alojar los datos descubiertos, actualizar o eliminar el software malicioso, además de descargar y ejecutar otras muestras maliciosas.

Variantes

Con base en las marcas de tiempo recopiladas y en la información del control de versiones en las peticiones HTTP al C&C por método POST, las variantes de "Backoff" fueron analizadas durante un periodo de 7 meses. Las 5 variantes de la familia de software malicioso "Backoff" tienen modificaciones notables. Los cambios se muestran a continuación:

1.55 "backoff"

- Agregó en almacenamiento temporal el archivo Local.dat para los datos descubiertos.
- Agregó funcionalidad de registro de pulsaciones del teclado.
- Agregó el parámetro "gr" en las peticiones por método POST para incluir el nombre de la variante.
- Agregó la habilidad de filtrar datos registrados por pulsaciones del teclado.
- Tiene soporte para múltiples dominios de filtración.
- Cambió la ruta de instalación.
- Cambió el User-Agent.

1.55 "goo"

- Intenta eliminar la versión anterior del software malicioso.
- Usa el DNS público de Google (IP 8.8.8.8) para resolver dominios.

1.55 "MAY"

- No hay actualizaciones significativas a excepción de los cambios en el nombre del Identificador de Recursos Uniforme (URI) y el nombre de la versión.

1.55 "net"

- Se eliminó el componente de inyección en el proceso explorer.exe.

1.56 "LAST"

- Agregó nuevamente el componente de inyección en el proceso explorer.exe.
- Soporta múltiples configuraciones de dominio, Identificador de Recursos Uniforme y puertos.
- Modificó el código responsable de la creación de hilos de filtración.
- Agregó técnicas de persistencia.

Comunicación Command & Control

La comunicación entre el C&C y "Backoff" se lleva a cabo a través de peticiones HTTP por método POST. Una serie de parámetros POST son incluidos cuando este software malicioso hace peticiones al servidor C&C:

- op: Valor estático de '1'.
- id: Genera una cadena con caracteres aleatorios.
- ui: Nombre y usuario de la máquina víctima.
- wv: Versión de Microsoft Windows.
- gr: Identificador del software malicioso (no está presente en la versión 1.4).
- bv: Versión del software malicioso.
- data: Es opcional, cifra los datos con RC4 y los codifica en Base 64.

El parámetro "id" está almacenado en la siguiente ubicación, para garantizar que sea consistente a través de las peticiones:

- HKCUSOFTWAREMicrosoftWindowsCurrentVersionidentifier

Si esta llave de registro no existe, la cadena se genera y se almacena. Los datos se cifran usando RC4 antes de ser codificados en Base 64. La contraseña para RC4 se genera a partir del parámetro 'id', además de la cadena estática ' jhgtsd7fjmytkr' y el parámetro 'ui'. Estos valores se concatenan y se obtiene su hash utilizando el algoritmo MD5 que forma la contraseña RC4. Para este ejemplo, la contraseña RC4 sería '56E15A1B3CB7116CAB0268AC8A2CD943' (firma MD5 de la cadena "vxeyHkSjhgtsd7fjmytkrJosh @ PC123456").

Indicadores de archivo

La siguiente lista son Indicadores de Compromiso (IOCs) que deben contemplarse en la seguridad de su red e identificar si están presentes y tomar acciones correctivas:

1.4

MD5 de la muestra empaquetada: 927AE15DBF549BD60EDCDEAFB49B829E
MD5 de la muestra desempaquetada: 6A0E49C5E332DF3AF78823CA4A655AE8
Ruta de instalación: %APPDATA%AdobeFlashPlayermswinsvc.exe
Objetos de exclusión mutua:
uhYtntr56uisGst
uyhnJmkuTgD
Archivos escritos:
%APPDATA%mskrnl
%APPDATA%winserv.exe
%APPDATA%AdobeFlashPlayermswinsvc.exe
Cadena estática (petición por método POST): zXqW9JdWLM4urgjRkX
Llaves de registro:
HKCUSOFTWAREMicrosoftWindowsCurrentVersionidentifier
HKCUSOFTWAREMicrosoftWindowsCurrentVersionRunWindows NT Service
User-Agent: Mozilla/4.0
URI(s): /aircanada/dark.php

1.55 "backoff"

MD5 de la muestra empaquetada: F5B4786C28CCF43E569CB21A6122A97E
MD5 de la muestra desempaquetada: CA4D58C61D463F35576C58F25916F258
Ruta de instalación: %APPDATA%AdobeFlashPlayermswinhost.exe
Objetos de exclusión mutua:
Undsa8301nskal
uyhnJmkuTgD
Archivos escritos:
%APPDATA%mskrnl
%APPDATA%winserv.exe
%APPDATA%AdobeFlashPlayermswinhost.exe
%APPDATA%AdobeFlashPlayerLocal.dat
%APPDATA%AdobeFlashPlayerLog.txt
Cadena estática (petición por método POST): ihasd3jasdhkas
Llaves de registro:
HKCUSOFTWAREMicrosoftWindowsCurrentVersionidentifier
HKCUSOFTWAREMicrosoftWindowsCurrentVersionRunWindows NT Service
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
URI(s): /aero2/fly.php

1.55 "goo"

MD5 de la muestra empaquetada: 17E1173F6FC7E920405F8DBDE8C9ECAC
MD5 de la muestra desempaquetada: D397D2CC9DE41FB5B5D897D1E665C549
Ruta de instalación: %APPDATA%OracleJavajavaw.exe
Objetos de exclusión mutua:
nUndsa8301nskal
nuyhnJmkuTgD
Archivos escritos:
%APPDATA% sskrnl
%APPDATA%winserv.exe
%APPDATA%OracleJavajavaw.exe
%APPDATA%OracleJavaLocal.dat
%APPDATA%OracleJavaLog.txt
Cadena estática (petición por método POST): jhgtsd7fjmytkr
Llaves de registro:
HKCUSOFTWAREMicrosoftWindowsCurrentVersionidentifier
HKCUSOFTWAREMicrosoftWindowsCurrentVersionRunWindows NT Service
User-Agent:
URI(s): /windows/updcheck.php

1.55 "MAY"

MD5 de la muestra empaquetada: 21E61EB9F5C1E1226F9D69CBFD1BF61B
MD5 de la muestra desempaquetada: CA608E7996DED0E5009DB6CC54E08749
Ruta de instalación: %APPDATA%OracleJavajavaw.exe
Objetos de exclusión mutua:
nUndsa8301nskal
nuyhnJmkuTgD
Archivos escritos:
%APPDATA% sskrnl
%APPDATA%winserv.exe

%APPDATA%OracleJavajavaw.exe
%APPDATA%OracleJavaLocal.dat
%APPDATA%OracleJavaLog.txt
Cadena estática (petición por método POST): jhgtsd7fjmytkr
Llaves de registro:
HKCUSOFTWAREMicrosoftWindowsCurrentVersionidentifier
HKCUSOFTWAREMicrosoftWindowsCurrentVersionRunWindows NT Service
User-Agent:
URI(s): /windowsxp/updcheck.php

1.55 "net"

MD5 de la muestra empaquetada: 0607CE9793EEA0A42819957528D92B02
MD5 de la muestra desempaquetada: 5C1474EA275A05A2668B823D055858D9
Ruta de instalación: %APPDATA%AdobeFlashPlayermswinhost.exe
Objetos de exclusión mutua:
nUndsa8301nskal
Archivos escritos:
%APPDATA%AdobeFlashPlayermswinhost.exe
%APPDATA%AdobeFlashPlayerLocal.dat
%APPDATA%AdobeFlashPlayerLog.txt
Cadena estática (petición por método POST): ihasd3jasdhkas9
Llaves de registro:
HKCUSOFTWAREMicrosoftWindowsCurrentVersionidentifier
HKCUSOFTWAREMicrosoftWindowsCurrentVersionRunWindows NT Service
User-Agent:
URI(s): /windowsxp/updcheck.php

1.56 "LAST"

MD5 de la muestra empaquetada: 12C9C0BC18FDF98189457A9D112EEBFC
MD5 de la muestra desempaquetada: 205947B57D41145B857DE18E43EFB794
Ruta de instalación: %APPDATA%OracleJavajavaw.exe
Objetos de exclusión mutua:
nUndsa8301nskal
nuyhnJmkuTgD
Archivos escritos:
%APPDATA% sskrnl
%APPDATA%winserv.exe
%APPDATA%OracleJavajavaw.exe
%APPDATA%OracleJavaLocal.dat
%APPDATA%OracleJavaLog.txt
Cadena estática (petición por método POST): jhgtsd7fjmytkr
Llaves de registro:
HKCUSOFTWAREMicrosoftWindowsCurrentVersionidentifier
HKCUSOFTWAREMicrosoftWindowsCurrentVersionRunWindows NT Service
HKLMSOFTWAREMicrosoftWindowsCurrentVersionRunWindows NT Service
HKCUSOFTWAREMicrosoftActive SetupInstalled
Components{B3DB0D62-B481-4929-888B-49F426C1A136}StubPath
HKLMSOFTWAREMicrosoftActive SetupInstalled
Components{B3DB0D62-B481-4929-888B-49F426C1A136}StubPath

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
URI(s): /windebug/updcheck.php

2. Impacto

El impacto de un sistema de Punto de Venta comprometido, afecta tanto al negocio como a los consumidores al exponer los datos de los clientes, como: nombre, dirección postal, número de tarjeta de crédito o débito, número telefónico y dirección de correo electrónico a los criminales. Estos incidentes pueden afectar la reputación del negocio, mientras que la información de los consumidores puede utilizarse para realizar compras fraudulentas. Es fundamental proteger las redes corporativas y servicios web, prevenir cualquier exposición innecesaria del negocio y mitigar cualquier daño que estuviera ocurriendo en este momento.

3. Solución

Para el momento en que este documento informativo se libera, las variantes de la familia de software malicioso "Backoff" no son detectadas por la mayoría de los proveedores antivirus. Sin embargo, poco después de la publicación de este análisis técnico las compañías antivirus comenzarán a detectar las variantes existentes. Es importante mantener los motores antivirus y sus firmas actualizadas para detectar nuevas amenazas como las que se presentan en este análisis y que continuamente se agregan a la bases de datos de las soluciones antivirus. Aunado a la detección de variantes de software malicioso por antivirus, los administradores de red pueden aplicar Indicadores de Compromiso (IOC) para una gran variedad de estrategias de prevención y detección [9] [10] [11]. Los Indicadores de Compromiso se encuentran más arriba en este documento.

Las investigaciones forenses de las redes comprometidas indican que se permitió la introducción del software malicioso a las terminales de pago. Los profesionales de seguridad de la información recomiendan un enfoque profundo de defensa para mitigar el riesgo que pudiera presentarse en los sistemas de pago. Si bien, algunas de las recomendaciones de mitigación de riesgos son de carácter general, las siguientes estrategias proporcionan una manera de minimizar la posibilidad de un ataque y disminuir el riesgo de comprometer datos sensibles:

Acceso por Escritorio Remoto:

- Configurar las opciones de bloqueo de cuentas para un determinado periodo de tiempo o número de intentos fallidos de acceso. Esto evita intentos de sesión no autorizados o ataques automatizados de fuerza bruta [12].
- Limitar el número de usuarios y estaciones de trabajo que puedan iniciar sesión utilizando Escritorio Remoto.
- Usar firewalls (tanto de software como de hardware de ser posible) para restringir el acceso a los puertos escucha de las aplicaciones de Escritorio Remoto (3389 TCP predeterminado) [13].
- Cambiar el puerto a la escucha predeterminado de las aplicaciones de Escritorio Remoto.
- Definir parámetros complejos para la contraseña. Al configurar el tiempo de expiración, longitud y complejidad de la cadena, se disminuye la cantidad de tiempo en el cual puede ocurrir un ataque exitoso [14].
- Implementar autenticación de dos factores (2FA) para el acceso a Escritorio Remoto [15].

- Instalar un Gateway de Escritorio Remoto para restringir el acceso a determinados usuarios [16].
- Agregar una capa extra de autenticación y cifrado en las conexiones de Escritorio Remoto por túneles a través de IPSec, SSH o SSL [17] [18].
- Requerir de la autenticación de dos factores al acceder a redes de procesamiento de pagos, incluso si se utiliza una Red Privada Virtual (VPN). Es importante implementar la autenticación de dos factores para ayudar a mitigar el registro de pulsaciones del teclado (keylogger) o ataques para robo de credenciales.
- Limitar privilegios administrativos para usuarios y aplicaciones.
- Revisar periódicamente los sistemas (locales y controladores de dominio) para identificar usuarios desconocidos o inactivos.

Seguridad de red:

- Revisar las configuraciones del firewall y asegurarse que solo los puertos, servicios y direcciones IP permitidas puedan comunicarse con la red interna. Esto es especialmente crítico para el tráfico saliente, ya que las reglas del firewall de una entidad comprometida pueden permitir puertos para comunicarse a cualquier dirección IP en Internet. Los atacantes aprovechan esta configuración para mandar datos a sus direcciones IP.
- Segmentar las redes de procesamiento de pagos de otras redes.
- Aplicar Listas de Control de Acceso (ACLs) en la configuración de los routers para limitar el tráfico no autorizado a las redes de procesamiento de pagos.
- Crear Listas de Control de Acceso estrictas para segmentar los sistemas públicos y los servicios de bases de datos para tarjetas de pago en casa.
- Implementar herramientas de prevención y detección de fuga de datos para identificar posibles robos de información.
- Implementar herramientas para detección de tráfico de red anómalo generado por los usuarios legítimos y que sus credenciales pudieran ser comprometidas.

Seguridad en Puntos de Venta y Cajas Registradoras:

- Implementar cifrado en conexiones punto a punto basado en hardware. Se recomienda habilitar en los dispositivos de entrada el estándar EMV (Europay MasterCard VISA) u otras capacidades que tengan los dispositivos como Lectura e Intercambio de Datos Segura (SRED).
- Instalar aplicaciones de pago compatibles con el Estándar de Seguridad de Datos para Aplicaciones de Pago (PA-DSS).
- Instalar la última versión del sistema operativo y asegurarse que esté actualizado con los últimos parches de seguridad, contar con software antivirus, monitorizar la integridad de los archivos e implementar un sistema de detección de intrusos basado en host.
- Asignar una contraseña fuerte a las soluciones de seguridad para evitar modificaciones en las aplicaciones. Utilizar la autenticación de dos factores siempre que sea posible.
- Efectuar una comparación binaria o comprobación de sumas (checksum) para asegurar que los archivos no autorizados no están instalados.
- Asegurarse de que cualquier actualización automática de terceros sea validada. Esto significa llevar a cabo una comparación en la comprobación de sumas de las actualizaciones antes de implementarlas en los sistemas de Puntos de Venta. Se recomienda que los comerciantes trabajen con sus proveedores de Puntos de Venta para obtener las firmas y los valores hash para realizar dicha comprobación de sumas.
- Deshabilitar los servicios y puertos innecesarios, las sesiones nulas y los usuarios invitados o predeterminados.
- Habilitar el registro de eventos y asegurarse de que hay un proceso supervisando los registros diariamente.

- Implementar privilegios mínimos y Listas de Control de Acceso en usuarios y aplicaciones del sistema.

4. **Referencias**

[1] Windows Remote Desktop
[2] Apple Remote Desktop
[3] Chrome Remote Desktop
[4] Splashtop
[5] Windows Pulseway
[6] Windows Join.me
[7] Attacker_s brute-force POS systems utilizing RDP in global botnet operation
[8] Brute force RDP attacks depend on your mistakes
[9] Understanding Indicators of Compromise (IOC)
[10] Using Indicators of Compromise in Malware Forensics
[11] Indicators of Compromise: The Key to Early Detection
[12] Configuring Account Lockout
[13] Securing Remote Desktop for System Administrators
[14] Account Lockout and Password Concepts
[15] NIST Guide to Enterprise Telework and Remote Access Security
[16] Installing RD Gateway
[17] Networking and Access Technologies
[18] Secure RDS Connections with SSL

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Jonathan Banfi Vázquez (jbanfi at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47