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

Boletin de Seguridad UNAM-CERT-2014-012 Campaña de phishing vinculada con el malware bancario "Dyre"

Desde mediados de octubre de 2014, una campaña de phishing se ha dirigido a una gran variedad de usuarios, empleando como archivo adjunto en los correos electrónicos el software malicioso bancario conocido como Dyre o también llamado Dyreza. Los elementos de esta campaña de phishing varían de un objetivo a otro, incluyendo remitentes, temas que se abordan, archivos adjuntos, exploits y payloads [1][2]. Si bien esta campaña utiliza diferentes tácticas, la intención del atacante es persuadir a los destinarios para abrir los archivos adjuntos y descargar software malicioso.

- **Fecha de Liberación:** 30-Oct-2014
- **Ultima Revisión:** 3-Nov-2014
- **Fuente:** us-cert.gov
- **Riesgo** Crítico
- **Problema de Vulnerabilidad** Local

1. Descripción

El software malicioso bancario Dyre tiene como objetivo específico conseguir las credenciales de las cuentas de usuario. La amenaza tiene la habilidad de capturar la información de inicio de sesión del usuario y enviar los datos a los atacantes [3]. Los correos electrónicos phishing utilizados en esta campaña a menudo contienen un archivo PDF malicioso adjunto que intenta explotar las vulnerabilidades encontradas en versiones no actualizadas de Adobe Reader [4][5]. Una vez explotada la vulnerabilidad, se descarga en el sistema del usuario el software malicioso bancario Dyre. Los principales proveedores de software antivirus han detectado satisfactoriamente este software malicioso antes de la publicación de esta alerta [6].

La siguiente lista de indicadores representa algunas de las características para esta campaña.

Características del correo electrónico Phishing:

- Asunto: "Unpaid invoic" (Los errores de ortografía en la línea de asunto son una característica de esta campaña)
- Adjunto: Invoice621785.pdf

Indicadores a nivel de sistema (en una explotación exitosa de la vulnerabilidad):

- Se copia a sí mismo en la ruta C:Windows[NombreAleatorio].exe
- Crea un servicio llamado "Google Update Service" mediante el establecimiento de las siguientes llaves en el registro de Windows:

HKLM\SYSTEM\CurrentControlSet\Services\googleupdate\ImagePath: "C:\WINDOWS\pfdOSwYjERDHrdV.exe"
HKLM\SYSTEM\CurrentControlSet\Services\googleupdate\DisplayName: "Google Update Service" [7]

2. Impacto

Un sistema infectado con el software malicioso bancario Dyre intentará recolectar credenciales de los servicios en línea, incluidos los servicios bancarios.

3. Solución

A los usuarios y administradores se les recomienda tomar las siguientes medidas preventivas para proteger sus redes de computadoras de campañas de phishing:

- No seguir enlaces web que no hayan sido solicitados por correo electrónico. Para obtener más información, consultar el Consejo de Seguridad para Evitar Ataques de Ingeniería Social y Phishing [8].
- Tener precaución de qué archivos adjuntos abrir desde el correo electrónico. Para obtener información sobre el manejo seguro de los archivos adjuntos en el correo electrónico, consultar Reconocer y Evitar Correos Electrónicos Fraudulentos [9].
- Seguir buenas prácticas de seguridad al navegar en Internet. Para más detalles, consultar Buenos Hábitos de Seguridad [10] y Resguardo de tu Información [11].
- Mantener actualizado el software antivirus.
- Actualizar el sistema operativo y las aplicaciones con los últimos parches de seguridad.

US-CERT recibe correos electrónicos referentes a phishing y sitios web que alojan páginas falsas para atender los incidentes y así evitar que más usuarios se conviertan en víctimas de estafas por phishing.

Los reportes de phishing son al correo electrónico: phishing-report@us-cert.gov.

4. Referencias

[1] MITRE Summary of CVE-2013-2729. Recuperado el 16 de octubre de 2014
[2] MITRE Summary of CVE-2010-0188. Recuperado el 16 de octubre de 2014
[3] New Banking Malware Dyreza. Recuperado el 16 de octubre de 2014
[4] Adobe Security Updates Addressing CVE-2013-2729. Recuperado el 16 de octubre de 2014
[5] Adobe Security Updates Addressing CVE-2010-0188. Recuperado el 16 de octubre de 2014
[6] Reporte del análisis en VirusTotal. Recuperado el 16 de octubre de 2014
[7] MS-ISAC CIS CYBER ALERT
[8] US-CERT Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks
[9] US-CERT Recognizing and Avoiding Email Scams
[10] US-CERT Security Tip (ST04-003) Good Security Habits
[11] US-CERT Security Tip (ST06-008) Safeguarding Your Data

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