DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png
Ministerio de Comunicaciones
Published on *Ministerio de Comunicaciones* (https://www.mincom.gob.cu)

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/ciberdelito190518.jpg

Investigan a gigantes tecnológicos por las patentes de pantalla táctil

Fuente:
Computer Word

Los ciberdelincuentes están aumentando sus operaciones para difundir 'malware' aprovechándose del teletrabajo y la preocupación global.

Si bien las empresas pueden tomar muchas medidas para garantizar que los empleados estén bien equipados para trabajar de forma remota de manera segura, los ciberdelincuentes están mandando amenazas de todo tipo relacionadas con el coronavirus. Están aumentando sus operaciones para difundir malware de seis maneras diferentes:

Correos electrónicos de ‘phishing’

El email es y seguirá siendo el mayor vector de amenazas para personas y organizaciones. Según un informe de Digital Shadows, en la dark web se está vendiendo malware de phishing que utiliza un archivo adjunto de correo malicioso disfrazado como un mapa de distribución del brote del virus entre 200 y 700 dólares.

Los temas de estos correos van desde informes de analistas específicos de ciertas industrias y detalles de consejos de salud oficiales de gobiernos, hasta vendedores que ofrecen mascarillas u otra información sobre operaciones y logística durante estos tiempos. Las cargas de estos correos van desde ransomware y keyloggers hasta troyanos de acceso remoto y ladrones de información.

El NCSC y la Organización Mundial de la Salud (OMS), entre otros, han hecho advertencias públicas sobre correos electrónicos fraudulentos que supuestamente provienen de estos organismos oficiales.
Aplicaciones maliciosas

Aunque Apple ha puesto límites a las aplicaciones relacionadas con el coronavirus en su marketplace, y Google ha eliminado algunas de ellas, las aplicaciones maliciosas aún pueden representar una amenaza para los usuarios. Domain Tools descubrió un sitio que instaba a los usuarios a descargar una aplicación de Android que proporciona información estadística y de seguimiento sobre el coronavirus, incluidas imágenes de mapas de calor. Sin embargo, ésta estaba cargada con un ransomware conocido como COVIDlock. La nota de rescate exige 100 dólares en bitcoin en 48 horas y amenaza con borrar sus contactos, fotos y vídeos, así como la memoria del teléfono. No obstante, ya se ha descubierto un token de desbloqueo.

Dominios maliciosos

Está habiendo un auge de creación de nuevas páginas web para difundir información relacionada con la pandemia. Sin embargo, muchos de ellos también forman parte de trampas para víctimas desprevenidas. Desde CheckPoint sugieren que los dominios relacionados con COVID-19 tienen un 50% más de probabilidades de ser maliciosos que otros dominios registrados en estas últimas semanas.

‘Endpoints’ inseguros

Con millones de empleados en todo el mundo trabajando de forma remota, aumentan los riesgos en torno a los endpoints y sus usuarios. Los dispositivos que la gente usa en el hogar podrían volverse más vulnerables si los trabajadores no actualizan sus sistemas regularmente.

Trabajar desde casa durante largos períodos también puede alentar a los usuarios a descargar aplicaciones ocultas o a incumplir las políticas que sí seguirían en la oficina.

Vulnerabilidades en proveedores y terceros

Es probable que cada partner, cliente y proveedor de servicios tengan los mismos problemas actuales que toda empresa. Es importante comunicarse con las partes críticas de cada ecosistema empresarial para asegurar que están tomando las medidas de protección adecuadas.

Ataques dirigidos a organizaciones de salud
En los últimos días, la página web de Salud Pública de Illinois (Estados Unidos) fue golpeada con un ransomware, mientras que el Departamento de Salud y Servicios Humanos (HHS) sufrió un intento de ataque de denegación de servicio. Es probable que las organizaciones de este calado de todo el mundo sean propensas a este tipo de intentos.

Disponible en:
https://cso.computerworld.es/cibercrimen/seis-tecnicas-que-usan-los-atac... [1]

Links
[1] https://cso.computerworld.es/cibercrimen/seis-tecnicas-que-usan-los-atacantes-para-aprovecharse-de-la-crisis-del-coronavirus