[Actualización 2] Campañas de Phishing se aprovechan del miedo por brote de Coronavirus en el Mundo

El Teletrabajo presenta su propio y único conjunto de desafíos de seguridad, que incluyen una serie de cambios en el entorno y una mayor dependencia del mundo digital por lo que todo debe ser considerado. ¿Qué dispositivos usarán los empleados y dónde los estarán usando? ¿Podrán otros tener fácil acceso a la información que es confidencial, ya sea en proximidad física o a través de una conexión WiFi compartida? ¿Cómo vamos a compartir información entre nosotros y si ese canal está siendo asegurado proactivamente? Realizar estas preguntas requiere que una organización planifique e implemente medidas de seguridad específicas para tener un camino claro si se presentan problemas.

Descripción

Dentro de los vectores de ataque que DigiSOC procesa y analiza en tiempo real, se ha observado un incremento sustancial en dos específicos, Fuerza Bruta en conexiones VPN SSL y campañas de Phishing. Dado el anterior comportamiento sugerimos fuertemente aplicar las recomendaciones emitidas en los pasados boletines y tener en cuenta estas recomendaciones adicionales enfocadas a la mitigación de los vectores de ataque anteriormente mencionados.

Publicación:
01/04/2020
Importancia:
Alta
Riesgo de explotación:
Media

Crear conciencia sobre información segura frente a información maliciosa

Los atacantes están lanzando campañas de malware que explotan el pánico en torno al COVID-19. Como ejemplo, una campaña se hace pasar por un mapa de infección por coronavirus https://thehackernews.com/2020/03/coronavirus-maps-covid-19.html.

Recordar a los empleados que hay muchos sitios web, incluido la web oficial de la Organización Mundial de la Salud http://www.who.int, donde puede obtener toda la información necesaria sin tener que descargar cualquier "software".

Emitir actualizaciones por correo electrónico a los empleados con informacion, políticas y protocolos alrededor de COVID-19, ayuda a prevenir la busqueda de informacion en fuentes externas y posiblemente ser victima de engaño. Asegurar que los empleados puedan saber qué correos electrónicos se envían oficialmente desde la empresa previene que los atacantes intenten explotar esta falta de certeza a su favor con campañas de Phishing.

Mitigación de vulnerabilidades enequipos de usuario final

La explotación de RAT (Remote Administration Tools) puede tener capacidades de robar credenciales del navegador de la víctima, listar procesos, unidades y directorios en ejecución en la máquina de la víctima, utilizar el protocolo TCP personalizado para sus comunicaciones C&C, recopilar informaciónsobre software antivirus y obtener capturas de pantalla, entre otras. Por las anteriores razones se recomienda contar con agentes EDR o en su defecto de AV instalados en las máquinas de los usuarios para que protejan y notifiquen acciones maliciosas detectadas.

Cree un plan para asegurar ubicaciones físicas

Muchas empresas están cerrando sus oficinas y pasándose al 100% de trabajo remoto. Mientras la seguridad cibernética puede estar con controles, asegúrese de que su seguridad física también lo esté. La información No Confidencial no debe dejarse en escritorios o al aire libre, las instalaciones físicas y las cajas fuertes deben estar debidamente aseguradas y bloqueadas, si tiene cámaras de seguridad, asegúrese que estén en línea y configuradas correctamente.

Definir un programa de respuesta rápida.

Cybereason Nocturnus ha observado campañas de malware que aprovechan el pánico del coronavirus para propagarse y los actores de amenazas están creando campañas de ransomware en torno al pánico COVID-19. Es importante verificar que todas sus copias de seguridad están en su lugar y que su empresa tiene un programa de respuesta rápida que le permitirá recuperarse rápidamente en el caso de un ataque de ransomware. Hacer que las personas trabajen de forma remota puede representar un desafío adicional. Por tal razón es importante que todos los integrantes del equipo de respuesta a incidentes esten listos y dispuestos a asumir nuevos desafíos.

Indicadores de Compromiso

Direcciones IP:
107.175.64.209
64.188.25.205

Dominos:
email.gov.in.maildrive.email/?att=1579160420
email.gov.in.maildrive.email/?att=1581914657
forvox.com
covidmaskpro.com
antivirus-covid19.site
coronavirusmundial.com
anticovidmask.com
endcoronavirus.net

Emails:
info_worldbank.coronavirusfunding@representative.com
revdonaldjohnson009@gmail.com

SHA-256:
876939aa0aa157aa2581b74ddfc4cf03893cede542ade22a2d9ac70e2fef1656
20da161f0174d2867d2a296d4e2a8ebd2f0c513165de6f2a6f455abcecf78f2a
0ee399769a6e6e6d444a819ff0ca564ae584760baba93eff766926b1effe0010
b67d764c981a298fa2bb14ca7faffc68ec30ad34380ad8a92911b2350104e748

Adversarios:
Chinese APTs: Vicious Panda, Mustang Panda
North Korean APTs: Kimsuky
Russian APTs: Hades group, TA542
Pakistan APTs: APT36
Other APTs: Sweed (Lokibot)

Referencias:

https://www.cybereason.com/blog/coronavirus-panic-security-and-you

https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/

Recomendaciones

- Ejecutar programas de concientización al personal sobre los últimos ataquesde phishing / spearphishing
- No hacer click a links en correos sospechosos y no confiar en correos de remitentes desconocidos.
- Actualización de firmas de antivirus y parches de sistema operativo.
- Mantener configurado el SPF del dominio de correo. Al hacerlo, restringir los privilegios de los usuarios parainstalar y ejecutar aplicaciones en las máquinas de la organización, usando el principio de mínimo privilegio.
- Implemente MFA (Multi-Factor Authentication) en todas las conexiones VPN para aumentar la seguridad. Si no se implementa MFA, solicite a los teletrabajadores que usen contraseñas seguras.