[Actualización 3] Campañas de Phishing se aprovechan del miedo por brote de Coronavirus en el Mundo

Desde que comenzó nuestro el reporte sobre las campañas de phishing con temática de Coronavirus, el crecimiento de las campañas han aumentado sin cesar, al igual que los diferentes tipos de malware asociadas a la campaña. Debido a que un gran numero de empresas y entidades gubernamentales ordenaron que los empleados trabajen desde casa, los atacantes aprovechan esta ordenanza para utilizar mensajes de correo utilizando la tematica "HomeOffice" o "Coronavirus". y estas se destacan por el aumento en la suplantación de marcas de confianza en campañas de phishing, teniendo mayor complejidad y sofisticación de estas campañas.

Descripción

Publicación:
03/04/2020
Importancia:
Alta
Riesgo de explotación:
Media

Principales Tendencias Observadas:
Durante el mes pasado, Se han identificado como tendencias prevalentes temáticas del COVID-19 campañas de phishing. Las campañas de phishing han sido las más comunes, aunque hemos visto variantes de malware siendo entregado en las campañas.

Mecanismos de entrega más comunes:

- Adjuntando hojas de calculo o documentos de word ejecutando el malware en segundo plano.
- Adjuntando archivos ejecutables.
- URL en el cuerpo del correo que entregan ransomware.
- Macros de Office
- Auto-IT Dropper (que explota la vulnerabilidad CVE-2017-1882)

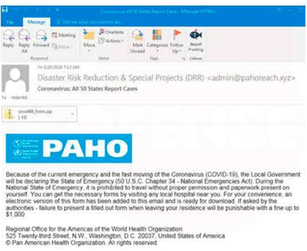
Tipo de Malware enviado:

- Agent Tesla Keylogger
- Ave_Maria Stealer
- Black RAT
- FormGrabber
- Hakbit Ransomware
- Hawkeye Keylogger
- KPOT Stealer
- Lime RAT
- Loki Bot
- NanoCore
- Nemty Ransomware
- Pony
- Remcos RAT
- SalityBot
- TrickBot

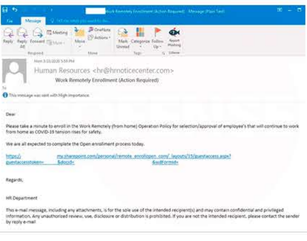
Tipos de Organizaciones con las que están Spoofed mayormente:

- Organización Mundial de la Salud
- Otras organizaciones mundiales/regionales de salud
- Asociaciones no profesionales/médicas relacionadas con la salud
- Departamentos Federales, Estatales y Locales de Salud/Ministerios de Salud
- Empresas de transporte
- Empresas de transporte marítimo

Muchas plantillas de phishing COVID-19 han sido más convincentes que su phish promedio. Por ejemplo en la siguiente imagen, los atacantes alojaron el logotipo de la organización falsa en Google Drive, y se añadió al final del cuerpo del correo una amenaza adicional de una multa de $ 1.000 si los formularios supuestamente adjuntados no se llenan para aprobar cualquier viaje fuera de la casa. El archivo adjunto contiene información KPOT a través de un script VBS a Auto-It que hace uso de ventanas legítimas para disfrazar sus acciones.



Cambios en el tiempo sobre las Amenaza de phishing:
Los temas de Coronavirus en estas semanas han crecido en popularidad y casi con seguridad seguirán haciéndolo. También es probable que las campañas de phishing se adapten con el tiempo para incorporar el trabajo relacionado desde casa, tele-conferencia o videoconferencia invitaciones o avisos, reembolso del gobierno, inscripción de desempleo, y temas en linea. Algunos atacantes ya han comenzado a hacerlo, como se muestra en la Figura 2, donde los actores de la amenaza utiliza un "Trabajo Inscripción remota (Acción Requerida)" en el asunto y es spoofing recursos humanos internos para entregar enlaces a las páginas de phishing brindando las credenciales alojadas en Sharepoint.



COVID-19 continuara afectando las operaciones comerciales durante un período prolongado de tiempo, es posible que esto comience a afectar el panorama de amenazas de phishing más ampliamente. Si bien muchas empresas continúan funcionando en algún nivel, Es probable que haya algunos cambios a largo plazo en las comunicaciones comerciales. Por ejemplo:
Un correo electrónico sobre una fiesta en la oficina o una reunión es más probable que haga sospechar a los usuarios de lo que hubiera sido anteriormente.

Es probable que este tipo de cambios también se extienda hacia los usuarios en casa. Por ejemplo:
Un correo electrónico sobre las nuevas entradas para conciertos o las ventas en la tienda probablemente levantarán una bandera roja.

Ahora las personas naran una pausa por unos segundos porque algo en los mensajes les parecerá sospechoso, puede no parecer particularmente monumental. Sin embargo, estos eventos sacaron a los usuarios de su mentalidad ordinaria,

Los atacantes seguramente se adaptarán también en sus plantillas de phishing. A medida que el coronavirus continúe afectando a todos, es probable que haya un cambio significativo en el panorama de amenazas de phishing para el malware más comúnmente visto y los temas más comunes, incluso excluyendo específicamente los relacionados con Coronavirus.

Referencias:

https://www.threathq.com/api/l/documents/592

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.

Red Queen Lab Report | DigiSert | Centro de Investigación e Inteligencia de Amenazas | Digiware

Este comunicado DigiHelp es una alerta de ciberseguridad, incluye información sensible, puede afectar el objetivo del negocio de su compañía. Este contenido que se encuentra en proceso, esta bajo investigación y análisis de las áreas de Digiware, compuestas por DigiSOC, DigiSert y el Centro de Investigación e Inteligencia de Amenazas, por lo tanto se desarrollarán << informes llamados RQL -Red Queen Lab Report >>, enviados posteriormente por medio de un comunicado oficial.

#Digiware | #DigiwareSuAliado
#DigiwareSecurity | #DigiwareVisionDay