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

El phishing ha sido desde principios de la década de los 2000 el vector de ataque más común empleado por ciber criminales. A medida que las empresas mejoran en la contención y bloqueo de ataques de correo electrónico, los atacantes están cambiando las tácticas, reduciendo el volumen total de ataques y lanzando ataques de phishing más específicos.

Las recientes noticias sobre la expansión del COVID-19 ha traído consigo el caos en muchos sectores económicos diferentes como es el caso del sector económico, manufactura, salud pública, entre otros. Sin embargo, también ha originado una amenaza de ciberseguridad, mediante las campañas de phishing con temática COVID-19 y dominios relacionados con COVID-19 recientemente registrados.

## Descripción

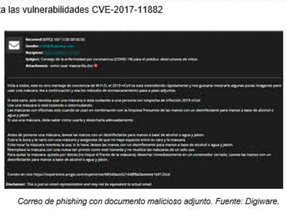
Empresa Afectada:
**Microsoft**
Publicación:
**13/03/2020**
Importancia:
**Alta**
Riesgo de explotación:
**Alta**
Tipo de explotación:
**Remoto**

**Fuentes:**

Recorded Future

Durante esta semana, observamos que la temática del COVID-19 o mayormente conocido como Coronavirus ha sido utilizado principalmente por los ciberdelincuentes como un tema predilecto para sus campañas de phishing.

Asimismo, la cantidad de dominios recientemente registrados relacionados con el Coronavirus ha aumentado desde que se masificó el brote a mediado de febrero. Un posible indicador de que los atacantes puede haber comenzado a darse cuenta de la utilidad de COVID-19 como un vector de ataque cibernetico estratégico.




*El gráfico muestra los registros de dominios relacionados con COVID-19. Dominios que contienen "corona", "covid19", "covid2019". Fuente: Recorded Future.*

Por otro lado, se observó que el malware AZORult se entregaba mediante documentos de phishing que usaban COVID-19 como temática a principios de febrero de 2020. Estos ataques involucraron correos electrónicos que contenían archivos adjuntos de documentos de Microsoft Office diseñados para atraer a las víctimas y explotar una vulnerabilidad de Microsoft Office, identificada como CVE-2017-11882, el cual permite a los atacantes ejecutar código arbitrario en el contexto del usuario actual.

A fines de enero del 2020, investigadores de IBM X-Force observó que los ciberdelincuentes utilizaban el coronavirus como temática de phishing para distribuir Emotet en una campaña dirigida principalmente a Japón. Los correos electrónicos de Phishing tenían adjuntos archivos de Microsoft Word, los cuales contenían una macro VBA maliciosa que instalaba un script de PowerShell, que luego descargaba el troyano Emotet.

En el panorama local de américa latina, el equipo de investigadores de Digiware identificó en la última semana campañas de Emotet que contenían un archivo de Microsoft Word adjunto con la temática de COVID-19. Se observó que este adjunto explota las vulnerabilidades CVE-2017-11882

*Correo de phishing con documento malicioso adjunto. Fuente: Digiware.*

Observamos que el adjunto "como usar mascarilla.doc" está identificado como malicioso y realiza un callback hacia la direcciòn IP 213[.]226[.]100[.]134 ubicada en Rusia.

*Análisis de VirusTotal al archivo malicioso. Fuente: VirusTotal.*

## Indicadores de Compromiso

**Direcciones IP:**
*213[.]226[.]100[.]134*
*150[.]95[.]52[.]104*
*118[.]127[.]3[.]247*
*153[.]120[.]181[.]196*
*112[.]140[.]180[.]26*
*13[.]239[.]26[.]132*

**URL:**
*hxxp://213[.]226[.]100[.]134/m1/webm.jpg213*

**Emails:**
*info@premecsaf[.]com[.]ar*
*contratos@climo[.]com[.]ar*

SHA-256:
*6da52a6ee47277a9a943c114e3bc9d541fe1de7c61d157bb2ecc5ca0f76a24cd*

## Referencias:

https://www.recordedfuture.com/coronavirus-panic-exploit/

https://thehackernews.com/2020/03/coronavirus-maps-covid-19.html

## Recomendaciones

- Ejecutar programas de concientización al personal sobre los últimos ataquesde phishing / spearphishing
- No hacer click a links en correos sospechosos yno confiar en correos de remitentes des conocidos.
- Actualización de firmas de antivirus y parchesde 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 elprincipio de mínimo privilegio.
- Limitar los privilegios para procesos desconocidos,escribiendo reglas para HIPS (sistemas de prevención de intrusiones de host) oreglas de protección de acceso.