INTERPOL

PANORAMA MUNDIAL DE LA CIBERAMENAZA RELACIONADA CON LA COVID-19

#WashYourCyberHands

Un gran número de delincuentes oportunistas se están aprovechando de la pandemia de COVID-19 para lanzar diversos tipos de ciberataques. En particular, desde el inicio del brote se han vuelto a detectar varios malware que se encontraban en estado relativamente latente y que han adoptado nuevas formas o cuyos autores han utilizado la COVID-19 para dar un nuevo impulso a sus tácticas de ingeniería social. Aunque estas ciberamenazas evolucionan constantemente, últimamente se han podido distinguir, entre otras, las siguientes:

PANORAMA MUNDIAL DE LA CIBERAMENAZA RELACIONADA CON LA COVID-19

Nombres de dominio malignos

Han aumentado los nombres de dominio registrados con las palabras clave "COVID" o "corona", para sacar partido del número creciente de personas que buscan información sobre la COVID-19. Se considera que muchos de ellos se crearon con malas intenciones: según Palo Alto Networks, hasta finales de marzo, entre los nombres de dominio recién registrados se habían descubierto 2 022 malignos y 40 261 que presentaban un alto riesgo.

Estafas en línea y phishing

Los ciberdelincuentes están creando sitios web falsos relacionados con la COVID-19, para incitar a las víctimas a abrir archivos adjuntos malignos o hacer clic en enlaces de phishing, lo que da lugar a una usurpación de identidad o al acceso ilícito a cuentas personales. Asimismo, la empresa Trend Micro informó de que, desde enero de 2020, cerca de un millón de mensajes de correo basura guardaban relación con el coronavirus.

Las estafas a empresas por e-mail mediante suplantación de identidad (estafas BEC), que implican la utilización de las direcciones de e-mail de proveedores y clientes –o el uso de direcciones casi idénticas–, se han convertido en el tipo de estafa preferido para perpetrar ataques. La extrema necesidad de suministros esenciales ofrece a los delincuentes una ocasión ideal para obtener datos o desviar hacia cuentas ilícitas millones de dólares cuya finalidad era la adquisición de tales suministros.

Malware destinados a la obtención de datos

Los malware destinados a la obtención de datos, tales como troyanos de acceso a distancia, ladrones de información, spyware (programas espía) o troyanos bancarios, se infiltran en los sistemas informáticos, utilizando información relacionada con la COVID-19 como señuelo, a fin de infectar redes, sustraer datos, desviar sumas de dinero y construir botnets.

Malware obstructivos (ransomware y DDoS)

Los ciberdelincuentes están utilizando malware obstructivos, tales como ransomware dirigidos contra infraestructuras esenciales e instituciones destinadas a combatir la pandemia (por ejemplo, hospitales y centros médicos), que están desbordados por la crisis sanitaria. Normalmente, estos ataques con ransomware o por denegación de servicio (DDoS) no tienen por objeto la sustracción de información, sino que impiden el acceso a datos de vital importancia o perturban el funcionamiento del sistema, agravando así una situación ya de por sí desesperada en el mundo físico.

Vulnerabilidad del trabajo a domicilio

Los autores de las ciberamenazas explotan las vulnerabilidades de los sistemas, redes y aplicaciones empleados por las empresas, las administraciones públicas y los centros de enseñanza para apoyar al personal que trabaja actualmente a distancia. Dado que el número creciente de personas que depende de las herramientas en línea pone a prueba las medidas de seguridad introducidas antes del brote de coronavirus, los delincuentes buscan nuevas oportunidades de intrusión para robar datos, obtener ganancias o provocar disfunciones.

Evolución prevista en el futuro

Las ciberamenazas a las que se enfrentan los particulares, las empresas y las infraestructuras esenciales seguirán evolucionando a la par de las rápidas transformaciones que se producirán en los ámbitos social y económico, causando daños a escala mundial. La ciberdelincuencia continuará aumentando, ya que los delincuentes buscarán nuevas fuentes de ingresos apoyándose en las facetas informáticas de otros tipos de delitos. Así, deberíamos asistir a:

- un incremento de las estafas en línea, el phishing y las estafas BEC, debido al bajón económico y a la modificación del panorama empresarial, que generarán nuevas actividades delictivas;
- un aprovechamiento del mercado clandestino por parte de los delincuentes para tratar de imponer la "ciberdelincuencia como servicio", dada la facilidad de acceso, el bajo coste y los altos beneficios potenciales que pueden ofrecer tales plataformas;
- una concentración de los autores de las ciberamenazas en la información personal de los particulares, a través de la suplantación y la explotación de los proveedores de contenidos digitales;
- una dependencia de las conexiones en línea y las herramientas de comunicación virtual por parte de las administraciones públicas, las empresas y los centros de enseñanza, debido a que los empleados seguirán trabajando a domicilio, lo que aumentará la vulnerabilidad de tales entidades y ofrecerá a los ciberdelincuentes más oportunidades de delinquir.

La respuesta de INTERPOL

En el marco del programa mundial de INTERPOL sobre ciberdelincuencia se está elaborando y dirigiendo la respuesta mundial de las fuerzas del orden contra las ciberamenazas que están prosperando al amparo del brote de coronavirus. Concretamente, utilizamos las notificaciones moradas para alertar a los países miembros sobre nuevas ciberamenazas que presentan un alto riesgo, aportamos asesoramiento técnico a las organizaciones afectadas, en apoyo de sus medidas de recuperación, y hemos realizado una encuesta mundial sobre la ciberdelincuencia, a fin de entender mejor la situación en todo el planeta, que evoluciona rápidamente. Asimismo, para prestar servicios adaptados a las necesidades de los países miembros, con fines de prevención, detección e investigación de la ciberdelincuencia, estamos colaborando con las comunidades en línea especializadas en la ciberseguridad y manteniendo reuniones virtuales de emergencia con diversas partes interesadas, incluidos los Jefes de las unidades nacionales y regionales dedicadas a la lucha contra la ciberdelincuencia, el Grupo Mundial de INTERPOL de Expertos en Ciberdelincuencia y nuestros socios del sector privado.

INTERPOL

INTERPOL General Secretariat
Tel: +33 4 72 44 70 00
www.interpol.int