Los hackers imitan cada vez más las aplicaciones legítimas como Skype, Adobe Reader y VLC Player como un medio para abusar de las relaciones de confianza y aumentar la probabilidad de un ataque de ingeniería social exitoso.

Otras aplicaciones legítimas más suplantadas por ícono incluyen 7-Zip, TeamViewer, CCleaner, Microsoft Edge, Steam, Zoom y WhatsApp, según revelaciones de un análisis de VirusTotal.

> *«Uno de los trucos de ingeniería social más simples que hemos visto consiste en hacer que una muestra de malware parezca un programa legítimo. El icono de estos programas es una característica fundamental que se utiliza para convencer a las víctimas de que estos programas son legítimos»,* dijo VirusTotal.

No sorprende que los atacantes recurran a una variedad de enfoques para comprometer los puntos finales al engañar a los usuarios involuntarios para que descarguen y ejecuten programas aparentemente inocuos.

Esto, a su vez, se logra principalmente aprovechando los dominios genuinos en un intento por sortear las defensas de firewall basadas en IP. Algunos de los principales dominios abusados son *discordapp[.]com, squarespace[.]com, amazonaws[.]com, mediafire[.]com y qq[.]com.*

En total, se han detectado no menos de 2.5 millones de archivos sospechosos descargados de 101 dominios pertenecientes a los 1000 principales sitios web de Alexa.

El mal uso de Discord ha sido documentado, ya que la red de entrega de contenido (CDN) de la plataforma se convirtió en un terreno fértil para alojar malware junto con Telegram, al tiempo que ofrece un *«centro de comunicaciones perfecto para los atacantes».*

Otra técnica usada con frecuencia es la práctica de firmar malware con certificados válidos robados a otros fabricantes de software. El servicio de escaneo de malware dijo que encontró

más de un millón de muestras maliciosas desde enero de 2021, de las cuales el 87% tenía una firma legítima cuando se cargaron por primera vez en su base de datos.

VirusTotal dijo que también descubrió 1816 muestras desde enero de 2020 que se hicieron pasar por software legítimo al empaquetar el malware en instaladores para otro software popular como Google Chrome, Malwarebytes, Zoom, Brave, Mozilla Firefox y Proton VPN.

Este método de distribución también puede resultar en una cadena de suministro cuando los atacantes logran entrar en un servidor de actualización de software legítimo u obtener acceso no autorizado al código fuente, lo que hace posible infiltrar el malware en forma de archivos binarios troyanos.

De forma alternativa, los instaladores legítimos se empaquetan en archivos comprimidos junto con archivos con malware, en un caso que incluye el instalador legítimo de Proton VPN y el malware que instala el ransomware Jigsaw.

Además, un tercer método, más sofisticado, implica incorporar el instalador legítimo como un recurso ejecutable portátil en la muestra maliciosa para que el instalador también se ejecute cuando se ejecuta el malware para dar la ilusión de que el software funciona según lo previsto.

> *«Al pensar en estas técnicas en su conjunto, se podría concluir que existen factores oportunistas de los que los atacantes pueden abusar (como certificados robados) a corto y mediano plazo, y los procedimientos rutinariamente automatizados en los que los atacantes pretenden replicar visualmente aplicaciones de distintas formas»,* dijeron los investigadores.