Los investigadores de seguridad cibernética identificaron otro ataque en la cadena de suministro llevado a cabo por hackers de tarjetas de pago, contra más de 17 mil dominios web, que también incluyen sitios web entre los 2 mil principales de Alexa.

Debido a que Magecart no es ni un solo grupo ni un malware específico, sino un término general que se otorga a todos los grupos cibernéticos e individuos que inyectan skimmers de tarjetas digitales en sitios web comprometidos, no es necesario que cada uno de ellos utilice técnicas similares con la misma sofisticación.

Un nuevo informe compartido con THN antes de su lanzamiento, detalla una nueva campaña de ataques a la supply-chain, en la que los piratas informáticos utilizan el enfoque de escopeta en lugar de ataques dirigidos para infectar una amplia gama de sitios web, prefiriendo un mayor alcance de infección como posible sobre precisión.

Hace casi dos meses, los investigadores de seguridad de RiskIQ descubrieron ataques en la cadena de suministro que involucraban a skimmers de tarjetas de crédito colocados en varios proveedores basados en la web, como AdMaxim, CloudCMS y Picreel, con la intención de infectar tantos sitios web como sea posible.

Sin embargo, luego de un monitoreo continuo de sus actividades, los investigadores encontraron que la escala real de esta campaña, que comenzó a inicios de abril de 2019, es mucho más grande de lo que se informó anteriormente.

Hackers de Magecart atacan los Buckets mal configurados de Amazon S3

Según los investigadores, desde el inicio de la campaña, este grupo de atacantes de Magecart ha estado explorando de forma continua la Internet en busca de depósitos de Amazon S3 mal configurados, lo que permite que cualquiera pueda ver y editar los archivos que contiene, e inyectar su código digital de marcado de tarjetas en la parte inferior de cada archivo JavaScript que encuentran.

> *«Aunque los atacantes han tenido mucho éxito en la difusión de su código de skimmer en miles de sitios web, sacrificaron la orientación en favor del alcance»,* dijeron los investigadores.

Ya que los piratas informáticos no siempre tienen la idea de si los archivos JavaScript sobrescritos están siendo utilizados por un sitio web o proyecto, es más como disparar una flecha en la oscuridad.

Además, tal parece que muchos de los archivos JavaScript infectados ni siquiera formaban parte de la página de pago, que es la ubicación principal desde donde los analizadores digitales capturan los datos de tarjetas bancarias de los usuarios y los envían a un servidor controlado por un hacker.

> *«Los actores utilizaron esta técnica para lanzar una red lo más amplia posible, pero muchos de los scripts comprometidos no se cargan en las páginas de pago. Sin embargo, la facilidad de compromiso que surge al encontrar cubos de S3 abiertos significa que incluso si solo una fracción de sus inyecciones de skimmer devuelve datos de pago, valdrá la pena, tendrán un retorno de inversión sustancial»,* dicen los investigadores.

Mientras tanto, en un informe separado publicado hoy por el equipo de Zscaler ThreatLabZ, los investigadores revelaron detalles acerca de una campaña de Magecart recién descubierta en la que los atacantes utilizan un enfoque sofisticado y específico para robar detalles de tarjetas de débito y crédito de sitios web de comercio electrónico.

Según el informe, en lugar de hacer uso del código de skimming digital en JavaScript simple, se encontró que el grupo utiliza una versión muy confusa de su skimmer de tarjetas con cargas cifradas en un intento por evitar que los investigadores identifiquen fácilmente los sitios web comprometidos.

Magecart llegó a los medios el año pasado luego de que los piratas informáticos realizaran varios ataques de alto perfil contra importantes compañías internacionales, como British Airways, Ticketmaster y Newegg.