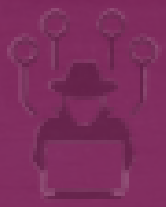
2024

Análisis Técnico del Kit de Phishing Tycoon 2FA: Metodología, Ofuscación y Técnicas de Ingeniería Social



Created by

Fernando Vargas Hincapié

https://www.alertasyseguridad.net

Ready to

ihackmyfuture

https://www.ihackmyfuture.com/

Introducción

En el panorama actual de ciberseguridad, los ataques de phishing han evolucionado significativamente, adoptando técnicas cada vez más sofisticadas para eludir las defensas tradicionales y engañar a los usuarios. Entre estos ataques, el kit de phishing Tycoon 2FA se destaca por su compleja cadena de ataque y su capacidad para engañar a las víctimas mediante una serie de redirecciones y técnicas de ofuscación avanzadas. Este kit malicioso explota la autenticación de dos factores (2FA) como una herramienta para incrementar la eficacia de sus campañas de phishing, empleando dominios comprometidos y técnicas de redirección para ocultar el dominio final del ataque. La cadena de ataque comienza con correos electrónicos de phishing que, a pesar de estar aparentemente bien firmados y provenientes de servicios legítimos como Amazon Simple Email Service, contienen archivos adjuntos vacíos que sirven como señuelos. Al hacer clic en los enlaces proporcionados, las víctimas son sometidas a múltiples redirecciones a través de dominios diseñados para enmascarar la verdadera naturaleza del phishing. Estas redirecciones culminan en un motor de phishing que se comunica con un servidor de comando y control (C2) para recolectar credenciales robadas. Este informe técnico desglosa detalladamente cada etapa del proceso, desde la recepción del correo electrónico inicial hasta la comunicación cifrada con el servidor C2, proporcionando una visión integral del funcionamiento interno y las técnicas utilizadas por el kit Tycoon 2FA para comprometer la seguridad de los usuarios y evadir la detección.

Funcionamiento

El kit de phishing Tycoon 2FA opera a través de una intrincada cadena de ataque diseñada para engañar a las víctimas y obtener credenciales de acceso mediante un sofisticado mecanismo de redirección y ofuscación. El ataque inicia con un correo electrónico de phishing enviado desde un cliente de Amazon Simple Email Service (SES), que a menudo incluye una firma legítima para parecer auténtico. Este correo contiene archivos PDF vacíos como archivos adjuntos y un enlace disfrazado, que lleva a la víctima a través de una serie de redirecciones encadenadas a través de múltiples dominios. Cada redirección está diseñada para ocultar el dominio final del phishing, utilizando técnicas como el abuso de redireccionamientos en redes sociales y medios de comunicación, así como redireccionamientos personalizados que enmascaran el destino real. Al hacer clic en el enlace, la víctima es redirigida a un motor de phishing que solicita sus credenciales a través de un formulario que simula un entorno legítimo. La comunicación entre el navegador de la víctima y el servidor de comando y control (C2) está cifrada utilizando AES en modo CBC, asegurando que las credenciales robadas se transmitan de manera segura al C2. El motor de phishing y el servidor C2 emplean técnicas de ofuscación avanzada, como el cifrado XOR y el uso de servicios externos de ofuscación, para dificultar el análisis y la detección del malware. El kit Tycoon 2FA también ha evolucionado para incluir variantes que utilizan mensajes de error falsos para engañar a los usuarios, haciéndoles creer que están resolviendo un problema técnico cuando en realidad están ingresando sus credenciales en una página de phishing. Además, se han descubierto variantes que se dirigen a organizaciones gubernamentales, filtrando direcciones de correo electrónico específicas para aumentar la precisión del ataque y mejorar la tasa de éxito.

Acciones maliciosas

El kit de phishing Tycoon 2FA emplea una serie de acciones maliciosas para comprometer las credenciales de las víctimas a través de un ataque elaborado que abarca varias fases.

1. Envío de Correos Electrónicos de Phishing: El ataque comienza con el envío de correos electrónicos fraudulentos que aparentan ser legítimos, utilizando servicios como Amazon Simple Email Service (SES). Estos correos a menudo incluyen archivos adjuntos en formato PDF vacíos y un enlace disfrazado que redirige a las víctimas a una página de phishing. La inclusión de firmas auténticas en los correos electrónicos busca aumentar su credibilidad y disminuir la sospecha de los destinatarios.
2. Redirección a Través de Varios Dominios: Al hacer clic en el enlace del correo electrónico, las víctimas son dirigidas a través de una serie de redirecciones encadenadas. Estas redirecciones pasan por varios dominios que ocultan el dominio final de phishing, utilizando técnicas como el abuso de redireccionamientos en redes sociales y medios de comunicación. Esto permite a los atacantes ocultar la verdadera ubicación del sitio web malicioso y evitar la detección temprana.
3. Interacción con el Motor de Phishing: Una vez que la víctima llega al motor de phishing, se le presenta un formulario que imita un entorno legítimo, como una página de inicio de sesión. El motor de phishing solicita las credenciales de la víctima, que son capturadas y enviadas al servidor de comando y control (C2) del atacante.
4. Comunicación con el Servidor C2: La información recopilada se transmite al servidor C2 a través de una comunicación cifrada utilizando AES en modo CBC. Esta comunicación asegura que las credenciales robadas se envíen de manera segura al servidor de los atacantes sin ser detectadas o interceptadas.
5. Ofuscación y Técnicas de Evasión: El código del kit de phishing se divide y ofusca para dificultar el análisis y la detección. Se utilizan técnicas como el cifrado XOR y servicios externos de ofuscación para proteger el código del motor de phishing y la comunicación con el C2.
6. Filtrado de Direcciones de Correo Electrónico: En algunas variantes, los atacantes filtran direcciones de correo electrónico específicas, como las asociadas con organizaciones gubernamentales. Las víctimas que ingresan correos electrónicos que coinciden con esta lista son redirigidas a páginas de phishing diseñadas para capturar contraseñas de cuentas específicas, como cuentas de Microsoft.

Mitigaciones

1. Implementación de Autenticación Multifactor (MFA):
    - La autenticación multifactor (MFA) añade una capa adicional de seguridad al proceso de inicio de sesión. Requiere que los usuarios proporcionen más de un tipo de autenticación, como un código enviado a su teléfono móvil o una aplicación de autenticación, además de su contraseña.
2. Educación y Concienciación del Usuario:
    - Realizar entrenamientos regulares sobre ciberseguridad para empleados y usuarios finales. Esto incluye cómo identificar correos electrónicos sospechosos, la importancia de no hacer clic en enlaces desconocidos, y la verificación de la autenticidad de los mensajes recibidos.
3. Implementación de Filtrado de Correo Electrónico y Seguridad de URL:
    - Utilizar soluciones de filtrado de correo electrónico avanzadas que identifiquen y bloqueen correos electrónicos de phishing. También, emplear herramientas de seguridad de URL que verifiquen los enlaces en los correos electrónicos y bloqueen accesos a sitios maliciosos.
4. Configuración y Monitoreo de SPF, DKIM y DMARC:
    - Configurar los registros SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting & Conformance) para proteger el dominio de correo electrónico contra el uso no autorizado y falsificación.
5. Uso de Soluciones de Seguridad Web y Análisis de Tráfico:
    - Implementar soluciones de seguridad web que monitoricen y analicen el tráfico en busca de comportamientos anómalos y patrones de ataque. Esto incluye la detección de redirecciones sospechosas y análisis de tráfico hacia dominios conocidos de phishing.
6. Actualización y Mantenimiento Regular de Software:
    - Asegurarse de que todos los sistemas, aplicaciones y navegadores estén actualizados con los últimos parches y versiones de seguridad. Esto incluye la actualización de plataformas de seguridad, sistemas operativos y software de navegador.

Fuentes web

1. **Cybereason - Tycoon Ransomware Overview**
   - https://www.cybereason.com/blog/tycoon-ransomware-overview
   - Proporciona un análisis detallado de las técnicas utilizadas por el ransomware Tycoon, incluyendo cómo afecta a las organizaciones y las mejores prácticas para defenderse contra él.
2. **ThreatPost - Tycoon Ransomware: A New Variant**
   - https://threatpost.com/tycoon-ransomware-new-variant/
   - Explora las características específicas del ransomware Tycoon, cómo se propaga y las estrategias recomendadas para la mitigación y protección contra este tipo de amenazas.
3. **BleepingComputer - Tycoon Ransomware: What You Need to Know**
   - https://www.bleepingcomputer.com/news/security/tycoon-ransomware-what-you-need-to-know/
   - Ofrece un resumen exhaustivo sobre el ransomware Tycoon, incluyendo detalles sobre su funcionamiento, técnicas de ataque y medidas de defensa efectivas.
4. **FireEye - Protecting Against Advanced Phishing Attacks**
   - https://www.fireeye.com/blog/threat-research/2021/06/protecting-against-advanced-phishing-attacks.html
   - Analiza las tácticas y técnicas utilizadas en ataques de phishing avanzados y ofrece recomendaciones sobre cómo protegerse contra estas amenazas.
5. **Check Point - How to Defend Against Phishing Attacks**
   - https://blog.checkpoint.com/2021/03/15/how-to-defend-against-phishing-attacks/
   - Proporciona estrategias y mejores prácticas para defenderse contra ataques de phishing, incluyendo la identificación de señales de phishing y la implementación de medidas preventivas.

Fuentes Escritas

- **"Ransomware: Defending Against Digital Extortion"**
  by Allan Liska and Timothy Gallo
  Este libro ofrece un análisis exhaustivo de los ataques de ransomware, incluyendo una sección sobre las técnicas y herramientas empleadas por grupos de ransomware como Tycoon, así como estrategias de mitigación y respuesta.

- **"Phishing and Countermeasures: Understanding the Risks and Defending Against Attackers"**
  by Markus Jakobsson and Steven Myers
  Este texto profundiza en las técnicas de phishing y los métodos utilizados por los atacantes para engañar a las víctimas. Incluye un análisis de campañas específicas y kits de phishing como Tycoon, proporcionando detalles sobre cómo operan y cómo defenderse contra ellos.

- **"Advanced Persistent Threats and How to Defend Against Them"**
  by John P. Carlin and Peter W. Singer
  Este libro examina las amenazas persistentes avanzadas (APT) y proporciona información sobre cómo los kits de phishing y ransomware, como Tycoon, se insertan en estas campañas. Ofrece un enfoque detallado sobre la identificación, análisis y mitigación de estas amenazas avanzadas.