Los actores maliciosos están aprovechando repositorios públicos de GitHub para alojar cargas útiles dañinas y distribuirlas a través de Amadey como parte de una campaña observada en abril de 2025.

"Los operadores del modelo MaaS [malware como servicio] utilizaron cuentas falsas en GitHub para almacenar cargas maliciosas, herramientas y complementos de Amadey, probablemente como una forma de evadir filtros web y facilitar su uso", señalaron los investigadores de Cisco Talos, Chris Neal y Craig Jackson, en un informe publicado hoy.

La firma de ciberseguridad indicó que las cadenas de ataque hacen uso de un *loader* malicioso llamado Emmenhtal (también conocido como PEAKLIGHT) para desplegar Amadey, el cual a su vez descarga cargas adicionales personalizadas desde repositorios públicos de GitHub operados por los atacantes.

Esta actividad comparte tácticas similares con una campaña de *phishing* por correo electrónico que en febrero de 2025 empleó señuelos relacionados con pagos de facturas para distribuir SmokeLoader mediante Emmenhtal, en ataques dirigidos a entidades ucranianas.

Tanto Emmenhtal como Amadey funcionan como descargadores de cargas útiles secundarias como *stealers*, aunque se ha observado que Amadey también ha distribuido *ransomware* como LockBit 3.0 en ocasiones anteriores.

Una diferencia clave entre ambas familias de malware es que, a diferencia de Emmenhtal, Amadey tiene la capacidad de recopilar información del sistema y puede expandirse funcionalmente mediante una serie de complementos DLL, que permiten funciones específicas como el robo de credenciales o la captura de pantallas.

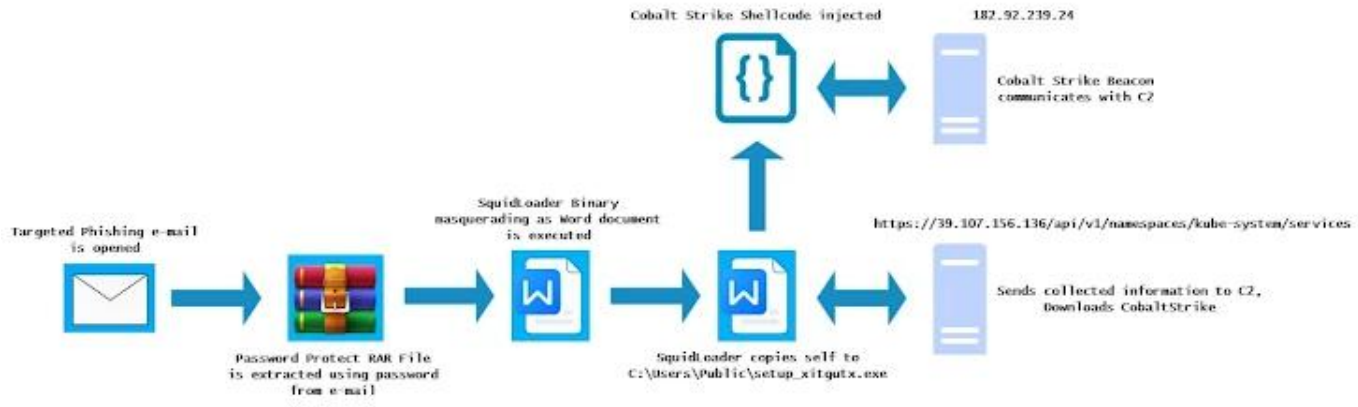
El análisis de Cisco Talos sobre la campaña de abril de 2025 reveló tres cuentas de GitHub (Legendary99999, DFfe9ewf y Milidmdds) que se utilizaban para alojar complementos de Amadey, cargas útiles secundarias y otros scripts maliciosos, incluyendo Lumma Stealer, RedLine Stealer y Rhadamanthys Stealer. Dichas cuentas ya han sido eliminadas por GitHub.

Algunos archivos JavaScript presentes en estos repositorios resultaron ser idénticos a los scripts Emmenhtal utilizados en la campaña de SmokeLoader, siendo la principal diferencia las cargas útiles descargadas. En concreto, los archivos del *loader* Emmenhtal en los repositorios servían como canal para distribuir Amadey, AsyncRAT y una copia legítima de PuTTY.exe.

También se halló un script en Python que probablemente representa una evolución de Emmenhtal, el cual incorpora un comando PowerShell embebido para descargar Amadey desde una dirección IP codificada de forma estática.

Se cree que las cuentas de GitHub utilizadas para alojar estas cargas forman parte de una operación MaaS más amplia, que explota la plataforma de alojamiento de código de Microsoft con fines maliciosos.

Esta revelación coincide con un informe de Trellix que detalla una campaña de *phishing* que propaga otro *loader* llamado SquidLoader, dirigido contra instituciones del sector financiero en Hong Kong. Evidencias adicionales descubiertas por la empresa de seguridad sugieren que podrían estar llevándose a cabo ataques similares en Singapur y Australia.



SquidLoader representa una amenaza considerable debido a su amplia gama de técnicas anti-análisis, anti-*sandbox* y anti-*debug*, lo que le permite evadir la detección y dificultar su

análisis. Además, puede establecer comunicación con un servidor remoto para enviar información del sistema infectado e inyectar la siguiente carga maliciosa.

"SquidLoader emplea una cadena de ataque que culmina con el despliegue de un beacon de Cobalt Strike para obtener control remoto del sistema", explicó el investigador en seguridad Charles Crofford. *"Sus complejas técnicas de evasión, combinadas con su baja tasa de detección, representan una amenaza significativa para las organizaciones objetivo."*

Los hallazgos también se suman al descubrimiento de múltiples campañas de ingeniería social diseñadas para distribuir diversas familias de malware:

- Ataques atribuidos a un grupo motivado financieramente conocido como UNC5952, que usan temas de facturación en correos electrónicos para entregar *droppers* maliciosos que finalmente instalan un descargador llamado CHAINVERB, el cual despliega el software de acceso remoto ConnectWise ScreenConnect.
- Ataques que emplean señuelos relacionados con impuestos para engañar a los usuarios y hacerles descargar un instalador de ConnectWise ScreenConnect, bajo el pretexto de abrir un documento PDF.
- Ataques con temáticas de la Administración del Seguro Social de EE.UU. (SSA) diseñados para robar credenciales o instalar versiones troyanizadas de ConnectWise ScreenConnect, tras lo cual se instruye a las víctimas a instalar y sincronizar la app *Phone Link* de Microsoft para posiblemente interceptar mensajes de texto y códigos de autenticación de dos factores.
- Ataques que utilizan un *phishing kit* llamado Logokit, que permite crear páginas de inicio de sesión falsas alojadas en la infraestructura de Amazon Web Services (AWS), integrando verificación CAPTCHA de Cloudflare Turnstile para dar una apariencia falsa de legitimidad.
- Ataques con otro *phishing kit* personalizado basado en Python Flask, que facilita el robo de credenciales con poco esfuerzo técnico.
- Campañas bautizadas como *Scanception*, que utilizan códigos QR en archivos PDF adjuntos para dirigir a las víctimas a páginas falsas de inicio de sesión de Microsoft.
- Ataques que usan la técnica *ClickFix* para distribuir Rhadamanthys Stealer y

NetSupport RAT.

- Campañas que se apoyan en servicios de ocultación como Hoax Tech y JS Click Cloaker para evadir los escáneres de seguridad y mostrar contenido malicioso solo a las víctimas seleccionadas.
- Ataques que emplean HTML y JavaScript para crear correos maliciosos con apariencia legítima, capaces de eludir tanto la sospecha del usuario como las herramientas de detección tradicionales.
- Campañas dirigidas a proveedores de servicios B2B que utilizan archivos de imagen SVG en correos de *phishing*, los cuales contienen JavaScript ofuscado que redirige a la infraestructura del atacante al abrirse en el navegador, usando la función `window.location.href`.

Según datos recopilados por Cofense, el uso de códigos QR representó el 57 % de las campañas con tácticas, técnicas y procedimientos avanzados (TTPs) en 2024. Otros métodos relevantes incluyen el uso de archivos comprimidos protegidos por contraseña en correos electrónicos para evadir los *secure email gateways* (SEG).

"Al proteger los archivos comprimidos con contraseña, los atacantes impiden que los SEG y otros métodos escaneen su contenido, el cual suele contener archivos claramente maliciosos", explicó el investigador Max Gannon de Cofense.