BOLETÍN COMITÉ NACIONAL DE SEGURIDAD DIGITAL

Boletín CNSD-20250830-001 Alerta Campaña de Phishing

Fecha: 20250830

TLP:CLEAR

Contexto

Imagina que un ladrón se disfraza de cartero. Te entrega una carta que parece real, pero su verdadero propósito es que le abras la puerta para entrar y robarte. El *phishing* funciona de la misma manera, pero en el mundo digital: es cuando un atacante se hace pasar por una entidad de confianza para robar tus datos.

Se ha identificado una campaña de correos electrónicos falsos *(phishing)* con el asunto **"Confirmación requerida para mantener la activación de su cuenta de correo**". enviando mensajes que parecen ser de una fuente legítima como las identificadas de los dominios **alcaldiasoacha.gov.co, defensajuridica.gov.co, mincit.gov.co y mintransporte.gov.co.**

Modo de operación de una campaña de phishing

Una campaña de phishing normalmente inicia con un correo electrónico malicioso que contiene un enlace o un archivo adjunto. El usuario, engañado por la urgencia o la apariencia legítima del mensaje, hace clic en el enlace, que lo dirige a una página web falsa diseñada para robar sus datos, o descarga un archivo que ejecuta un programa dañino (Malware). Una vez que la cuenta del usuario es comprometida, los atacantes la utilizan para enviar el mismo mensaje malicioso a todos sus contactos, lo que provoca una rápida propagación del ataque. Este método de auto-replicación convierte un simple engaño en una amenaza viral que se distribuye desde el interior de la propia red de la víctima.

Acciones Inmediatas

El phishing es una amenaza constante, afectando la seguridad digital de entidades y organizaciones, por esta razón **es imperativo que revisen con urgencia las recomendaciones y apreciaciones en esta alerta e implementen planes de mitigación inmediatos, para asegurar la protección de activos críticos**, evitando que las entidades y organizaciones sean víctima de este tipo de campaña y salvaguardar la continuidad de las operaciones.

BOLETÍN COMITÉ NACIONAL DE SEGURIDAD DIGITAL

Boletín CNSD-20250830-001 Alerta Campaña de Phishing

Fecha: 20250830

TLP:CLEAR

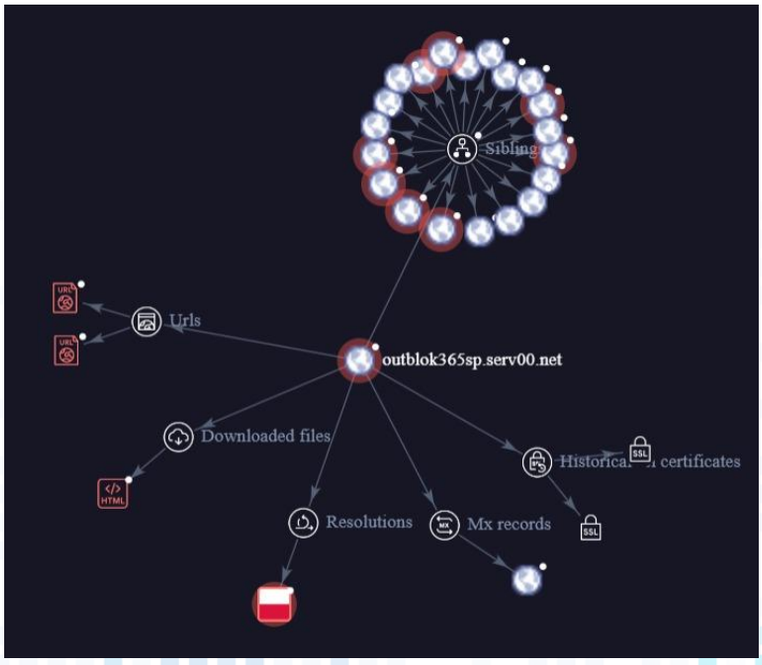
Modo de operación la campaña identificada

Según información suministrada al equipo **ColCERT**, la campaña, fue originada desde el buzón adriana.pinilla de la Alcaldía de Soacha el pasado 16 de agosto, enviado a un buzón de la defensa jurídica, así las cosas, la defensa jurídica genera un comunicado a través de la red X, replicada por el **ColCERT**, el pasado 25 de agosto.

De: Adriana Maria Pinilla Sanchez <adriana.pinilla@alcaldiasoacha.gov.co>
Enviado: sábado, 16 de agosto de 2025 1:57 p. m.
Para: Oscar Eduardo Albarracin Malaver <oscar.albarracin@defensajuridica.gov.co>

Análisis y Comportamiento

En el siguiente grafo se evidencia que **outblok365sp.serv00.net** es un dominio malicioso de phishing vinculado a **Outlook 365**, con resoluciones DNS, registros MX, certificados SSL históricos y archivos descargados asociados. Los múltiples dominios hermanos (siblings) indican infraestructura compartida usada para campañas coordinadas, orientadas al robo de credenciales.



BOLETÍN COMITÉ NACIONAL DE SEGURIDAD DIGITAL

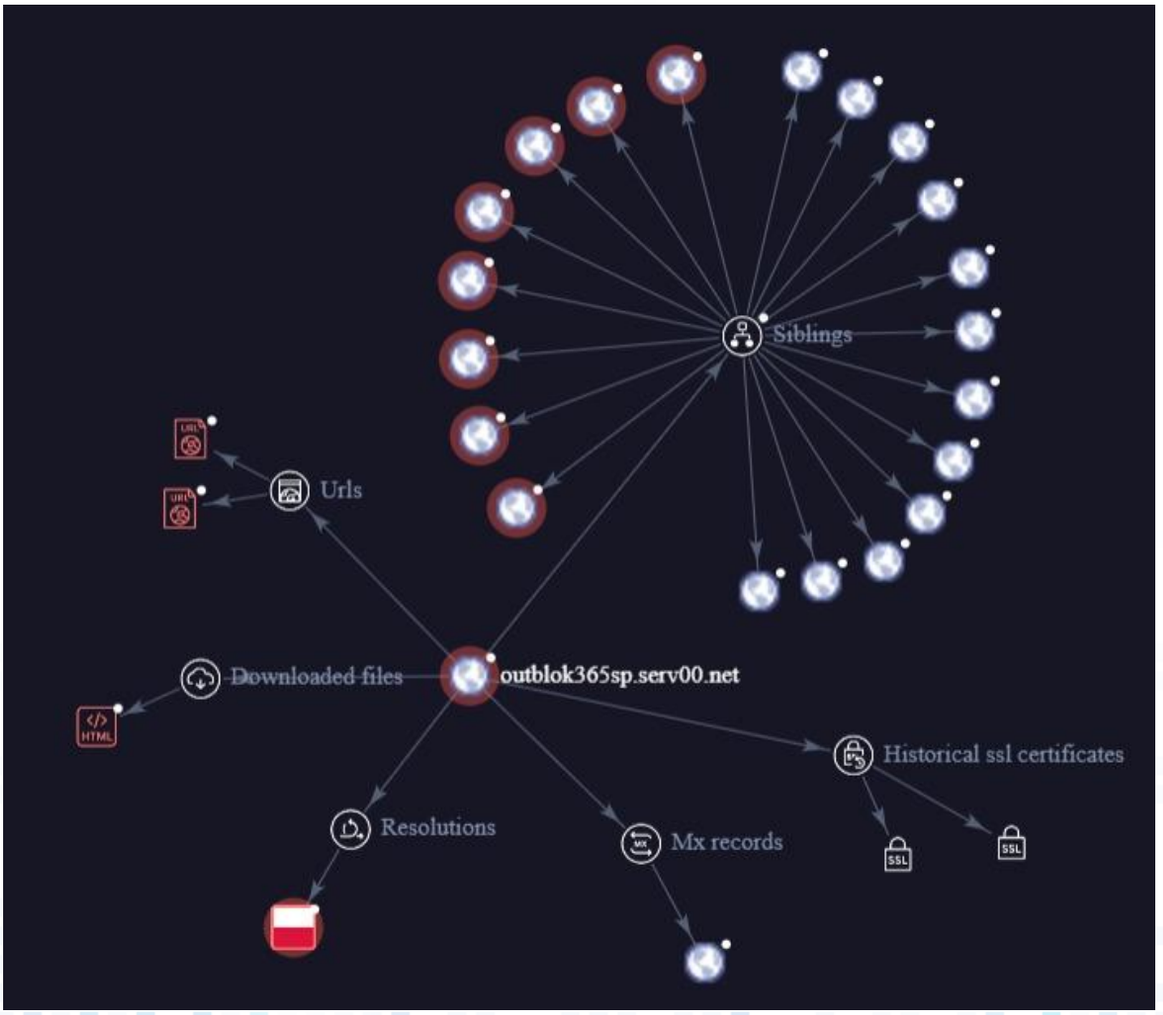
Boletín CNSD-20250830-001 Alerta Campaña de Phishing

Fecha: 20250830

TLP:CLEAR

Análisis y Comportamiento

Los dominios hermanos (siblings) corresponden a otros subdominios o dominios registrados dentro de la misma infraestructura o proveedor, que comparten patrones técnicos como IPs, certificados o registros DNS. Su presencia indica que el actor de amenaza opera un conjunto de dominios maliciosos coordinados, lo que refuerza la hipótesis de una campaña masiva de phishing o distribución de malware basada en la misma red de recursos.



BOLETÍN COMITÉ NACIONAL DE SEGURIDAD DIGITAL

Boletín CNSD-20250830-001 Alerta Campaña de Phishing

Fecha: 20250830

TLP:CLEAR

Análisis y Comportamiento

Los siguientes son los subdominios o dominios registrados por el mismo proveedor, que se encuentran activos, los cuales van a ser utilizados en campañas nuevas de phishing. Asimismo, se listan los dominios que ya fueron suspendidos.

Se recomienda validar esta información con los administradores de plataformas de seguridad perimetral y tenant para poner en vigilancia y monitoreo los dominio activos de manera permanente e identificar trafico hacia los dominios suspendidos.

Dominios activos

Name: 0nlin30ficce.serv00.net
Name: 0xzain.serv00.net
Name: 06xinika.serv00.net
Name: 10mfxx.serv00.net
Name: 0shorturi.serv00.net
Name: 113da.serv00.net
Name: 02verifing.serv00.net
Name: 13th.serv00.net
Name: 1661c.serv00.net
Name: 13sasd.serv00.net
Name: 123asd789.serv00.net
Name: 1637045610a.serv00.net

Dominios suspendidos

Name: 02creditcheck.serv00.net
Name: 02admin01.serv00.net
Name: 01deutsche-de.serv00.net
Name: 001cancelar-ya.serv00.net
Name: 000note.serv00.net
Name: 05admin0info01.serv00.net
Name: 0utcopilotv.serv00.net
Name: 0nlin30ficce.serv00.net

Hallazgos principales

Dominio maliciosos identificados: **outlvloog[.]kesug[.]com**, categorizado como Phish.LIVE.DTI.URL. Se observa un intento de suplantación probablemente asociado a correos de phishing.

Artefactos maliciosos asociados: http://outlvloog[.]kesug[.]com/ http://outlvloog[.]kesug[.]com/aes[.]js - http://outlvloog[.]kesug[.]com/?i=1

Dominio adicional en uso: suspended-domain[.]net (detectado en las comunicaciones DNS).

Infraestructura de terceros involucrada: referencias a cdnjs[.]cloudflare[.]com, cdn[.]tailwindcss[.]com y fonts[.]gstatic[.]com, posiblemente usados para camuflar tráfico malicioso entre servicios legítimos.

BOLETÍN COMITÉ NACIONAL DE SEGURIDAD DIGITAL

Boletín CNSD-20250830-001 Alerta Campaña de Phishing

Fecha: 20250830

TLP:CLEAR

Se ha identificado que los atacantes usan plataformas como Weebly para crear rápidamente sitios de phishing, evadiendo los firewalls que clasifican estos dominios como seguros. Esta táctica permite que los correos maliciosos lleguen a las bandejas de entrada, desde donde se propagan internamente a través de los contactos de la víctima.

- ❑ **weebly.com/co**
- ❑ **confirmar-cuenta-29a.weebly.com**
- ❑ **confirmar-cuenta-29m.weebly.com**

Mapeo MITRE ATT&CK

Initial Access: Drive-by Compromise.

Execution: Malicious Link.

Persistence & Privilege Escalation: Windows Service / Modify Registry.

Defense Evasion: Registry modification.

Discovery: System Service Discovery.

C2: uso de External Proxy, DNS, DGA.

Esto muestra una cadena de ataque orientada a enganchar a la víctima mediante phishing y posteriormente mantener persistencia en el sistema.

Indicadores de Compromiso (IoCs) Dominios

outlvloog[.]kesug[.]com

suspended-domain[.]net

Direcciones IP: 185[.]27[.]134[.]95

Recursos HTTP solicitados: /, /aes.js, /?i=1

BOLETÍN COMITÉ NACIONAL DE SEGURIDAD DIGITAL

Boletín CNSD-20250830-001 Alerta Campaña de Phishing

Fecha: 20250830

TLP:CLEAR

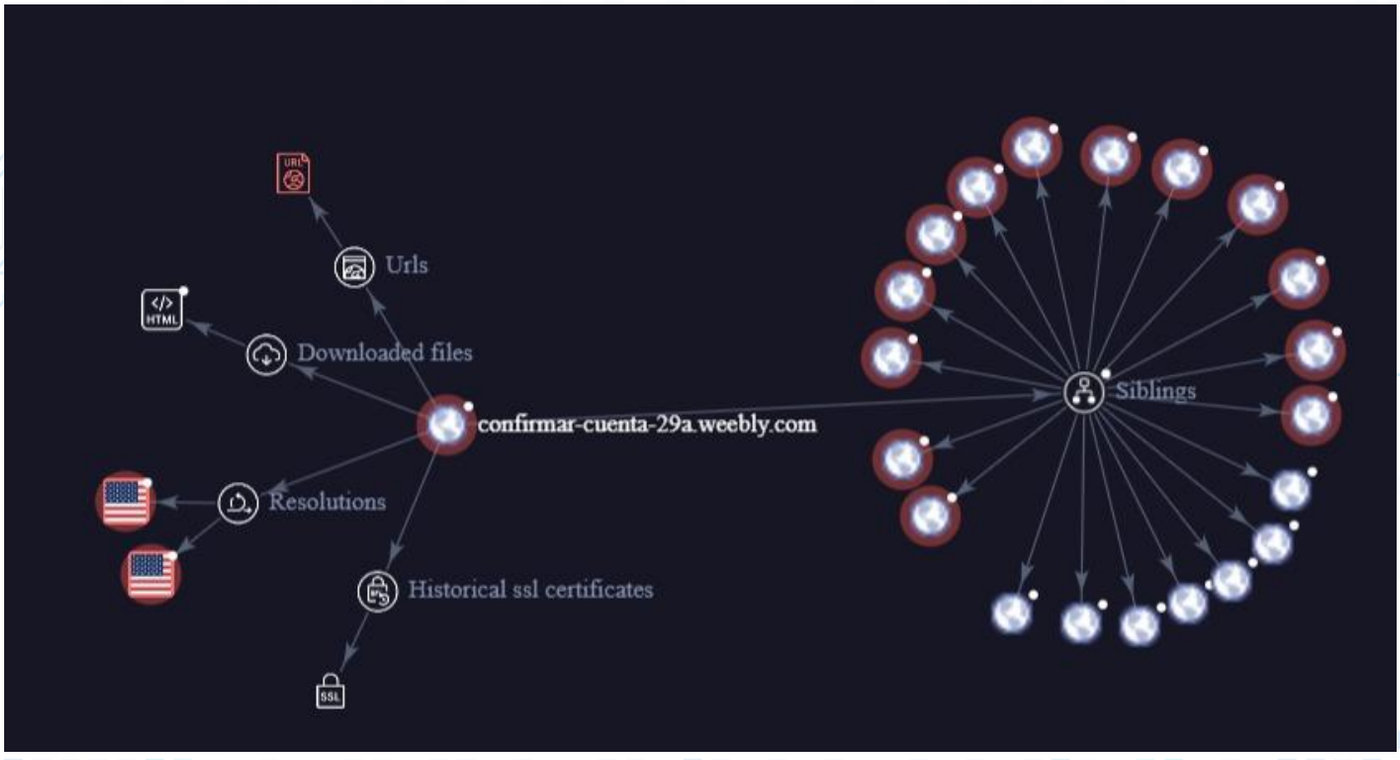
Análisis y Comportamiento

Se ha identificado que los atacantes usan igualmente plataformas como Weebly para crear rápidamente sitios de phishing, evadiendo los firewalls que clasifican estos dominios como seguros. Esta táctica permite que los correos maliciosos lleguen a las bandejas de entrada, desde donde se propagan internamente a través de los contactos de la víctima.

weebly.com/co

confirmar-cuenta-29a.weebly.com

confirmar-cuenta-29m.weebly.com



BOLETÍN COMITÉ NACIONAL DE SEGURIDAD DIGITAL

Boletín CNSD-20250830-001 Alerta Campaña de Phishing

Fecha: 20250830

TLP:CLEAR

Análisis y Comportamiento

Los siguientes son los subdominios o dominios registrados en la plataformas Weebly, así las cosas se recomienda validar con sus administradores de plataformas de seguridad perimetral y tenant para poner en vigilancia y monitoreo los dominio activos de manera permanente e identificar tráfico hacia los dominios suspendidos.

.

Dominios activos

0-range-fr-doc-cijoint.weebly.com
0-yahoo-mail.weebly.com
0-model-store.weebly.com
0-gluten-vege-brest.weebly.com
0-6packabsreview.weebly.com
0-cycu.weebly.com
00-6653-33678-86952-8779.weebly.com

Dominios suspendidos

confirmar-cuenta-29a.weebly.com
00-00-00.weebly.com
00-11.weebly.com
0-att.weebly.com
0-amazon.weebly.com
0-0nlinebanking-rbc-verify-details.weebly.com
00-1529.weebly.com
00-023.weebly.com
0-utl00k.weebly.com
00-002.weebly.com
00-0002.weebly.com
0-yahoo-com.weebly.com
0-att-login.weebly.com
0-m2.weebly.com

Recomendaciones

Dominio maliciosos identificados: **confirmar-cuenta-29a.weebly.com - weebly.com/co confirmar-cuenta-29m.weebly.com**.

- Validar el bloqueo de inmediato de las direcciones web asociadas al dominio Weebly.
- Configurar los correos electrónicos para que eviten la conversión de texto a enlaces.
- Utilizar herramientas que detecten y bloqueen automáticamente enlaces sospechosos.
- Informar y capacitar a todas las personas sobre cómo identificar este tipo de ataques.
- Ajustar la configuración de los sistemas de correo corporativo para optimizar los filtros de protección.
- Utilizar sistemas de seguridad avanzados para detectar accesos a dominios de alto riesgo.

BOLETÍN COMITÉ NACIONAL DE SEGURIDAD DIGITAL

Boletín CNSD-20250830-001 Alerta Campaña de Phishing

Fecha: 20250830

TLP:CLEAR

Recomendaciones

1. Bloqueo de los dominios e IPs identificados en firewalls, DNS y proxies.
2. Monitoreo en SIEM de consultas DNS y tráfico HTTP hacia los IoCs listados.
3. Campaña de concientización sobre phishing: la similitud del dominio outlvloog busca confundir con “outlook”.
4. Verificación de endpoints para asegurar que no existan persistencias por modificación de servicios de Windows.
5. Correlación con otras fuentes CTI/OSINT para verificar si la infraestructura está relacionada con campañas activas en LATAM.
6. Validar las recomendaciones de seguridad publicadas las plataformas de correo electrónico:

   https://learn.microsoft.com/es-es/defender-office-365/anti-phishing-protection-tuning

   Cómo defenderse de los ataques de malware y phishing | Google Workspace Blog

7. Solicitar al equipo ColCERT través del buzón contacto@colCERT.gov.co charlas virtuales de concienciación sobre phishing para colaboradores, funcionarios y contratistas.

Fuentes

- ❑ CSIRT Salud – alertas CSIRTSALUD-AL-2025089-23 -CSIRTSALUD-AL-20250830-24
- ❑ CSIRT Defensa – alerta Alerta Campaña Masiva Phishing 30082025
- ❑ Trellix IVX Cloud – Dynamic Analysis Report ID: 0dd8bc83-5edd-421a-aeb7-266bf37cac16 (2025).
- ❑ MITRE ATT&CK® Framework. https://attack.mitre.org/
- ❑ CISA – Alertas sobre phishing y bloqueo de IoCs. https://www.cisa.gov/
- ❑ VirusTotal – Verificación de indicadores de compromiso. https://www.virustotal.com/
- ❑ URLScan.io – Análisis de comportamiento de URLs maliciosas. https://urlscan.io/
- ❑ Cloudflare Security Blog – Abuso de servicios legítimos en campañas de phishing.