ALERTA

Análisis de Malware

[COLCERT AL-0520-025]

TLP:CLEAR

Se ha identificado actividad maliciosa en el sitio web **http[:]//fase[.]daderam[.]com**, que contiene varios tipos de malware como virus, gusanos, troyanos, spyware y ransomware, dirigidos a entidades públicas y privadas , usando la **IP 172[.]67[.]150[.]183.**

Detalles técnicos

- Sitio Web: http://fase.daderam.com/
- Estado HTTP: 200 (Sitio operativo y accesible).
- Protección CDN: Cloudflare.
- Proveedores de Seguridad que Detectaron Malware: Antiy-AVL, Avira, BitDefender, CyRadar, G-Data, Trellix, Kaspersky, Sophos, VIPRE.
- Malware Detectado: Virus, gusanos, troyanos, spyware, ransomware.

Indicadores de Compromiso

Tipo	Valor
IP	172[.]67[.]150[.]183
URL	http[:]//fase[.]daderam[.]com
MD5	2BD6383862F47A7AE640C6496C374C1B7
SHA1	71249106169AA025BF0188768A4751310C15A5A8
SHA256	F20618995451AA5F9D320A96D2BA4D0CC1FFB0C3729B4292O27F6208AD72DBF

Recomendaciones:

- Implementar bloqueos a nivel de firewall para http://fase.daderam.com/ y URLs asociadas.
- Usar herramientas actualizadas de detección de malware.
- Capacitar a usuarios sobre los riesgos y cómo reconocer amenazas.
- Asegurar que antimalware, antivirus y firewalls estén actualizados.
- Desarrollar y practicar un plan de respuesta para incidentes de seguridad.
- Realizar auditorías de seguridad y evaluaciones de vulnerabilidades.
- Usar entornos de sandboxing y aplicar análisis forense en caso de incidentes.
- Realizar revisión periódica de precursores e indicadores en los diferentes dispositivos de seguridad e infraestructura.

Impacto Potencial

- Exfiltración de información sensible mediante keylogging, ram scraping, backdoors y ransomware.
- Consumo excesivo de CPU y memoria RAM, saturación del ancho de banda.
- Pérdida de confianza del cliente, impacto negativo en el valor de marca, posibles sanciones regulatorias.

Manténgase alerta y siga las mejores prácticas de seguridad para proteger nuestros sistemas y datos.

NIVEL DE RIESGO

Alto

FUENTES:

1. https://umbrella.cisco.com/
2. https://www.virustotal.com/
3. https://www.kaspersky.es/blog/
4. https://developers.cloudflare.com/

COLCERT