# ALERTA DE SEGURIDAD

## Contenido

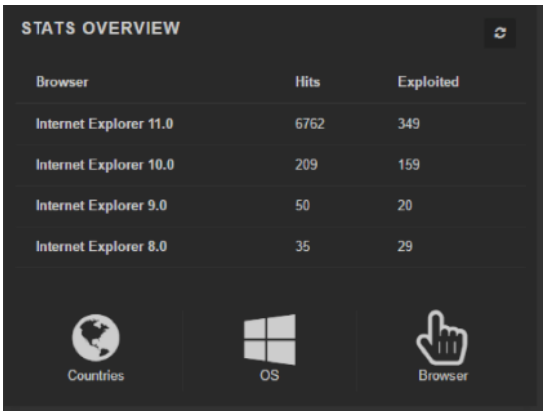
## NIVEL DE ALERTA

Muy Alta

## DESCRIPCIÓN DE LA AMENAZA

El **Centro de Seguridad y Vigilancia Digital** de A3SEC ha sido alertado sobre un Kit de Exploits, descubierto por el investigador de seguridad peruano David Montenegro, el exploit kit llamado **Disdain**, está disponible para alquiler en una base diaria, semanal o mensual. Los precios son $ 80, $ 500 y $ 1.400, respectivamente.

**Disdain** se aprovecha de vulnerabilidades conocidas que se encuentran en un navegador desactualizado o complementos desactualizados del navegador de la víctima; **Disdain** está alojado en un servidor remoto, al cual transfiere la información de la víctima a un servidor malicioso. Cuando una víctima entra en contacto con el servidor malicioso, el kit escanea el explorador para encontrar vulnerabilidades explotables y luego toma ventaja de ellas para ejecutar remotamente malware.



## NAVEGADORES AFECTADOS

Disdain explota las siguientes vulnerabilidades:

| CVE | Objetivo |
|---|---|
| CVE-2017-5375 | Firefox |
| CVE-2017-0037 | Internet Explorer |
| CVE-2016-9078 | Firefox |
| CVE-2016-7200 | Edge e Internet Explorer |
| CVE-2016-4117 | Flash |
| CVE-2016-1019 | Flash |
| CVE-2016-0189 | Internet Explorer |
| CVE-2015-5119 | Flash |
| CVE-2015-2419 | Internet Explorer |
| CVE-2014-8636 | Firefox |
| CVE-2014-6332 | Internet Explorer |
| CVE-2014-1510 | Firefox |
| CVE-2013-2551 | Internet Explorer |
| CVE-2013-1710 | Firefox |
| CVE-2017-3823 | Extensión (Cisco Web Ex) |

## INDICADORES DE COMPROMISO

Conexiones hacia el siguiente dominio

http://layer7.site

## ACCIONES RECOMENDADAS

- Actualizar los navegadores utilizados en su organización a su última versión.
- Deshabilitar el uso de extensiones innecesarias en los navegadores.
- Fortinet
    - https://fortiguard.com/encyclopedia/ips/43660/ms-ie-columnspanning-element-handling-memory-corruption
    - https://fortiguard.com/search?q=CVE-2017-5375&engine=3
    - https://fortiguard.com/search?q=CVE-2016-9078&engine=3
    - https://fortiguard.com/search?q=CVE-2013-1710&engine=1
- Symantec
    - https://www.symantec.com/security_response/writeup.jsp?docid=2015-070910-1625-99
    - https://www.symantec.com/security_response/writeup.jsp?docid=2016-052709-3632-99
    - https://www.symantec.com/security_response/writeup.jsp?docid=2016-040806-5155-99&tabid=2
- Rapid 7 (InsightVM)
    - https://www.rapid7.com/db/vulnerabilities/cisco-webex-cisco-sa-20170124-cve-2017-3823
    - https://blog.rapid7.com/2015/03/23/r7-2015-04-disclosure-mozilla-firefox-proxy-prototype-rce-cve-2014-8636/
    -

## REFERENCIAS

**NOTICIA:** Nuevo Exploit Kit Disdain afecta organizaciones a nivel mundial.
http://blog.trendmicro.com/trendlabs-security-intelligence/new-disdain-exploit-kit-detected-wild/
https://www.theregister.co.uk/2017/08/16/disdain_exploit_kit/