RANSOMWARE SATURNO

Bogotá D.C; Colombia, 13 de Marzo de 2018

CONFIDENCIAL

RANSOMWARE SATURNO

NIVEL DE ALERTA

Critico

DESCRIPCIÓN DE LA AMENAZA

El **Centro de Seguridad y Vigilancia Digital** de A3SEC ha sido alertado sobre un nuevo ramsomware llamado **"Saturno",** trabaja como **Ransomware as a Service** y cuando aterriza en una máquina, en primer lugar determina si se está ejecutando dentro de un entorno virtual de análisis (Sandboxing). Si lo determina, saldrá del proceso para evitar la captura; mientras que si determina que ha aterrizado en un entorno real, intenta eliminar copias de volúmenes ocultos, desactivar la reparación de inicio de Windows y también borrar el catálogo de copias de seguridad.

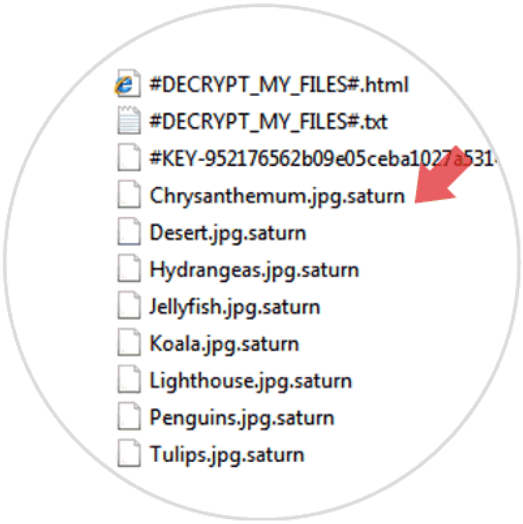
DISPOSITIVOS Y PLATAFORMAS AFECTADOS

El principal sistema operativo de ataque del virus es **Windows** en todas sus plataformas y se caracteriza por cambiar los archivos a la extensión **.saturn**; las extensiones afectadas son:

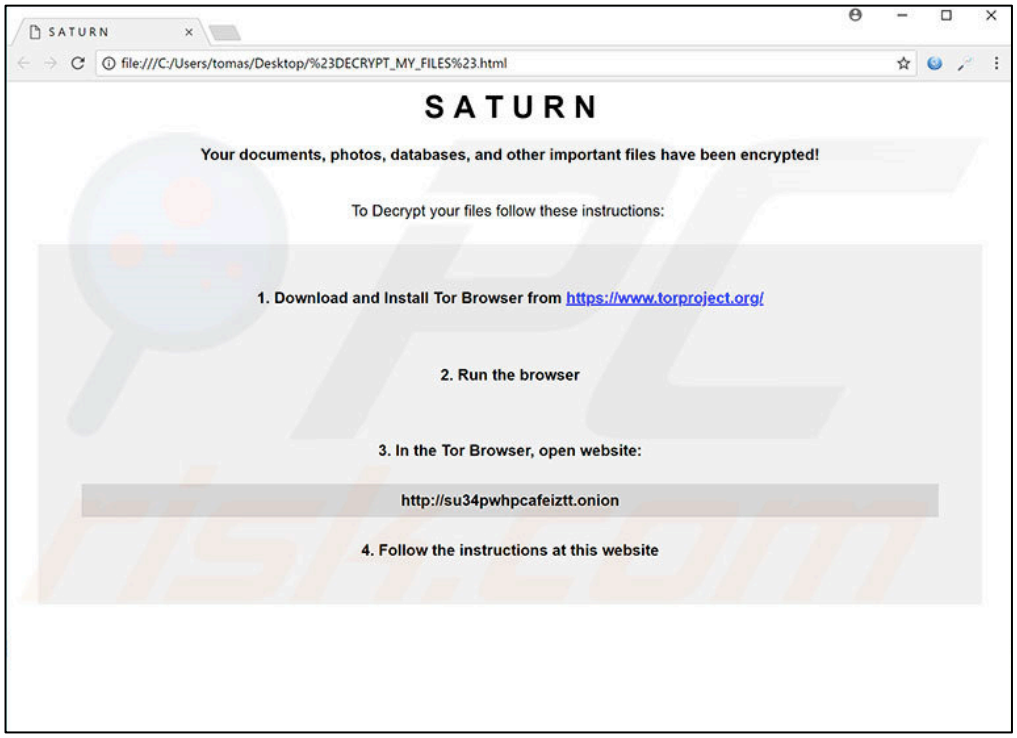
txt, psd, dwg, pptx, pptm, ppt, pps, 602, csv, docm, docp, msg, pages, wpd, wps, text, dif, odg, 123, xls, doc, xlsx, xlm, xlsb, xlsm, docx, rtf, xml, odt, pdf, cdr, 1cd, sqlite, wav, mp3, wma, ogg, aif, iff, m3u, m4a, mid, mpa, obj, max, 3dm, 3ds, dbf, accdb, sql, pdb, mdb, wsf, apk, com, gadget, torrent, jpg, jpeg, tiff, tif, png, bmp, svg, mp4, mov, gif, avi, wmv, sfk, ico, zip, rar, tar, backup, bak, ms11, ms11 (Security copy), veg, pproj, prproj, ps1, json, php, cpp, asm, bat, vbs, class, java, jar, asp, lib, pas, cgm, nef, crt, csr, p12, pem, vmx, vmdk, vdi, qcow2, vbox, wallet, dat, cfg, config

La amenaza deja 3 archivos:

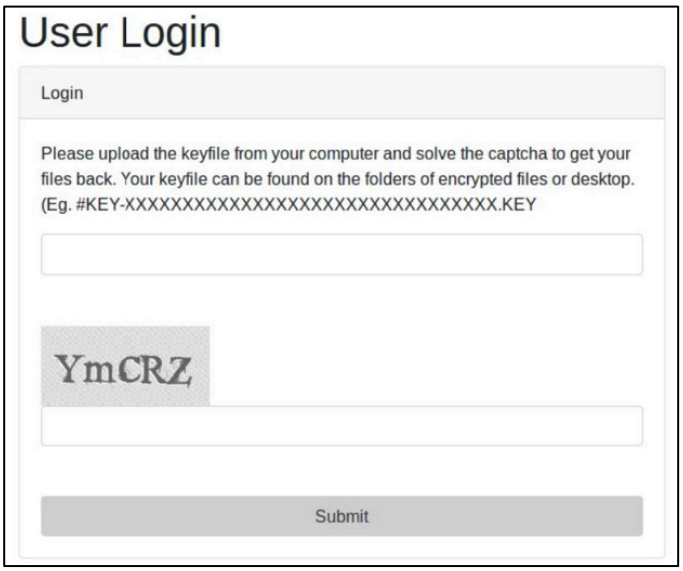
- #DECRYPT_MY_FILES#.html
- #DECRYPT_MY_FILES#.txt
- #KEY-[id asociada al equipo afectado].KEY



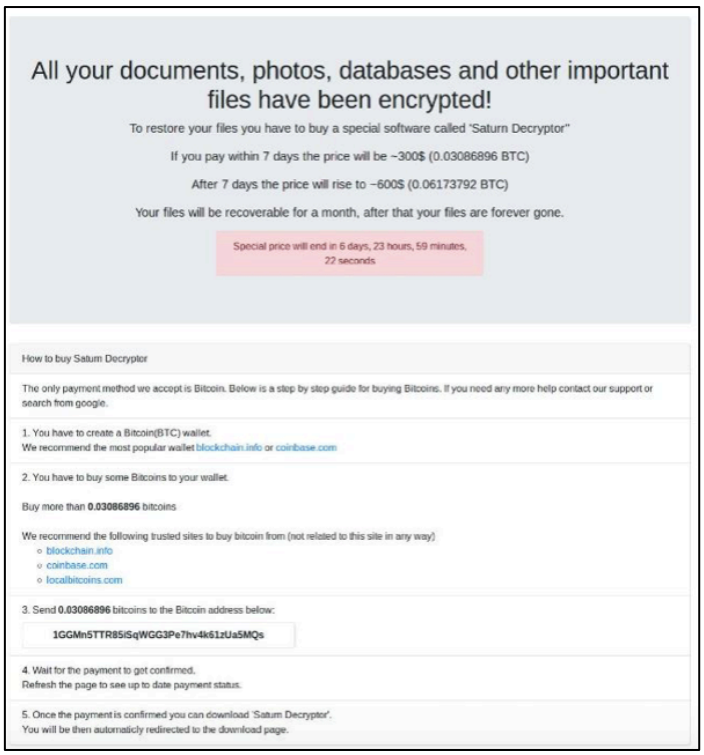
Estos archivos contienen las instrucciones para realizar el pago a un monedero perteneciente a un servicio de la red TOR. El archivo .KEY será utilizado cuando el usuario acceda al servicio, siendo necesario para acceder a la sección personal en la que se realizará el pago de la cantidad demandada.



Despues de que las victimas logran abrir la página del ransomware, se muestra el siguiente inicio de sesión.



En el formulario se solicita a las victimas que ingresen su respectiva llave, con el proposito de identificarlos y brindarles accesos a las instrucciones de rescate.



CVEs IDENTIFICADOS:

En la actualidad no se referencian CVEs del malware que aprovechen una vulnerabilidad para su propagación.

ACTUALIZACIONES

Muchas de las consolas de antivirus ya detectan el ransomware y generaron la actualizaciones de seguridad para sus clientes, por tanto, se recomienda que realice la actualización de su antivirus a la ultima versión con el fin de contar con un listado actual de firmas.

RECOMENDACIONES

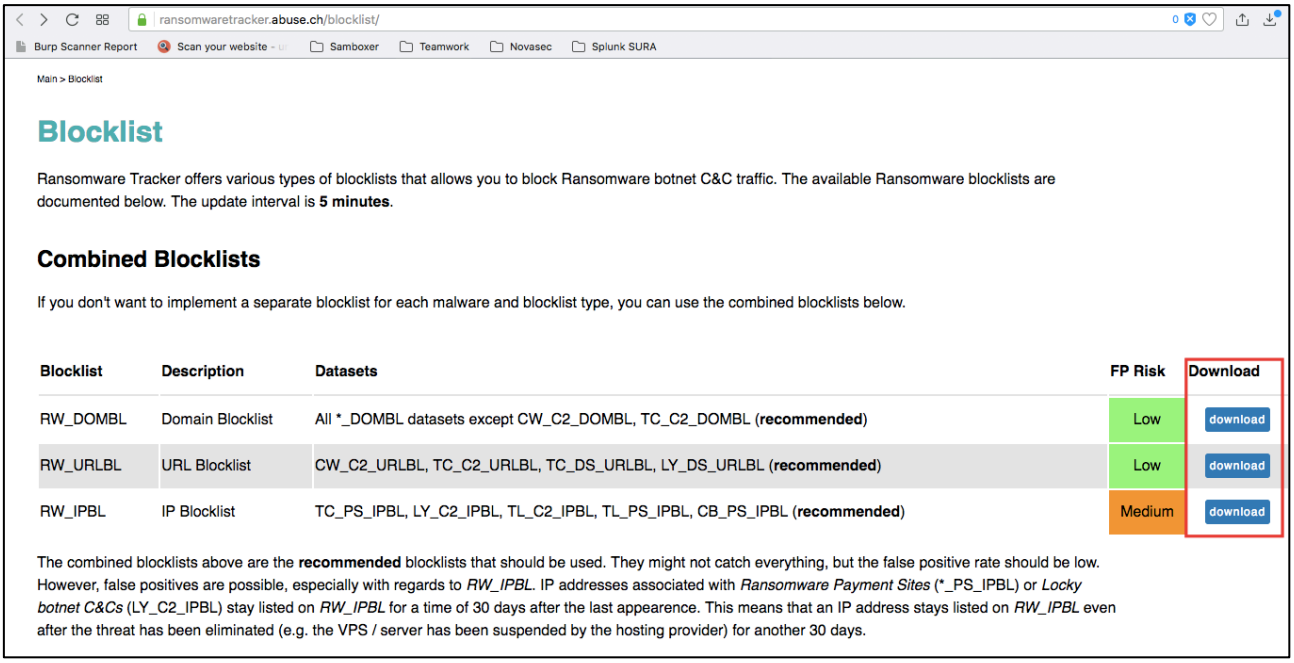
Las formas más comunes para la propagación del virus son las siguientes:

- Correos basura
- Fuentes de descarga de terceros
- Herramientas de actualización de software fraudulentas y troyanos.

Algunos mensajes de correo basura contienen adjuntos maliciosos (p. ej. documentos MS Office, archivos JavaScript, etc.) que cuando se abren, descargan e instalan malware. Fuentes de descarga no oficiales propagan el software malicioso a través de ejecutables maliciosos como software legítimo. Se engaña a los usuarios para que descarguen e instalen software malicioso. Las herramientas de actualización de software falso infectan el sistema aprovechándose de errores en versiones de software antiguas o instalando malware en vez de la aplicación seleccionada. Los troyanos son los más simples; solo abren "puertas" para que entren otros programas maliciosos en el sistema. Para la no propagación del virus se recomienda que:

1. Descargue y actualice los archivos requeridos de los **sitios web oficiales**.
2. Tenga cuidado cuando hace clic, descarga o abre cualquier archivo y correo electrónico.
3. Respalde archivos importantes regularmente.
4. Mantenga su consola de antivirus actualizado a la ultima versión.

Adicional, es posible que el virus se conecte mediante dominios, url´s y direcciones ip especificos para ejecutar el proceso de cifrado, se recomienda que se genere el bloqueo de los dominios, url y direcciones ip compartidas y mantener la lista actualizada de la fuente (*Adjunto al documento se encuentran las listas actualizadas a 2018-03-13 14:05:01 UTC*)



ransomwaretracker.abuse.ch/blocklist/

Burp Scanner Report | Scan your website | Samboxer | Teamwork | Novasec | Splunk SURA

Main > Blocklist

Blocklist

Ransomware Tracker offers various types of blocklists that allows you to block Ransomware botnet C&C traffic. The available Ransomware blocklists are documented below. The update interval is **5 minutes**.

Combined Blocklists

If you don't want to implement a separate blocklist for each malware and blocklist type, you can use the combined blocklists below.

Blocklist	Description	Datasets	FP Risk	Download
RW_DOMBL	Domain Blocklist	All *_DOMBL datasets except CW_C2_DOMBL, TC_C2_DOMBL (**recommended**)	Low	download
RW_URLBL	URL Blocklist	CW_C2_URLBL, TC_C2_URLBL, TC_DS_URLBL, LY_DS_URLBL (**recommended**)	Low	download
RW_IPBL	IP Blocklist	TC_PS_IPBL, LY_C2_IPBL, TL_C2_IPBL, TL_PS_IPBL, CB_PS_IPBL (**recommended**)	Medium	download

The combined blocklists above are the **recommended** blocklists that should be used. They might not catch everything, but the false positive rate should be low. However, false positives are possible, especially with regards to *RW_IPBL*. IP addresses associated with *Ransomware Payment Sites* (*_PS_IPBL) or *Locky botnet C&Cs* (LY_C2_IPBL) stay listed on *RW_IPBL* for a time of 30 days after the last appearence. This means that an IP address stays listed on *RW_IPBL* even after the threat has been eliminated (e.g. the VPS / server has been suspended by the hosting provider) for another 30 days.

```
################################################################################
# Ransomware Domain Blocklist (RW_DOMBL)                                       #
# Generated on 2018-03-13 14:15:02 UTC                                         #
#                                                                              #
# For questions please refer to:                                               #
# https://ransomwaretracker.abuse.ch/blocklist/                                #
################################################################################
25z5g623wpqpdwis.onion.to
27c73bq66y4xqoh7.dorfact.at
27lelchgcvs2wpm7.3lhjyx.top
27lelchgcvs2wpm7.7jiff7.top
27lelchgcvs2wpm7.7zv8o2.top
27lelchgcvs2wpm7.9ildst.top
27lelchgcvs2wpm7.adevf4.top
27lelchgcvs2wpm7.ag082d.top
27lelchgcvs2wpm7.apperloads.win
27lelchgcvs2wpm7.asd3r3.top
27lelchgcvs2wpm7.b7mciu.top
27lelchgcvs2wpm7.bedrastic.bid
27lelchgcvs2wpm7.bestfordownload.click
27lelchgcvs2wpm7.bonbestal.asia
27lelchgcvs2wpm7.fm0cga.top
27lelchgcvs2wpm7.h9ihx3.top
27lelchgcvs2wpm7.laverhants.link
27lelchgcvs2wpm7.liopakerb.black
27lelchgcvs2wpm7.marksgain.kim
27lelchgcvs2wpm7.nfgpeb.top
27lelchgcvs2wpm7.redefined.click
27lelchgcvs2wpm7.rt4e34.win
27lelchgcvs2wpm7.tankbe.pro
27lelchgcvs2wpm7.thyx30.top
27lelchgcvs2wpm7.uboys5.top
27lelchgcvs2wpm7.vrid8l.top
27lelchgcvs2wpm7.wins4n.win
27lelchgcvs2wpm7.wishsends.mobi
27lelchgcvs2wpm7.xkfi59.top
```

Fuente Blocklist: *https://ransomwaretracker.abuse.ch/blocklist/*

REFERENCIAS

https://tools.cisco.com/security/center/viewAlert.x?alertId=57126&vs_f=Alert%20RSS&vs_cat=Security%20Intelligence&vs_type=RSS&vs_p=Saturn%20Malware%20Initial%20Download%20Activity&vs_k=1

https://www.virustotal.com/en/file/daea4b5ea119786d996f33895996396892fa0bdbb8f9e9fcc184a89d0d0cb85e/analysis/1517915525/

https://blog.barkly.com/gandcrab-saturn-data-keeper-ransomware-as-a-service-2018

https://www.sequretek.com/saturn-ransomware/

https://www.solvetic.com/page/noticias/s/seguridad/conoce-el-nuevo-ataque-ransomware-con-nombre-de-planeta-saturn

https://ransomwaretracker.abuse.ch/blocklist/

A3SEC. ESPAÑA C/ Aravaca, 6 2º Piso 28040 Madrid, España T.+34 915330978	**A3SEC S.A.S** Carrera 49A # 94-76 Oficina 304 Edificio Empresarial Castellana Bogotá, COLOMBIA **T.**+57 1 3099533	**A3SEC USA** 1401 Brickell Ave #320 Miami, FL 33131, USA T. +1 786 556 90 32	**A3SEC. México** **Gral. Mariano Escobedo, 748 Piso 9 C.P. 11590 México D.F.** **T. +52 (55) 5980-3547**