## I. DATOS GENERALES:

**Clase de alerta:** Incidente
**Tipo de Incidente:** Ransomware
**Nivel de riesgo:** Alta

## II. ALERTA

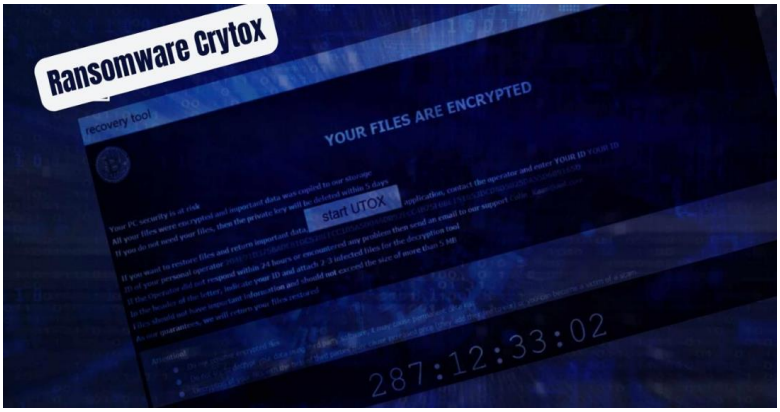



***Figura 1.-*** Ransomware Crytox - figura referencial

Ransomware Crytox instala la aplicación de mensajería uTox en el sistema infectado, lo que permite a la víctima comunicarse y negociar con los autores de la amenaza. Pertenece a la familia de ransomware que consta de varias etapas de código cifrado, a diferencia de otros ejerce presión dejando una nota de rescate con tiempo de comunicación.

## III. INTRODUCCIÓN

Ransomware Crytox identificado desde 2020, cifra archivos en discos locales y en unidades de red sin realizar exfiltración de datos ni doble extorsión. El malware está típicamente empaquetado con UPX o Ultimate Packer for eXecutables (es un compresor de archivos ejecutables de código abierto free and open-source diseñado para reducir el tamaño de archivos binarios como .exe o .dll en Windows, o binarios en Linux/macOS sin afectar su funcionalidad); al desempaquetar el binario libera el embebido de uTox, emplea técnicas de evasión como API hashing, configuraciones cifradas, shellcode cifrado e inyección remota de hilos.

Como método de contacto, este Ransomware Crytox exhibe una nota de rescate con un ultimátum de 5 días.

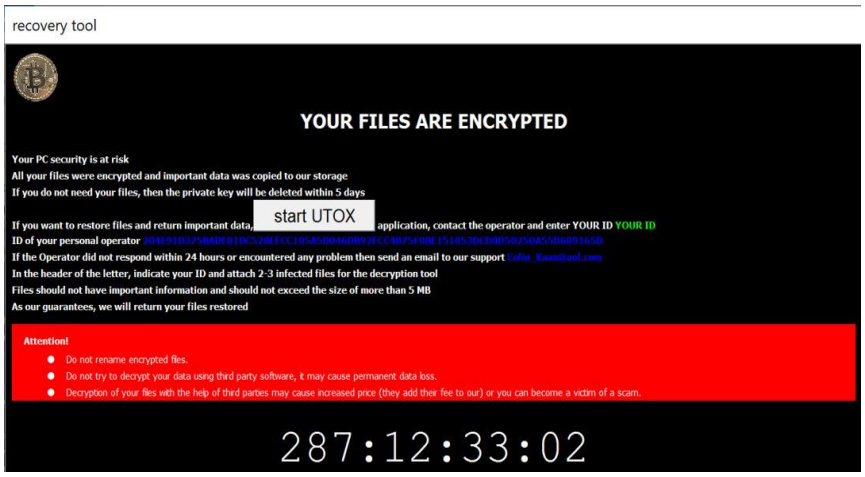



***Figura 2.*** Nota de Rescate - Ransomware Crytox

## IV. VECTOR DE ATAQUE

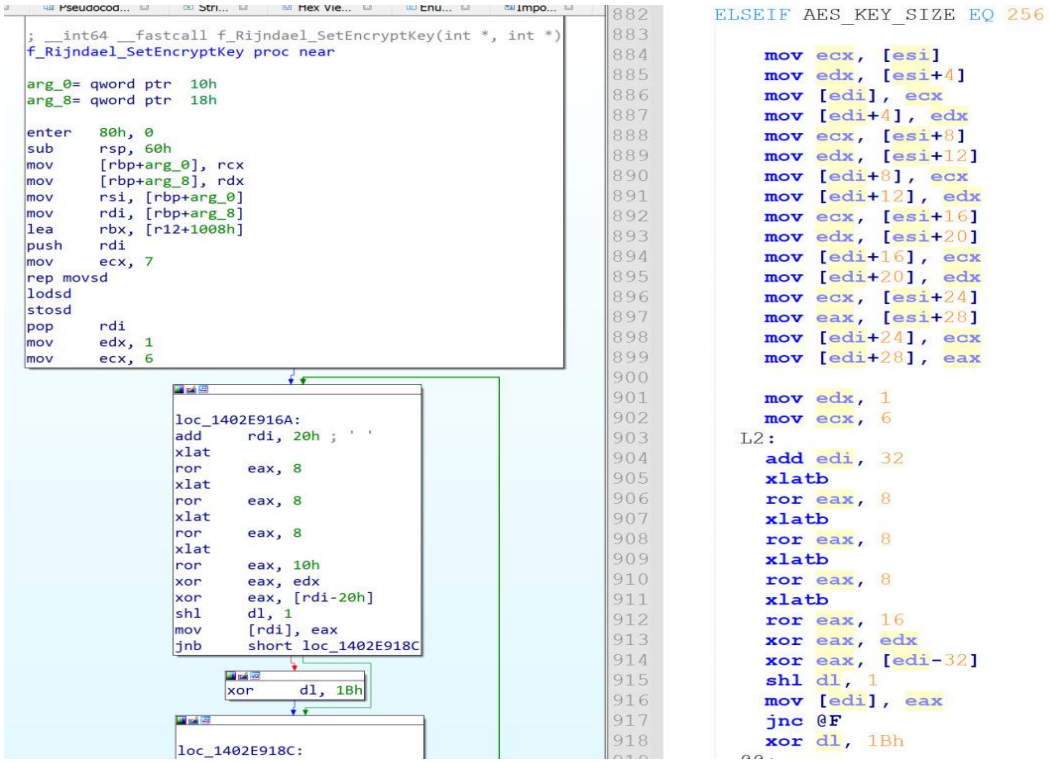
Una muestra analizada por ThreatLabz tiene el siguiente hash SHA256:

32e267a1192a9a9a739ccaaae0266bc6707bb64768a764541ecb039a50cba67

Con esto se determinó que utiliza diferentes técnicas para frustrar el análisis estático, entre las que se incluyen las siguientes:

- Hash de API
- Configuraciones cifradas
- Código shell cifrado
- Inyección remota de subprocesos

Algunas partes del malware parecen estar escritas directamente en lenguaje ensamblador. Lo más destacable es el uso de una implementación específica de AES-CBC, como se muestra en la imagen a continuación:



```
; __int64 __fastcall f_Rijndael_SetEncryptKey(int *, int *)
f_Rijndael_SetEncryptKey proc near

arg_0= qword ptr  10h
arg_8= qword ptr  18h

enter   80h, 0
sub     rsp, 60h
mov     [rbp+arg_0], rcx
mov     [rbp+arg_8], rdx
mov     rsi, [rbp+arg_0]
mov     rdi, [rbp+arg_8]
lea     rbx, [r12+1008h]
push    rdi
mov     ecx, 7
rep movsd
lodsd
stosd
pop     rdi
mov     edx, 1
mov     ecx, 6

loc_1402E916A:
add     rdi, 20h ; ' '
xlat
ror     eax, 8
xlat
ror     eax, 8
xlat
ror     eax, 8
xlat
ror     eax, 10h
xor     eax, edx
xor     eax, [rdi-20h]
shl     dl, 1
mov     [rdi], eax
jnb     short loc_1402E918C

xor     dl, 1Bh

loc_1402E918C:
```

```
ELSEIF AES_KEY_SIZE EQ 256
    mov ecx, [esi]
    mov edx, [esi+4]
    mov [edi], ecx
    mov [edi+4], edx
    mov ecx, [esi+8]
    mov edx, [esi+12]
    mov [edi+8], ecx
    mov [edi+12], edx
    mov ecx, [esi+16]
    mov edx, [esi+20]
    mov [edi+16], ecx
    mov [edi+20], edx
    mov ecx, [esi+24]
    mov eax, [esi+28]
    mov [edi+24], ecx
    mov [edi+28], eax

    mov edx, 1
    mov ecx, 6
  L2:
    add edi, 32
    xlatb
    ror eax, 8
    xlatb
    ror eax, 8
    xlatb
    ror eax, 8
    xlatb
    ror eax, 16
    xor eax, edx
    xor eax, [edi-32]
    shl dl, 1
    mov [edi], eax
    jnc @F
    xor dl, 1Bh
```

***Figura 3***.- Aplicación de la AES - Ransomware Crytox

Se detalla el procedimiento del Ransomware Crytox:

**Primera etapa – Configuración y generación de clave**

Cifra una configuración inicial con AES-CBC usando una clave derivada de la tabla Te1 (es una de las tablas de consulta lookup tables utilizadas en la implementación optimizada del algoritmo AES -Advanced Encryption Standard en su variante de cifrado por bloques como AES-CBC, AES-ECB, etc. Estas tablas son clave para acelerar el proceso de cifrado/descifrado en software), luego genera localmente un par RSA (2048 bits), almacena la clave pública y la privada cifrada con esa clave en el registro de Windows, y establece persistencia mediante entrada en Run Key.

**Segunda etapa**

Al ejecutarse el Ransomware Crytox descifra un archivo de configuración adicional utilizando el algoritmo AES, coloca la aplicación uTox en la ruta especificada en el archivo de configuración e inyecta un shellcode en un proceso nativo de Windows mencionado en la configuración.

Este shellcode elimina las copias de sombra del volumen (VSS Volume Shadow Copies) y luego inyecta otro shellcode en otro proceso nativo, que se ejecuta con un argumento específico en la línea de comandos en procesos que afecta a explorer.ex o svchost.exe. El shellcode final inyectado es el responsable de cifrar los archivos del usuario en el disco, añadiéndoles la extensión **.**waiting**.**

**Etapa final**

Desencripta una configuración final (también por AES-CBC), que incluye un "seed" para la generación de claves, plantilla de nota de rescate (.hta), expresión regular para búsqueda de archivos, extensión cifrada (por ejemplo, **.**waiting) y privilegios para eliminación de backups. Cifra archivos con una clave AES única por archivo, protegida con RSA, y les agrega la extensión **.**waiting. El ID de víctima y la clave AES dependen del valor de GetTickCount, lo que permite un posible ataque de fuerza bruta si se conoce parte del contenido original del archivo (plaintext).

## V. IMPACTO

Hash: 823E4C4E47E8DABE32FC700409A78537
K7 Security Labs Detection Name: Trojan (00564c011)

## VI. INDICADORES DE COMPROMISO

| Hash SHA-256: |
|---|
| 8faa3d285cffaa5a8d2a21cba2bce8d35e47c690cc9ea303bc6b46281479ef53 |
| 1A13D8B891A987C22D67A4BF7645164E23A6730F6534FD6EA0ED7AB76D1AD413 |
| 8721429e0aab024d4306e9d5ac5562acfad17fe9f08aecff1f6c77780b3eefed |
| c418b88bc52442b3469eb882c277aa6ffbf87350887faadaa937baf75df5d5af |
| 1c0bf0c2e7d0c34ec038a8b717bb19d9c4cf3382ada1412f055a9786d3069d78 |
| 2115c4c859d497eec163ca33798c389649543d8a6e4db5806a791c6186722b71 |
| 307c83924e90f4627f08c2f744cf51f18ec6e246687282a0c1794369ff084f42 |
| 3764200cfa673e8796e7c955454b57c20852c2a7931fb9f632ef89d267bbd4c8 |
| 6d4e75bc0cc095fef94b9d98a4e94ce9145890b435012b5624aa73621ba6e312 |
| 79aff06385c16a98594c6fd314c572bfbe07fbe923f30a627e9b86ac3ab7c071 |
| 8ee4a58699ecf02dca516dc6b5b72d93fd9968f672b2be6f8920dfec027d7815 |
| c5550f44332750552921cb5d685ccfbeefa2ab4b03aed8c51c5db52bbe2ff5d4 |
| d60dc6965f6d68a3e7c82d42e90bfda7ad3c5874d2c59a66df6212aef027b455 |
| 0aa9c3d901f7d0447417ca0d7315dec99f1607efd397a660365b3be601ddd882 |

***Tabla 1***.- SHA-256 - Ransomware Crytox

| Direcciones IP: |
|---|
| 185.14.30.213 |
| 2a00:1ca8:a7::e8b |
| 136.243.141.187 |

| Direcciones IP: |
|---|
| 2a01:4f8:212:2459::a:1337 |
| 148.251.23.146 |
| 2a01:4f8:201:8493::2 |
| 193.124.186.205 |
| 2a02:f680:1:1100::542a |
| 130.133.110.14 |
| 2001:6f8:1c3c:babe::14:1 |
| 194.249.212.109 |
| 2001:1470:fbfe::109 |
| 104.223.122.15 |
| 2607:ff48:aa81:800::35eb:1 |
| 51.254.84.212 |
| 2001:41d0:a:1a3b::18 |
| 185.58.206.164 |
| 2a02:f680:1:1100::3313 |
| 195.93.190.6 |
| 2a01:d0:ffff:a8a::2 |
| 95.215.44.78 |
| 2a02:7aa0:1619::c6fe:d0cb |
| 163.172.136.118 |
| 2001:bc8:4400:2100::1c:50f |
| 37.97.185.116 |
| 80.87.193.193 |
| 2a01:230:2:6::46a8 |
| 46.229.52.198 |
| 85.21.144.224 |
| 37.187.122.30 |
| 205.185.116.116 |
| 198.98.51.198 |
| 2605:6400:1:fed5:22:45af:ec10:f329 |
| 104.233.104.126 |
| 195.93.190.6 |
| 185.58.206.164 |
| 205.185.116.116 |
| 37.187.122.30 |
| 85.21.144.224 |
| 46.229.52.198 |
| 51.254.84.212 |
| 104.223.122.15 |
| 80.87.193.193 |
| 37.97.185.116 |
| 163.172.136.118 |
| 95.215.44.78 |
| 130.133.110.14 |
| 194.249.212.109 |
| 130.133.110.14 |
| 194.249.212.109 |
| 198.98.51.198 |
| 193.124.186.205 |
| 148.251.23.146 |

| Direcciones IP: |
|---|
| 37.97.185.116 |
| 194.249.212.109 |
| 130.133.110.14 |
| 51.254.84.212 |
| 198.98.51.198 |
| 195.93.190.6 |
| 185.58.206.164 |
| 205.185.116.116 |
| 85.21.144.224 |
| 46.229.52.198 |
| 104.233.104.126 |
| 193.124.186.205 |
| 104.223.122.15 |
| 95.215.44.78 |
| 163.172.136.118 |
| 80.87.193.193 |
| 37.187.122.30 |
| 195.93.190.6 |
| 185.58.206.164 |
| 205.185.116.116 |
| 37.187.122.30 |
| 85.21.144.224 |
| 46.229.52.198 |
| 51.254.84.212 |
| 104.223.122.15 |
| 80.87.193.193 |
| 37.97.185.116 |
| 163.172.136.118 |
| 95.215.44.78 |

***Tabla 2***.- IPs - Ransomware Crytox

## VII. RECOMENDACIONES:

- Mantener todos los sistemas operativos, aplicaciones y frameworks actualizados con los parches de seguridad más recientes, mitigando vectores de explotación conocidos.

- Inhabilitar macros en documentos de Microsoft Office y scripts automáticos (VBScript, JavaScript) cuando no sean requeridos, minimizando la superficie de ataque.

- Aplicar el principio de menor privilegio (PoLP) en cuentas de usuario y servicios, limitando privilegios administrativos y reduciendo la posibilidad de escalamiento lateral.

- Implementar segmentación lógica de la red, con restricciones de comunicación entre zonas (por ejemplo, producción, usuarios, servidores) y monitoreo de tráfico intersegmentado.

- Revisar y limitar el acceso a carpetas compartidas en red (SMB/NFS), asegurando autenticación y permisos mínimos necesarios.

- Utilizar soluciones EDR/NGAV capaces de detectar técnicas de evasión, incluyendo el empaquetamiento con UPX, API hashing, inyección de código y ejecución en memoria.

- Auditar claves sensibles como HKCU\Software\Microsoft\Windows\CurrentVersion\Run y HKLM\..., identificando persistencias anómalas o manipulaciones maliciosas.

## VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## IX. REFERENCIAS:

**LAKSHMANAN, R. (2025, MAYO 7).** Play Ransomware Exploited Windows CVE-2025-29824 as Zero-Day to Breach U.S. Organization. The Hacker News. https://thehackernews.com/2025/05/play-ransomware-exploited-windows-cve.html

**ZSCALER THREATLABZ (2025).** Technical Analysis of Crytox Ransomware. https://www.zscaler.com/blogs/security-research/technical-analysis-crytox-ransomware

**K7 LABS (2023, JUNIO 1).** Encrypted Chaos: Analysis of Crytox Ransomware. https://labs.k7computing.com/index.php/encrypted-chaos-analysis-of-crytox-ransomware/

**NORDVPN (2025).** Crytox Threat Description. https://nordvpn.com/cybersecurity/threat-center/crytox/