Código	202211067	Fecha	23/12/2022

Ransomware STOP (DJVU)

Recomendaciones técnicas

Sistemas afectados

A la fecha se ha identificado que esta campaña de malware tiene como objetivo los sistemas operativos Windows.

Vulnerabilidades aprovechadas

Los cuadros Recientemente se ha identificado actividad de una nueva importante familia de ransomware denominada DJVU, también conocida como STOP, apareció inicialmente en los titulares en 2018 y desde entonces ha estado atacando a personas de todo el mundo. Está muy extendido en sitios de torrents y otras plataformas en paquetes de software crack y paquetes de adware. El ransomware STOP/DJVU es un troyano que encripta archivos, se infiltra en su computadora de manera invisible y encripta todos sus datos. Deja una advertencia de carta de rescate que exige dinero a cambio de descifrar sus datos y ponerlos a su disposición nuevamente. El malware se entrega a través de aplicaciones descifradas, generadores de claves de aplicaciones de configuración falsas, activadores y actualizaciones de Windows. No utiliza información local como diseños de teclado o configuraciones de zona horaria para evitar infectar a las víctimas en ciertos países; en su lugar, utiliza la información devuelta por una solicitud a https[:]//api.2ip.ua/geo.json.

El algoritmo de criptografía utilizado por STOP/DJVU es AES-256, que es uno de los más utilizados por los grupos de ransomware, si sus archivos se cifraron con una clave de descifrado específica, que es totalmente distinta y no hay otras copias, la triste realidad es que es imposible restaurar la información sin la clave única disponible. El enfoque

principal del grupo son los sistemas operativos Windows.
Dado que DJVU no tiene un método de infección preestablecido, el vector de infección inicial de DJVU puede variar. Esto permite que los actores de amenazas sean extremadamente flexibles en su enfoque, lo que también hace que los signos iniciales

de compromiso sean difíciles de predecir y detectar para los defensores. Debido a que existen tantas variaciones, las extensiones agregadas a los archivos cifrados son variadas, entre las principales están: .eucy, .ckae, .qnty, . ccps, .iips, .avyu, .cuag, .bbbr, .bbbe, .qqqr, .maiv, .bbbw, .yoqs, .qqqe, .qqqw, .maak, .fhkf, .vfgj, .yber, .zaqi, .nqhd, .vgkf, .dehd, .loov entre otros. Después de que invade el sistema, descarga automáticamente varios programas que ayudan al ransomware a cifrar todos los archivos sin ninguna interrupción.

El ransomware DJVU aparece en escena disfrazado de servicios o aplicaciones legítimos, o incluido con archivos de señuelo, para parecer benigno. El grupo de malware también se asocia con otras amenazas, dándoles la opción de descargar e implementar ladrones de información para exfiltrar datos, brindando a los actores de amenazas una segunda forma de beneficiarse a expensas de las víctimas. La nueva variante también incluye varias capas de ofuscación, en un intento de ralentizar la inspección por parte de los investigadores y las herramientas de análisis automatizadas.

DJVU es una familia de ransomware en constante evolución, lo que la convierte en una amenaza frecuente tanto para individuos como para empresas. El malware cuenta con múltiples capas de ofuscación, lo que dificulta su detección y análisis. Esto da como resultado una variedad potente de ransomware que no revela sus verdaderas intenciones hasta que es demasiado tarde.

Remediación

Para mitigar el riesgo de ser afectado por el ransomware STOP/DJVU se recomienda tanto a los usuarios finales como a las organizaciones seguir las siguientes prácticas de seguridad:

- Mantener sus sistemas y motores antivirus actualizados para evitar que atacantes o malware aprovechen vulnerabilidades en el sistema, así como para estar protegidos ante las amenazas más recientes.
- Mantenga una política estricta de respaldo de la información debido a que el objetivo de este tipo de malware son los datos del sistema afectado. Respete la regla 3-2-1 al realizar copias de seguridad de archivos importantes. Esto implica

crear tres copias de seguridad en dos formatos de archivo diferentes, con una de las copias almacenada en una ubicación separada.

- Evite navegar en sitios que puedan comprender contenido malicioso, así como descargar información recibida en correos electrónicos no deseados o de dudosa procedencia.
- Parchee y actualice los sistemas regularmente, es importante mantener los sistemas operativos y las aplicaciones actualizados, evitando que los actores maliciosos exploten las vulnerabilidades del software.
- No comprometas tu seguridad, para evitar malware y otras amenazas, descarga solo a través de enlaces oficiales.
- Absténgase de abrir enlaces y archivos adjuntos de correo electrónico que no sean de confianza sin verificar su autenticidad.
- Proporcione capacitación en ingeniería social y explique a los empleados cómo seguir reglas simples ayuda a evitar incidentes de ransomware. También eduque sobre las mejores prácticas de seguridad de datos, para asegurarse de que estén atentos cuando se trata de identificar y reportar correos electrónicos sospechosos.
- Utilice sistemas de monitoreo y administración de vulnerabilidades para identificar fallas potenciales sin parchear y detectar incidentes en tiempo real. Utilice una solución de tiempo real que pueda detectar y responder automáticamente a los eventos que coincidan con una condición de umbral predefinida, como cuando se copia o cifra x número de archivos dentro de un período de tiempo determinado. Si se cumple la condición de umbral, se ejecutará un script personalizado, que puede deshabilitar cuentas, detener procesos específicos, cambiar la configuración del firewall, apagar el dispositivo/servidor infectado, etc.
- Realice auditorías de ciberseguridad y mitigue las debilidades descubiertas para prevenir ataques en la naturaleza tanto desde una perspectiva interna como externa.
- Aplique el modelo de acceso de "privilegios mínimos" para garantizar que los usuarios obtengan los privilegios mínimos que necesitan para desempeñar su función. Esto incluye revocar permisos de administrador local para cuentas de dominio.

- No realice el pago en caso de ser afectado por un ransomware, debido a que esto no garantiza que la información sea recuperada.

Adicionalmente se recomienda identificar y bloquear en su entorno corporativo y sus dispositivos de seguridad perimetral los siguientes Indicadores de compromiso (IoC's) relacionados al origen de ataques de la explotación de STOP/DJVU.

IoC's

Los IoC's en color rojo se encuentran activos.

Dominios:

- acacaca[.]org
- api.2ip[.]ua
- rgyui[.]top
- mas[.]to
- x1.c.lencr[.]org
- fresherlights[.]com
- uaery[.]top

IPs:

- 1[.]248[.]122[.]240
- 109[.]102[.]255[.]230
- 109[.]98[.]58[.]98
- 114[.]114[.]114[.]114
- 115[.]88[.]24[.]203
- 115[.]88[.]24[.]203
- 116[.]121[.]62[.]237
- 116[.]202[.]5[.]121
- 138[.]36[.]3[.]134
- 149[.]154[.]167[.]99
- 159[.]69[.]102[.]99
- 175[.]119[.]10[.]231
- 175[.]120[.]254[.]9
- 175[.]126[.]109[.]15
- 179[.]53[.]95[.]243

- 186[.]6[.]62[.]174
- 186[.]182[.]55[.]44
- 187[.]190[.]48[.]135
- 189[.]143[.]170[.]233
- 190[.]107[.]133[.]19
- 195[.]158[.]3[.]162
- 196[.]200[.]111[.]5
- 201[.]103[.]222[.]246
- 210[.]182[.]29[.]70
- 211[.]119[.]84[.]111
- 211[.]171[.]233[.]129
- 222[.]232[.]238[.]243
- 222[.]236[.]49[.]124
- 222[.]236[.]49[.]124
- 37[.]34[.]248[.]24
- 41[.]41[.]255[.]235
- 46[.]194[.]108[.]30
- 8[.]8[.]8[.]8

Nameservers:

- ns1[.]kriston[.]ug
- ns2[.]chalekin[.]ug
- ns3[.]unalelath[.]ug
- ns4[.]andromath[.]ug

URLS:

- hxxp[://]116[.]202[.]180[.]202/8069076584[.]zip
- hxxp[://]acacaca[.]org/test1/get[.]php?pid=53B1E5DA52C0B1B73B57A5129A43BC5D&first=true
- hxxp[://]rgyui[.]top/dl/build2[.]exe
- hxxp[://]acacaca[.]org/files/1/build3[.]exe

Direcciones de correo electrónico:

- Support[at]bestyourmail[.]ch
- Datarestorehelp[at]airmail[.]cc

SHA256:

- db41e055496b7eb3dfed7bc50a2afe8636c742a1d0963489569134d9e95aa1fc
- 5fc8f1eddeb98d127899c15663275da4a30b734e0c812ea4ca24fc99023329da
- bd5114b7fcb628ba6f8c5c5d1d47fc7bb16214581079b3cc07273618b0c41fd8
- 5991ce7d26c823874d3439650b6b92e6ea2724df2c8a3ef5e82419600bc0bd42

SHA-1:

- 0adb95ab0ccf8f2de5b7ebb1d363f763db88504c
- 7b3df698434a2a2489500bbdfc79844e5883d8cb
- 8c6ff6f1baab749399afcba7b6bc58de102d1d06
- 0849c94fabdc00cb470cb999ad2d57192c36a330

Hash MD5:

- 1b0c7ba301fc47d3b8c661cbeaa374f7
- 800a40eb8c1f5de6664dabb8c21c01ad
- 2a41808217d5741e34ee4e7c71bc01cc
- 84fe2a8cdefb5f451dd8cf5383201f2a

Referencias

- blogs.blackberry.com/en/2022/09/djvu-the-ransomware-that-seems-strangely-familiar
- https://www.rewterz.com/rewterz-news/rewterz-threat-alert-stop-djvu-ransomware-active-iocs-46
- https://www.pcrisk.es/guias-de-desinfeccion/9152-djvu-ransomware