Alerta i advertència per augment de sistemes infectats per codi maliciós tipus *Ransomware*

CESICAT informa del creixement significatiu de màquines infectades per codi maliciós de tipus *Ransomware.* Aquest tipus de codi maliciós infecta el sistema i xifra el seu contingut amb la finalitat d'extorsionar per a la seva recuperació. L'extorsió, visible mitjançant arxiu de text o accés a pàgina web oberta pel codi maliciós, obliga a pagar un rescat per tal de revertir la situació (desxifrar els fitxers afectats i recuperar l'accés a l'equip).

El pagament del rescat en cap cas assegura que es pugui recuperar l'accés als fitxers xifrats o recuperar l'accés a l'equip. A més, hi ha casos que l'execució de l'aplicació proporcionada per revertir la situació, infecta novament l'equip amb una altra variant de codi maliciós. CESICAT recomana no pagar, en cap cas, el rescat.

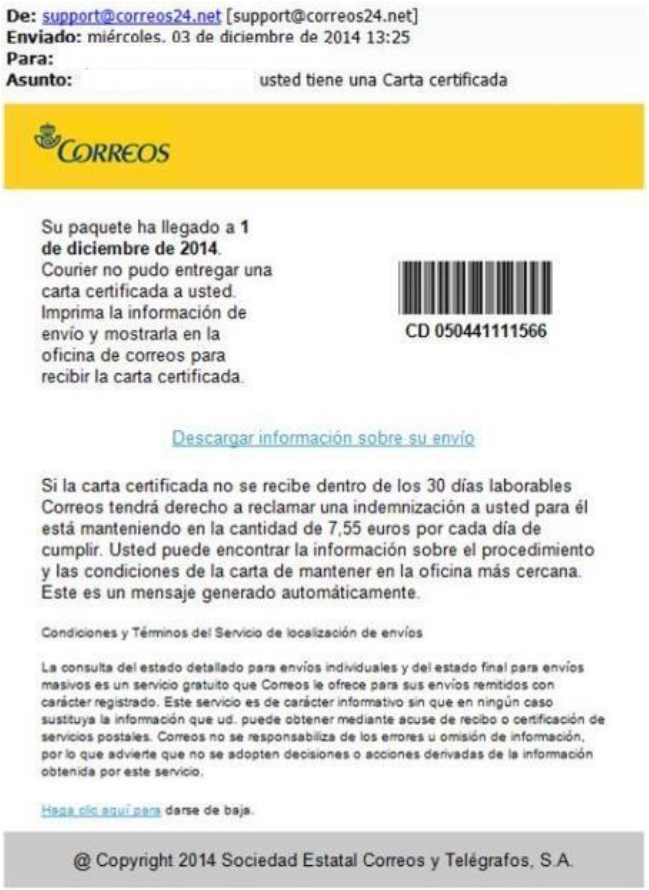
Impacte

Denegació de servei, pèrdua d'accés a l'equip compromès, i contingut de la informació pels fitxers local, dispositius físics o remots connectats a l'equip compromès (Dropbox, GoogleDrive, etc.). Els documents xifrats són de tipus ofimàtic, vídeo, àudio i imatges...

Identificació de l'amenaça

Una de les últimes campanyes detectades es distribueix mitjançant correu electrònic simulant ser remès des de l'operador espanyol de servei postal i paqueteria (CORREOS) indicant que una carta certificada no ha pogut ser entregada al destinatari. Si un usuari realitza els diferents passos indicats al correu electrònic finalment es realitza la descàrrega a l'equip local d'un fitxer ZIP que conté el codi maliciós.

A continuació es mostra un exemple de correu electrònic maliciós enviat des de la bústia electrònica 'support@correos24.net':



De: support@correos24.net [support@correos24.net]
Enviado: miércoles, 03 de diciembre de 2014 13:25
Para:
Asunto: usted tiene una Carta certificada

CORREOS

Su paquete ha llegado a **1 de diciembre de 2014**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.

CD 050441111566

Descargar información sobre su envío

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para él está manteniendo en la cantidad de 7,55 euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado automáticamente.

Condiciones y Términos del Servicio de localización de envíos

La consulta del estado detallado para envíos individuales y del estado final para envíos masivos es un servicio gratuito que Correos le ofrece para sus envíos remitidos con carácter registrado. Este servicio es de carácter informativo sin que en ningún caso sustituya la información que ud. puede obtener mediante acuse de recibo o certificación de servicios postales. Correos no se responsabiliza de los errores u omisión de información, por lo que advierte que no se adopten decisiones o acciones derivadas de la información obtenida por este servicio.

Haga clic aquí para darse de baja.

@ Copyright 2014 Sociedad Estatal Correos y Telégrafos, S.A.

Productes Afectats

Sistemes operatius Microsoft Windows

Prevenció

Amb la sofisticació dels mecanismes d'infecció i xifrat utilitzats per les noves variants, les mesures de prevenció cobren molta més importància amb la finalitat de reduir l'impacte produït pel compromís de l'equip per aquest tipus de codi maliciós.

Còpies de seguretat

Aquesta és sens dubte la mesura de seguretat més important per als casos de *ransomware*. Si es disposa de còpies de seguretat actualitzades, l'impacte d'aquest tipus de *malware* és veu reduït pràcticament a zero. En el pitjor dels casos, seria necessària la restauració del sistema al seu estat original, reinstal·lant el sistema operatiu i copiant els documents i altres dades des d'una còpia de seguretat.

Alguns consells a l'hora de configurar les còpies de seguretat:

- Realitzar-ne amb tanta freqüència com sigui possible.
- Comprovar la efectivitat periòdicament. Moltes vegades es deixa de banda aquest pas fins que a l'hora de recuperar les dades, es descobreix que les còpies no són vàlides.
- Tenir les còpies de seguretat duplicades, amb una còpia secundària emmagatzemada en un lloc físicament separat de la còpia principal.
- Emmagatzemar les còpies en un mitjà desconnectat del servidor. Les últimes variants de *ransomware* busquen còpies de seguretat accessibles des del servidor compromès i les inutilitzen.

Securització de navegador i plugins

- Mantenir actualitzat el navegador.
- Mantenir actualitzats els plugins del navegador: Java, Adobe Flash, Adobe Reader (PDF). Per comprovar si els tenim actualitzats es pot utilitzar la següent pàgina:
- https://www.mozilla.org/es-ES/plugincheck/
- Desactivar l'execució automàtica de connectors de navegador, i utilitzar la funcionalitat "clic to play".

Recomanacions generals en cas d'infecció

Per tal de tenir alguna possibilitat de recuperar els fitxers:

1. Si és possible, apagar el sistema afectat el més aviat possible, fins i tot desendollant el cable de corrent. El xifrat de fitxers és un procés llarg, si s'aconsegueix aturar-lo aviat, és possible que la majoria dels fitxers continuïn intactes.
2. Assegurar la preservació de les evidències per tal de que puguin arribar a ser utilitzades en d'un procés judicial.
3. No intentar desinfectar la màquina immediatament, esborrant fitxers sospitosos o formatant la màquina. Es podrien perdre fitxers necessaris per trencar el xifrat dels fitxers.
4. Identificar tota la informació disponible en relació a la variant de r*ansomware*. Els mecanismes de desxifrat són molt específics per a cada tipus de codi maliciós, i utilitzar una eina inadequada pot impedir que es puguin desxifrar els arxius modificats.
5. Notificar l'incident de seguretat a CESICAT-CERT per correu electrònic a l'adreça cert@cesicat.cat, o mitjançant el telèfon de contacte 902 112 444, facilitant tota la informació recopilada com per exemple, captures de pantalla, extensió dels fitxers xifrats o l'arxiu de text amb les instruccions per realitzar el pagament.

Descripció

Ransomware és un tipus de codi maliciós que és capaç de fer-se amb el control d'un equip i denegar l'accés al mateix amb la finalitat de treure benefici econòmic mitjançant el pagament d'un "rescat".

Encara que aquest tipus de codi maliciós no és nou, recentment ha gaudit d'un augment molt important tant en el nombre de variants com en la quantitat d'usuaris afectats. Actualment és una de les principals amenaces a la xarxa per al ciutadà i les empreses, i els estudis de tendències indiquen que anirà agafant més importància en un futur pròxim.

Característiques generals que presenten aquest tipus de codi maliciós:

- Bloqueig de la pantalla: Fent que un usuari no pugui executar res en el sistema.
- Xifrat de fitxers: Impedir l'ús d'arxius amb informació.

En la majoria dels casos, els bloquejadors poden desactivar-se i eliminar-se més o menys fàcilment. En canvi, les variants que xifren els arxius tenen un major impacte pels afectats, la recuperació dels arxius xifrats pot ser difícil o en determinats casos impossible.

La tècnica d'enginyeria social que s'utilitza en les variants més populars de bloqueig, mostren un text o imatge on s'indica que les autoritats han detectat la realització d'una acció il·legal des de l'equip de l'usuari, i s'ha de pagar una multa per recuperar l'accés al sistema. A les versions més actuals on hi ha xifrat de fitxers, es fa saber directament a l'usuari que l'equip ha estat "segrestat" i es demana un "rescat" per poder recuperar els arxius que han estat xifrats.

Hi ha informació a la xarxa de la recuperació d'arxius parcial després de realitzar el pagament del xantatge, però en cap cas CESICAT recomana el pagament pels següents motius:

- No garanteix la recuperació dels arxius.
- Assenyala la víctima com un objectiu atractiu per a futurs atacs o perquè els criminals demanin encara més diners.
- Es fomenta aquest tipus d'extorsions entre els cibercriminals.

Referències

Referències relacionades amb les recomanacions tècniques

- http://www.anas.co.in/2010/02/enabling-system-restore-in-group-policy.html
- http://www.windows7library.com/blog/bkup/shadow-copies/
- http://www.windows7library.com/blog/bkup/group-policy-settings-for-previous-versions/
- http://www.sbs-rocks.com/Windows%20Server%20Hacks%20Excerpt.htm
- http://www2.slac.stanford.edu/comp/winnt/system-administration/OU_Admin_Meeting_Minutes/volume_shadow_copy_Microsoft.htm
- http://www.computerworld.com/s/article/9243537/Cryptolocker_How_to_avoid_getting_infected_and_what_to_do_if_you_are_?pageNumber=2
- http://support.microsoft.com/kb/310791
- http://technet.microsoft.com/es-es/library/cc786941%28v=ws.10%29.aspx
- http://blogs.msdn.com/b/patricka/archive/2010/03/18/where-should-i-store-my-data-and-configuration-files-if-i-target-multiple-os-versions.aspx