Telefónica

etisalat

TREND REPORT_

Impacto del malware de tipo Wiper en Oriente Medio y América del Sur

19.06.2018

CYBER SECURED BY ElevenPaths

elevenpaths.com

Index

1. Introducción

Dos de los miembros actuales de la **Telco Security Alliance**, Etisalat y Telefónica, han detectado conductas de *malware* similares en sus "territorios" respectivos y están dispuestos a proporcionar consultoría sobre Amenazas de Ciberseguridad para la concienciación de los usuarios, ayudando a que tomen las medidas correctivas que ayuden a proteger su información crítica.

Se debe de tener en cuenta que la información recibida de las distintas fuentes sobre el ciberataque llamado **Wiper *Malware*** podría borrar el disco duro de los sistemas infectados.

La intención principal de estos ataques es **destruir sistemas y / o datos**, causando grandes daños financieros y de reputación. Shamoon, Black Energy, Destover, ExPetr / Not Petya y Olympic Destroyer: todas estas versiones de *malware* de Wiper, y otros como ellos, tienen el único propósito de destruir sistemas o datos, causando generalmente grandes daños financieros y de reputación a las compañías afectadas.

1.1. Análisis del *malware* denominado Wiper

Los códigos del *malware* Wiper han estado activos desde 2012 cuando apareció el *malware* Shamoon. Las distintas versiones de Wiper atacan al *master boot record* y las operaciones realizadas por el *core file system*, dificultando la posible recuperación del equipo. Una vez que el *malware* accede a un sistema, se propaga y, en la mayoría de los casos, puede ser muy difícil de detectar y de eliminar, lo que puede provocar una interrupción con graves consecuencias. La capacidad destructiva de Wiper puede variar, desde la sobrescritura de archivos específicos hasta la destrucción de todo el sistema de archivos. La cantidad de datos impactados será una consecuencia directa de la técnica utilizada que tendrá un impacto directo en la empresa. Cuanto más difícil sea el proceso de recuperación de datos/sistema, mayor será el impacto comercial.

Por lo general, el malware Wiper tiene tres vectores de ataque: **archivos** (datos), **sector de arranque** del sistema operativo y los **datos**. La destrucción de la copia de seguridad se realiza normalmente eliminando las copias del *volume shadow copy* y las propias copias de seguridad.

Simplemente borra los primeros 10 sectores del disco físico, o el *malware* podría reescribir estos primeros 10 sectores con un nuevo gestor de arranque que causará daños adicionales.

El *malware* puede realizar la destrucción del disco duro de la siguiente manera:

- Creando una lista de archivos específicos
- Listando archivos en carpetas específicas
- Rescribiendo una cierta cantidad de *bytes* al comienzo de cada archivo
- Sobrescribiendo el archivo por completo si los archivos son más pequeños que un determinado tamaño
- Escribiendo cierta cantidad de *bytes* cada cierta cantidad de bytes

Shamoon: esta versión evita cualquier protección aplicada a los archivos ejecutados por el sistema operativo, lo que permite la destrucción de archivos mientras el sistema se está en ejecutando.

La propagación de las distintas versiones de este *malware* difiere unos de otros; en casos recientes, como el **Olympic Destroyer**, el *malware* fue lanzado en forma de gusano que se auto-replicaba y posteriormente realizaba un movimiento lateral dentro de la red.

Además, los módulos de replicación generalmente se usan junto con los módulos de recolección de credenciales y algunos de los gusanos también llevan consigo el código para explotar las vulnerabilidades que permiten la ejecución remota de código.

2. Cronología de los ataques

En los últimos 10 años ha habido múltiples incidentes relacionados con *malwares* Wiper, desde **Shamoon1** en 2012 hasta el ataque **Olympic** en febrero de 2018.

Los diferentes *malwares* han utilizado técnicas específicas para alcanzar sus objetivos: lanzamiento de M.E.Doc, exfiltración de datos y publicación en un dominio público, ataques sobre el protocolo SMB de Microsoft Windows, comprometiendo al proveedor M.E.Doc usando el *software* para ejecutar su propio código en el dispositivo atacado.

Imagen 1: Cronología de ataques Wiper desde 2012

2.1.Ataques Wiper en Oriente Medio

Los dos Wipers principales que han afectado activos en Oriente Medio son **StoneDrill** y **Shamoon**. Shamoon, también llamado W32.Disttrack, se descubrió por primera vez en agosto de 2012, cuando comprometió miles de ordenadores en los estados del Golfo. Shamoon fue usado contra **compañías petroleras nacionales**.

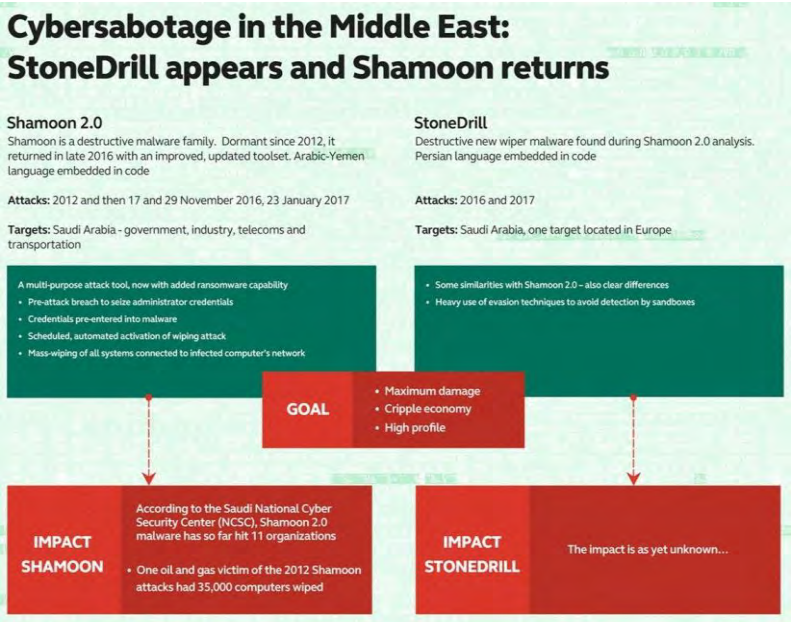

Imagen 2: Stonedrill y Shamoon – Detalles de Kaspersky

En 2017, los investigadores observaron un resurgimiento de ataques dirigidos a la destrucción y robos de datos. También descubrieron un *malware* previamente desconocido que parece atacar únicamente a organizaciones en Oriente Medio. Llamaron a esta nueva versión StoneDrill. StoneDrill posee varias similitudes de "estilo" con Shamoon, con múltiples factores y técnicas interesantes, permitiéndoles una mejor evasión en su detección.

Imagen 3: Cronología de muestras de Stonedrill

2.2.Amenazas actuales en Oriente Medio

Este tipo de amenazas se han relacionado generalmente con vulnerabilidades en los sistemas de Microsoft. Es por eso que muchos tuits que relacionan la última vulnerabilidad de Microsoft como un posible vector de ataque son extremadamente interesantes para los Ejércitos.

Hackers Found Using A New Way to Bypass Microsoft Office 365 Safe Links

Tuesday, May 08, 2018 Mohit Kumar

I am using:	Am I Vulnerable to baseStriker?
Office 365	Yes - you are vulnerable
Office 365 with ATP and Safelinks	Yes - you are vulnerable
Office 365 with Proofpoint MTA	Yes - you are vulnerable
Office 365 with Mimecast MTA	No - you are safe
Gmail	No - you are safe
Gmail with Proofpoint MTA	We are still in testing and will be updated soon
Gmail with Mimecast MTA	No - you are safe
Other configurations not here?	Contact us if you want us to help you test it

Imagen 4: Omitir enlaces seguros de Office

Como dice la imagen del tuit, "Existen errores graves en los productos de Microsoft y los ejércitos pueden usarlos. Actualice sus sistemas y elimine cualquier conexión innecesaria a Internet."

La recomendación general sería mantener actualizados todos los sistemas de Microsoft.

2.3.Ataques Wiper en LATAM

En 2015, se descubrió una variante específica de Wiper popularmente conocido como **KillDisk** que atacaba a varios sectores industriales en **todo el mundo**: energía, minería, banca... Desde entonces, se ha utilizado como arma de **extorsión** digital. Desde enero de 2018 se han detectado incidentes graves relacionados con el *malware* wiper, concretamente en las redes de bancos de América Latina.

Fue descrito como una potente herramienta de borrado. Esta variante de KillDisk no sólo fue capaz de borrar varios archivos importantes en el sistema, sino también el MBR de todas las unidades físicas del sistema, por lo que no hay forma de iniciarlos. Fue capaz de sobrescribir los primeros sectores 0x20 de cada dispositivo con "0x00". Después de esperar unos 15 minutos, el *malware* obligaba al sistema a reiniciarse, matando los procesos esenciales del sistema operativo. Una vez reiniciado, el ordenador **no podía volver a iniciar el sistema operativo**, por lo que los archivos no sólo se eliminaron, sino que **el sistema completo permaneció inaccesible**.

Este programa ha evolucionado desde entonces y no sólo como un arma de extorsión, sino también como una **cortina de humo para distraer** a los administradores de la red mientras los atacantes realizaban otros ataques relacionados con actividades bancarias y obtenían beneficios. Estas variantes de KillDisk generalmente se distribuyen de diferentes maneras innovadoras.

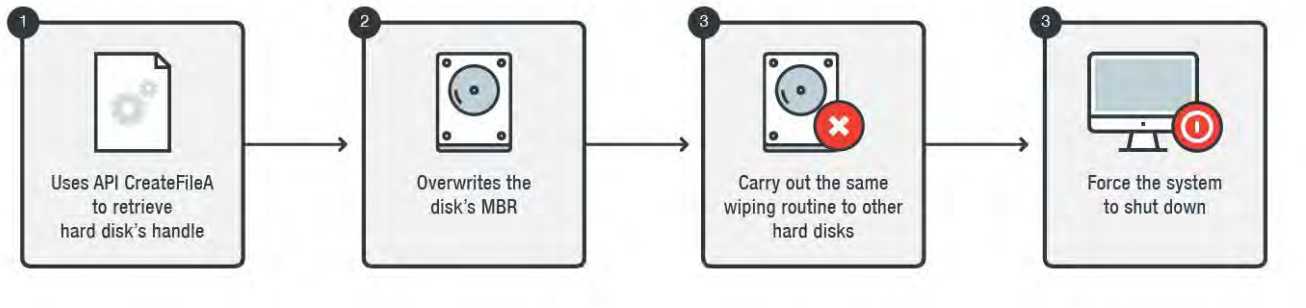

Imagen 6: Rutina básica del Wiper KillDisk

2.4. Ataques Wiper en LATAM usados como pantalla de humo

En enero de 2018, se detectaron algunos incidentes relacionados con los sistemas bancarios en **Bancomext** (Banco Nacional de Comercio Exterior), cuando un grupo norcoreano intentó atacar la red interna del banco **SWIFT** (Society for Worldwide Interbank Financial Telecommunication) con el objetivo de robar 110 millones de dólares. Los atacantes accedieron a la red, tomaron el control de ella y luego lanzaron este ataque de distracción mientras trataban de llegar al objetivo real.

Más tarde, en mayo de 2018, varios bancos en Chile y otros países de LATAM observaron ataques similares de Wiper. Esta vez, esta **variante de KillDisk** se utilizó claramente como **pantalla de humo** para llegar a donde estaba el objetivo real: **la red local de SWIFT en el banco**. Mientras los administradores intentaban comprender lo que sucedía con miles de ordenadores de escritorio reiniciándose y sin poder arrancar, los atacantes intentaron acceder a la red SWIFT.

Desde el punto de vista técnico y táctico, estas muestras particulares de Wipers utilizadas en estos ataques tenían algunas particularidades interesantes. Por ejemplo, se creó utilizando el **lenguaje NSIS**, normalmente utilizado para crear programas de instalación para Windows. Además, se **ofuscó fuertemente usando VMprotect**, programa muy sofisticado para evitar la ingeniería inversa de la muestra, y hace muy difícil saber cómo funciona el *malware*. El *malware* fue concebido para "romper" sistemas, **no para controlarlos**, ya que ni siquiera usaba ninguna comunicación a un C&C (como suele hacerse en cualquier otro *malware*). Esta muestra específica borró el primer sector solamente (512 *bytes*) con 0x00.

Este Wiper usó una forma interesante de propagarse en la red interna, **utilizando irónicamente los agentes antivirus** para propagarse desde un servidor a los *desktops*. Dado que estos programas antivirus pueden instalar programas desde el servidor a los clientes, realizar actualizaciones de firmas de antivirus y otras rutinas desde un servidor central, esta variante de KillDisk lo utilizó como una forma de alcanzar e infectar las computadoras en la red interna. Todo esto sucedió mientras los atacantes intentaban realizar operaciones fraudulentas en la red SWIFT.

Imagen 7: Los sistemas dejan de funcionar después del reinicio

3. Mitigación

Los ataques Wiper son extremadamente destructivos, aunque se implementen tácticas defensivas incluidas las firmas de posibles intrusiones o las soluciones antivirus; simple-mente no son lo suficientemente efectivas por sí mismas para mitigar este tipo de ata-que. Debido a las diferentes características y el origen de este tipo de ataques, se re-comienda que las organizaciones establezcan diferentes acciones para prevenir cualquier daño generado por los atacantes. La mayoría de las organizaciones de seguridad y sitios web especializados, aconsejan que las organizaciones enfoquen su estrategia de defensa contra estos ataques mediante las siguientes acciones:

- ***Assessment* de seguridad**: realizar un *assessment* de seguridad de la red de gestión para identificar y eliminar cualquier posible fallo de seguridad.
- Desarrollo de un **plan de seguridad** que cubra cualquier actualización de los productos utilizados por la compañía, lo cual ayudará a prevenir cualquier agujero de seguridad y la propagación de este tipo de ataques.
- **Inteligencia contra amenazas**: solicitud de asesoramiento externo contra este tipo de ataques y uso de los servicios de alerta temprana contratados.
- **Formación**: desarrollar un plan de formación para los empleados de las empresas, con el fin de informarles de cómo deben trabajar para prevenir este tipo de ataques.
- **Planificar** el uso de programas para evaluar y actualizar los principales productos del proveedor y los servicios desarrollados *in-house*. El sistema debe de estar actualizado, dado que este tipo de *malware* se propaga al beneficiarse de las vulnerabilidades más comunes de los sistemas operativos como Windows (Shamoon).
- **Aislar** la información importante en redes bastionadas, accediendo sólo a través de conexiones seguras.
- **Utilizar copias de seguridad de datos** para la información crítica.
- **No habilitar macros** de los archivos adjuntos en el Office de Microsoft y prestar atención a los posibles *phishing*, sin hacer click en los enlaces web no solicitados.
- Restringir la posibilidad **(permisos)** de que los usuarios instalen y ejecuten aplicaciones de *software* no deseadas y aplicar el principio de "Mínimo privilegio" a todos los sistemas y servicios.
- **Restringir la ejecución de PowerShell / WSCRIPT / PSEXEC / WMIC** en el entorno empresarial. Asegurar la instalación y el uso de la **última versión de PowerShell**, con el registro habilitado.

4. Indicadores de compromiso

4.1. MD5s de Shamoon

00c417425a73db5a315d23fac8cb353f

271554cff73c3843b9282951f2ea7509

2cd0a5f1e9bcce6807e57ec8477d222a

33a63f09e0962313285c0f0fb654ae11

38f3bed2635857dc385c5d569bbc88ac

41f8cd9ac3fb6b1771177e5770537518

5446f46d89124462ae7aca4fce420423

548f6b23799f9265c01feefc6d86a5d3

63443027d7b30ef0582778f1c11f36f3

6a7bff 614a1c2fd2901a5bd1d878be59

6bebb161bc45080200a204f0a1d6fc08

7772ce23c23f28596145656855fd02fc

7946788b175e299415ad9059da03b1b2

7edd88dd4511a7d5bcb91f2ff177d29d

7f399a3362c4a33b5a58e94b8631a3d5

8405aa3d86a22301ae62057d818b6b68

8712cea8b5e3ce0073330fd425d34416

8fbe990c2d493f58a2afa2b746e49c86

940cee0d5985960b4ed265a859a7c169

9d40d04d64f26a30da893b7a30da04eb

aae531a922d9cca9ddca3d98be09f9df

ac8636b6ad8f946e1d756cd4b1ed866daf

053352fe1a02ba8010ec7524670ed9

b4ddab362a20578dc6ca0bc8cc8ab986

baa9862b027abd61b3e19941e40b1b2d

c843046e54b755ec63ccb09d0a689674

d30cfa003ebfcd4d7c659a73a8dce11e

da3d900f8b090c705e8256e1193a18ec

dc79867623b7929fd055d94456be8ba0

ec010868e3e4c47239bf720738e058e3ef

ab909e4d089b8f5a73e0b363f471c1

4.2.MD5s de StoneDrill

ac3c25534c076623192b9381f 926ba0d 0ccc9ec82f 1d44c243329014b82d3125 8e67f 4c98754a2373a49eaf 53425d79afb21f3cea1aa051ba2a45e75d46b98b8

4.3.C2s de StoneDrill

www.eservic[.]com www.securityupdated[.]com www.actdire[.]com www.chromup[.]com

4.4.C2s de NewsBeef

www.chrome-up[.]date service1.chrome-up[.]date service.chrome-up[.]date webmaster.serveirc[.]com

4.5.Droppers de Disttrack

47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51d1fe1ac34 (x64)

394a7ebad5dfc13d6c75945a61063470dc3b68f7a207613b79ef000e1990909b (x86)

4.6.Componentes de comunicación

772ceedbc2cacf7b16ae967de310350e42aa47e5cef19f4423220d41501d86a5 (x64)

61c1c8fc8b268127751ac565ed4abd6bdab8d2d0f2ff6074291b2d54b0228842 (x86)

4.7.Componentes Wiper

c7fc1f9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a (x64)

128fa5815c6fee68463b18051c1a1ccdf28c599ce321691686b1efa4838a2acd (x86)

4.8.Muestras de EldoS RawDisk

5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a (x64)

4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6 (x86)

4.9.OlympicDestroyer

0311CEC923C57A435E735E106517797F

104ECBC2746702FA6ECD4562A867E7FB

12668F8D072E89CF04B9CBCD5A3492E1

19C539FF2C50A0EFD52BB5B93D03665A

221C6DB5B60049E3F1CDBB6212BE7F41

3514205D697005884B3564197A6E4A34

3C0D740347B0362331C882C2DEE96DBF

47E67D1C9382D62370A0D71FECC5368B

4C8FA3731EFD2C5097E903D50079A44D

4F43F03783F9789F804DCF9B9474FA6D

51545ABCF4F196095ED102B0D08DEA7E

52775F24E230C96EA5697BCA79C72C8E

567D379B87A54750914D2F0F6C3B6571

5778D8FF5156DE1F63361BD530E0404D

583F05B4F1724ED2EBFD06DD29064214

58DD6099F8DF7E5509CEE3CB279D74D5

59C3F3F99F44029DE81293B1E7C37ED2

64AA21201BFD88D521FE90D44C7B5DBA

65C024D60AF18FFAB051F97CCDDFAB7F

68970B2CD5430C812BEF5B87C1ADD6EA

6E0EBEEEA1CB00192B074B288A4F9CFE

7C3BF9AB05DD803AC218FC7084C75E96

83D8D40F435521C097D3F6F4D2358C67

86D1A184850859A6A4D1C35982F3C40E

4.10.CVE-2018-8174 | Vulnerabilidad en el motor VBScript

b48ddad351dd16e4b24f3909c53c8901 – RTF documento

15eafc24416cbf4cfe323e9c271e71e7 – Internet Explorer exploit (CVE-2018-8174)

1ce4a38b6ea440a6734f7c049f5c47e2 – Payload autosoundcheckers[.]com

4.11.TROJ_KILLDISK.IUB

8a81a1d0fae933862b51f63064069aa5af3854763f5edc29c997964de5e284e5

1a09b182c63207aa6988b064ec0ee811c173724c33cf6dfe36437427a5c23446

a3f2c60aa5af9d903a31ec3c1d02eeeb895c02fcf3094a049a3bdf3aa3d714c8

5. Referencias

- Global SOCS de Etisalat y Telefónica
- Threat Post: "*Secrets of the Wiper: Inside the World's Most Destructive Malware*". https://threatpost.com/secrets-of-the-wiper-inside-the-worlds-most-destructive-malware/131836/
- Kaspersky: https://www.kaspersky.com/
- Blog Talos Intelligence: "Wipers - Destruction as a means to an end". https://blog.talosintelligence.com/2018/05/wipers-destruction-as-means-to-end.html
- Blog Trend Micro: "New KillDisk Variant Hits Financial Organizations in Latin America". https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/

Acerca de ElevenPaths

En ElevenPaths, la Unidad de Ciberseguridad de Telefónica, creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre la seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y de esta manera, ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com

Acerca de Etisalat

Etisalat, con sede en Abu Dhabi, fue fundada hace cuatro décadas en los Emiratos Árabes Unidos como primer proveedor nacional de servicios de telecomunicaciones. Como empresa internacional de primer nivel, Etisalat Group proporciona soluciones y servicios innovadores a 163 millones de abonados de 17 países de Oriente Medio, Asia y África.

www.etisalat.ae
@etisalat