Eleven Paths

APTualizador: El malware dirigido que parchea Windows

Un análisis del CSIRT-SCC en colaboración con el área de innovación y laboratorio de ElevenPaths

Telefónica CYBER SECURITY UNIT

elevenpaths.com

Este informe está realizado por el equipo de investigadores del CSIRT-SCC con la colaboración de ElevenPaths.

A finales de junio de 2019 asistimos a un incidente en el que los equipos comienzan a reiniciarse prácticamente a la vez y sin causa aparente. En paralelo, Kaspersky detecta la presencia de un archivo llamado *swaqp.exe*, aparentemente no disponible en ningún agregador de antivirus o plataforma pública en ese momento. Intentamos determinar si este archivo puede ser el causante de los reinicios y si realmente estamos ante una amenaza de malware.

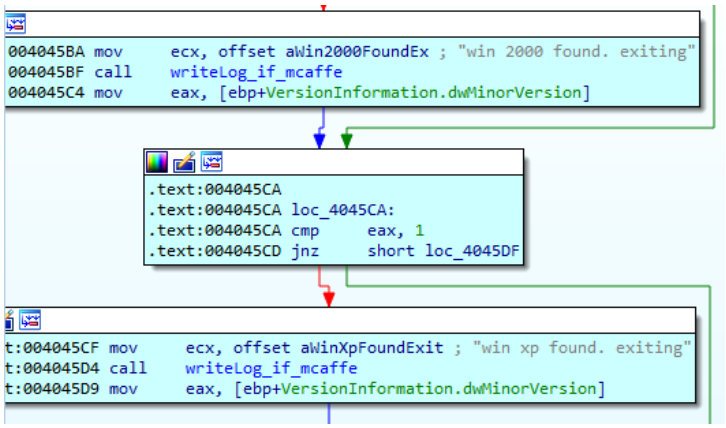
Nos llama la atención que en un primer análisis rápido observamos que la muestra descargaba la actualización de seguridad legítima de Windows KB3033929, aunque lo hacía desde un servidor no oficial. En otras palabras: instalaba el archivo legítimo (firmado por Microsoft) desde un servidor no oficial. No es un comportamiento habitual del malware por dos razones.

- Los creadores de malware suelen crear sus artefactos minimizando dependencias adicionales (librerías) que podrían no estar incluidas en los equipos de las potenciales víctimas.
- Por otro lado, el malware no suele estar interesado en que los equipos se encuentren actualizados, y mucho menos intenta actualizarlos con parche alguno. No es el comportamiento habitual en el contexto de una posible muestra de malware.

A partir de aquí, comenzamos a investigar.

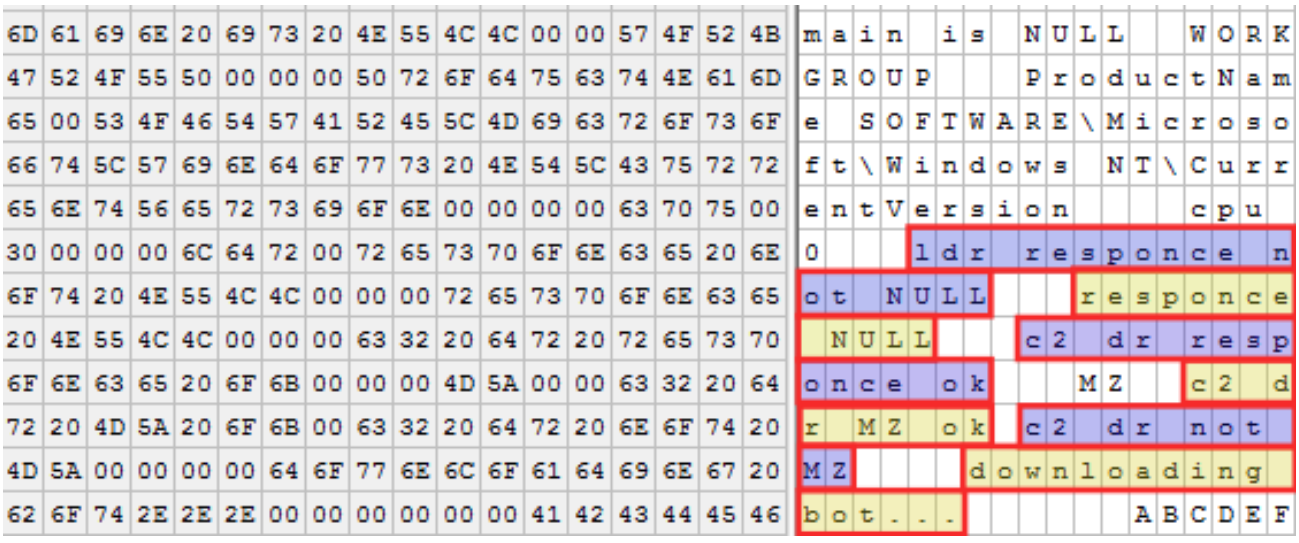
1. La actualización KB3033929

El código de *swaqp.exe* comprueba si el sistema posee una versión anterior a Windows 7 en escritorio y Windows Server 2008 R2 en versión servidor. En tal caso, se terminará la ejecución del código. El parche de seguridad mencionado está solo disponible para esas versiones, por lo que deja claro su objetivo con esta acción.

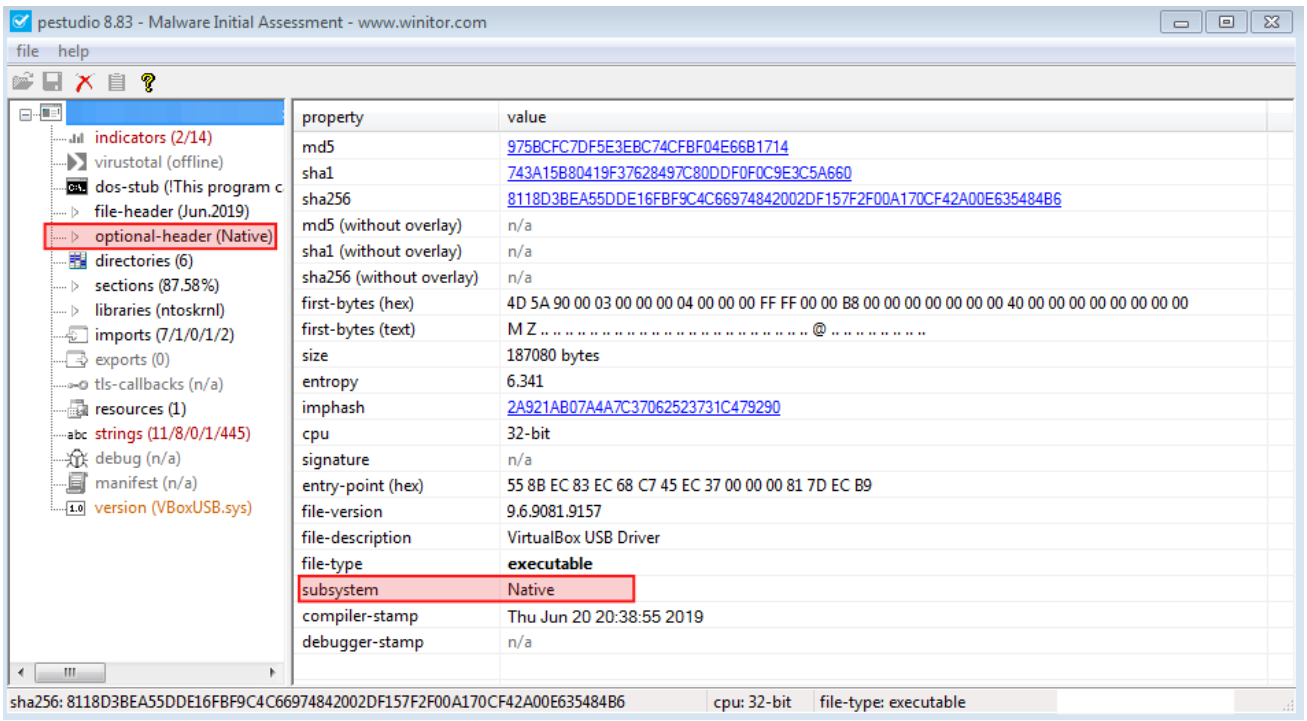


2. Descarga de un rootkit

Según el binario avanza en su ejecución, descubrimos que va generando un log en el que describe las acciones que lleva a cabo. Este *log.txt* (que se encuentra en la misma carpeta que el ejecutable y que muy probablemente ha sido olvidado por el atacante en la muestra final) va completándose con mensajes personalizados de depuración que habrían ayudado al creador del malware a poder seguir la ejecución de este en el momento de su desarrollo, o a detectar fallos en la ejecución en las máquinas víctima. Un ejemplo de los mensajes de log que encontramos se muestra en la siguiente imagen.



En los mensajes de log se pueden ver las palabras "rootkit" y "driver". Efectivamente, tras la descarga del KB, continúan realizándose más conexiones contra la IP del atacante. Una vez descifrado uno de los objetos recibidos, encontramos un ejecutable. El campo 'subsystem' en su cabecera tiene el valor 'Native'. Esto indica que se trata de un driver del sistema que se ejecuta a nivel del kernel, lo que a su vez apunta a que este archivo sería el encargado de ocultar la infección en el sistema.



Para que el ejecutable descargado desde el C&C pueda correr a nivel de kernel será instalado como un driver del sistema operativo. Como sabemos, en Windows esto implica que el binario debe estar firmado por una de las Autoridades de Certificación permitidas en el sistema operativo para poder ejecutarse como Kernel, lo que permite ofrecer ciertas garantías al software crítico que se lanza en el sistema. El sistema de autorización y firma de drivers en Windows se ha vuelto muy exigente en los últimos tiempos.

3. ¿Por qué actualizar?

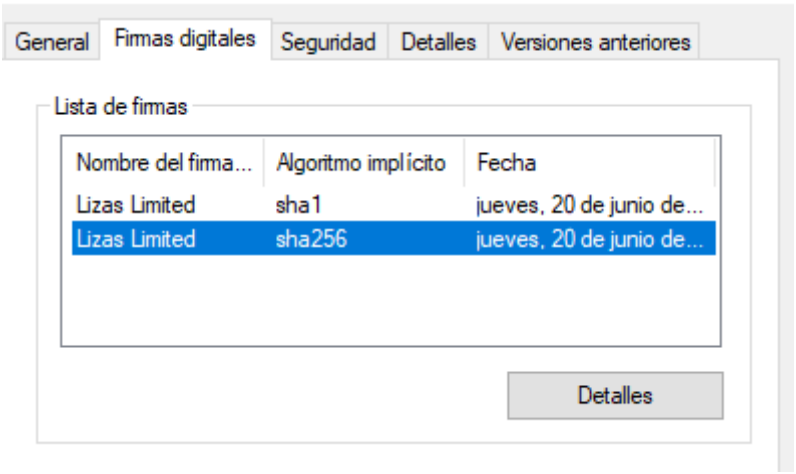
Hasta ahora, tenemos un malware que aplica una actualización legítima en el sistema, y que descarga lo que parece un driver (que debe estar firmado para poder ser instalado). ¿Por qué actualizar el sistema operativo de una víctima? Para responder a esta pregunta es necesario comprender los cambios que incluía este parche y cómo se relaciona con la instalación del rootkit.

Si entramos en los detalles del certificado con el que se firmó este ejecutable, podemos ver que se hace uso de SHA256 como algoritmo de hash. Aquí comienza a tener sentido el comportamiento del malware. KB3033929 es una actualización de Microsoft aparecida en 2015 como actualización a su vez de un parche de finales de 2014. Las versiones de Windows 8 en adelante, soportan de forma nativa la verificación de firmas con SHA256, pero Windows 7 o Windows 2008 R2, no. Microsoft tuvo que sacar este parche para poder seguir dando soporte a estas versiones

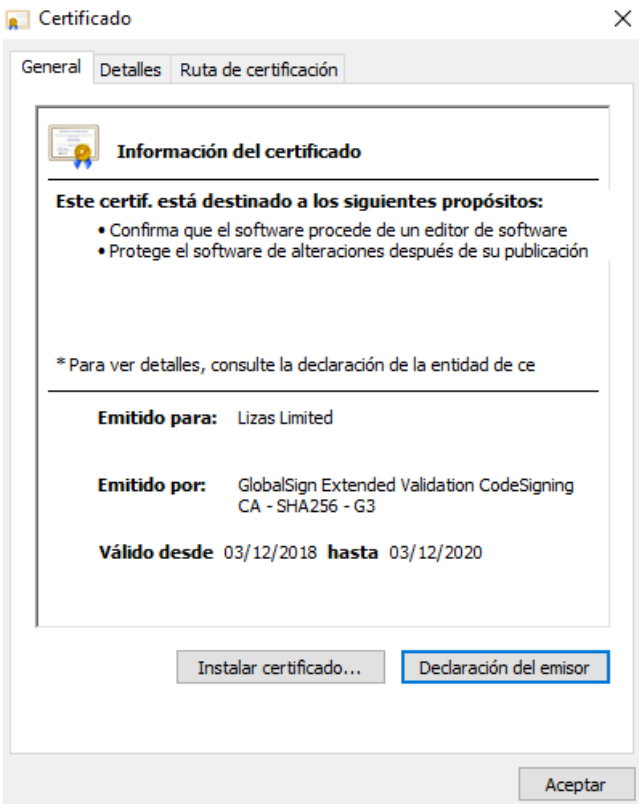
(Windows 7 y 2008 R2), mientras que los anteriores (Vista, 2003, XP...) siguen sin poder comprobar firmas creadas con hashes SHA256

De ese modo, los atacantes aplican el parche KB3033929 para que la verificación de su driver firmado sea válida. Entendemos que los atacantes solo disponían de esta posibilidad de firmado y, por tanto, tuvieron que adaptar la víctima al malware (actualizando las capacidades del sistema operativo) y no al revés.

Para ello, comprobamos la firma del driver:



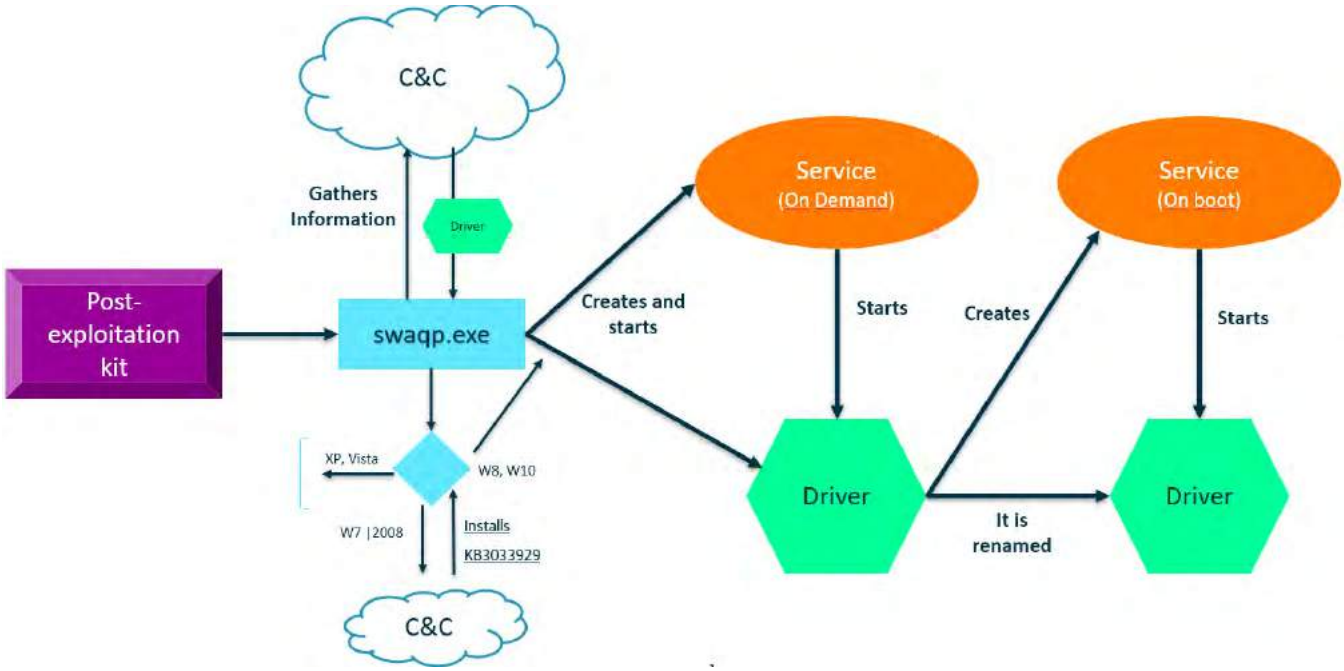
Sorprendentemente, se encuentra firmado con SHA256, pero también con SHA1. Esto es una práctica habitual en las actualizaciones de Windows, desde hace algún tiempo, por ejemplo, precisamente para que puedan funcionar en Windows 7, 2008 R2 y el resto de sistemas. Pero en el caso de las actualizaciones, los hashes SHA1 están firmados por certificados diferentes a los hashes SHA256 en la misma muestra. En el caso de este malware, tanto el hash SHA1 como el hash SHA256, están firmados por un certificado SHA256.



Esto es un movimiento un poco extraño por parte del atacante. Entendemos que solo disponía de un certificado SHA256, y necesitaba actualizar el sistema para que el Windows víctima pudiese comprobar la validez. El hecho de que esté firmado por SHA1 puede ser una simple prueba previa del atacante.

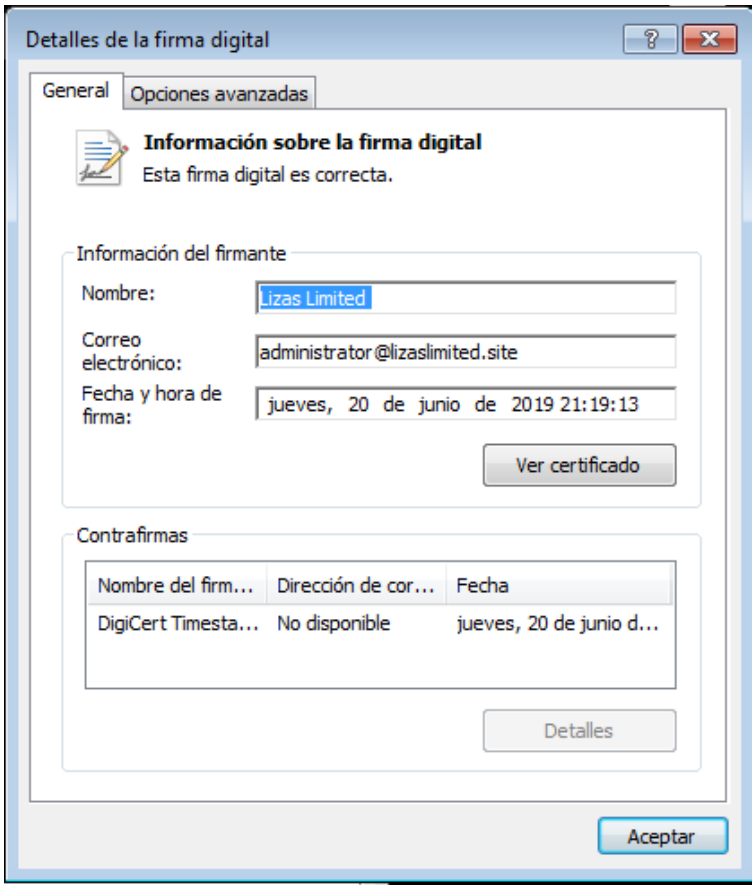
El rootkit es descargado en la carpeta C:\WINDOWS\SYSTEM32\Drivers, y se crea un servicio a nivel de kernel que referencia al archivo *.sys* con el mismo nombre que el servicio. El nombre que se le da a este rootkit viene determinado por una unión de fragmentos de nombres de otros drivers que se encuentran en esta carpeta. por lo que la detección a simple vista del fichero podría no ser trivial.

Para asegurarse de la completa actualización de la DLL y la aplicación del parche, los atacantes forzaban el reinicio de la máquina tras la instalación del parche.



4. El certificado y la firma digital

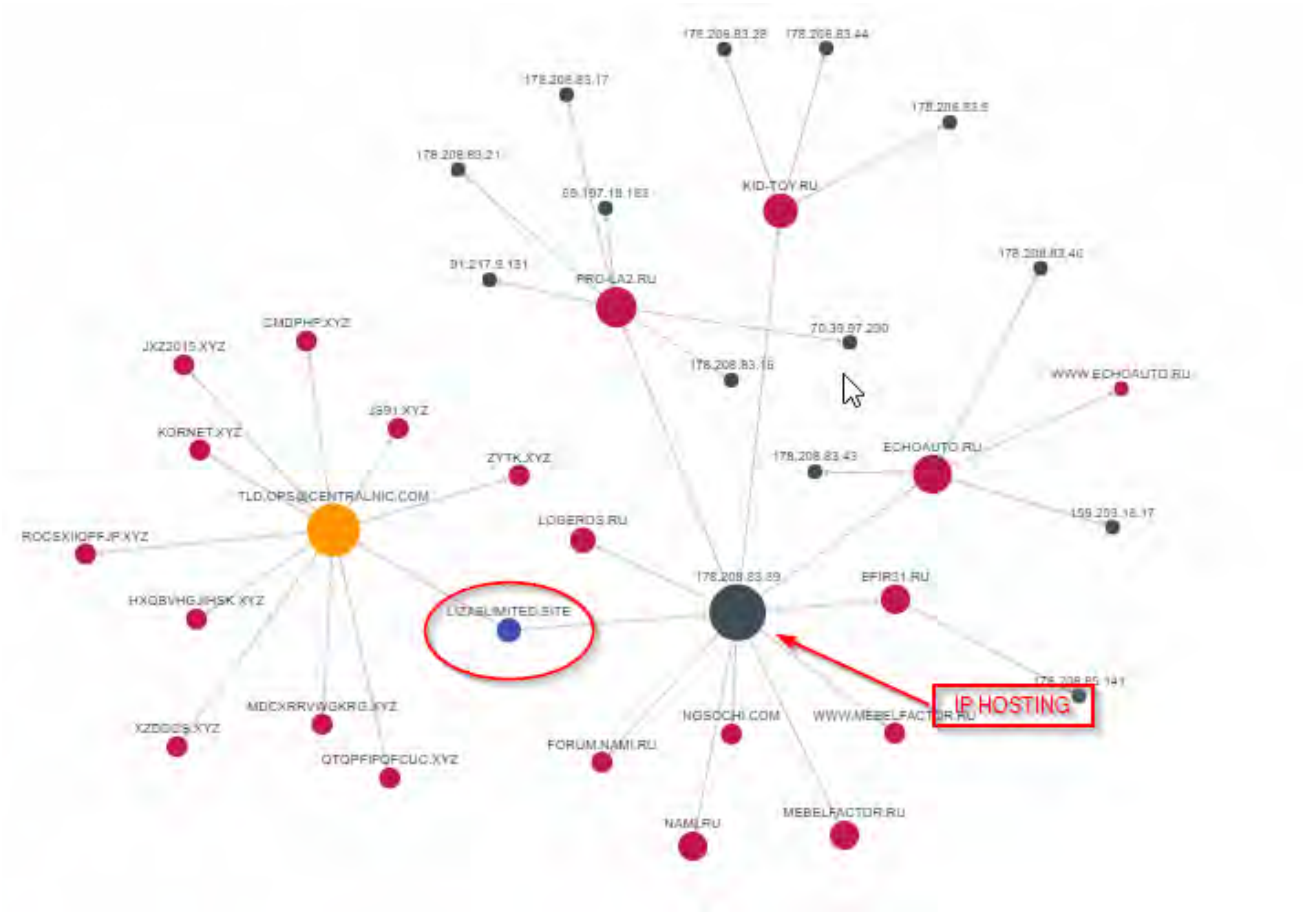
La muestra fue firmada el 20 de junio de 2019 con un certificado **Lizas Limited** emitido por GlobalSign.



De acuerdo con la información de la firma digital, observamos que **Lizas Limited** es una empresa ubicada en Manchester, Reino Unido.

EMAILADDRESS=administrator@lizaslimited.site, CN=Lizas Limited, O=Lizas Limited, STREET=4 Herevale Grange, L=Worsley, ST=Greater Manchester, C=GB, OID.1.3.6.1.4.1.311.60.2.1.3=GB, SERIALNUMBER=06794337, OID.2.5.4.15=Private Organization	CN=GlobalSign Extended Validation CodeSigning CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE Serial: 4d1473a40ace93522a2abf3b	12/03/2018 15:18:28 12/03/2020 15:18:28	1D:9A:5A:EC:BB:BC:59:23:52:AB:C2:EE:B0:97:09:24 11:14:E9:7C:21:0A:8A:EC:35:7C:F6:43:D7:FE:F5:CC:1A:1F:84:DA

Sin embargo, no hay información pública que indique que exista relación entre esta empresa y el dominio *lizaslimited.site*, que está registrado y hospedado en Rusia. Actualmente, el sitio web de *lizaslimited.site* no muestra información relevante.

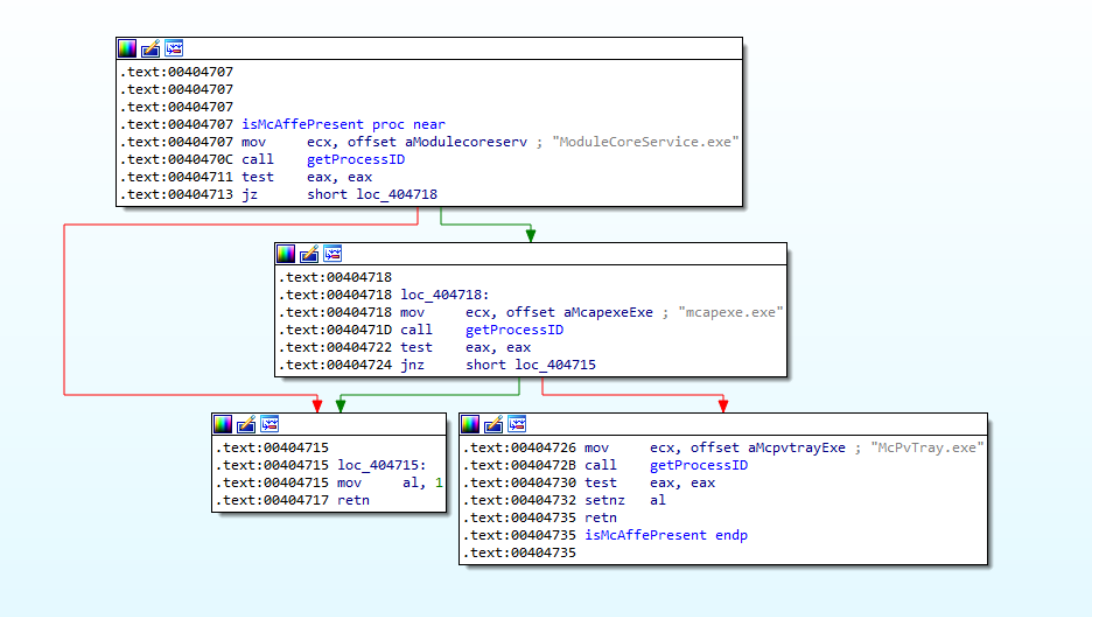


Podríamos estar ante un caso de suplantación, en el que se ha usurpado la identidad de una empresa legítima ante **GlobalSign**. Hay evidencias de que este comportamiento se extiende tiempo atrás, con más muestras de software malicioso firmado por **Lizas Limited**, con certificados de firma de código emitidos por **Sectigo**.

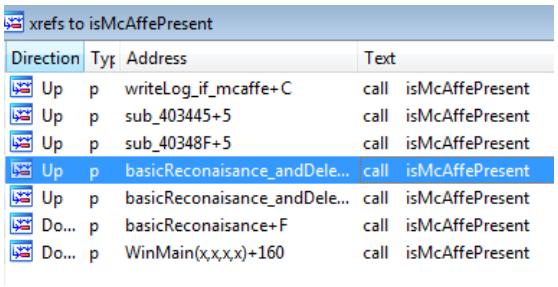
5. Referencias a McAfee

A lo largo de la ejecución de la muestra existen constantes referencias a McAfee que hacen cambiar el comportamiento del malware según si los procesos del antivirus están corriendo o no. Este es el principal motor antivirus en los equipos afectados. Buena parte del comportamiento del malware está supeditado a si existe este antivirus en el equipo o no. Esto puede ser un indicio de ataque dirigido.

Uno de los comportamientos que dependen de la existencia de McAfee o no, es la creación del archivo de log que se apuntaba anteriormente. Este archivo de log solo será escrito si la víctima no cuenta con este antivirus instalado en la máquina.



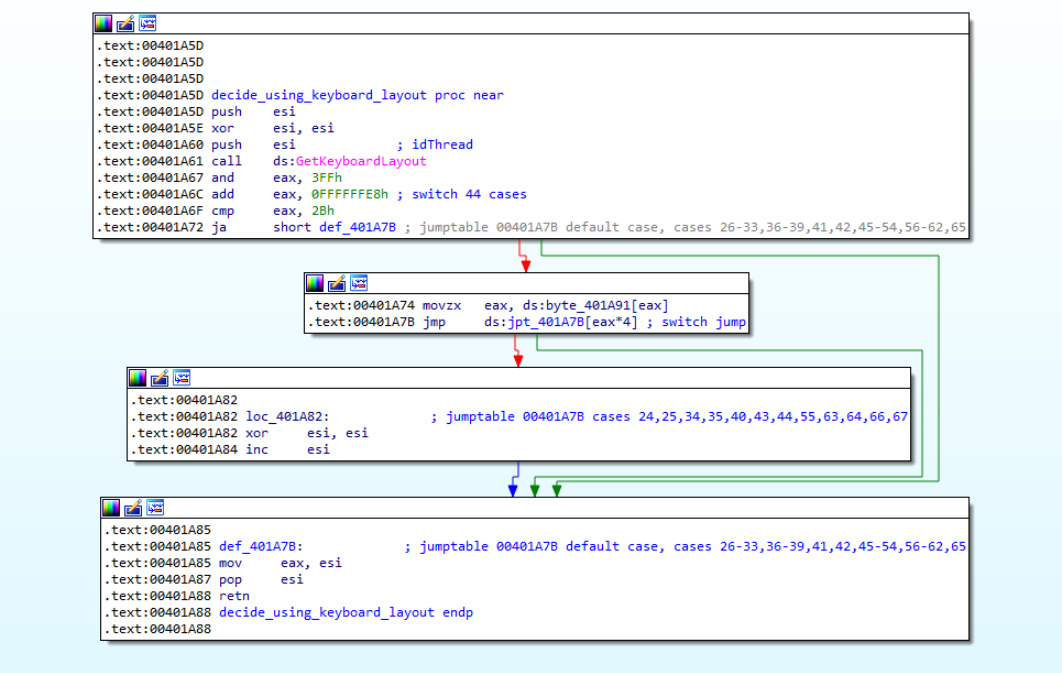
Como ejemplo, en la primera línea de la imagen siguiente podemos ver una referencia a una función que hemos renombrado como *writeLog_if_mcafee*. Encontramos al menos otras siete referencias a comprobaciones internas que tienen que ver con la existencia o no de McAfee.



6. Posible atribución por país

Encontramos además un fragmento de código en el que la muestra comprueba el idioma en el que está configurado el teclado de la víctima y, según este, proseguirán o no con la infección. Esto es habitual, los autores de malware suelen hacerlo para que, en caso de ejecución en su propia máquina por error, el malware no les infecte. Otros casos pueden ser ataques muy dirigidos a ciertos países en los que solo se ejecutará para una zona en particular.

No obstante, el caso encontrado aquí es un poco diferente. En vez de lo anterior, encontramos un rango de hasta 43 idiomas que, mediante códigos numéricos (LANGUAGE IDENTIFIER) **consecutivos**, se librarían de la infección.



Los países que no se verían afectados y entre los que se encuentra presumiblemente la fuente de la amenaza son los rangos comprendidos entre 0x18 y 0x43. Precisamente, Rusia se encuentra dentro de la lista de estos 43 países, lugar que relacionábamos con la firma **Lizas Limited**.

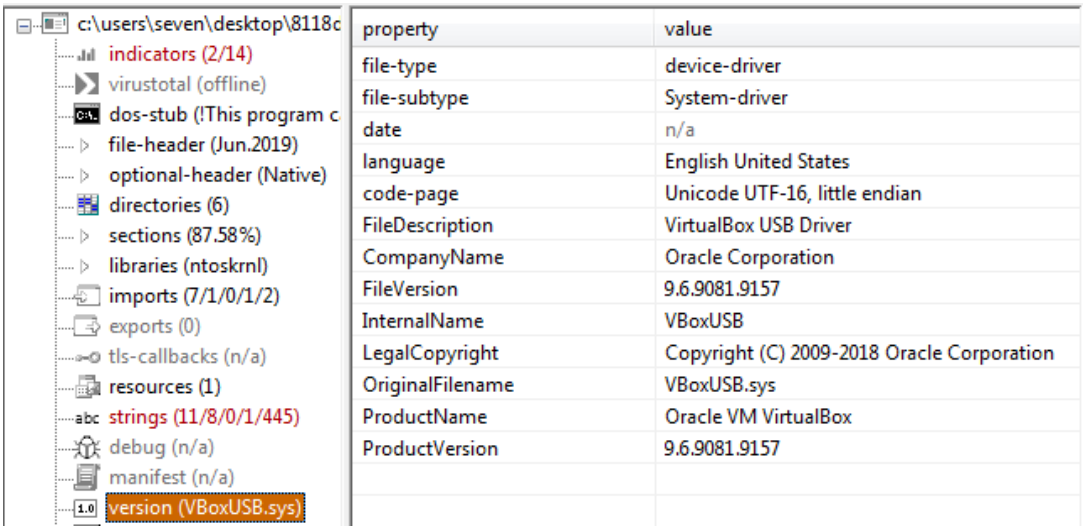
Puede consultarse la lista de códigos en https://docs.microsoft.com/en-us/windows/desktop/intl/language-identifier-constants-and-strings.

Esto pudiera indicar que:

- Los autores se encuentran dentro de este rango, y los demás están incluidos para no dejar clara la atribución del ataque
- El ataque fue **dirigido**, puesto que si se tratase de un malware sin víctima definida, no tendría sentido excluir tantas posibles infecciones (hasta 43 códigos diferentes estarían excluidos del ataque). Es importante señalar que la única relación que tienen los códigos entre sí es que son consecutivos, es decir, no constituyen un grupo geográficamente cercano ni políticamente afín.

7. El driver

En la descripción del archivo .sys puede verse cómo los atacantes han usado información falsa relativa a Oracle para intentar pasar algo más desapercibidos:



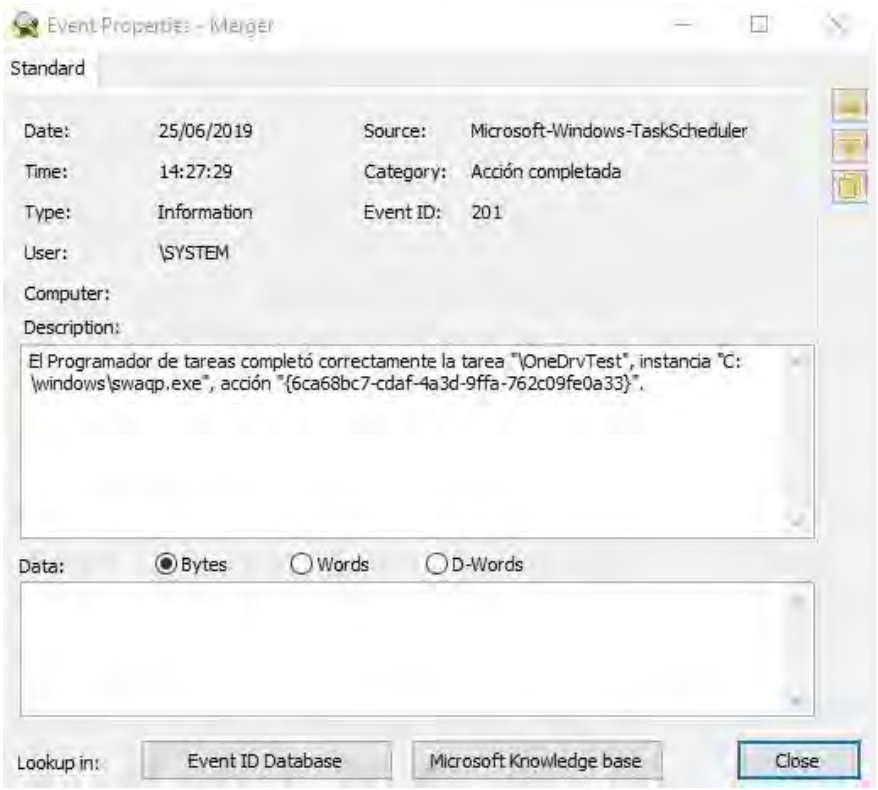
Este driver fue subido a VirusTotal el día 27-06 con una detección mínima de dos motores en estático. Poco después se unen más motores a la detección.

Sin embargo, como se ha mencionado antes, buscando archivos firmados por **Lizas Limited** en su certificado, encontramos archivos subidos desde abril de este mismo año. En particular, encontramos uno llamado *rootkit.sys* que es detectado ya por la mayoría de los motores el 18 de mayo. Hubiese resultado más útil tomar medidas preventivas contra el certificado firmado por **Lizas Limited** y no limitarse a detectar los archivos por otras características.

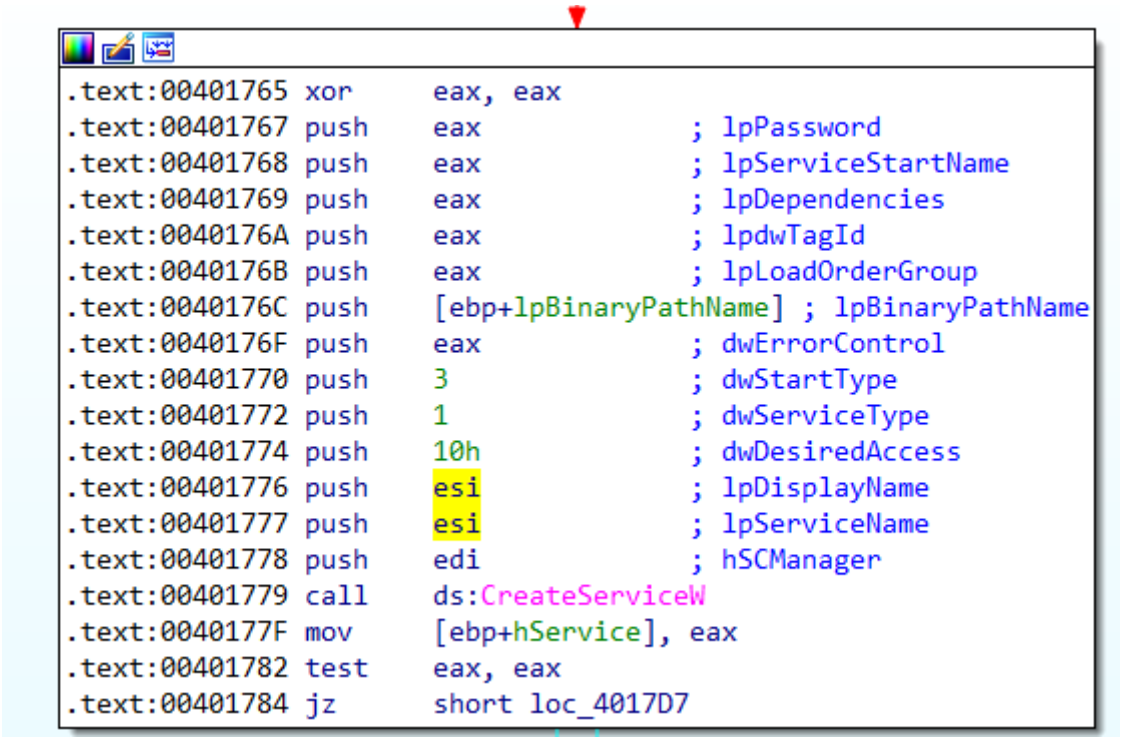
Por nuestra parte, desde que tuvimos constancia de la existencia y uso de esta firma, procedimos a solicitar su revocación, por lo que esta firma ya no es aceptada. Podemos observar más referencias de muestras similares desde al menos el 25 de abril. También aparecía en este hilo de Twitter, el 30 del mismo mes, referencias e incluso imágenes del panel de control de una muestra bastante similar.

8. Persistencia

La muestra *swaqp.exe* no revela ningún indicador de compromiso relacionado con la persistencia en las máquinas que lo ejecutasen. Sin embargo, el análisis forense de equipos infectados mostró que los atacantes accedían de manera remota a los equipos y creaban tareas programadas para iniciarla:



Sin embargo, la razón para crear la tarea programada es poder volver a iniciar el malware en caso de que las actualizaciones de Windows de las que se hablaba en puntos anteriores hubieran sido instaladas con éxito, y por tanto no supone una técnica de persistencia como tal. Por tanto (teniendo en cuenta la fórmula del ataque y los artefactos utilizados) identificamos este ejecutable como un dropper/instalador de la amenaza sin persistencia, cuyo objetivo principal es el de crear el servicio malicioso.



Con respecto a la persistencia del driver en sí, como puede verse en la imagen de la instalación del servicio, el tipo StartType y ServiceType indican que se inicia de forma manual (SERVICE_DEMAND_START = 3) y que se trata de un servicio relacionado con un driver del kernel (SERVICE_KERNEL_DRIVER = 1). Aunque más adelante, es el propio driver el que crea una nueva copia del driver con un nombre distinto y un servicio homónimo, pero con arranque al inicio del sistema. El primer driver y servicio instalados son borrados en este proceso. Así, es el driver el que consigue la persistencia.

El objetivo principal de swaqp.exe es instalar un conjunto de herramientas en el equipo infectado, entre las que se encuentra un rootkit firmado con certificado SHA256 y que, por tanto, obliga a actualizar el sistema operativo objetivo. En próximas entregas hablaremos del resto de artefactos introducidos en los sistemas infectados.

9. IOCs

- 45.227.252.54
- 139.60.160.6
- 185.55.243.15
- 92.223.73.11
- **Mutex:** system32_host_service
- **Mutex:** system32_mutant_service
- ***Swapqp.exe:*** 6c865c6864c8d77efe1002b73fc1dda1a4a357d30237c6bfcefb63057e745c41
- ***Driver:*** 8118d3bea55dde16fbf9c4c66974842002df157f2f00a170cf42a00e635484b6

Otros hashes firmados por el mismo certificado:

- c0cff7ff5663c7c9c6c69dc645b86222b74ef2dc5d2b2633a6aa79d4959d7d2b
- 8118d3bea55dde16fbf9c4c66974842002df157f2f00a170cf42a00e635484b6
- c554148084d05195a08bf00e3331beb85dc362787d88bdb7a8088f1336131d91
- b6f156e4a9bd4070d0e502b94ec143e1e349cfff5b10797fae8e36bface8605f
- fb112fc76835d02f0ec2f830b0cd1bb87e17e03cb3c7bff66e7cbf485b6af71f

-----BEGIN CERTIFICATE-----
MIIFlzCCBL+gAwIBAgIMIRRzpArOk1IqKr8/MA0GCSqGSIb3DQEBCwUAMG4xCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMUQwQgYDVQQDEztH
bG9iYWxTaWduIEV4dGVuZGVkIFZhbGlkYXRpb24gQ29kZVNpZ25pbmcgQ0EgLSBI
SEEyNTYgLSBHMzAeFw0xODEyMDMxNTE4MjhaFw0yMDEyMDMxNTE4MjhaMIH/MR0w
GwYDVQQPDBRQcml2YXRlIE9yZ2FuaXphdGlvbjERMA8GA1UEBRMIMDY3OTQzMzcx
EzARBgsrBgEEAYI3PAIBAxMCR0IxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVh
dGVyIExhbmNoZXN0ZXIxEDAOBgNVBAcTB1dvcnNsZXkxGjAYBgNVBAkTEUgaSGVy
ZXZhbGUgR3JhbmdlMRYwFAYDVQQKEw1MaXphcyBMaW1pdGVkMRYwFAYDVQQDEw1M
aXphcyBMaW1pdGVkMS4wLAYJKoZIhvcNAQkBFh9hZG1pbmlzdHJhdG9yQGxpemFz
bGltaXRlZC5zaXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAl05B
EUfpErPpREHoq1M+//N638+NF6iZE/I/S+0FBNoX1p9OcMXD+ZIDfnWZSHPtP0wc
4UpsZGEEdboY5dEIHSCUj/KmoAJI/k3JHMc25eHIQIPU/jxbH8zlb5Ku/RuJVs2
Q0dkfiSG/emHres+dIKXjMjQixWZxOEtOdX2X/cM5ybUECi62LY1WuO6Kz2/nj/D
/9m9hC0YAdmBL4liaP8QB50tkmbgGH4I8rupwHrvwPou1Yq/66RQcqnRw+Y4WiQ1
HEM9rw366lsPhMvUfIDkr03zgoL/+x0mieMq3SdF55Vakv1dIMP+Rkf0IBSuwSqL
jDHAntpnioXWiW/fGQIDAQABo4IB4TCCAd0wDgYDVR0PAQH/BAQDAgeAMIGgBggr
BgEFBQcBAQSBkzCBkDBOBggrBgEFBQcwAoZCaHR0cDovL3NlY3VyZS5nbG9iYWxz
aWduLmNvbS9jYWNlcnQvZ3NleHRlbmRjb2Rlc2lnbnNoYTJnM29jc3AuY3J0MD4G
CCsGAQUFBzABhjJodHRwOi8vb2NzcDIuZ2xvYmFsc2lnbi5jb20vZ3NleHRlbmRj
b2Rlc2lnbnNoYTJnMzBVBgNVHSAETjBMMEEGCSsGAQQBoDIBAjA0MDIGCCsGAQUF
BwIBFiZodHRwczovL3d3dy5nbG9iYWxzaWduLmNvbS9yZXBvc2l0b3J5LzAHBgVn
gQwBAzAJBgNVHRMEAjAAMEUGA1UdHwQ+MDwwOqA4oDaGNGh0dHA6Ly9jcmwuZ2xv
YmFsc2lnbi5jb20vZ3NleHRlbmRjb2Rlc2lnbnNoYTJnMy5jcmwwKgYDVR0RBCMw
IYEfYWRtaW5pc3RyYXRvckBsaXphc2xpbWl0ZWQuc2l0ZTAfBgNVHSUEGDAKBggr
BgEFBQcDAzAdBgNVHQ4EFgQUFeavK8qKjtluSAQeuEeIY9/HKKIwHwYDVR0jBBgw
FoAU3CxYLCpvNS2feZWoSF3Eb1l5lv/kwDQYJKoZIhvcNAQELBQADggEBAMY/uhfn
ssh6Nc/9c11lAp+QasEyN/juRv6GUWwfy8sXNAkDPGgR/aan8s+khjVpH2iapzut
XG0f9qtg9kGAfnSHwnEEA/Cv3Z5xrnHXZppFOhsc1nd4pW3MNZchlCYqg3urn09hdA
Cb3MtefroAvLACdJjFIR8CB8ugBPEgqQhudYd58/PSHcv1V/eA/QdC0PlL/WGvb6
sNFYuV1d0GGG5eeHVqbqeDtyArfoVjHbwQ3EDRIS3dB8dpw1u+EAtRO93b9f6rnYh
Yo3dcFafk/vXONIWW2L2iZgd68rsoZup3cB8S61vFWCoJlwwSkXUo8cLz/2rnz4WX
OoqoUS1In5KbP1I=
-----END CERTIFICATE-----

Acerca de ElevenPaths

En ElevenPaths, la unidad global de ciberseguridad del Grupo Telefónica, creemos que es posible un mundo digital más seguro. Apoyamos a nuestros clientes en su **transformación digital,** creando **innovación disruptiva**, aportando la privacidad y la confianza necesaria en nuestra vida digital diaria.

Combinamos la frescura y energía de una start-up con la potencia, conocimiento y robustez de Telefónica, contribuyendo con soluciones que posibilitan la prevención, detección y respuesta ante amenazas diarias en nuestro mundo digital.

Generamos alianzas estratégicas que permiten ampliar la seguridad de nuestros clientes y además, colaboramos con organismos y entidades como la Comisión Europea, Cyber Threat Alliance, ECSO, EuroPol, Incibe, y la Organización de los Estados Americanos (OEA).

Acerca del CSIRT-SCC

El CSIRT-SCC (Security Cyberoperations Center) es el equipo de respuesta ante emergencias informáticas de clientes de Telefónica España. Está integrado por un conjunto de profesionales especializados en las diferentes disciplinas de la atención de incidentes: gestión, análisis forenses y análisis de malware.

El CSIRT-SCC cuenta, además, con el respaldo del resto de áreas de seguridad del SOC (gestión de dispositivos de seguridad, threat hunting...) y con el apoyo en las últimas tecnologías disponibles así como con el soporte del equipo de ElevenPaths.

2019 © Telefónica Digital España, S.L.U. Todos los derechos reservados.