



UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

MALWARE ANALYSIS: JIGSAW

Presentato da:

Lorenzo Esposito M63001417
Michele De Fazio M63001440
Armando Zevola M63001514





Roadmap

Scopriamo i rischi che possiamo correre facendo un largo utilizzo della realtà virtuale.

1

ANALISI STATICÀ

- PEStudio
 - VirusTotal
 - Dependency Walker
 - Capa
-

2

DISASSEMBLER

- dotPeek
-

3

ANALISI DINAMICA

- Esecuzione
 - Autoruns
 - ProcMon
-

4

MALWARE DETECTION AND PREVENTION

- Yara rule
- MITRE ATT&CK



Analisi statica

1

L'**analisi statica** assume un ruolo cruciale nella comprensione del malware Jigsaw, consentendo di esaminare in dettaglio le caratteristiche e i comportamenti del malware **senza attivarlo**.

Questo approccio rivela le firme peculiari del ransomware, come le **stringhe di testo distintive** e le **funzioni crittografiche**.

Attraverso strumenti specializzati, è possibile identificare indicatori di compromissione e pattern comportamentali, essenziali per la rilevazione e la mitigazione delle minacce.

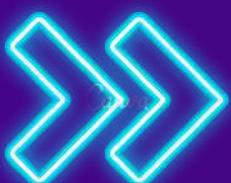


PEStudio 1

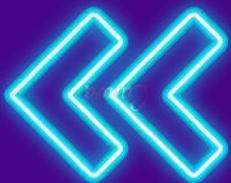
Il tool **PEStudio** ha consentito l'individuazione dell'InternalName del file eseguibile, identificato sotto il nome di **BitcoinBlackmailer.exe**.

Le informazioni relative alla natura del file rivelano che, secondo la voce **FileDescription**, il malware si maschera da **Firefox**.

The screenshot shows the PEStudio interface with the file structure of `c:\users\unina\Desktop\malware-basic\jigsaw.exe`. The left pane lists sections such as indicators, virus total results, dos-header, rich-header, file-header, optional-header, directories, sections, libraries, and functions. The right pane provides a detailed view of the functions, namespaces, and libraries used by the malware, highlighting the presence of `EncryptFile` and `DecryptFile` functions.



property	value
md5	9A4913BBDA97F3A1389B9213806F20FA
sha1	18DFA329B62BE64A12135615DE48C2821AF2D8ED
sha256	7C4287724AD22DEE386319CDD1B7592357F7798D2FAC080BD97E35226F59D6CC
file-type	executable
language	neutral
code-page	Unicode UTF-16, little endian
Comments	n/a
CompanyName	n/a
FileDescription	Firefox
FileVersion	37.0.2.5583
InternalName	BitcoinBlackmailer.exe
LegalCopyright	Copyright 1999-2012 Firefox and Mozilla developers. All rights reserved.
LegalTrademarks	n/a
OriginalFilename	BitcoinBlackmailer.exe
ProductName	Firefox
ProductVersion	37.0.2.5583
Assembly Version	37.0.2.5583



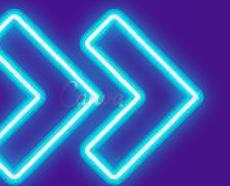
Dalla sezione dedicata alle funzioni (functions), si evince che ci si trova di fronte a un possibile **ransomware**, data la presenza delle funzioni **EncryptFile** e **DecryptFile**.

Inoltre, la funzione **WinExec** indica la possibilità di avviare un nuovo processo a livello utente.

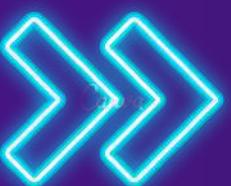
PEStudio

1

encoding (2)	size (bytes)	location	blacklist (17)	hint (1207)	value (8428)
ascii	17	0x00045035	x	utility	ConfuserEx v0.6.0
ascii	14	0x00039118	x	function	VirtualProtect
ascii	11	0x00040383	x	function	EncryptFile
ascii	11	0x0004038F	x	function	DecryptFile
ascii	12	0x00042A54	x	function	MemoryStream
ascii	15	0x000430CF	x	function	ProcessedByFody
ascii	19	0x000430DF	x	function	ConfusedByAttribute
ascii	18	0x000439F7	x	function	GetProcessesByName
ascii	14	#Strings	x	function	VirtualProtect
ascii	11	#Strings	x	function	EncryptFile
ascii	11	#Strings	x	function	DecryptFile
ascii	12	#Strings	x	function	MemoryStream
ascii	15	#Strings	x	function	ProcessedByFody
ascii	19	#Strings	x	function	ConfusedByAttribute
ascii	18	#Strings	x	function	GetProcessesByName
ascii	7	0x0003F221	x	-	WinExec
ascii	7	#Strings	x	-	WinExec



indicator (39)	detail	level
strings > blacklist	count: 17	1
virustotal > score	value: 67/74	1
functions > blacklist	count: 2	1
section > blacklist	section: ??!mmUPp	1
section > first > writable	section: ??!mmUPp	1
entry-point > location	section: :0x004E00A	1
sections > writable > executable	count: 1	1
URL > pattern	url: http://btc.blockr.io/api/v1/	1
sections > nameless	count: 1	2



ConfuserEx è un popolare strumento open-source utilizzato per offuscare applicazioni .NET, che è il framework con cui è scritto il codice del ransomware.

Il suo obiettivo è modificare il codice in modo tale da rendere difficile da comprendere e analizzare per chi tenta di eseguire il reverse engineering.

Nella sezione URL > pattern, è stato individuato un URL sospetto. Questo sarà oggetto di un'ulteriore analisi nella prossima fase dell'indagine.

VirusTotal

1

L'indagine su **VirusTotal** ha riportato una segnalazione da parte di un security vendor, indicando che il file potrebbe essere **malevolo**.

Dall'analisi della **risposta HTTP** corrispondente, si evince che l'URL finale effettua un reindirizzamento al sito di **Coinbase**, utilizzato come intermediario per effettuare la transazione in bitcoin richiesta dall'attaccante come possibile **riscatto**.

Questo rafforza ulteriormente l'ipotesi che ci troviamo di fronte a un **ransomware**.

The screenshot shows the VirusTotal interface. On the left, a summary bar indicates 1/89 security vendor flagged the URL as malicious. The main panel displays the URL `http://btc.blockr.io/api/v1/` with a status of 200, content type `text/html; charset=utf-8`, and a last analysis date of "1 year ago". To the right, detailed analysis results are shown, including:

Parameter	Value
First Submission	2016-09-11 13:20:57 UTC
Last Submission	2023-04-28 14:45:49 UTC
Last Analysis	2023-04-28 14:45:49 UTC
HTTP Response	(details: Final URL https://www.coinbase.com/)
Serving IP Address	104.16.151.172
Status Code	200
Body Length	47.19 KB
Body SHA-256	77b8d39d3b60ff7b24ea93b688d75089824634bca1959f6418d2571d6dd339c

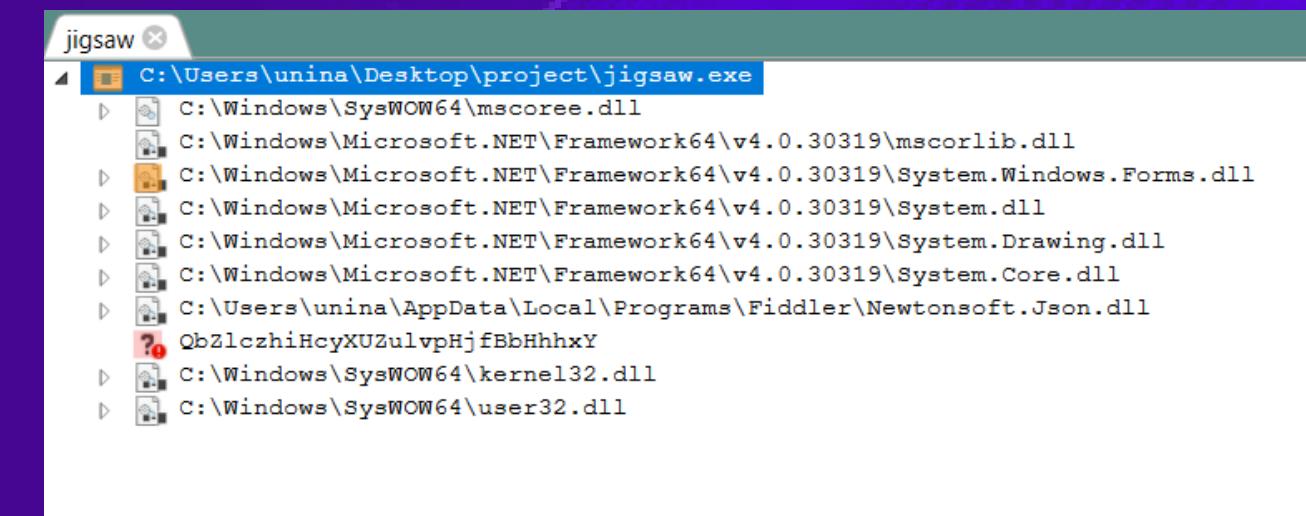
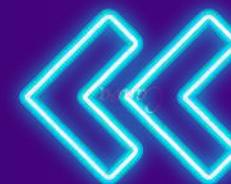
Dependency Walker 1

È stata eseguita un'analisi delle dipendenze utilizzando il tool **Dependency Walker**.

In primo luogo, è stata individuata una **libreria offuscata**, resa indecifrabile intenzionalmente dall'attaccante.

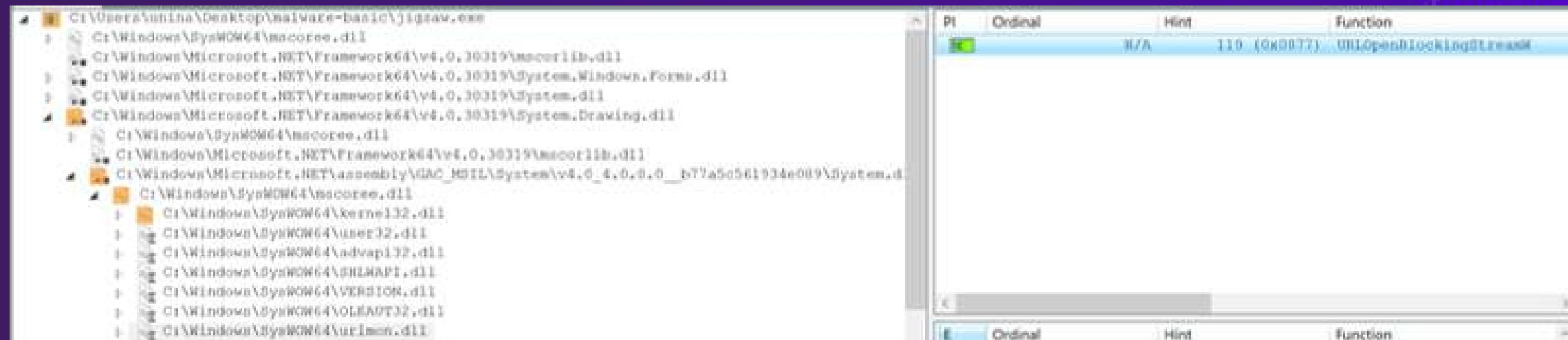
Di particolare interesse è la libreria **mscoree.dll**, che contiene le funzioni di **crittografia** e **decrittografia**.

```
C:\Windows\SysWOW64\ole32.dll
C:\Windows\SysWOW64\CRYPT32.dll
C:\Windows\SysWOW64\rasapi32.dll
C:\Windows\SysWOW64\secur32.dll
C:\Windows\SysWOW64\WS2_32.dll
C:\Windows\SysWOW64\httpapi.dll
C:\Windows\SysWOW64\wininet.dll
```



Tra gli import di mscoree.dll si nota una libreria denominata **CRYPT32.dll**, che presumibilmente impiegata per fare crittografia sfruttando il sistema operativo ospitante.

Dependency Walker ①



La funzione **URLOpenBlockingStreamW** è parte dell'API di Windows e viene utilizzata per aprire un URL e ottenere un flusso di dati a blocchi. Questa funzione è utile quando si desidera scaricare dati da un URL in modo sincrono, ovvero il thread chiamante viene bloccato fino a quando l'operazione non è completata. La versione **W** indica che la funzione utilizza stringhe wide-character.

Capa

1

```
packed with Confuser
namespace anti-analysis/packer/confuser
author william.ballenthin@mandiant.com
scope file
att&ck Defense Evasion::Obfuscated Files or Information::Software Packing [T1027.002]
mbc Anti-Static Analysis::Software Packing::Confuser [F0001.009]
examples b9f5bd514485fb06da39beff051b9fdc
or:
string: "ConfusedByAttribute" @ 0x430DF

contain a resource (.rsrc) section
namespace executable/pe/section/rsrc
author moritz.raabe@mandiant.com
scope file
examples A933A1A402775CFA94B6BEE0963F4B46:0x41fd25
section: .rsrc @ 0x44A000
```



```
(internal) dotnet file limitation
namespace internal/limitation/file
author william.ballenthin@mandiant.com
description This sample appears to be a .NET module.

.NET is a cross-platform framework for running managed applications.
capa cannot handle non-native files. This means that the results may be misleading or incomplete.
You may have to analyze the file manually, using a tool like the .NET decompiler dnSpy.

scope file
examples b9f5bd514485fb06da39beff051b9fdc
or:
match: runtime/dotnet @ 0x0
or:
import: mscoree._CorExeMain @ 0x44E000

(internal) packer file limitation
namespace internal/limitation/file
author william.ballenthin@mandiant.com
description This sample appears to be packed.

Packed samples have often been obfuscated to hide their logic.
capa cannot handle obfuscation well. This means the results may be misleading or incomplete.
If possible, you should try to unpack this input file before analyzing it with capa.

scope file
examples CD2CBA9E6313E8DF2C1273593E649682
or:
match: anti-analysis/packer @ 0x0
or:
string: "ConfusedByAttribute" @ 0x430DF
```



Il tool **Capa** non riporta informazioni rilevanti
riguardo al malware in questione.

Questo indica che il malware è **offuscato**.

È consigliato utilizzare un **decompiler .NET**,
poiché il malware è stato compilato utilizzando
il framework .NET.

```
compiled to the .NET platform
namespace runtime/dotnet
author william.ballenthin@mandiant.com
scope file
examples b9f5bd514485fb06da39beff051b9fdc
or:
import: mscoree._CorExeMain @ 0x44E000
```

Disassembler ②

L'uso del **disassembler** ha permesso di applicare tecniche di **reverse engineering**, traducendo il codice macchina eseguibile di un programma in un linguaggio assembly leggibile dall'uomo.

L'obiettivo è comprendere il comportamento e la logica interna del malware **senza disporre del suo codice sorgente originale**.

È stato perciò impiegato il disassembler **dotPeek**.



dotPeek ②

```
using System;
using System.Collections;
using System.Collections.Generic;
using System.IO;
using System.Runtime.CompilerServices;
using System.Runtime.InteropServices;
using System.Security.Cryptography;

#nullable disable
namespace Main.Tools

{
    internal static class Locker
    {
        private static readonly string EncryptedFilePath;
        private static readonly HashSet<string> EncryptedFiles;
        private const string EncryptionFileExtension = ".fun";
        private const string EncryptionPassword = "OoIsAwwF23cICQoLDA00De==";

        internal static void EncryptFileSystem()
        {
            // ISSUE: unable to decompile the method.
        }

        internal static HashSet<string> GetEncryptedFiles()
        {
            // ISSUE: unable to decompile the method.
        }
    }
}
```



```
using Microsoft.Win32;
using System;
using System.IO;
using System.Runtime.InteropServices;
using System.Windows.Forms;

#nullable disable
namespace Main.Tools

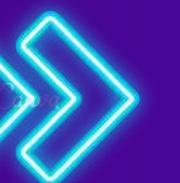
{
    internal static class Windows
    {
        private static readonly IntPtr HWND_TOPMOST;
        private const uint SWP_NOSIZE = 1;
        private const uint SWP_NOMOVE = 2;

        internal static void SetStartup(Main.Tools.Windows.StartupMethodType startupMethod)
        {
            // ISSUE: unable to decompile the method.
        }

        private static void SetStartupFolder()
        {
            // ISSUE: unable to decompile the method.
        }

        private static void SetStartupRegistry(string exePath)
        {
            // ISSUE: unable to decompile the method.
        }

        internal static void RemoveStartupRegistry(string exePath)
        {
            // ISSUE: unable to decompile the method.
        }
    }
}
```



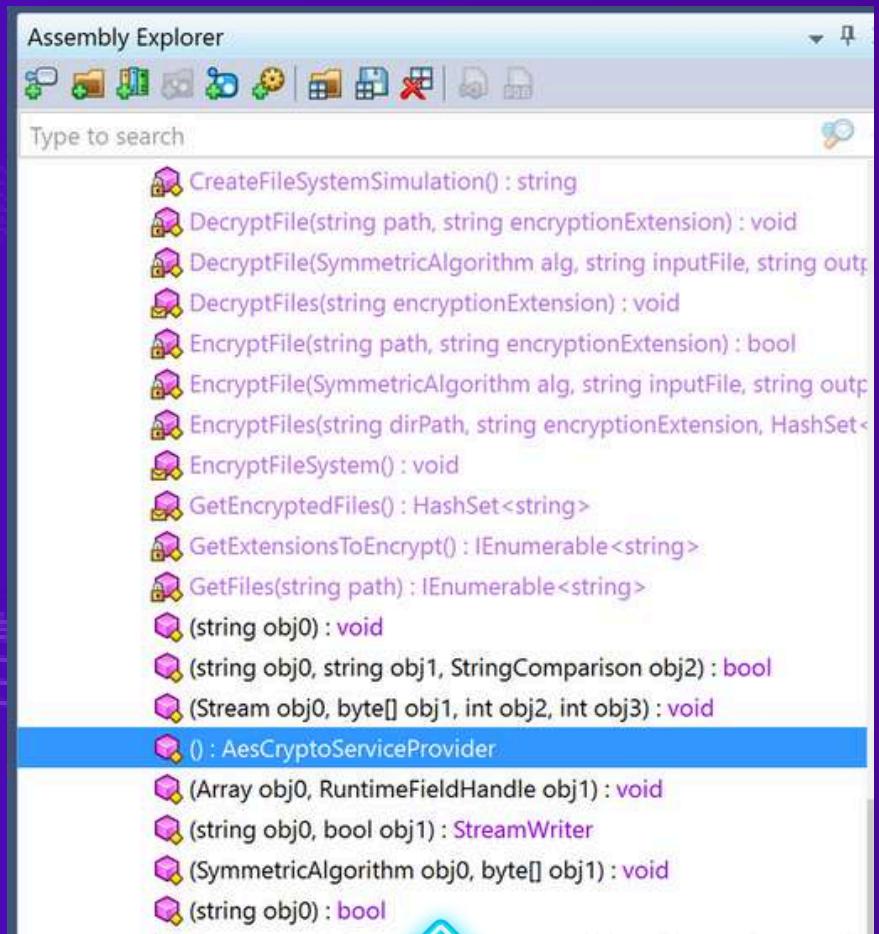
Attraverso lo strumento **dotPeek**, abbiamo individuato la classe **Locker**, situata all'interno del namespace **Main.Tools**, che contiene tutti gli strumenti utilizzati dal ransomware durante l'esecuzione.

In particolare, si nota che i dati criptati sono identificati con l'estensione **.fun**, e viene individuata, inoltre, anche la **password** utilizzata per l'encryption.

Tuttavia, non tutti i metodi all'interno delle classi del namespace sono **decompilabili**.

In particolare, quelli appartenenti alla classe **Windows**, responsabili della **persistenza** e dell'esecuzione del virus sotto il falso nome di **Firefox** (o **Dropbox**).

dotPeek ②



```
Users > lorenzoesposito > public AesCryptoServiceProvider()<cs>
1  public AesCryptoServiceProvider()
2  {
3      string providerName = "Microsoft Enhanced RSA and AES Cryptographic Provider";
4      if (Environment.Version.Major == 5 && Environment.Version.Minor == 1)
5      {
6          providerName = "Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)";
7      }
8      this.m_cspHandle = CapINative.AcquireCspnull(providerName, CapINative.ProviderType.RsaAes, CapINative.CryptAcquireContextFlags.VerifyContext, true);
9      this.FeedbackSizeValue = 8;
10     int keySizeValue = 0;
11     KeySizes[] array = AesCryptoServiceProvider.FindSupportedKeySizes(this.m_cspHandle, out keySizeValue);
12     if (array.Length != 0)
13     {
14         this.KeySizeValue = keySizeValue;
15     }
16     return;
17     throw new PlatformNotSupportedException(SR.GetString("Cryptography_PlatformNotSupportedException"));
18 }
19 [SecuritySafeCritical]
20 internal
21 {
22     public override ICryptoTransform CreateDecryptor()
23     {
24         if (this._key == null || this._key.Invalid || this._key.Closed)
25         {
26             throw new CryptographicException(SR.GetString("Cryptography_DecryptWithNoKey"));
27         }
28         return this.CreateDecryptor(this._key, this._value);
29     }
30 }
```



AesCryptoServiceProvider risulta essere un metodo standard per la crittografia fornito dal sistema operativo.

Dal disassemblatore si evince che l'algoritmo di cifratura utilizzato è di tipo **simmetrico**. Nello specifico, l'algoritmo in questione è **AesCryptoServiceProvider**

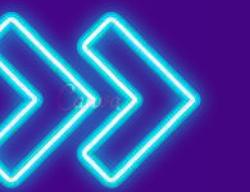
Per questo motivo, è stata realizzata una nostra versione della chiamata ad AesCryptoServiceProvider per ipotizzare come il malware possa utilizzarla.

dotPeek ②

```
static int (
    [In] Stream obj0,
    [In] byte[] obj1,
    [In] int obj2,
    [In] int obj3)
{
    return obj0.Read(obj1, obj2, obj3);
}

static void (
    [In] Stream obj0,
    [In] byte[] obj1,
    [In] int obj2,
    [In] int obj3)
{
    obj0.Write(obj1, obj2, obj3);
}

static ICryptoTransform ([In] SymmetricAlgorithm obj0)
{
    return obj0.CreateDecryptor();
}
```



La manipolazione degli oggetti tramite crittografia simmetrica è confermata dalla presenza di funzioni che criptano i file presenti nel file system.

In particolare, la funzione **ICryptoTransform()** è responsabile di queste manipolazioni, andando a trasformare gli oggetti passati come parametri.

IDA Pro

2

```
seg000:00002070 Main_Tools_Locker_EncryptFile proc far
seg000:00002070             cmp    edi, esp
seg000:00002072             jp     short near ptr Main_Tools_Locker_____+1
seg000:00002074             stosd
seg000:00002075             cmpsb
seg000:00002076             nop
seg000:00002077             lock   xor ebx, [ecx+edi*8]
seg000:00002078             adc    edi, esp
seg000:0000207D             lds    edi, [eax+65h]
seg000:00002080             lahf
seg000:00002081             shl    byte ptr [ecx-74h], 48h
seg000:00002085             inc    ebp
seg000:00002086             cmc
seg000:00002087             int    3          ; Trap to Debugger
seg000:00002088             xchg   eax, ebp
seg000:00002089             push   esp
seg000:0000208A             xor    ch, [ecx]
seg000:0000208C             mov    ebx, 0C7BA6FBAh
seg000:00002091             retf   92BEh
seg000:00002091 Main_Tools_Locker_EncryptFile endp.; sp-analysis failed
seg000:00002091
```



L'analisi effettuata con il disassemblatore **IDA Pro** ha rivelato che anche questo strumento incontra **difficoltà nel ricostruire il codice assembly** del malware a causa delle **tecniche di offuscamento** utilizzate.

Tuttavia, a differenza del precedente tool, IDA Pro ha fornito informazioni utili riguardanti la **gestione dei debugger** durante l'esecuzione del codice.

Come mostrato in figura, la linea "**int 3**" funge da breakpoint, interrompendo l'esecuzione del codice per **ostacolare l'analisi** da parte degli analisti di malware.



Analisi dinamica 3

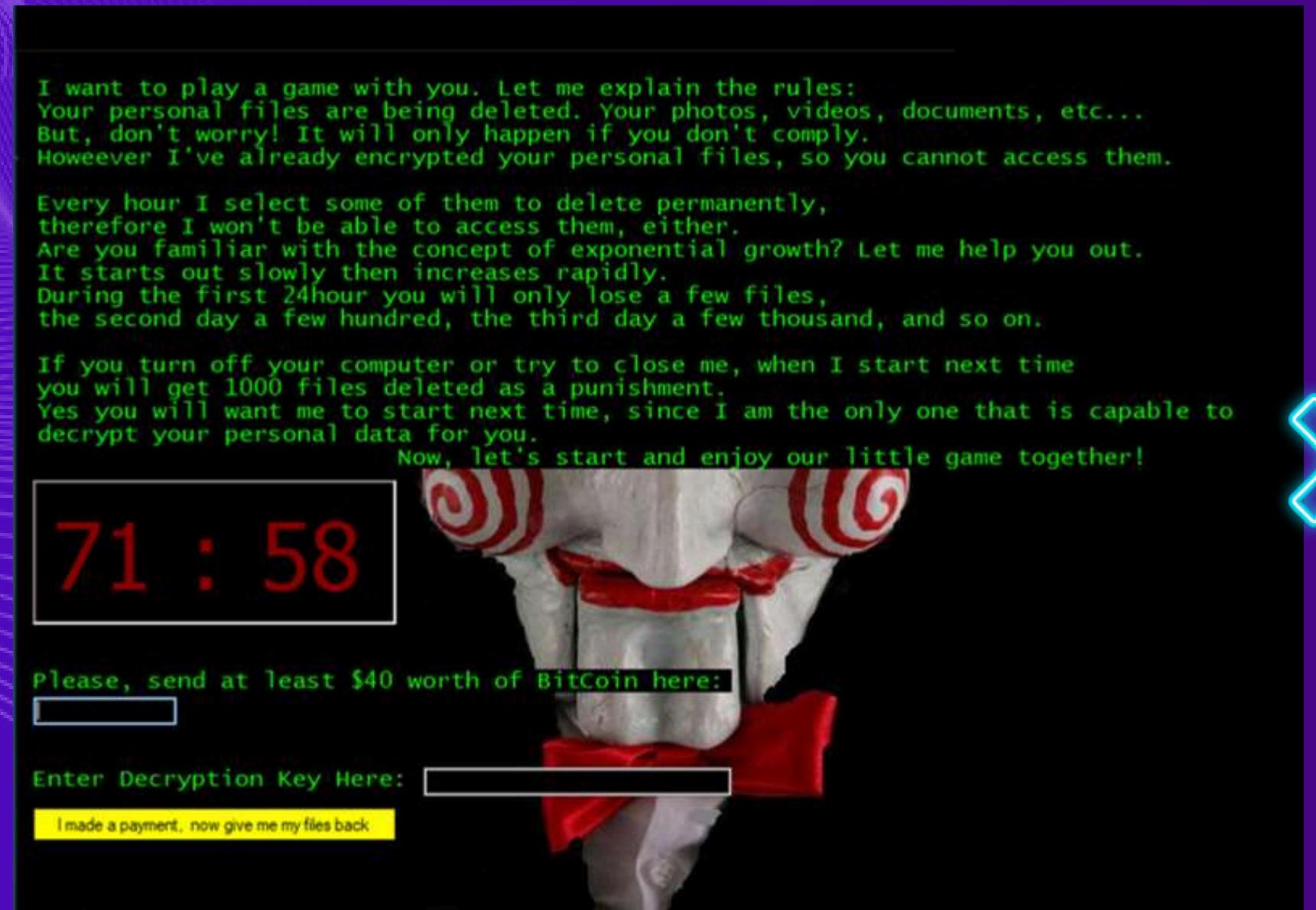
L'**analisi dinamica** è fondamentale nello studio del ransomware Jigsaw, poiché permette di osservare il comportamento del malware in un **ambiente controllato**.

Questo processo aiuta a comprendere **come Jigsaw crittografa i file**, manipolando le risorse di sistema.

L'analisi dinamica è essenziale per identificare le tecniche di **evasione** e **persistenza** del malware, confermando, inoltre, le ipotesi effettuate nell'analisi statica.



Esecuzione 3

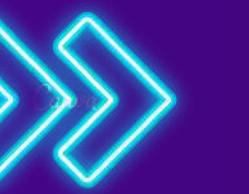
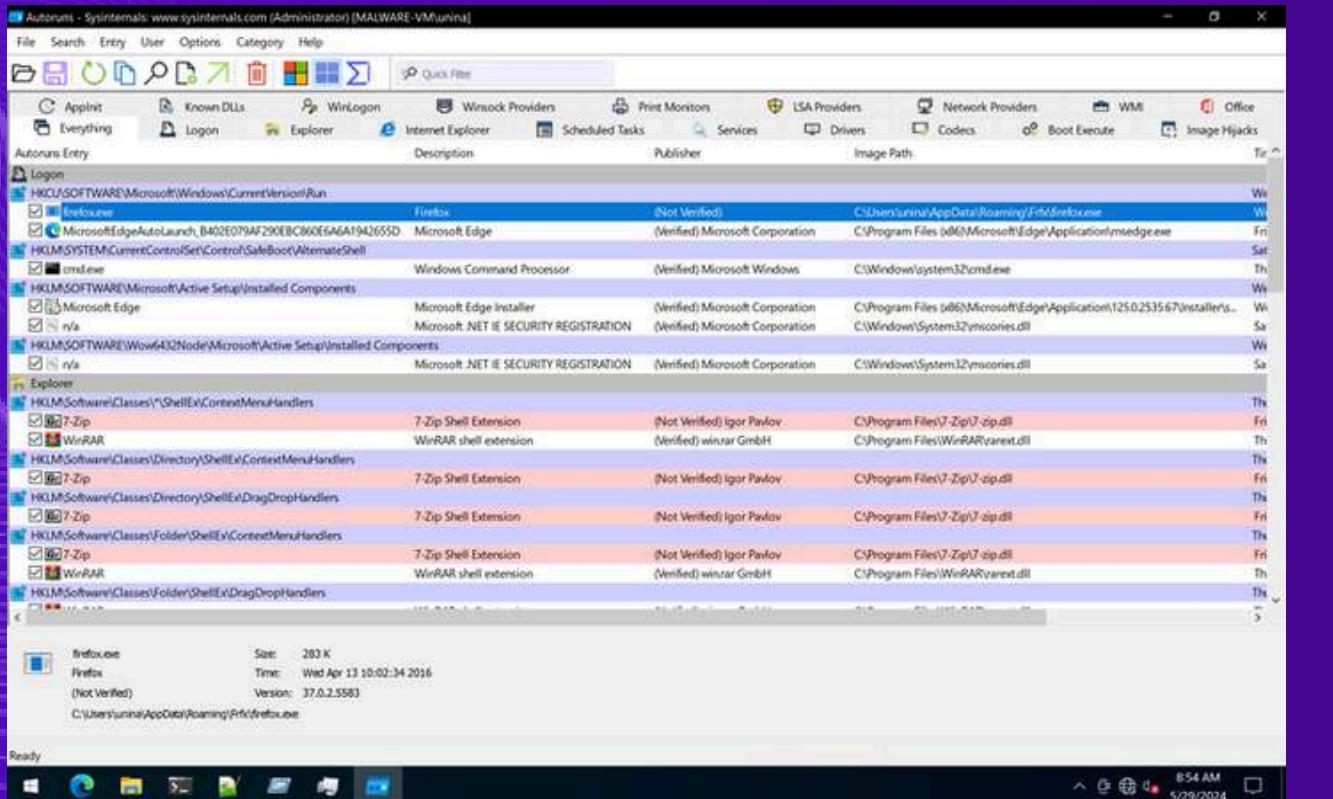


Alla fine della crittografia di tutti i file del file system, il ransomware Jigsaw avvia un'interfaccia grafica (**GUI**) in cui vengono fornite le istruzioni per il "gioco". Questo gioco richiede il pagamento di un **riscatto in bitcoin**, con la minaccia che, col passare del tempo senza pagamento, un numero crescente di file verrà eliminato.

L'esecuzione è stata realizzata in un **ambiente controllato**, utilizzando una **macchina virtuale Windows** con tutte le opzioni di Windows Defender disattivate. Inoltre, sono state disabilitate le funzionalità di drag and drop e copy-paste tra la macchina virtuale e l'host, isolando ulteriormente l'ambiente e prevenendo qualsiasi fuoriuscita del malware.

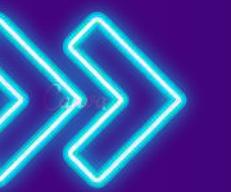
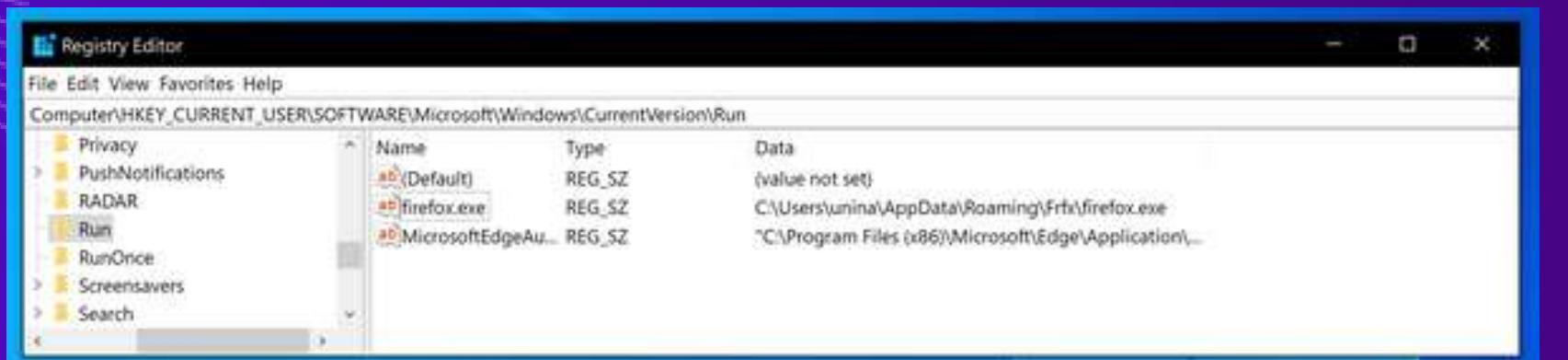
Persistenza

3



Il malware interviene sui registri di Windows, inserendo una chiave per avviare un'istanza di **Firefox**.

Questo comportamento è stato rilevato utilizzando il tool **Autoruns**.



Mediante l'ausilio del tool ProcMon, si ottiene la conferma che la path fornita da Autoruns è stata modificata dall'eseguibile Jigsaw

ProcMon

3

Time	Process	Event ID	Action	Target Path	Result	Details
10:32:14	jigsaw.exe	1836	RegQueryValue	HKEY\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup	SUCCESS	Type: REG_EXPAND_SZ
10:32:14	jigsaw.exe	1836	RegCloseKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	SUCCESS	
10:32:14	jigsaw.exe	1836	QueryOpen	C:\Users\unina\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	SUCCESS	CreationTime: 4/27/2018 10:32:14 AM
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	SUCCESS	Offset: 811,000, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.dll	SUCCESS	Offset: 6,984,704, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscowks.dll	SUCCESS	Offset: 6,956,032, Len: 1,000,000
10:32:14	jigsaw.exe	1836	RegQueryKey	HKEY\CLL	SUCCESS	Query: HandleTag
10:32:14	jigsaw.exe	1836	RegOpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Read
10:32:14	jigsaw.exe	1836	RegQueryValue	HKEY\Software\Microsoft\Windows\CurrentVersion\Run\firefox.exe	NAME NOT FOUND	Length: 12
10:32:14	jigsaw.exe	1836	RegSetValue	HKEY\Software\Microsoft\Windows\CurrentVersion\Run\firefox.exe	SUCCESS	Type: REG_SZ, Len: 12
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	SUCCESS	Offset: 1,556,480, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	SUCCESS	Offset: 1,540,096, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	SUCCESS	Offset: 2,285,568, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	SUCCESS	Offset: 4,186,112, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	SUCCESS	Offset: 2,904,056, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	SUCCESS	Offset: 1,462,272, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	SUCCESS	Offset: 2,199,552, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	SUCCESS	Offset: 380,928, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	SUCCESS	Offset: 3,846,144, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	SUCCESS	Offset: 1,093,632, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	SUCCESS	Offset: 4,141,056, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	SUCCESS	Offset: 2,191,360, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	SUCCESS	Offset: 364,544, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	SUCCESS	Offset: 4,042,752, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	SUCCESS	Offset: 2,965,504, Len: 1,000,000
10:32:14	jigsaw.exe	1836	ReadFile	C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll	SUCCESS	Offset: 4,247,552, Len: 1,000,000



Analizzando i **log** generati dal tool **ProcMon**, si ottiene un'ulteriore prova della **persistenza** del file **firefox.exe**.

Questa persistenza viene realizzata tramite l'operazione **RegSetValue** in corrispondenza del percorso mostrato in figura.

ProcMon

3

10:32:14.4372405 AM	■ jigsaw.exe	1836	QueryAttributeInformation...C:\Users\unina\AppData\Roaming\Frfix\firefox.exe
10:32:14.4372685 AM	■ jigsaw.exe	1836	QueryBasicInformationFile C:\Users\unina\AppData\Roaming\Frfix\firefox.exe
10:32:14.4372829 AM	■ jigsaw.exe	1836	QueryAttributeInformation...C:\Users\unina\Desktop\malware-basic\jigsaw.exe
10:32:14.4374789 AM	■ jigsaw.exe	1836	QueryOpen C:\Windows\System32\ntmarta.dll
10:32:14.4375451 AM	■ jigsaw.exe	1836	CreateFile C:\Windows\System32\ntmarta.dll
10:32:14.4375984 AM	■ jigsaw.exe	1836	CreateFileMapping C:\Windows\System32\ntmarta.dll
10:32:14.4376268 AM	■ jigsaw.exe	1836	CreateFileMapping C:\Windows\System32\ntmarta.dll
10:32:14.4378195 AM	■ jigsaw.exe	1836	Load Image C:\Windows\System32\ntmarta.dll
10:32:14.4379373 AM	■ jigsaw.exe	1836	CloseFile C:\Windows\System32\ntmarta.dll
10:32:14.4381790 AM	■ jigsaw.exe	1836	CreateFile C:\Windows\System32\ntmarta.dll
10:32:14.4382117 AM	■ jigsaw.exe	1836	QuerySecurityFile C:\Windows\System32\ntmarta.dll
10:32:14.4382233 AM	■ jigsaw.exe	1836	QuerySecurityFile C:\Windows\System32\ntmarta.dll
10:32:14.4382338 AM	■ jigsaw.exe	1836	CloseFile C:\Windows\System32\ntmarta.dll
10:32:14.4384002 AM	■ jigsaw.exe	1836	QueryRemoteProtocolInf... C:\Users\unina\Desktop\malware-basic\jigsaw.exe
10:32:14.4384200 AM	■ jigsaw.exe	1836	QuerySecurityFile C:\Users\unina\Desktop\malware-basic\jigsaw.exe
10:32:14.4384326 AM	■ jigsaw.exe	1836	QueryRemoteProtocolInf... C:\Users\unina\AppData\Roaming\Frfix\firefox.exe
10:32:14.4384448 AM	■ jigsaw.exe	1836	QuerySecurityFile C:\Users\unina\AppData\Roaming\Frfix\firefox.exe
10:32:14.4384819 AM	■ jigsaw.exe	1836	ReadFile C:\Windows\System32\ntdll.dll
10:32:14.4396021 AM	■ jigsaw.exe	1836	ReadFile C:\Windows\System32\ntdll.dll



Jigsaw sfrutta la libreria **ntmarta.dll** per realizzare la **privilege escalation**. Questa operazione consente al malware di accedere alla libreria di interfaccia con il kernel di Windows, **ntdll.dll**, per eseguire operazioni avanzate a basso livello e manipolare la sicurezza del sistema al fine di evitare la rilevazione.

ProcMon

3

10:32:14.6451299 AM	jigsaw.exe	1836	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\BAM
10:32:14.6451739 AM	jigsaw.exe	1836	Process Create	C:\Users\unina\AppData\Local\Drpbx\drpbx.exe
10:32:14.6451808 AM	drpbx.exe	2608	Process Start	
10:32:14.6451878 AM	drpbx.exe	2608	Thread Create	
10:32:14.6452280 AM	jigsaw.exe	1836	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls
10:32:14.6452395 AM	jigsaw.exe	1836	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls
10:32:14.6452572 AM	jigsaw.exe	1836	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option
10:32:14.6452683 AM	jigsaw.exe	1836	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option
10:32:14.6452886 AM	jigsaw.exe	1836	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
10:32:14.6453065 AM	jigsaw.exe	1836	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
10:32:14.6453168 AM	jigsaw.exe	1836	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\AuthenticodeEnabled
10:32:14.6453280 AM	jigsaw.exe	1836	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
10:32:14.6453415 AM	jigsaw.exe	1836	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
10:32:14.6454253 AM	jigsaw.exe	1836	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
10:32:14.6454418 AM	jigsaw.exe	1836	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
10:32:14.6454601 AM	jigsaw.exe	1836	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
10:32:14.6454778 AM	jigsaw.exe	1836	RegOpenKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion
10:32:14.6454911 AM	jigsaw.exe	1836	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
10:32:14.6455183 AM	jigsaw.exe	1836	QuerySecurityFile	C:\Users\unina\AppData\Local\Drpbx\drpbx.exe
10:32:14.6456019 AM	jigsaw.exe	1836	CreateFile	C:\Windows\apppatch\sysmain.sdb



Durante l'esecuzione, Jigsaw crea il processo **drpbx.exe**, il quale è direttamente responsabile della crittografia dei dati del file system.

ProcMon

3

10:32:24.1816541 AM	drpbx.exe	2608	QueryOpen	C:\Users\unina\AppData\Local\Drpbx\CRYPTSP.dll
10:32:24.1817414 AM	drpbx.exe	2608	QueryOpen	C:\Windows\System32\cryptsp.dll
10:32:24.1817974 AM	drpbx.exe	2608	CreateFile	C:\Windows\System32\cryptsp.dll
10:32:24.1818587 AM	drpbx.exe	2608	CreateFileMapping	C:\Windows\System32\cryptsp.dll
10:32:24.1818799 AM	drpbx.exe	2608	CreateFileMapping	C:\Windows\System32\cryptsp.dll
10:32:24.1820351 AM	drpbx.exe	2608	Load Image	C:\Windows\System32\cryptsp.dll
10:32:24.1821648 AM	drpbx.exe	2608	CloseFile	C:\Windows\System32\cryptsp.dll
10:32:24.1823656 AM	drpbx.exe	2608	CreateFile	C:\Windows\System32\cryptsp.dll
10:32:24.1823985 AM	drpbx.exe	2608	QuerySecurityFile	C:\Windows\System32\cryptsp.dll
10:32:24.1824090 AM	drpbx.exe	2608	QuerySecurityFile	C:\Windows\System32\cryptsp.dll
10:32:24.1824184 AM	drpbx.exe	2608	CloseFile	C:\Windows\System32\cryptsp.dll
10:32:24.1825398 AM	drpbx.exe	2608	ReqQueryKey	HKLM

10:32:24.1826144 AM	drpbx.exe	2608	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography
10:32:24.1826205 AM	drpbx.exe	2608	RegQueryValue	C:\Windows\System32\rsaenh.dll
10:32:24.1827137 AM	drpbx.exe	2608	QueryOpen	C:\Windows\System32\rsaenh.dll
10:32:24.1827677 AM	drpbx.exe	2608	CreateFile	C:\Windows\System32\rsaenh.dll
10:32:24.1828082 AM	drpbx.exe	2608	CreateFileMapping	C:\Windows\System32\rsaenh.dll
10:32:24.1828254 AM	drpbx.exe	2608	CreateFileMapping	C:\Windows\System32\rsaenh.dll
10:32:24.1829930 AM	drpbx.exe	2608	Load Image	C:\Windows\System32\rsaenh.dll
10:32:24.1831492 AM	drpbx.exe	2608	Load Image	C:\Windows\System32\bcrypt.dll
10:32:24.1833043 AM	drpbx.exe	2608	CloseFile	C:\Windows\System32\rsaenh.dll
10:32:24.1834075 AM	drpbx.exe	2608	CreateFile	C:\Windows\System32\bcrypt.dll
10:32:24.1834372 AM	drpbx.exe	2608	QuerySecurityFile	C:\Windows\System32\bcrypt.dll
10:32:24.1834461 AM	drpbx.exe	2608	QuerySecurityFile	C:\Windows\System32\bcrypt.dll
10:32:24.1834540 AM	drpbx.exe	2608	CloseFile	C:\Windows\System32\bcrypt.dll
10:32:24.1835267 AM	drpbx.exe	2608	CreateFile	C:\Windows\System32\rsaenh.dll
10:32:24.1835463 AM	drpbx.exe	2608	QuerySecurityFile	C:\Windows\System32\rsaenh.dll
10:32:24.1835537 AM	drpbx.exe	2608	QuerySecurityFile	C:\Windows\System32\rsaenh.dll
10:32:24.1835610 AM	drpbx.exe	2608	CloseFile	C:\Windows\System32\rsaenh.dll
10:32:24.1837210 AM	drpbx.exe	2608	RegQueryKey	HKLM
10:32:24.1837329 AM	drpbx.exe	2608	RegOpenKey	HKLM\Software\Policies\Microsoft\Cryptogr



Successivamente, il processo drpbx.exe importa le **librerie** di funzioni di crittografia, tra cui **cryptsp.dll**, **rsaenh.dll** e **bcrypt.dll**

ProcMon

3

10:32:24.1510226 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files
10:32:24.1511388 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files
10:32:24.1511539 AM	drpbx.exe	2608	CloseFile	C:\Program Files
10:32:24.1512475 AM	drpbx.exe	2608	CreateFile	C:\Program Files
10:32:24.1512756 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files*
10:32:24.1512976 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files
10:32:24.1513513 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files
10:32:24.1513635 AM	drpbx.exe	2608	CloseFile	C:\Program Files
10:32:24.1514630 AM	drpbx.exe	2608	CreateFile	C:\Program Files (x86)
10:32:24.1514870 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files (x86)*
10:32:24.1515122 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files (x86)
10:32:24.1515895 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files (x86)
10:32:24.1516038 AM	drpbx.exe	2608	CloseFile	C:\Program Files (x86)
10:32:24.1516948 AM	drpbx.exe	2608	CreateFile	C:\Program Files (x86)
10:32:24.1517154 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files (x86)*
10:32:24.1517374 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files (x86)
10:32:24.1517691 AM	drpbx.exe	2608	QueryDirectory	C:\Program Files (x86)
10:32:24.1517855 AM	drpbx.exe	2608	CloseFile	C:\Program Files (x86)
10:32:24.1518804 AM	drpbx.exe	2608	CreateFile	C:\ProgramData
10:32:24.1519028 AM	drpbx.exe	2608	QueryDirectory	C:\ProgramData*
10:32:24.1519246 AM	drpbx.exe	2608	QueryDirectory	C:\ProgramData
10:32:24.1519578 AM	drpbx.exe	2608	QueryDirectory	C:\ProgramData
10:32:24.1519702 AM	drpbx.exe	2608	CloseFile	C:\ProgramData
10:32:24.1520888 AM	drpbx.exe	2608	CreateFile	C:\ProgramData
10:32:24.1521115 AM	drpbx.exe	2608	QueryDirectory	C:\ProgramData*
10:32:24.1521322 AM	drpbx.exe	2608	QueryDirectory	C:\ProgramData
10:32:24.1521596 AM	drpbx.exe	2608	QueryDirectory	C:\ProgramData
10:32:24.1521710 AM	drpbx.exe	2608	CloseFile	C:\ProgramData
10:32:24.1522381 AM	drpbx.exe	2608	CreateFile	C:\Recovery
10:32:24.1532605 AM	drpbx.exe	2608	QueryDirectory	C:\Recovery*
10:32:24.1532845 AM	drpbx.exe	2608	QueryDirectory	C:\Recovery
10:32:24.1533016 AM	drpbx.exe	2608	QueryDirectory	C:\Recovery
10:32:24.1533145 AM	drpbx.exe	2608	CloseFile	C:\Recovery
10:32:24.1534240 AM	drpbx.exe	2608	CreateFile	C:\Recovery
10:32:24.1534432 AM	drpbx.exe	2608	QueryDirectory	C:\Recovery*
10:32:24.1534627 AM	drpbx.exe	2608	QueryDirectory	C:\Recovery
10:32:24.1534779 AM	drpbx.exe	2608	QueryDirectory	C:\Recovery
10:32:24.1534893 AM	drpbx.exe	2608	CloseFile	C:\Recovery
10:32:24.1535580 AM	drpbx.exe	2608	CreateFile	C:\System Volume Information
10:32:24.1538353 AM	drpbx.exe	2608	CreateFile	C:\System Volume Information
10:32:24.1540367 AM	drpbx.exe	2608	CreateFile	C:\tmp
10:32:24.1548358 AM	drpbx.exe	2608	QueryDirectory	C:\tmp*
10:32:24.1548713 AM	drpbx.exe	2608	QueryDirectory	C:\tmp
10:32:24.1549005 AM	drpbx.exe	2608	QueryDirectory	C:\tmp
10:32:24.1549158 AM	drpbx.exe	2608	CloseFile	C:\tmp



Il processo **drpbx.exe** esplora il file system per mapparlo e crittografare i dati presenti nelle varie cartelle.

ProcMon

3

10:32:24.2139286 AM	drpbx.exe	2608	CreateFile	C:\Program Files\7-Zip\History.txt
10:32:24.2148179 AM	drpbx.exe	2608	CreateFile	C:\Program Files\7-Zip\History.txt.fun
10:32:24.2224256 AM	drpbx.exe	2608	ReadFile	C:\Windows\System32\bcrypt.dll
10:32:24.2232469 AM	drpbx.exe	2608	ReadFile	C:\Windows\System32\bcrypt.dll
10:32:24.2242049 AM	drpbx.exe	2608	ReadFile	C:\Windows\System32\bcryptprimitives.dll
10:32:24.2248136 AM	drpbx.exe	2608	ReadFile	C:\Windows\System32\bcryptprimitives.dll
10:32:24.2285847 AM	drpbx.exe	2608	ReadFile	C:\Windows\System32\rsaenh.dll
10:32:24.2290940 AM	drpbx.exe	2608	ReadFile	C:\Windows\System32\rsaenh.dll
10:32:24.2363332 AM	drpbx.exe	2608	ReadFile	C:\Program Files\7-Zip\History.txt
10:32:24.2364443 AM	drpbx.exe	2608	ReadFile	C:\Program Files\7-Zip\History.txt
10:32:24.2431746 AM	drpbx.exe	2608	ReadFile	C:\Windows\System32\rsaenh.dll
10:32:24.2437966 AM	drpbx.exe	2608	ReadFile	C:\Windows\System32\rsaenh.dll
10:32:24.2488272 AM	drpbx.exe	2608	WriteFile	C:\Program Files\7-Zip\History.txt.fun
10:32:24.2490227 AM	drpbx.exe	2608	ReadFile	C:\Program Files\7-Zip\History.txt
10:32:24.2552869 AM	drpbx.exe	2608	WriteFile	C:\Program Files\7-Zip\History.txt.fun
10:32:24.2560381 AM	drpbx.exe	2608	CloseFile	C:\Program Files\7-Zip\History.txt.fun
10:32:24.2566257 AM	drpbx.exe	2608	CloseFile	C:\Program Files\7-Zip\History.txt
10:32:24.2591027 AM	drpbx.exe	2608	CreateFile	C:\Program Files\7-Zip\History.txt
10:32:24.2591497 AM	drpbx.exe	2608	QueryAttributeTagFile	C:\Program Files\7-Zip\History.txt
10:32:24.2591649 AM	drpbx.exe	2608	SetDispositionInformationEx	C:\Program Files\7-Zip\History.txt
10:32:24.2591829 AM	drpbx.exe	2608	CloseFile	C:\Program Files\7-Zip\History.txt



Viene fornito un **esempio** di criptazione di un file.

Il file "**History.txt**" viene crittografato con l'estensione "**.fun**", rendendolo inaccessibile e inutilizzabile.

Questa operazione coinvolge le librerie **bcrypt.dll**, **bryptprimitives.dll** e **rsaenh.dll**.



Malware Detection and Prevention

4

L'analisi del malware Jigsaw ha previsto l'implementazione di tecniche avanzate per la sua **rilevazione e prevenzione**.

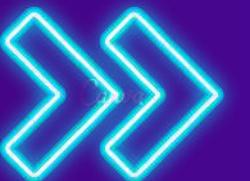
Per la **rilevazione**, è stata utilizzata **Yara**, uno strumento efficace per creare regole personalizzate in grado di identificare specifici pattern nel codice del malware. Una **regola Yara** è stata sviluppata appositamente per individuare Jigsaw con precisione.

Sul fronte della **prevenzione**, è stato adottato il framework **MITRE ATT&CK**, che fornisce un **modello** dettagliato delle **tecniche** e **tattiche** utilizzate dai malware. L'applicazione delle conoscenze di MITRE ATT&CK ha permesso di implementare misure preventive mirate a contrastare le attività dannose di Jigsaw..



Yara Rule 4

```
detyara  x
detyara
1 rule jig_check{
2
3     strings:
4         $by = {4D 5A}
5         $vs1 = "Copyright 1999-2012 Firefox and Mozilla developers. All rights reserved." ascii wide nocase
6         $vs2 = "QbZlczhiHcyXUZulvpHjfBbHhxY" ascii wide nocase
7
8         $s1 = "OoIsAwF23cICQoLDA00De==" ascii wide nocase
9         $s2 = "http://btc.blockr.io/api/v1/" ascii wide nocase
10        $s3 = "Drpbx\\drpbx.exe" ascii wide nocase
11        $s4 = "Frfx\\firefox.exe" ascii wide nocase
12
13        $c1 = "Jigsaw" ascii wide nocase
14        $c2 = "I want to play a game" ascii wide nocase
15        $c3 = ".fun" ascii wide nocase
16        $c4 = "BitcoinBlackmailer.exe" ascii wide nocase
17        $c5 = "Your computer files have been encrypted. Your photos, videos, documents, etc...." ascii wide nocase
18
19
20
21
22
23     condition:
24         ($by at 0) and ( (1 of ($vs*)) or (2 of ($s*)) or (all of ($c*)) )
25
26
27
28 }
```



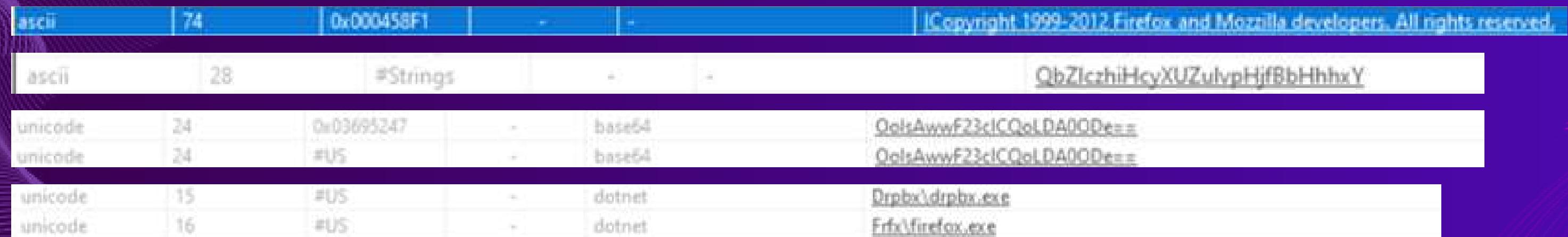
Per implementare la detection del malware, è stata creata una **regola Yara** denominata "**jig_check**". Nella sezione di codice "**strings**" sono state dichiarate le seguenti variabili:

- **\$by**: byte che identificano il file indipendentemente dall'estensione
- **\$vs1**: dichiarazione di copyright
- **\$vs2**: import non codificato
- **\$s1**: chiave di crittografia
- **\$s2**: URL malevolo che reindirizza al sito di CoinBase
- **\$s3**: eseguibile per crittografare
- **\$s4**: eseguibile per la persistenza
- **\$c***: stringhe comuni mostrate sulla GUI del programma

Nella sezione "**condition**" viene definita, infine, al condizione da rispettare per la detection.

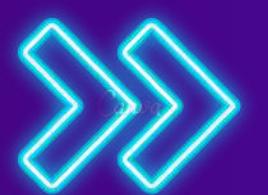
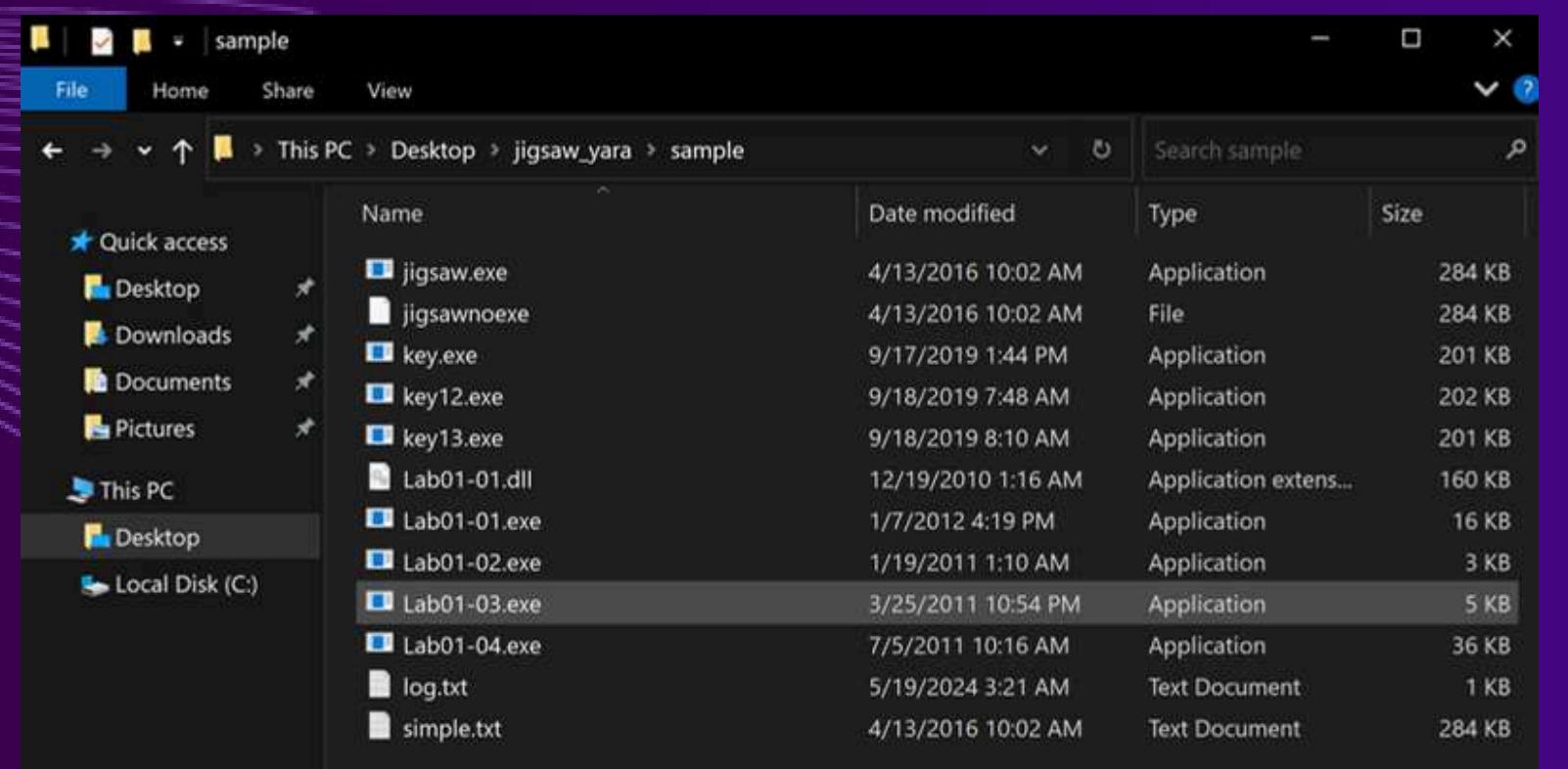
Yara Rule 4

Le informazioni necessarie per assegnare i valori alle variabili sono state ricavate utilizzando il tool PEStudio.



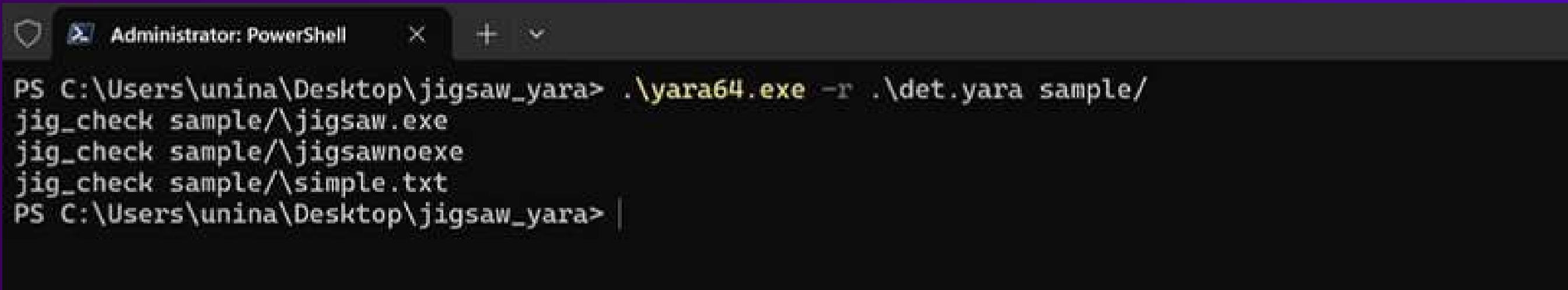
The screenshot shows the PEStudio interface with the 'Strings' tab selected. It displays several string entries:

Type	Length	Address	String Value
ascii	28	0x000458F1	QbZlczhiHcyXUZulvpHjfBbHhhgY
unicode	24	0x03695247	QolsAwwF23cICQoLDA00D==
unicode	24	#US	QolsAwwF23cICQoLDA00D==
unicode	15	#US	Dpbx\dpbx.exe
unicode	16	#US	Ffh\firefox.exe



Viene inoltre definita una cartella “**sample**” di campioni, che sarà utilizzata come directory target da cui rilevare Jigsaw secondo la regola Yara **jig_check**. Vengono introdotte diverse tipologie di eseguibili per verificare che la regola riesca a individuare il file corretto.

Yara Rule ④



A screenshot of a Windows PowerShell window titled "Administrator: PowerShell". The command run is ".\yara64.exe -r ..\det.yara sample/jig_check sample/\jigsaw.exe". The output shows three matches: "jig_check sample/\jigsaw.exe", "jig_check sample/\jigsawnoexe", and "jig_check sample/\simple.txt". The PowerShell window has a dark theme.

```
PS C:\Users\unina\Desktop\jigsaw_yara> .\yara64.exe -r ..\det.yara sample/
jig_check sample/\jigsaw.exe
jig_check sample/\jigsawnoexe
jig_check sample/\simple.txt
PS C:\Users\unina\Desktop\jigsaw_yara>
```



Viene presentato un esempio di esecuzione di **Yara** con l'applicazione della regola implementata. La regola funziona correttamente, individuando non solo la versione standard di Jigsaw (**jigsaw.exe**), ma rilevando anche Jigsaw senza estensione (**jigsawnoexe**) e Jigsaw con un'estensione txt (**simple.txt**).

Initial Access (TA0001)

- **Phishing (T1566):** Il ransomware Jigsaw viene tipicamente distribuito tramite email di phishing con allegati infetti o link a siti web compromessi che permettono il download dell'exe.

Execution (TA0002)

- **User Execution (T1204):** Gli utenti eseguono il malware involontariamente aprendo allegati di email dannosi o facendo clic sul file exe scaricato.

Persistence (TA0003)

- **Registry Run Keys / Startup Folder (T1547.001):** Jigsaw crea voci nei registry di windows per lanciare l'istanza firefox all'avvio della macchina vittima.

Defense Evasion (TA0005)

- **Obfuscated Files or Information (T1027):** Utilizza tecniche di offuscamento per rendere il malware più difficile da analizzare con l'analisi statica.
- **Debugger Evasion (T1622):** Utilizza delle tecniche di rilevazione della modalità di debug per impedire l'impiego di break point.

Discovery (TA0007)

- **File and Directory Discovery (T1083):** Scansione di file e directory per individuare la struttura del filesystem e dei file da crittografare.

Impact (TA0040)

- **Data Encrypted for Impact (T1486):** Crittografa i file dell'utente e richiede un riscatto per la decrittazione.
- **Data Destruction (T1485):** Elimina periodicamente file fino a quando non viene pagato il riscatto.
- **Inhibit System Recovery (T1490):** Cancella i punti di ripristino del sistema per impedire il recupero dei dati.

Grazie per l'attenzione



UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II