

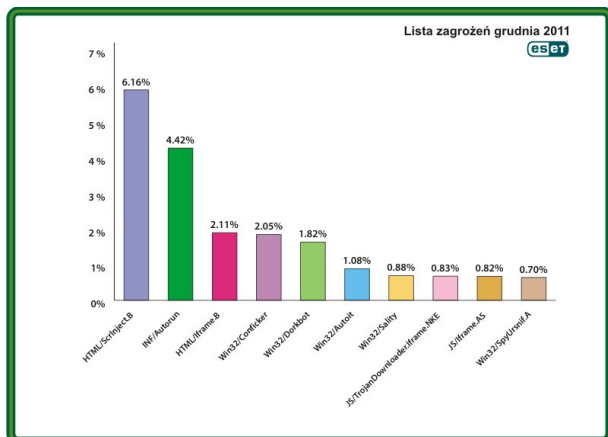


# Global threat report

GRUDZIEŃ 2011

Globalne trendy w rozwoju zagrożeń





W ostatnim miesiącu minionego roku najczęściej atakującymi zagrożeniami komputerowymi okazały się złośliwe programy z rodziny ScrInject.B, które infekują za pośrednictwem stron WWW. Równie popularne okazały się aplikacje z rodziny Iframe.B, które ukrywają się na stronach HTML jako niewidoczne ramki. Ich kliknięcie powoduje przeniesienie do innego serwisu.

### 1. HTML/ScrInject.B

Pozycja w poprzednim rankingu: 3

Odsetek wykrytych infekcji: 6.16%

ESET oznacza jako HTML/ScrInject.B wszystkie zagrożenia wykrywane na stronach HTML jako skrypty powodujące automatyczne pobieranie na komputer użytkownika kolejnych złośliwych programów.

### 2. INF/Autorun

Pozycja w poprzednim rankingu: 1

Odsetek wykrytych infekcji: 4.42%

Programy tego typu wykorzystują pliki autorun.inf, powodujące automatyczne uruchamianie nośników, do infekowania komputerów użytkowników. Programy rozprzestrzeniają się bardzo szybko z powodu popularnej metody przenoszenia danych za pomocą nośników pendrive, zawierających właśnie pliki autorun.

### 3. HTML/Iframe.B

Pozycja w poprzednim rankingu: 4

Odsetek wykrytych infekcji: 2.11%

To zagrożenia ukrywające się na stronach WWW w postaci niewidocznych ramek, których kliknięcie powoduje przekierowanie do innego serwisu internetowego i zainfekowanie komputera nowym zagrożeniem.

### 4. Win32/Conficker

Pozycja w poprzednim rankingu: 5

Odsetek wykrytych infekcji: 2.05%

Robak internetowy, który rozprzestrzenia się wykorzystując załataną już lukę w usłudze RPC systemów operacyjnych Windows. Po zagnieżdzeniu się w systemie Conficker łączy się z ustalonymi domenami, z których otrzymuje instrukcje dalszego działania, m.in. pobrania kolejnych zagrożeń. W zależności od wariantu Conficker może rozprzestrzeniać się za pośrednictwem załączników do poczty elektronicznej lub przenośnych dysków USB, wykorzystując do infekowania pliki automatycznego startu.

### 5. Win32/Dorkbot

Pozycja w poprzednim rankingu: 2

Odsetek wykrytych infekcji: 1.82%

Win32/Dorkbot.A to robak rozprzestrzeniający się za pomocą wymiennych nośników danych. Zawiera on backdoor i może być kontrolowany zdalnie. Podczas gdy użytkownik przegląda różne witryny, robak zbiera podawane przez niego dane – m.in. nazwy użytkownika i hasła, a następnie wysyła zgromadzone informacje do zdalnej maszyny.

## 6. Win32/Autoit

Pozycja w poprzednim rankingu: 6

Odsetek wykrytych infekcji: 1.08%

Robak internetowy, który rozprzestrzenia się za pośrednictwem nośników danych lub przez MSN. Win32/Autoit przedostaje się do komputera z zainfekowanej strony internetowej lub jako jeden z elementów innego złośliwego programu. Po zainfekowaniu systemu zagrożenie szuka na dysku wszystkich plików wykonywalnych i zastępuje je kopią zawierającą swój złośliwy kod.

## 7. Win32/Sality

Pozycja w poprzednim rankingu: 7

Odsetek wykrytych infekcji: 0.88%

Sality to zagrożenie polimorficzne. Po zagnieżdzeniu się w komputerze swojej ofiary usuwa z rejestru klucze powiązane z aplikacjami zabezpieczającymi, a następnie tworzy w rejestrze wpis, dzięki któremu może uruchamiać się każdorazowo przy starcie systemu operacyjnego. Sality modyfikuje pliki z rozszerzeniami EXE oraz SCR.

## 8. JS/TrojanDownloader.Iframe.NKE

Pozycja w poprzednim rankingu: 9

Odsetek wykrytych infekcji: 0.83%

Koń trojański, który przekierowuje przeglądarkę na określony adres URL, gdzie znajduje się złośliwe oprogramowanie. Kod Iframe.NKE zwykle ukrywa się na stronach HTML.

## 9. JS/Iframe.AS

Pozycja w poprzednim rankingu: 24

Odsetek wykrytych infekcji: 0.82%

Koń trojański, który po zainfekowaniu komputera przekierowuje internautę na strony WWW, zawierające złośliwe oprogramowanie. Zagrożenie ukrywa się w kodzie HTML.

## 10. Win32/Spy.Ursnif.A

Pozycja w poprzednim rankingu: 15

Odsetek wykrytych infekcji: 0.70%

Zagrożenia tego typu wykradają informacje z zainfekowanego komputera PC i wysyłają je prosto do hakera. Spy.Ursnif.A umożliwia atakującemu przejście kontroli nad maszyną użytkownika i instalację kolejnych zagrożeń.

## Globalne raporty z systemu ThreatSense.Net

Lista zagrożeń powstaje dzięki ThreatSense.Net, innowacyjnej technologii zbierania próbek wirusów od ponad 140 milionów użytkowników na całym świecie. Gromadzone w ten sposób informacje poddawane są analizie statystycznej w laboratoriach ESET tworząc najbardziej kompleksowy wśród istniejących raportów o zagrożeniach obecnych w sieci. Każdego dnia dzięki ThreatSense.Net analizowane jest od 200 do 300 tysięcy próbek różnego rodzaju zagrożeń.

ThreatSense.Net ewoluował z witryny virusradar.com, której system raportujący wyposażono w udoskonalone narzędzia do gromadzenia danych statystycznych. W przeciwieństwie do virusradar.com ThreatSense.Net nie gromadzi danych za pośrednictwem poczty elektronicznej - informacje o aktualnych zagrożeniach trafiają do laboratoriów ESET prosto od użytkowników ESET NOD32 Antivirus oraz ESET Smart Security.

Z uwagi na niezwykle tempo rozprzestrzeniania się i mutowania większości współczesnych złośliwych programów ważne jest, aby rozwiązanie antywirusowe posiadało nie tylko często aktualizowaną bazę sygnatur, ale również żeby dany program dysponował ochroną proaktywną, a więc aby chronił przed nowymi jeszcze nieznanymi zagrożeniami.

### Dystrybucja w Polsce:

Biuro Bezpieczeństwa IT firmy DAGMA

ul. Bażantów 4/2

40-668 Katowice

[www.eset.pl](http://www.eset.pl)

### Zakupy:

tel.: 32 259 11 00

e-mail: [handel@dagma.pl](mailto:handel@dagma.pl)

### Wsparcie techniczne:

e-mail: [pomoc@dagma.pl](mailto:pomoc@dagma.pl)