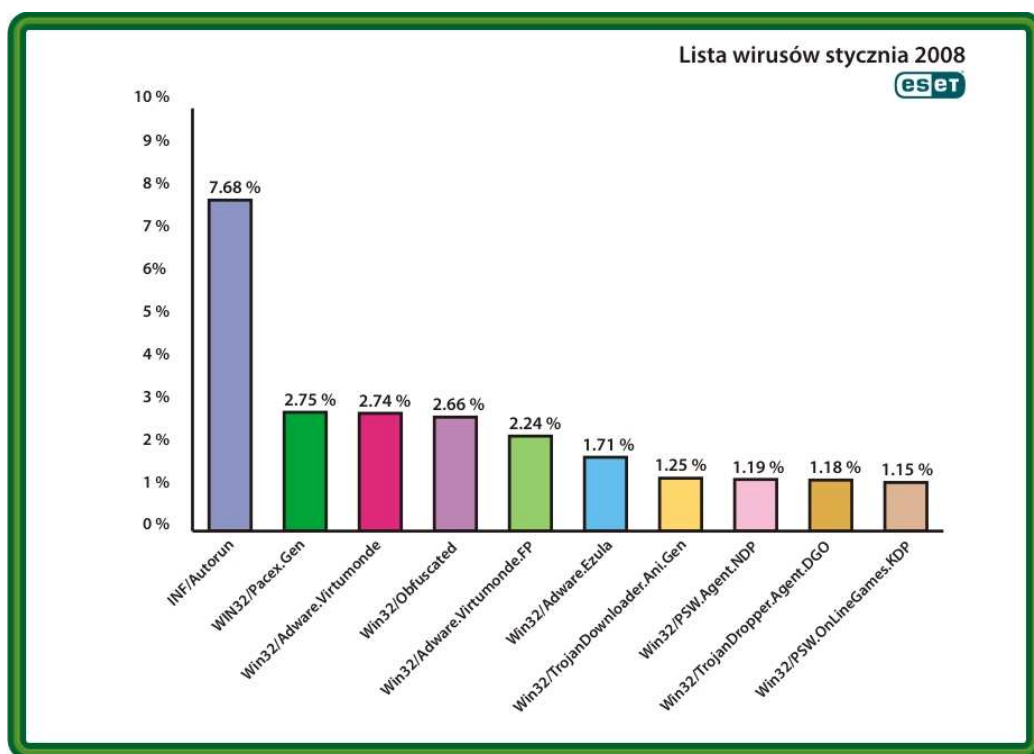




Wirusy stycznia - globalne trendy w rozwoju zagrożeń

W styczniu najczęściej atakującym użytkowników zagrożeniem okazała się rodzina złośliwych programów INF/Autorun infekujących komputery poprzez pliki powodujące automatyczne uruchamianie danego nośnika po włożeniu go do stacji. Według danych zabranych przez system ThreatSense.Net od użytkowników programów firmy ESET zagrożenia te stanowiły ponad 7% wszystkich wykrytych w styczniu infekcji.



1. INF/Autorun

Pozycja w poprzednim rankingu: 2

Odsetek wykrytych infekcji: 7.68%

Prawie 7% wykrytych przez ThreatSense infekcji stanowiły zagrożenia oznaczane przez laboratoria ESET jako INF/Autorun. Wykorzystują one pliki autorun.inf do infekowania komputerów użytkowników. Zagrożenie może rozprzestrzeniać się bardzo szybko z powodu popularnej obecnie metody przenoszenia danych za pośrednictwem nośników typu pendrive zawierających właśnie pliki autorun.

2. Win32/Pacex.Gen

Pozycja w poprzednim rankingu: 7

Odsetek wykrytych infekcji: 2.75%

Nazwa ta służy do określania różnego rodzaju złośliwych programów, które ukrywają swoją obecność przed użytkownikiem i są wykorzystywane m.in. przez konie trojańskie do kradzieży haseł użytkowników.

3. Win32/Adware.Virtumonde

Pozycja w poprzednim rankingu: 3

Odsetek wykrytych infekcji: 2.74%

Rodzina potencjalnie niechcianych aplikacji typu adware, które ściągają i wyświetlają na monitorze użytkownika setki irytujących reklam.

4. Win32/Obfuscated.A1

Pozycja w poprzednim rankingu: 1

Odsetek wykrytych infekcji: 2.66%

Zagrożenia systemu Windows, które instalują się na komputerze użytkownika bez jego wiedzy i zgody podczas wizyty na podejrzanej stronie internetowej. Programy te wykorzystują techniki maskujące takie jak kompresja pliku wykonalnego, polimorfizm i dołączanie nadmiarowego kodu. Bardzo często aplikacje te należą do jednej rodziny.

5. Win32/Adware.Virtumonde.FP

Pozycja w poprzednim rankingu: 14

Odsetek wykrytych infekcji: 2.24%

Virtumonde.FP to kolejny program adware należący do rodziny Virtumonde. Aplikacja zasypuje użytkownika denerwującymi reklamami.

6. Win32/Adware.Ezula

Pozycja w poprzednim rankingu: 4

Odsetek wykrytych infekcji: 1.71%

Złośliwy program, który niepostrzeżenie instaluje się na komputerze użytkownika. Aplikacja ściąga na dysk kolejne niechciane programy z serwera zlokalizowanego na Filipinach oraz śledzi i rejestruje wszystkie słowa wpisywane przez użytkownika w oknie przeglądarki internetowej. Program potrafi również sporadycznie wyświetlać niechciane reklamy podczas surfowania w sieci dopasowując ich treść do aktualnej tematyki przeglądanej strony.

7. Win32/TrojanDownloader.Ani.Gen

Pozycja w poprzednim rankingu: 6

Odsetek wykrytych infekcji: 1,71 %

Koń trojański Ani.Gen należący do rodziny zagrożeń wykorzystuje lukę systemu operacyjnego Windows w obsłudze animowanych kursorów.

8. Win32/PSW.Agent.NDP

Pozycja w poprzednim rankingu: 5

Odsetek wykrytych infekcji: 1.19%

Trojan wykorzystywany przez hakerów do wykradania haseł oraz danych o użytkowniku. Największą aktywność wykazywał w listopadzie 2007 roku, kiedy to był najczęściej infekującym użytkowników zagrożeniem.

9. Win32/TrojanDropper.Agent.DGO

Pozycja w poprzednim rankingu: -

Odsetek wykrytych infekcji: 1.18%

Dropper.Agent jest złośliwym programem, który instaluje na komputerze ofiary groźnego konia trojańskiego.

10. Win32/PSW.OnLineGames.KDP

Pozycja w poprzednim rankingu: 53

Odsetek wykrytych infekcji: 1.15%

Program wykradający hasła użytkowników gier online.

Globalne raporty z systemu ThreatSense.Net

Lista zagrożeń powstaje dzięki ThreatSense.Net, innowacyjnej technologii zbierania próbek wirusów od ponad 10 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. Dzięki pomocy użytkowników udało się do tej pory zidentyfikować ponad 10.000 różnych 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:
DAGMA sp. z o.o.
ul. Pszczyńska 15
40-478 Katowice
www.eset.pl

Zakupy oraz wsparcie techniczne:
tel.: (032) 259 11 00
e-mail: sales@dagma.pl

Copyright © 1997 – 2007 ESET. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET. All other names and brands are trademarks of their respective companies.



1.866.343.ESET (3738)