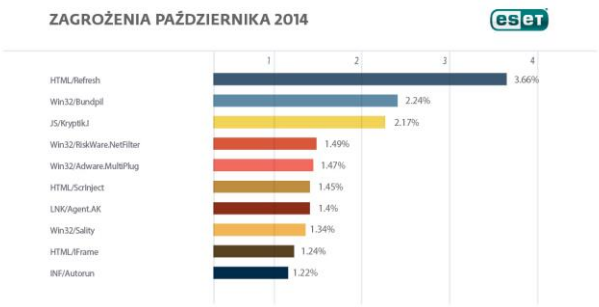
Październik 2014

Globalne trendy w rozwoju zagrożeń

ESET ENJOY SAFER TECHNOLOGY™



W październiku, przyczyną największej liczby infekcji komputerów domowych na świecie był trojan HTML/Refresh, który przekierowuje do określonej lokalizacji URL ze szkodliwym oprogramowaniem

1. HTML/Refresh

Pozycja w poprzednim rankingu: 1

Odsetek wykrytych infekcji: 3.66%

HTML/Refresh to trojan, który przekierowuje do określonej lokalizacji URL ze szkodliwym oprogramowaniem.Kod zagrożenia jest zazwyczaj osadzony na stronach HTML.

2. Win32/Bundpil

Pozycja w poprzednim rankingu: 2

Odsetek wykrytych infekcji: 2.24%

Robak internetowy, który rozprzestrzenia się za pośrednictwem nośników danych np. za pomocą dysków USB. Po zainfekowaniu komputera zagrożenie łączy się z konkretnym adresem URL i pobiera z niego złośliwe aplikacje.

3. JS/Kryptik.I

Pozycja w poprzednim rankingu: 3

Odsetek wykrytych infekcji: 2.17%

Zagrożenie ukrywające się w kodzie JavaScript stron WWW. Zazwyczaj powoduje przekierowanie do innego serwisu internetowego w celu zainfekowania komputera kolejnymi zagrożeniami.

4. Win32/RiskWare.NetFilter

Pozycja w poprzednim rankingu: 4

Odsetek wykrytych infekcji: 1.49%

Win32/RiskWare.NetFilter to aplikacja, która zawiera złośliwy kod mający na celu zmusić zainfekowany komuter do zaangażowania się w niechciane zachowania. Pozwala ona atakującemu na zdalne łączenie się z zainfekowanym systemem i kontrolowanie go w celu kradzieży poufnych informacji lub zainstalowania innego złośliwego oprogramowania.

5. Win32/Adware.MultiPlug

Pozycja w poprzednim rankingu: 4

Odsetek wykrytych infekcji: 1.47%

Win32/Adware.Multiplug jest Aplikacją Potencjalnie Niepożądaną (PUA), która raz pojawiając się w systemie użytkownika może przyczynić się do wyświetlania banerów reklamowych podczas przeglądania stron internetowych.

6. HTML/ScrInject

Pozycja w poprzednim rankingu: 15

Odsetek wykrytych infekcji: 1.45%

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

7. LNK/Agent.AK

Pozycja w poprzednim rankingu: 6

Odsetek wykrytych infekcji: 1.40%

ESET oznacza jako LNK/Agent.AK te odnośniki, których kliknięcie uruchamia aplikację nieszkodliwą dla komputera oraz sprawia, że w tle swoje działanie rozpoczyna złośliwy kod. Jak twierdzą eksperci, ten typ zagrożenia może już wkrótce stać się częścią nowej rodziny zagrożeń typu INF/Autorun.

8. Win32/Sality

Pozycja w poprzednim rankingu: 7

Odsetek wykrytych infekcji: 1.34%

Sality to zagrożenie polimorficzne, które modyfikuje pliki z rozszerzeniami EXE oraz SCR. Usuwa również z rejestru klucze powiązane z aplikacjami antywirusowymi i tworzy wpis, dzięki któremu może uruchamiać się każdorazowo przy starcie systemu.

9. HTML/Iframe

Pozycja w poprzednim rankingu: 8

Odsetek wykrytych infekcji: 1.24%

Zagrożenie ukrywające się w kodzie HTML stron WWW. Powoduje przekierowanie do innego seriwsu internetowego i powoduje zainfekowanie komputera kolejnymi zagrożeniami.

10. INF/Autorun

Pozycja w poprzednim rankingu: 10

Odsetek wykrytych infekcji: 1.22%

To programy wykorzystujące pliki autorun.info, powodujące automatyczne uruchamianie nośników do infekowania komputerów użytkowników. Zagrożenia rozprzestrzeniają się bardzo szybko z powodu popularnej metody przenoszenia danych za pomocą nośników pendrive, zawierających właśnie pliki autorun.

Raporty Globalne trendy w rozwoju zagrożeń

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 niezwykłe 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

Zakupy:
tel.: 32 793 11 00
e-mail: handel@dagma.pl
Wsparcie techniczne:
e-mail: pomoc@eset.pl

ENJOY SAFER TECHNOLOGY™