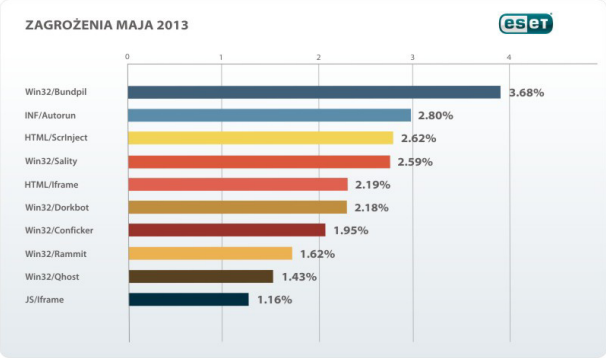
Maj 2013

Globalne trendy w rozwoju zagrożeń



W maju, po raz pierwszy od wielu miesięcy, liderem zestawienia najaktywniejszych zagrożeń komputerowych w skali całego globu nie była rodzina aplikacji INF/Autorun. Najaktywniejszym zagrożeniem ubiegłego miesiąca okazał się robak internetowy Win32/Bundpil.

1. Win32/Bundpil

Pozycja w poprzednim rankingu: 6

Odsetek wykrytych infekcji: 3.68%

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

2. INF/Autorun

Pozycja w poprzednim rankingu: 1

Odsetek wykrytych infekcji: 2.80%

To programy wykorzystujące pliki autorun.inf, 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.

3. HTML/ScrInject.B

Pozycja w poprzednim rankingu: 2

Odsetek wykrytych infekcji: 2.62%

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

4. Win32/Sality

Pozycja w poprzednim rankingu: 3

Odsetek wykrytych infekcji: 2.59%

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.

5. HTML/Iframe.B

Pozycja w poprzednim rankingu: 5

Odsetek wykrytych infekcji: 2.19%

To zagrożenia, ukrywające się w kodzie HTML stron WWW. Powoduje przekierowanie do innego serwisu internetowego i zainfekowanie komputera nowym zagrożeniem.

6. Win32/Dorkbot

Pozycja w poprzednim rankingu: 4

Odsetek wykrytych infekcji: 2.18%

Win32/Dorkbot.A to robak rozprzestrzeniający się za pomocą wymiennych nośników danych. Zawiera 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.

7. Win32/Conficker

Pozycja w poprzednim rankingu: 9

Odsetek wykrytych infekcji: 1.95%

Robak internetowy, który rozprzestrzenia się wykorzystując załataną już lukę w usłudze RPC systemów operacyjnych Windows. Po zagnieżdżeniu 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.

8. Win32/Ramnit

Pozycja w poprzednim rankingu: 7

Odsetek wykrytych infekcji: 1.62%

To wirus komputerowy, który uruchamia się przy każdym starcie systemu. Infekuje pliki dll, exe, htm oraz html. Zagrożenie wykorzystuje lukę CVE-2010-2568, dzięki której może uruchamiać dowolny kod wykonywalny. Ramnit może być kontrolowany zdalnie. Zagrożenie potrafi, m.in. wykonać zrzut ekranu, wysłać informację do zdalnego komputera, pobrać na zainfekowany komputer dowolny plik oraz uruchamić plik wykonywalny lub włączać/wyłączać komputer.

9. Win32/Qhost

Pozycja w poprzednim rankingu: 22

Odsetek wykrytych infekcji: 1.43%

Grupa koni trojańskich, które modyfikują ustawienia DNS na zainfekowanej maszynie przez co zmianie ulega mapowanie nazwy domeny do konkretnego adresu IP. Zmiany poczynione przez Qhost bardzo często uniemożliwiają poprawne połączenie się komputera z serwerem producenta oprogramowania zabezpieczającego (np. programu antywirusowego) w celu pobrania z sieci aktualnej bazy sygnatur.

10. JS/Iframe.B

Pozycja w poprzednim rankingu: 12

Odsetek wykrytych infekcji: 1.16%

To zagrożenia, ukrywające się w kodzie HTML stron WWW. Powoduje przekierowanie do innego serwisu internetowego i zainfekowanie komputera nowym zagrożeniem.

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 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