

[Akceptuję](#)

W ramach naszej witryny stosujemy pliki cookies w celu świadczenia państwu usług na najwyższym poziomie, w tym w sposób dostosowany do indywidualnych potrzeb. Korzystanie z witryny bez zmiany ustawień dotyczących cookies oznacza, że będą one zamieszczone w Państwa urządzeniu końcowym. Możecie Państwo dokonać w każdym czasie zmiany ustawień dotyczących cookies. Więcej szczegółów w naszej [Polityce Prywatności](#)

[Portal](#) [Informacje](#) [Katalog firm](#) [Praca](#) [Szkolenia](#) [Wydarzenia](#) [Porównania międzylaboratoryjne](#)
[Kontakt](#)



[Laboratoria](#)
[.net](#)
[Innowacje](#)
[Nauka](#)
[Technologie](#)



[Logowanie](#) [Rejestracja](#) [pl](#)

Newsletter

zapisz się

Naukowy styl życia

Nauka i biznes

- [Nowe technologie](#)
- [Felieton](#)
- [Tygodnik "Nature"](#)
- [Edukacja](#)
- [Artykuły](#)
- [Przemysł](#)

[Strona główna](#) > [Informacje](#)

Ponad 10, 5 mln zgłoszeń o zagrożeniach w sieciach komputerowych

Ponad 10, 5 mln zgłoszeń dotyczących naruszania bezpieczeństwa w polskich sieciach komputerowych otrzymał CERT Polska w 2012 roku. Najczęściej dotyczyły one rozsyłania spamu i działania botnetów, czyli sieci komputerów kontrolowanych przez

cyberprzestępców.



CERT Polska (z ang. Computer Emergency Response Team) jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskim internecie. Raport za rok 2012 powstał na podstawie danych otrzymanych z różnych automatycznych systemów rejestrujących pojawiające się w sieci zagrożenia. Drugim źródłem informacji były bezpośrednie zgłoszenia do CERT informujące o zagrożeniach.

Z raportu wynika, że najczęściej zgłoszenia dotyczyły rozsyłania spamu internetowego (niechciane lub niepotrzebne wiadomości elektroniczne dostarczane za pośrednictwem poczty elektronicznej) i działania botnetów (czyli sieci komputerów zarażonych złośliwym oprogramowaniem i będących pod zdalną kontrolą cyberprzestępców).

W 2012 roku zespół CERT Polska otrzymał ponad 5 mln (5 189 274) zgłoszeń dotyczących rozsyłania spamu z polskich adresów IP (adres IP to numer, który identyfikuje urządzenie podłączone do sieci, jest on nadawany automatycznie każdemu urządzeniu w momencie podłączenia do internetu). Duża liczba rozsyłanego spamu może być związana z dużą liczbą wykrytych w Polsce sieci botnetów, które bardzo często są wykorzystywane m.in. do rozsyłania spamu, ale także do kradzieży danych, ataków mających doprowadzić do zawieszania konkretnych stron internetowych (tzw. ataki DDoS) oraz oszustw polegających na generowaniu fałszywych kliknięć, na przykład na reklamy.

W ubiegłym roku prawie 2 mln (1 980 941) komputerów polskich użytkowników było częścią kontrolowanych przez cyberprzestępców botnetów. Zdaniem specjalistów, to efekt działalności w polskim internecie botnetu o nazwie "Viruta", złośliwego oprogramowania "DNSChanger" oraz dwóch odmian wirusa bankowego "Zeusa" (tzw. koń trojański). W raporcie podkreślono także, że 137 zgłoszeń dotyczyło zlokalizowanych w Polsce serwerów (specjalnych komputerów) zarządzających sieciami botnetów. Autorzy raportu dodali, że lokalizacja tych serwerów w naszym kraju jest nowym niebezpiecznym trendem.

Drugim istotnym źródłem informacji o pojawiających się zagrożeniach w polskim internecie są zgłaszane bezpośrednio do ekspertów CERT Polska, informacje o atakach czy próbach ataków przeprowadzanych przez cyberprzestępców. Jak podkreślają eksperci są to często najpoważniejsze przypadki, wymagające analizy i bezpośredniego kontaktowania się z zaatakowanymi osobami lub firma w celu przekazania informacji jak poradzić sobie z zagrożeniem.

W 2012 roku zarejestrowano 1082 takich zgłoszeń.

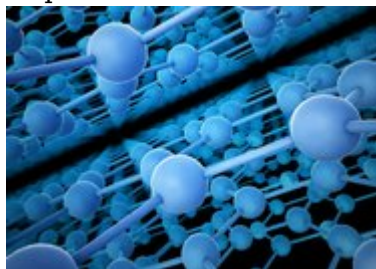
Najwięcej (50 proc.) zgłoszeń dotyczyło tzw. phishingu, czyli zjawiska polegającego na wyłudzeniu poufnych informacji od użytkowników. Cyberprzestępcy najczęściej podszywali się pod zaufaną osobę lub instytucję taką jak bank czy sklep internetowy i w ten sposób zdobywali pożądane informacje.

Pozostałe zgłoszenia do CERT Polska dotyczyły niezidentyfikowanego złośliwego oprogramowania (19,96 proc.), spamu (9,89 proc.) i innych zagrożeń. Jak czytamy w raporcie najczęściej informacje o ataku zgłaszały firmy komercyjne.

Niestety jak wynika z raportu w prawie 80 proc. (78,7 proc.) wypadków, atakujący pozostał nieznanym.

Źródło: <http://www.naukawpolsce.pap.pl>

<http://laboratoria.net/aktualnosci/17581.html>



28-05-2024

[Drżące nanorurki](#)

Właściwości zależą m.in. od tego, w jaki sposób struktury te wibrują.



28-05-2024

[Naukowcy znaleźli sposób na recykling betonu](#)

Informuje "Nature".



28-05-2024

ADHD zdiagnozowano u co dziewiątego dziecka w USA

W roku 2022 dzieci z diagnozą ADHD było o milion więcej niż w roku 2016.



28-05-2024

Testy na obecność HPV

Co osiem lat równie skuteczne, co regularna cytologia.



28-05-2024

Do środowiska trafiło ponad 1 mld komarów GMO

Przeznaczonych do walki z malarią.



28-05-2024

Może to owady uratują nas przed zwałami

plastiku

Niektóre gatunki owadów są w stanie zjadać plastik.



28-05-2024

Terapia daremna przedłuża cierpienie, przedłuża agonię

Terapia daremna nie jest w stanie pomóc pacjentowi.



28-05-2024

Widzimy eskalację zaburzeń związanych ze stresem

Szeroko rozumianych lękowo-depresyjnych.

Informacje dnia: [Drżące nanorurki](#) [Naukowcy znaleźli sposób na recykling betonu](#) [ADHD zdiagnozowano u co dziewiątego dziecka w USA](#) [Testy na obecność HPV](#) [Do środowiska trafiło ponad 1 mld komarów GMO](#) [Może to owady uratują nas przed zwałami plastiku](#) [Drżące nanorurki](#) [Naukowcy znaleźli sposób na recykling betonu](#) [ADHD zdiagnozowano u co dziewiątego dziecka w USA](#) [Testy na obecność HPV](#) [Do środowiska trafiło ponad 1 mld komarów GMO](#) [Może to owady uratują nas przed zwałami plastiku](#) [Drżące nanorurki](#) [Naukowcy znaleźli sposób na recykling betonu](#) [ADHD zdiagnozowano u co dziewiątego dziecka w USA](#) [Testy na obecność HPV](#) [Do środowiska trafiło ponad 1 mld komarów GMO](#) [Może to owady uratują nas przed zwałami plastiku](#)

Partnerzy