

# Kaspersky Security Bulletin 2008

## Ewolucja spamu

Daria Gudkowa  
Tatiana Kulikowa  
Katerina Kalimanowa  
Daria Bronnikowa

## Spis treści

<b>Wprowadzenie</b> .....	<b>3</b>
Przegląd 2008 roku	3
<b>Trendy w 2008 roku</b> .....	<b>4</b>
Oszustwa spamowe wykorzystujące wiadomości tekstowe	4
Spam a portale społecznościowe	5
<b>Rozkład kategorii spamu</b> .....	<b>7</b>
Główne źródła spamu	9
Rodzaje i rozmiar wiadomości spamowych	9
<b>Phishing</b> .....	<b>11</b>
<b>Zainfekowane załączniki i odsyłacze do zainfekowanych stron internetowych</b> .....	<b>12</b>
E-maile z zainfekowanymi załącznikami	12
E-maile z odsyłaczami do stron internetowych zawierających zainfekowane pliki	15
<b>Techniki i taktyki spamerów</b> .....	<b>16</b>
Spam HTML	16
Reklama na darmowych serwisach hostingowych	18
<b>Spam według kategorii</b> .....	<b>19</b>
<b>Spam a globalne wydarzenia</b> .....	<b>22</b>
<b>Wnioski</b> .....	<b>24</b>

## Wprowadzenie

Rok 2008 był szczególny z kilku powodów. Z jednej strony, podjęto pierwsze poważne kroki w celu zwalczania spamu na skalę międzynarodową. Rezultatem tych wysiłków był spadek liczby głównych platform, z których rozsyłano spam, który z kolei spowodował zmniejszenie się całkowitego udziału procentowego spamu w ruchu pocztowym.

Z drugiej strony, na biznes spamowy wpłynął globalny kryzys gospodarczy, który rozpoczął się w 2008 roku, a do Rosji dotarł wczesną jesienią. Kryzys ten znalazł odzwierciedlenie w zmianach w strukturze spamu: obecnie pojawia się mniej reklam rzeczywistych produktów, za to więcej spamu przestępczego.

### Przegląd 2008 roku

- Spam stanowił 82,1% wszystkich wiadomości e-mail, o 2,1% więcej niż w 2007 r.
- Odsetek spamu w ruchu pocztowym zmniejszył się w okresie letnich wakacji
- W okresie kilku dni po zamknięciu McColo, serwisu hostingowego wykorzystywanego do kontrolowania kilku botnetów, w Rosji i Stanach Zjednoczonych zarejestrowano odpowiednio dwukrotnie i trzykrotnie mniej spamu
- Wzrosła ilość spamu kierowanego do użytkowników portali społecznościowych oraz ilość spamu na takich portalach
- Wzrosła popularność spamu zachęcającego użytkowników do wysyłania kosztownych wiadomości tekstowych na krótkie numery
- W drugim półroczu zmniejszył się odsetek spamu z kategorii „Inne towary i usługi”, co odzwierciedlało liczbę zamówień otrzymywanych przez spamerów w realnej gospodarce
- Liczba spamu przeznaczonego dla dorosłych wzrosła o 10%, co spowodowało wzrost ruchu na stronach pornograficznych
- W 2008 roku pojawiła się nowa kategoria rosyjskojęzycznego spamu: podrabiane towary luksusowe
- Globalny kryzys gospodarczy oraz nowy amerykański prezydent to dwa tematy najczęściej wykorzystywane w celu zwrócenia uwagi na towary i usługi reklamowane w spamie
- W celu obejścia filtrów spamowych spamerzy wykorzystywali niektóre z właściwości HTML-a

## Trendy w 2008 roku

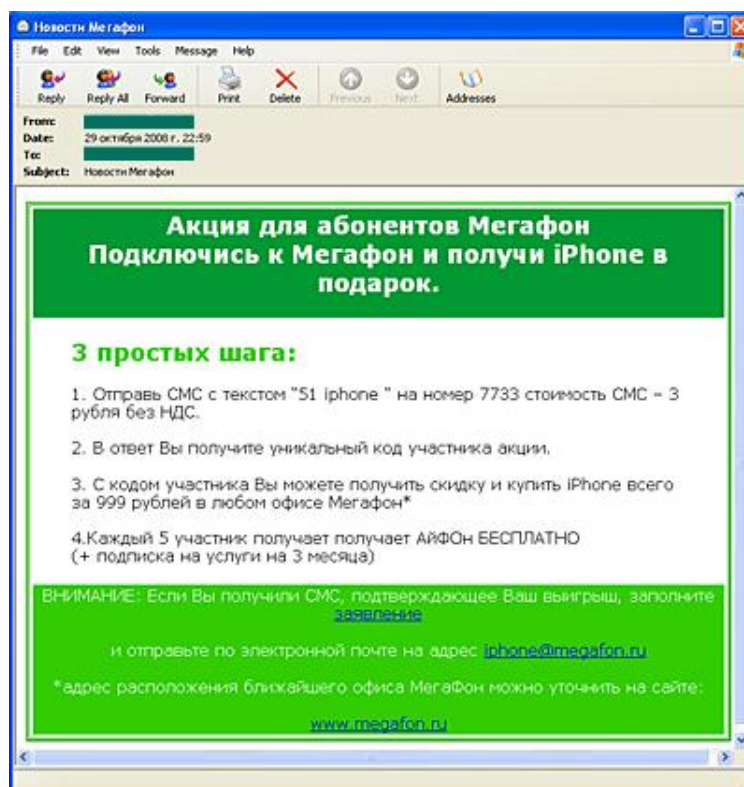
### Oszustwa spamowe wykorzystujące wiadomości tekstowe

W 2008 roku coraz więcej użytkowników Internetu było zachęcanych do wysyłania wiadomości tekstowych na krótkie numery wydzierżawione przez oszustów, którzy zarabiali na wysokich kosztach związanych z wysyłaniem takich wiadomości. Ten typ oszustwa stał się szczególnie rozpowszechniony w 2008 roku.

Spamerzy wykorzystywali różne fałszywe obietnice i groźby, np.:

- Obietnica wygranej w nieistniejącej loterii
- Oferta odczytu rzekomo wysłanej do użytkownika wiadomości e-mail, która może być udostępniona dopiero po wysłaniu wiadomości tekstowej
- Ostrzeżenie o zamknięciu konta pocztowego odbiorcy, jeżeli nie zostanie wysłana wiadomość tekstowa

Poniższy e-mail ma wyglądać jak wiadomość od operatora telefonii komórkowej:



Wiadomość informuje odbiorcę o nowej specjalnej ofercie: podpisz umowę z MegaFon i zdobądź iPhone'a z niewiarygodnie wysokim rabatem. Odbiorca musi tylko wysłać wiadomość tekstową na krótki numer, po czym otrzyma specjalny kod promocyjny, który będzie mógł wykorzystać do zakupu iPhone'a za jedyne 999 rubli (około \$30). Oprócz tego,

co piąta osoba otrzyma iPhone'a oraz możliwość korzystania z usług telefonii komórkowej przez trzy miesiące za darmo.

Rosja stanowi podatny grunt dla tego typu oszustw, ponieważ, w przeciwieństwie do większości innych państw, do wydzierżawienia i wykorzystywania krótkich numerów nie jest wymagana licencja. Trzeba tylko podpisać umowę partnerską z dostawcą rozwiązań opartych na wykorzystywaniu krótkich numerów, który posiada umowę z dostawcą usług telefonii komórkowej. Jeżeli ten sam numer jest wykorzystywany przez kilka firm (tak zwany „współdzielony” numer), każda firma będzie posiadała hasło lub prefiks. Wydzierżawiający otrzymują część dochodów generowanych przez wysłane wiadomości tekstowe.

Rosyjscy użytkownicy przywykli do płacenia za drobne usługi przy użyciu wiadomości tekstowych i często nie podejrzewają oszustwa. Krótkie numery są legalnie wykorzystywane do głosowania, w konkursach oraz quizach. Wysyłając wiadomość tekstową, użytkownicy mogą płacić za zawartość swoich telefonów komórkowych (dzwonki, tapety, gry oparte na Javie itd.), umieszczać wiadomości na stronach internetowych, forach i blogach oraz uzyskiwać dostęp do stron WAP. Wiadomości tekstowe są również wykorzystywane przez wiele różnych serwisów (serwisy randkowe, informacyjne itd.).

Wszystkie te czynniki wykorzystują oszuści. Wydzierżawiają krótkie numery z prefiksami, a następnie rozsyłają wiadomości spamowe, które mają wyglądać jak oficjalne e-maile od administratorów różnych zasobów i usług. Maile te zawierają specjalne oferty zachęcające odbiorców do wysłania wiadomości tekstowych na krótki numer, nie podają jednak kosztu wysłania takiej wiadomości (150–300 rubli lub około 4–9 dolarów).

Dostawcy rozwiązań opartych na wykorzystywaniu krótkich numerów próbują kontrolować działalność swoich partnerów poprzez blokowanie numerów wykorzystywanych do oszustw. Wydaje się jednak, że tego typu oszustwa będą stosowane tak długo, jak długo oszuści będą mogli zarabiać na nich pieniądze. Aby uniknąć nieoczekiwanych wydatków, radzimy nie wierzyć w treści wiadomości spamowych. A przynajmniej, zawsze sprawdzić informacje znajdujące się na stronie internetowej firmy, która rzekomo wysyła taką wiadomość.

## Spam a portale społecznościowe

Portale społecznościowe stały się bardzo popularne w ostatnich latach (bez wątpienia stanowią gotowe bazy informacji o użytkownikach). Stanowią również popularny cel spammerów.

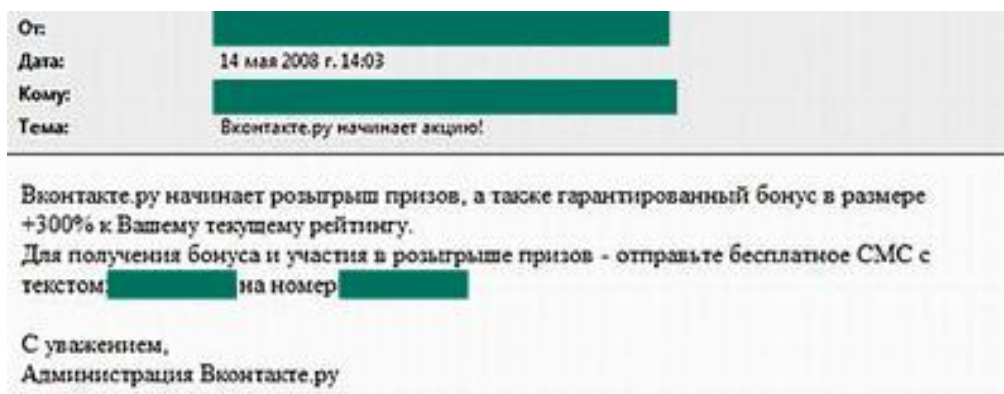
Spamerzy wysyłają fałszywe powiadomienia (pochodzące rzekomo od administratorów portali społecznościowych), aby skłonić użytkowników do odwiedzenia strony zainfekowanej szkodliwym oprogramowaniem lub wysłania wiadomości tekstowej na krótki numer, jak również pomóc phisherom, którzy zbierają loginy i hasła użytkowników.

W czerwcu pojawiła się masowa wysyłka imitująca wiadomości pochodzące z dobrze znanego rosyjskiego portalu społecznościowego, [www.odnoklassniki.ru](http://www.odnoklassniki.ru). Wiadomość „udawała” komunikat, jaki osoby odwiedzające tę stronę często mogły tam znaleźć. Jed-

nak uważny użytkownik potrafiłby dostrzec różnicę: odsyłacz nie prowadził do oficjalnej strony, ale do sfalszowanej (odnoklassniks.info, odnoklass.ru lub odnoklassniks.ru). Adres URL, notabene zarejestrowany w Singapurze, był ładząco podobny do oryginalnego. Z tą różnicą, że użytkownicy, którzy kliknęli odsyłacz, nieświadomie pobierali trojana Trojan.Win32.Agent.qxk, po czym automatycznie byli przekierowywani na oryginalną stronę, [www.odnoklassniki.ru](http://www.odnoklassniki.ru).

Wiadomości te otrzymali nie tylko zarejestrowani użytkownicy odnoklassniki.ru, ale również osoby, które nie odwiedzały tego portalu. Bez wątplenia głównymi odbiorcami tej wysyłki mieli być członkowie odnoklassniki.ru. Atak został misternie zaplanowany, mimo to nie powiódł się: konfiguracja zainfekowanych stron umożliwiała odwiedzenie jej w tym samym czasie przez ograniczoną liczbę użytkowników; poza tym w większości przypadków użytkownicy nie pobrali trojana na swoje maszyny.

W innym ataku spamerzy wykorzystali popularność portali społecznościowych do wyłudzenia pieniędzy od użytkowników Internetu: wiadomość pochodząca rzekomo od administratorów innego rosyjskiego portalu społecznościowego, VKontakte, zachęcała odbiorców do wzięcia udziału w loterii i wysłania „darmowej” wiadomości tekstowej na krótki numer:



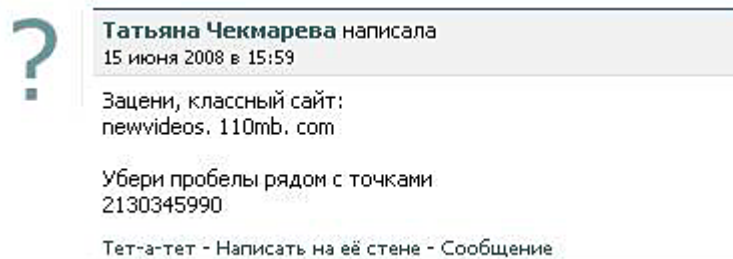
Wiadomość informowała odbiorcę, że VKontakte.ru uruchomił specjalną pulę nagród oraz gwarantowany bonus „+300%”. Aby otrzymać bonus i wziąć udział w loterii, użytkownik musiał wysłać na krótki numer darmową wiadomość tekstową z określonym kodem.

W październiku spamerzy zrobili „kolejny” krok, organizując następną masową wysyłkę, która rzekomo pochodziła z portalu VKontakte. Użytkownicy zostali poproszeni o sprawdzenie nowego serwisu, który mieli oferować administratorzy tego portalu. Ci, którzy kliknęli odsyłacz, byli przekierowywani na fałszywą stronę internetową, na której proszono ich o zarejestrowanie się na VKontakte. Po wprowadzeniu swoich danych, użytkownicy dowiadawali się, że ich adres e-mail nie jest zarejestrowany lub że źle podali swoje hasło; w rezultacie phisherzy mieli dostęp do wprowadzonych loginów i haseł.

Portale społecznościowe stały się tak popularne, że szkodliwi użytkownicy stworzyli nawet specjalny program do automatycznego pobierania loginów i haseł podczas odwiedzania prywatnej strony użytkownika na portalu społecznościowym. Program ten, reklamowany w wiadomościach spamowych, w rzeczywistości automatycznie wypełniał formu-

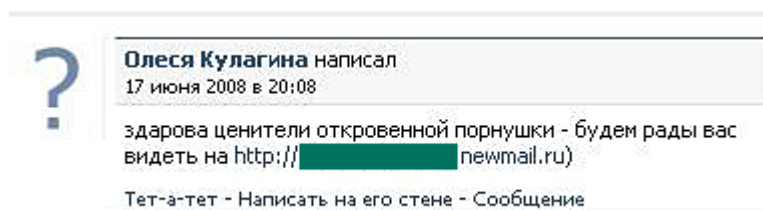
larz rejestracyjny dla użytkowników portalu, a jednocześnie przesyłał wszystkie dane osobowe użytkowników na strony internetowe szkodliwych użytkowników.

Portale społecznościowe wykorzystywane są również do bezpośredniego rozprzestrzeniania spamu. W czerwcu 2008 roku użytkownicy VKontakte zaczęli znajdować wiadomości podobne do tej, jaką widzimy poniżej:



W wiadomości tej można przeczytać: "Hej, sprawdź tę wspaniałą stronę! Wystarczy, że usuniesz spacje po kropkach".

Lub:



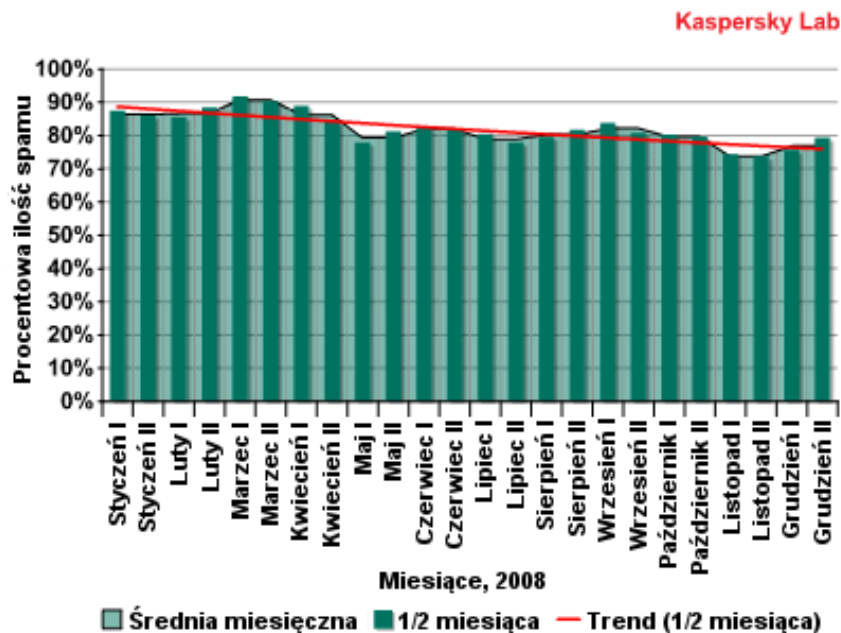
Wiadomość ta ma następującą treść: "Co słyhać, miłośnicy porno? Zajrzyjcie na stronę <http://{adres strony}>"

Odsyłacze te prowadziły do stron pornograficznych.

Rozwój portali społecznościowych w oraz ataki spamerów na użytkowników tych zasobów przyczyniły się do powstania nowego typu spamu: spam związany z portalami społecznościowymi. Ten nowy rodzaj spamu jest rozprzestrzeniany za pośrednictwem poczty elektronicznej oraz bezpośrednio na portalach społecznościowych. Portale społecznościowe stały się kolejną niszą dla branży spamowej. Spamerzy wykorzystują je do infekowania komputerów użytkowników, zarabiania pieniędzy na kosztownych wiadomościach tekstowych oraz kradzieży danych użytkownika (phishing).

## Rozkład kategorii spamu

Odsetek spamu w 2008 roku wynosił średnio 82,1% (o 2,1% więcej niż w 2007 r.). Najniższy odsetek został odnotowany 13 listopada (50,5%), najwyższy natomiast 1 marca (97,8%).



Odsetek spamu w rosyjskim Internecie w 2008 r.

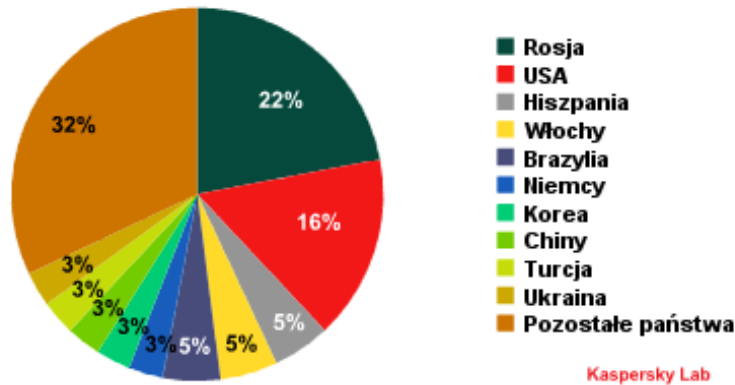
Powyższy wykres pokazuje odsetek spamu w rosyjskim Internecie w 2008 roku. Wyraźnie widoczny jest spadek udziału procentowego spamu w całym ruchu pocztowym. Nieprawdziwe byłoby jednak twierdzenie, że trend ten jest wynikiem spadku aktywności spamerów.

W pierwszym kwartale 2008 roku udział procentowy spamu zwiększył się, natomiast w drugim kwartale zaczął spadać i latem utrzymywał się na stosunkowo niskim poziomie (80%). We wrześniu ilość spamu w ruchu pocztowym zaczęła wzrastać, po czym już w listopadzie nastąpił gwałtowny spadek. Spadek ten spowodowany był zamknięciem McColo, serwisu hostingowego wykorzystywanego jako centrum kontroli kilku największych botnetów (Rustock, Srizbi, Dedler, Storm, Mega-D oraz Pushdo).

Pod koniec listopada ilość spamu zaczęła powracać do poprzedniego poziomu, a w grudniu odsetek spamu w rosyjskim Internecie wynosił 82,5%.

W 2008 roku miało miejsce bezprecedensowe zdarzenie: zamknięcie jednego z dostawców usług hostingowych miało ogromny wpływ na odsetek spamu w całkowitym ruchu pocztowym (kilka dni po zamknięciu McColo w Rosji i Stanach Zjednoczonych odnotowano odpowiednio dwa i trzy razy mniej spamu). Mimo że spam stopniowo powrócił do poprzedniego poziomu, incydent ten pokazuje, że spam może – i powinien – być zwalczany nie tylko przy użyciu odpowiedniego oprogramowania, ale również poprzez podejmowanie działań na szczeblu międzynarodowym, zarówno na obszarze technologicznym jak i prawnym.

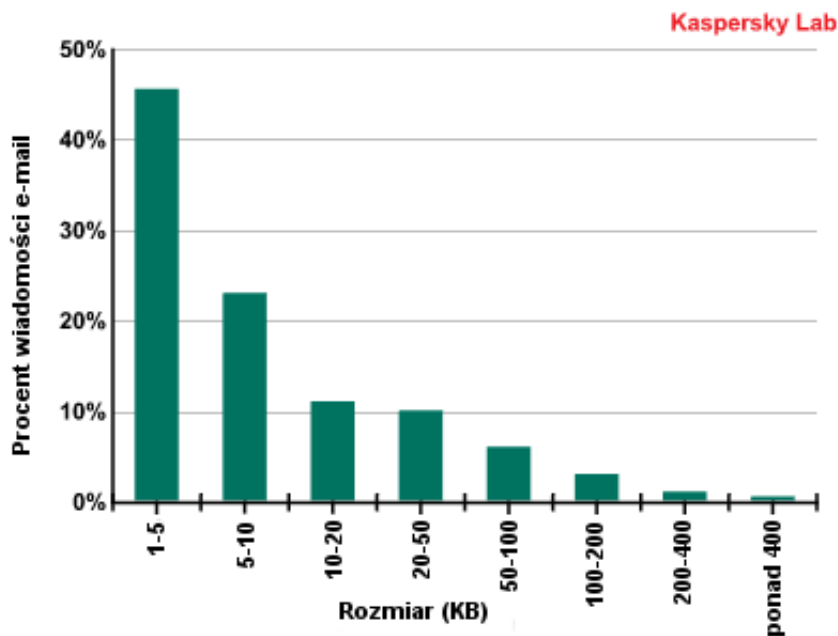
## Główne źródła spamu



Państwa stanowiące źródła spamu

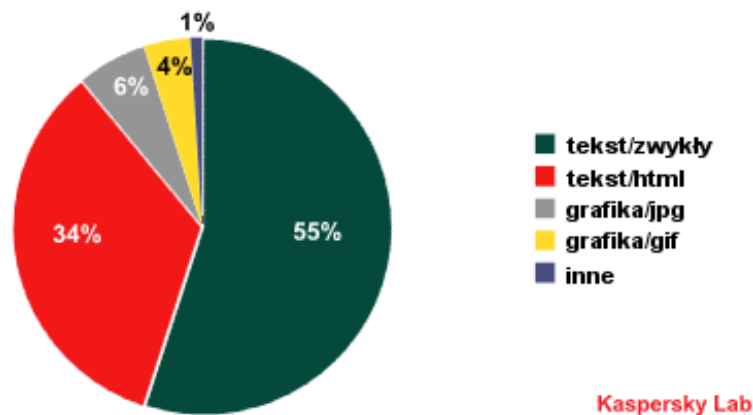
Wśród państw będących źródłem spamu w rosyjskim Internecie w 2008 roku prowadzenie objęła Rosja (w 2007 roku najwięcej spamu pochodziło z USA). Na drugim miejscu uplasowały się Stany Zjednoczone. Rozkład źródeł spamu dla całego roku różni się od rozkładu dla poszczególnych miesięcy. Na przestrzeni roku Hiszpania stanowiła źródło 5% spamu krążącego w rosyjskim Internecie, jednak w niektórych miesiącach z państwa tego pochodziło aż 10% spamu.

## Rodzaje i rozmiar wiadomości spamowych



Rozmiar wiadomości spamowych

Podobnie jak w poprzednich latach, rozmiar przeważającej większości wiadomości spamowych nie przekraczał 10 KB. W 2008 roku spamerzy nadal preferowali wykorzystywanie niewielkich wiadomości e-mail.



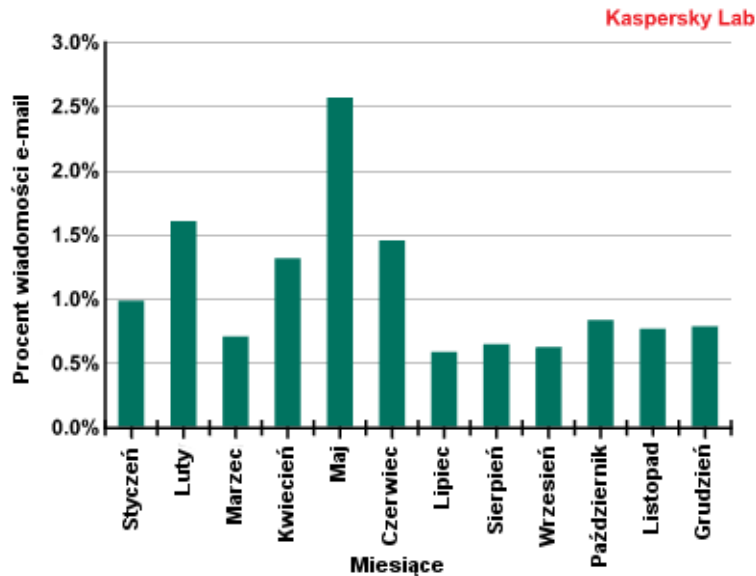
#### Rodzaje wiadomości spamowych

Rozkład głównych rodzajów wiadomości spamowych nie uległ większym zmianom w 2008 roku. Większość wiadomości spamowych nadal opiera się na tekście, przez co takie wiadomości mają niewielki rozmiar.

Najpopularniejszym językiem wykorzystywanym w spamie w rosyjskim Internecie był (naturalnie) język rosyjski, który stanowił 77% wszystkich wiadomości spamowych. Drugim pod względem popularności językiem był angielski (14%). Odsetek innych języków wykorzystywanych w spamie w rosyjskim Internecie stanowił łącznie 9% i obejmował takie języki jak francuski, niemiecki, włoski i portugalski.

## Phishing

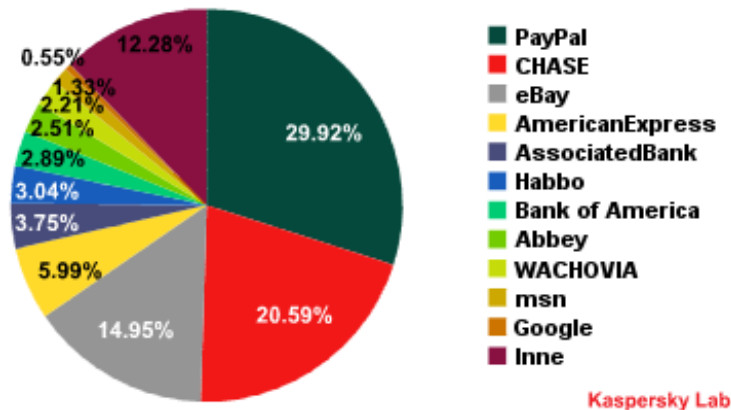
Spam zawierający odsyłacze do stron internetowych wynosił średnio 1,01%. W pierwszej połowie roku phisherzy byli o wiele bardziej aktywni niż w drugiej połowie (odpowiednio 1,32% i 0,7%). Znaczny wzrost liczby ataków phishingowych został również odnotowany w okresie maj-czerwiec 2008 roku.



E-maile zawierające odsyłacze do stron phishingowych w 2008 r.

Pod koniec roku spodziewaliśmy się o wiele większej aktywności phisherów. Byłoby logiczne, gdyby w świetle kryzysu finansowego dotyczącego setki banków, phisherzy zintensyfikowali swoje ataki na klientów banków i wykorzystali do swoich celów pogłoski o bankructwie i inne. Co więcej, w okresie Świąt Bożego Narodzenia i Nowego Roku wiele osób dokonuje zakupów online, jak również wysyła i otrzymuje świąteczne kartki okolicznościowe. Stwarza to cyberprzestępcom wiele możliwości przeprowadzania ataków.

To, że w okresie tym nie zwiększyła się drastycznie liczba ataków phishingowych, można wytłumaczyć zamknięciem serwisów hostingowych McColo i Atrivo, wykorzystywanych przez oszustów do utrzymywania fałszywych stron internetowych oraz jako centra kontroli botnetów wykorzystywanych do przeprowadzania masowych ataków phishingowych i wysyłek spamowych.



Główne cele ataków phishingowych

W 2008 roku najpopularniejszym celem ataków phisherów był systemem płatności PayPal. To wysokie miejsce na liście phisherów wynika z faktu, że coraz więcej użytkowników Internetu dokonuje i otrzymuje płatności przy użyciu tego typu zasobów. Znacznie mniejszym zainteresowaniem phisherów cieszyły się poufne dane klientów bankowych (w szczególności Bank of America and Wachovia). Chase Manhattan Bank stał się celem największego ataku, jaki miał miejsce w listopadzie i grudniu 2008 r.; atak był tak poważny, że Chase znalazł się wysoko na liście głównych celów ataków phishingowych w 2008 roku.

W 2008 roku każdego miesiąca przeprowadzane były ataki na serwis pocztowy Mail.Ru oraz popularne w Rosji portale społecznościowe. Poza tym cyberprzestępcy nadal podejmowali próby kradzieży pieniędzy od użytkowników Internetu za pośrednictwem ataków phishingowych na system płatności elektronicznych Yandex.

Powinniśmy spodziewać się wzrostu liczby prób kradzieży danych użytkowników, gdyż botnety, które ucierpiały w wyniku wydarzeń, jakie miały miejsce jesienią 2008 roku, zaczęły odzyskiwać swoją „moc”. Jest to szczególnie prawdopodobne w warunkach obecnego kryzysu, który może sprzyjać oszustwom. Aby nie stać się ofiarą cyberprzestępców, należy pamiętać, że żaden wiarygodny zasób internetowy nie poprosi klientów o podanie poufnych informacji na stronie internetowej, do której prowadził odsyłacz zawarty w wiadomości e-mail.

## Zainfekowane załączniki i odsyłacze do zainfekowanych stron internetowych

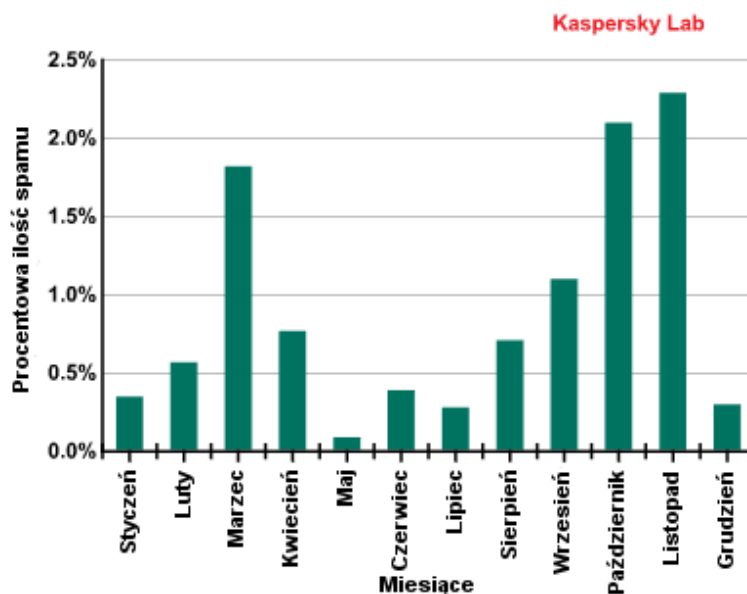
*Dane dotyczące zainfekowanych załączników do wiadomości e-mail zostały zebrane przy użyciu Kaspersky Hosted Security, usługi firmy Kaspersky Lab oferowanej klientom w Europie Środkowej, Wielkiej Brytanii, Stanach Zjednoczonych oraz Rosji.*

### E-maile z zainfekowanymi załącznikami

Obecnie poczta elektroniczna nie jest już głównym sposobem dostarczania szkodliwego oprogramowania, przez co wiąże się ze znacznie mniejszym ryzykiem infekcji niż w po-

przednich latach. Wiadomości e-mail z zainfekowanymi załącznikami stają się coraz mniej rozpowszechnione, ponieważ spamerzy preferują wysyłanie e-maili z odsyłaczami do zainfekowanych stron.

Mimo znacznego wzrostu (1,81%), jaki miał miejsce w marcu 2008 roku, oraz niewielkiego spadku, jaki nastąpił niedługo po nim, pod koniec roku odsetek tego typu wiadomości nadal rósł. W drugiej połowie 2008 roku wykryto znacznie więcej wiadomości z zainfekowanymi załącznikami (1,12% ruchu pocztowego) niż w pierwszej połowie (0,66%). Średni odsetek wiadomości e-mail zawierających zainfekowane załączniki wynosił w 2008 roku 0,89%.



Odsetek wiadomości e-mail z zainfekowanymi załącznikami

20 najczęściej wykrywanych szkodników w wiadomościach e-mail w 2008 r.:

Nazwa	Udział procentowy
Trojan-Downloader.JS.Iframe.sh	31,07%
Backdoor.Win32.Hijack.e	8,98%
Trojan-Clicker.HTML.Agent.ag	7,73%
Backdoor.Win32.UltimateDefender.tt	4,42%
Trojan-Dropper.Win32.Agent.yzp	2,94%
Trojan-Dropper.Win32.Agent.xgg	2,72%
Worm.Win32.AutoRun.svl	2,02%
Trojan-Downloader.JS.Agent.cye	1,96%
Trojan-Downloader.Win32.Agent.algj	1,60%
Trojan-Downloader.Win32.Agent.afqa	1,52%
Trojan-Spy.Win32.Goldun.axt	1,46%
Trojan-PSW.Win32.Agent.lcc	1,37%
Trojan-Downloader.HTML.Agent.km	1,32%

Trojan-Dropper.Win32.Agent.xql	1,30%
Trojan-Downloader.JS.Agent.ckn	1,22%
Email-Worm.Win32.NetSky.q	1,12%
Trojan-Spy.Win32.Goldun.azl	1,11%
Trojan-Spy.Win32.Goldun.bbg	1,04%
Trojan.Win32.Buzus.hrp	0,98%
Trojan-Spy.Win32.Zbot.fql	0,92%

Po raz pierwszy od czasu opublikowania naszych raportów na pierwszym miejscu listy najczęściej rozsyłanych zainfekowanych załączników nie znalazł się robak pocztowy. Bezwzględnym liderem 2008 roku okazał się trojan downloader, lframe.sh, stworzony w języku programowania JavaScript w celu wykonywania specjalnego kodu potrafiącego pobierać i uruchamiać inne trojany na komputerach odbiorców wiadomości.

Poniżej przedstawiamy najczęściej wykrywane szkodliwe programy pogrupowane ze względu na zachowanie:

Nazwa kategorii	Udział procentowy
Trojan-Downloader	39,66%
Backdoor	13,39%
Trojan-PSW	9,09%
Trojan-Spy	8,49%
Trojan-Clicker	8,02%
Trojan-Dropper	7,72%
Worm	3,96%
Exploit	1,96%
Trojan	1,62%
Email-Worm	1,45%

Tabela ta pokazuje radykalne zmiany, jakie zaszły w krajobrazie szkodliwego oprogramowania na przestrzeni kilku ostatnich lat. Robak pocztowy, który został stworzony w taki sposób, aby mógł być rozprzestrzeniany za pośrednictwem poczty elektronicznej, i stanowił dominujące zachowanie w latach 2000–2005, znajduje się obecnie na ostatnim miejscu pod względem rozpowszechnienia. Robak ustąpił miejsca takim zachowaniom, jak trojan downloader, backdoor oraz innym trojanom.

Szkodliwi użytkownicy uciekali się do szeregu najróżniejszych chwytów, aby nakłonić użytkowników Internetu do odwiedzenia strony lub otwarcia załącznika zawierającego szkodliwe oprogramowanie. Jedną z popularniejszych taktyk spamerów było dostarczanie szkodliwych programów na osobiste konta pocztowe w formie zarchiwizowanego pliku. Niektóre z metod wykorzystywanych w celu skłonienia użytkowników Internetu do rozpakowania zarchiwizowanego pliku mogą być szokujące.

Na przykład, angielskojęzyczna wiadomość e-mail informowała odbiorcę, że jego lub jej dziecko zostało porwane, i zawierała żądanie wysokiego okupu. W celu obejrzenia zdjęć

uprowadzonych dzieci użytkownicy mieli otworzyć załączony plik, który w rzeczywistości zawierał szkodnika: Trojan-Downloader.Win32.Delf.bfc.

**We have hijacked your baby**

Hey We have hijacked your baby but you must pay once to us \$50 000. The details we will send later...

We has attached photo of your fume

Rosyjskojęzyczny spam zawierający zainfekowane załączniki nie wykorzystywał tak bezlistnych metod. Zamiast tego spamerzy próbowali wzbudzić zainteresowanie odbiorców, zapraszając użytkowników do udziału w spotkaniach absolwentów.

## E-maile z odsyłaczami do stron internetowych zawierających zainfekowane pliki

Najpowszechniejszym sposobem rozprzestrzeniania szkodliwych programów w 2008 roku było umieszczanie w wiadomościach e-mail odsyłaczy do zainfekowanych stron internetowych. Spamerzy preferowali tę taktykę w okresie letnim. Angielskojęzyczne wiadomości e-mail próbowały „oszukać” odbiorców, imitując e-maile pochodzące od znanych agencji informacyjnych (takich jak MSNBC i CNN). Każdemu użytkownikowi, który próbował przeczytać takiego kontrowersyjnego newsa, ukazywało się okienko informujące o tym, że jego flash player nie jest aktualny i należy pobrać nowy program w postaci pliku .exe. Jednak zamiast uaktualnionej aplikacji w rzeczywistości pobierany był trojan downloader. Szkodliwe oprogramowanie było również umieszczane na zhakowanych stronach internetowych znajdujących się w różnych strefach domen.

msnbc.com: BREAKING NEWS: London named top literary destination

Find out more at <http://breakingnews.msnbc.com>

=====  
See the top news of the day at MSNBC.com, and the latest from Today Show and NBC Nightly News.

=====  
This e-mail is never sent unsolicited. You have received this MSNBC Breaking News Newsletter newsletter because you subscribed to it or, someone forwarded it to you.

To remove yourself from the list (or to add yourself to the list if this message was forwarded to you) simply go to

<http://www.msnbc.msn.com/id/61402101>, select unsubscribe, enter the email address receiving this message, and click the Go button.

Microsoft Corporation - One Microsoft Way - Redmond, WA 98052 MSN PRIVACY STATEMENT

<http://privacy.msn.com> (<http://privacy.msn.com/>>)

Rosyjskojęzyczni spamerzy wykazali się dużą pomysłowością, utrzymując, że nazwisko odbiorcy zostało wymienione w pewnym dokumencie, rzekomo opublikowanym w Internecie. Następnie próbowali zwabić odbiorcę do zasobu znajdującego się w domenie .tk, w którym znajdował się trojan downloader w postaci pliku .doc.

Inną sztuczką wykorzystywaną do zwabienia użytkowników na stronę internetową było zapraszanie do bezpłatnego pobrania oprogramowania – łącznie z rozwiązaniami antywirusowymi. W rzeczywistości, na komputery ofiar pobierał się jeden z wariantów trojana Trojan-PSW.Win32. Zakres oferowanych „usług” obejmował zarówno programy do automatycznego wypełniania haseł i loginów dla portali społecznościowych, takich jak [www.odnoklassniki.ru](http://www.odnoklassniki.ru), jak również najnowszy program antywirusowy, który działał poprawnie tylko wtedy, gdy użytkownik wyłączył aktualną ochronę antywirusową.

Wiadomości o intrygujących tematach w stylu nagłówek tabloidów zawierały tylko odsyłacze do stron internetowych. Odbiorcy nie musieli pobierać żadnych specjalnych programów w celu przeglądania „newsów” – program pobierał się automatycznie, po kliknięciu przez odbiorcę odsyłacza.

## Techniki i taktyki spamerów

### Spam HTML

Rok 2006 można nazwać rokiem spamu graficznego, 2007 - rokiem eksperymentów z załącznikami, natomiast 2008 – rokiem spamu HTML. Spamerzy stosowali wiele starych sztuczek, jednak sama koncepcja została zrewidowana, tak aby można było wykorzystać cechy charakterystyczne HTML-a.

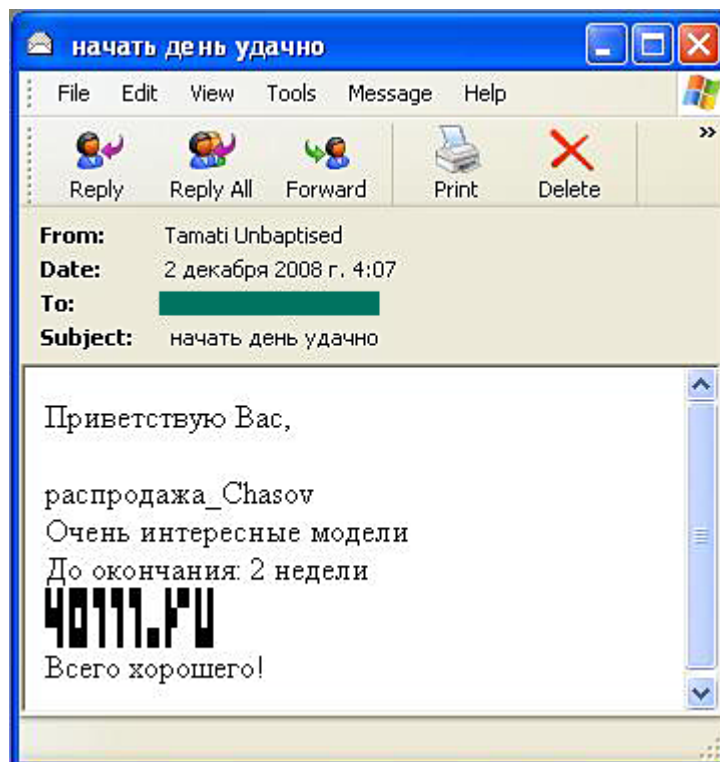
Wykorzystywanie losowo wybranych symboli i znaków w celu stworzenia tzw. „szumu” jest jedną z popularniejszych taktyk spamerów. Tym razem w znacznikach umieszczano losowo wybrane znaki, które nie są widoczne dla czytelników. Metoda ta przypomina klasyczną technikę „białego tekstu”. Spamerzy dodają losowo wybrane sekwencje do tekstu przy użyciu znaczników HTML, które większość klientów pocztowych postrzega jako pomocnicze, co oznacza, że nie są one widoczne dla odbiorcy wiadomości. Są to znaczniki komentarzy, znaczniki koloru itd. Użytkownikowi zostanie wyświetlony tylko tekst reklamy, który stanowi jedynie niewielką część wiadomości e-mail.

<i>E-mail napisany przy użyciu znaczników HTML</i>	<i>Ten sam e-mail w postaci, jaką widzi odbiorca</i>
<pre> &lt;html&gt; &lt;!--losowa sekwencja liter lub słów--&gt; &lt;body&gt; Hi! &lt;br&gt; &lt;!--kolejna losowa sekwencja liter lub słów--&gt; Come visit my awesome site &lt;br&gt; &lt;a href="http://www.spammersite.com"&gt;supersite.com&lt;/a&gt; &lt;!--jeszcze jedna losowa sekwencja liter lub słów--&gt; &lt;/html&gt; </pre>	<p>Hi!</p> <p>Come visit my awesome site</p> <p><u><a href="#">adres strony</a></u>.com</p>

Spamerzy wykorzystywali również pseudo-tekst lub losowo wybrane sekwencje znaków w załącznikach HTML, które w rzeczywistości nie były żadnymi znacznikami. Większość klientów pocztowych analizuje te „niepoprawne” znaczniki jako błąd i nie wyświetla ich odbiorcy.


Zidentyfikowaliśmy również metodę, którą w pewnym momencie określaliśmy jako metodę „Mona Lisy”. Sztuczka ta polega na pokazywaniu użytkownikowi informacji kontaktowych w formie obrazu składającego się ze znaków i symboli. Wcześniej, spamerzy wykorzystywali głównie litery i spacje, teraz jednak używają kombinacji czarnych i białych komórek w tabelach HTML.

Poniższy przykład pokazuje adres URL wyświetlany w postaci tabeli HTML:



Wiadomość ta proponuje odbiorcy, aby na dobry początek dnia odwiedził stronę internetową sprzedającą zegarki. Adres strony, 40777.ru, jest obrazem stworzonym z tabeli HTML.

Format tabeli został użyty w celu rozbicia słów kluczowych w wiadomościach e-mail. W ten sposób spamerzy próbowali obejść filtry spamowe:

<i>E-mail wykorzystujący kod HTML</i>	<i>Ten sam e-mail w postaci, jaką widzi odbiorca</i>
<pre> &lt;table&gt; &lt;tr&gt; &lt;td align=right&gt;VI&lt;/td&gt; &lt;td align=left&gt;AGRA&lt;/td&gt; &lt;/tr&gt; &lt;tr&gt; &lt;td align=right&gt;CIA&lt;/td&gt; &lt;td align=left&gt;LIS&lt;/td&gt; &lt;/tr&gt; &lt;/table&gt; </pre>	

Oprócz omówionych wyżej metod spamerzy wykorzystywali następującą „lukę” w przeglądarce: symbole wykorzystywane w adresie URL mogą być kodowane przy pomocy różnych metod (16-bit ASCII, 8-bit ASCII, ASCII for HTML itd.). Ponadto, przeglądarka poprawnie otworzy stronę, jeżeli zostanie wykorzystany odsyłacz w e-mailu. Przeglądarka otworzy właściwą stronę, nawet jeżeli w odsyłaczu używany jest inny kod lub odsyłacz zawiera błędy.

Na przykład, narod.ru może zostać zapisany jako:

[%6e%61%72%6f%64%2e%72%75](#)

Lub nawet jako:

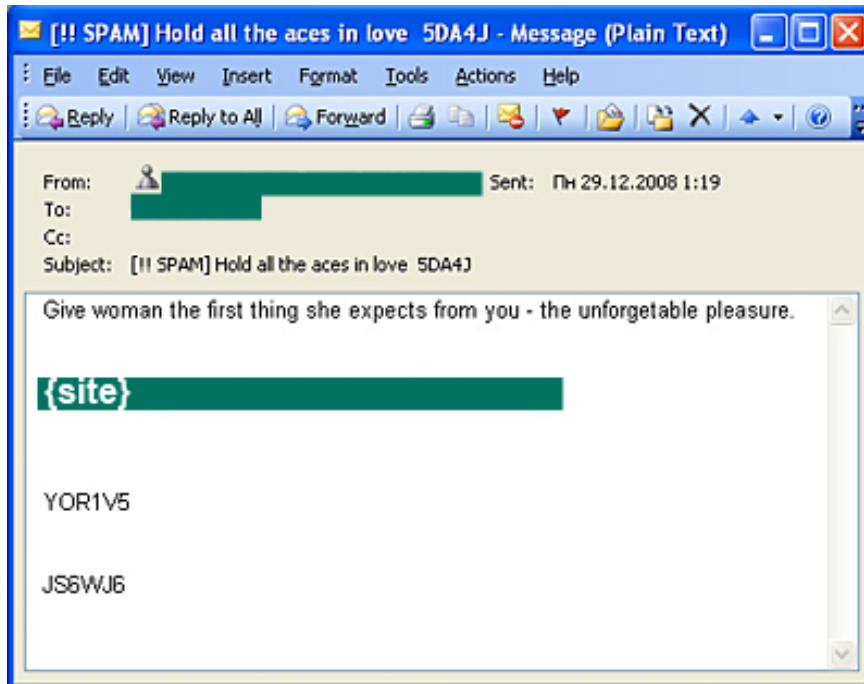
[&#x006e;&#x0061;&#x0072;&#x006f;&#x0064;&#x002e;&#x000072;&#x000075](#)

Nawet przy dowolnej liczbie zer odsyłacz “otworzy” stronę.

## Reklama na darmowych serwisach hostingowych

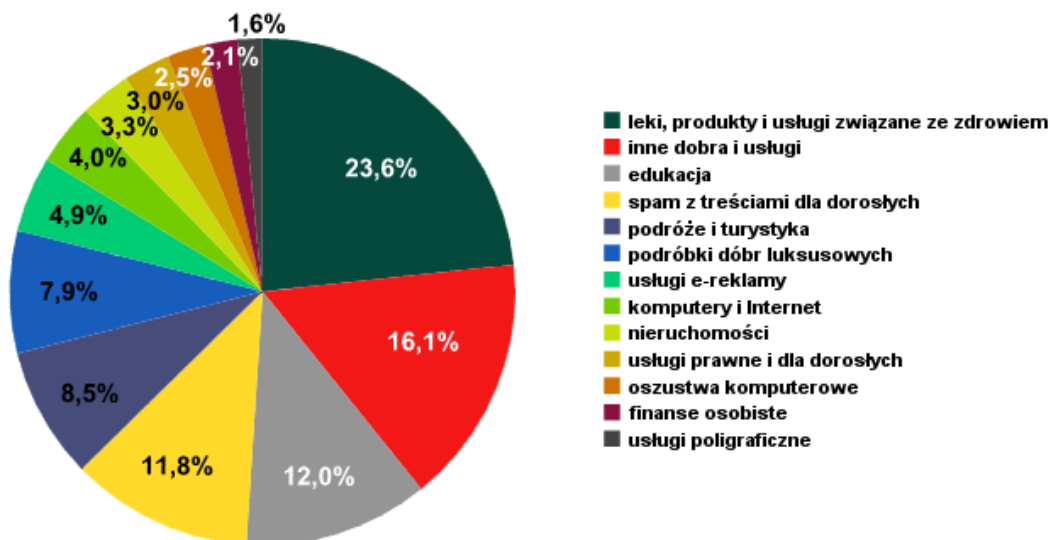
Kolejną popularną techniką rozprzestrzeniania spamu w 2008 roku było wykorzystywanie darmowych, publicznych serwisów sieciowych. Spamerzy utrzymywali stronę internetową (lub przekierowanie do swojej strony) na znanym serwisie hostingowym lub blogowym, do których prowadziły odsyłacze zawarte w wiadomości spamowej.

Podejście to ma na celu głównie omińnięcie filtrów, które opierają się na reputacji. Spamerzy wykorzystują również fakt, że filtr nie zablokuje ich strony, ponieważ odsyłacz prowadzi do znanego, legalnego serwisu. Spamerzy korzystali z dużych serwisów hostingowych, takich jak Google Docs, Microsoft SkyDrive, Microsoft Livefilestore i inne.



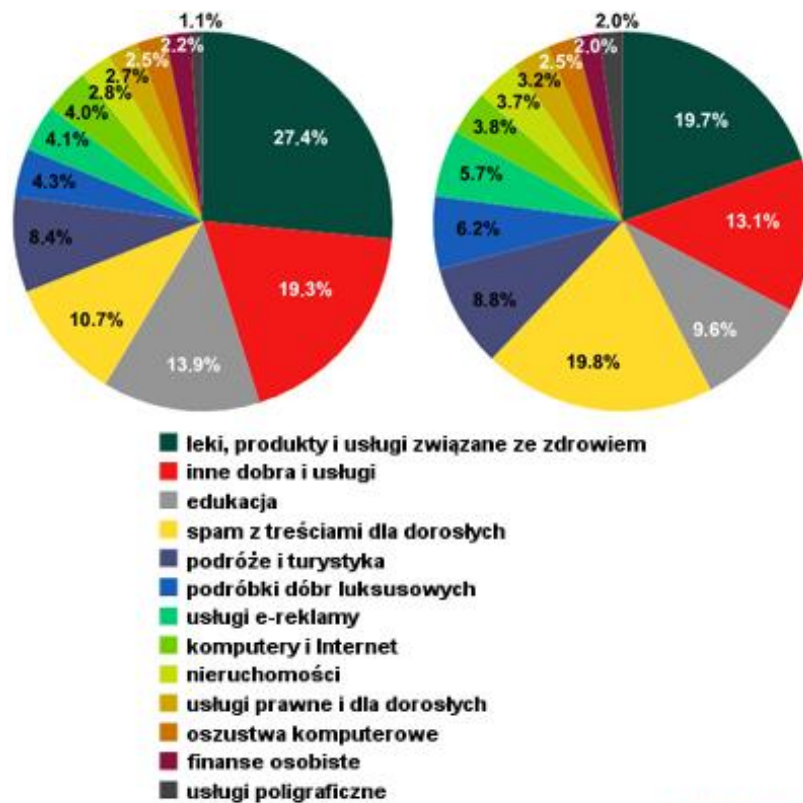
Wiele darmowych serwisów oferowanych przez dostawców poczty elektronicznej oraz innych dużych zasobów internetowych nie monitoruje zawartości zbyt dokładnie. Należy zauważyć, że wiele starszych portali hostingowych i blogów, dla których usługa ta jest jedyną lub główną funkcją (takich jak LiveJournal i LiveInternet), nie padło ofiarą ataków spamowych. Najwyraźniej bezpieczeństwo i ochrona przed spamem na takich serwisach są znacznie lepsze niż na nowych serwisach. To właśnie ze względu na dostępność i brak ochrony spamery korzystają z tych nowych serwisów.

## Spam według kategorii



Spam według kategorii w rosyjskim Internecie w 2008 roku

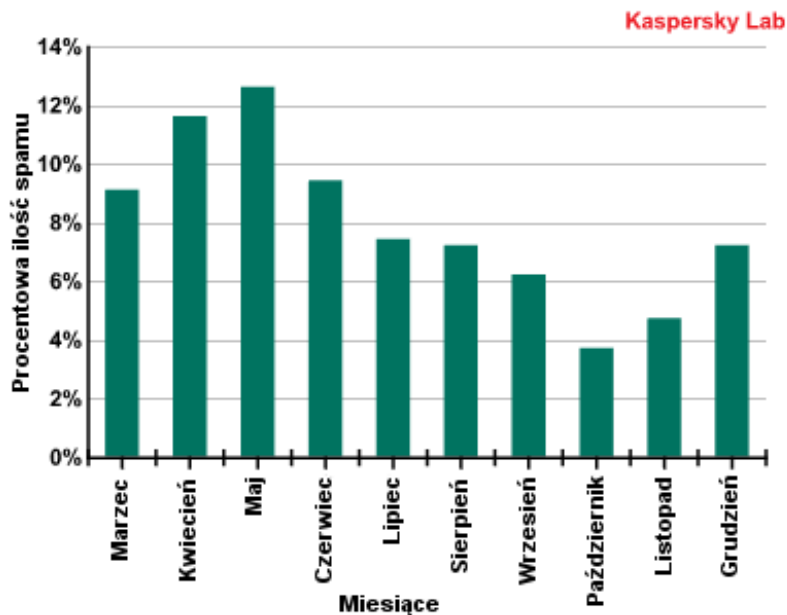
W 2008 roku znacznie zmienił się rozkład kategorii spamu. W ciągu roku pojawiły się nowe kategorie, zmieniły się również najbardziej dominujące kategorie. Widać to wyraźnie, jeżeli porównamy zmiany, jakie nastąpiły w kategoriach spamu w pierwszej połowie roku, ze zmianami, jakie miały miejsce w drugim półroczu.



Spam według kategorii w pierwszej i drugiej połowie 2008 r.

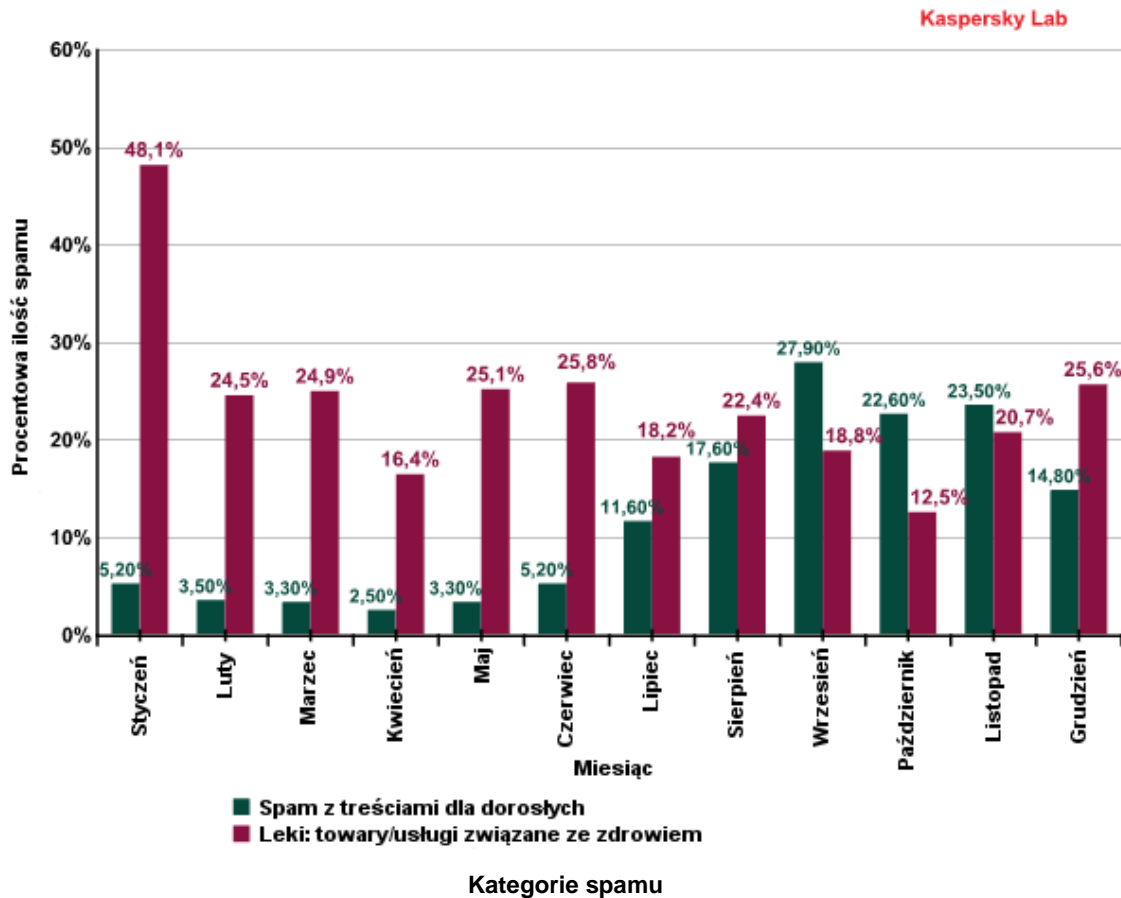
Warto zauważyć, że w drugiej połowie 2008 roku ilość spamu z kategorii „Inne towary i usługi” zmniejszyła się o 6,4%. Kategoria ta odzwierciedla liczbę zamówień otrzymywanych przez spamerów z „realnego” rynku.

W marcu pojawiły się rosyjskojęzyczne reklamy podrabianych dóbr luksusowych. Kategoria ta od razu znalazła się wśród trzech najpopularniejszych kategorii spamu. Po osiągnięciu najwyższego poziomu w maju udział spamu z tej kategorii zaczął stopniowo spadać. Spodziewamy się jednak, że ten typ niechcianych wiadomości znajdzie niszę wśród rosyjskojęzycznego spamu (podobnie jak wśród angielskojęzycznego spamu) i utrzyma się na poziomie 5–6% całego spamu.



#### Podrabiane towary luksusowe

W lipcu zaczęła wzrastać liczba rosyjskojęzycznych wiadomości e-mail zawierających odsyłacze do stron pornograficznych. W drugiej połowie roku ilość spamu z kategorii „treści dla dorosłych” zwiększyła się o ponad 15%. Spamerzy zarabiają na takim spamie między innymi poprzez napędzanie ruchu na takich stronach. Dzięki temu gwałtownemu wzrostowi kategoria ta uplasowała się na pierwszym miejscu, spychając niżej kategorię „Leki oraz produkty i usługi związane ze zdrowiem”, która od dłuższego czasu utrzymywała się na pierwszym miejscu. Spam z kategorii „Treści dla dorosłych” utrzymał najwyższą pozycję przez trzy miesiące.



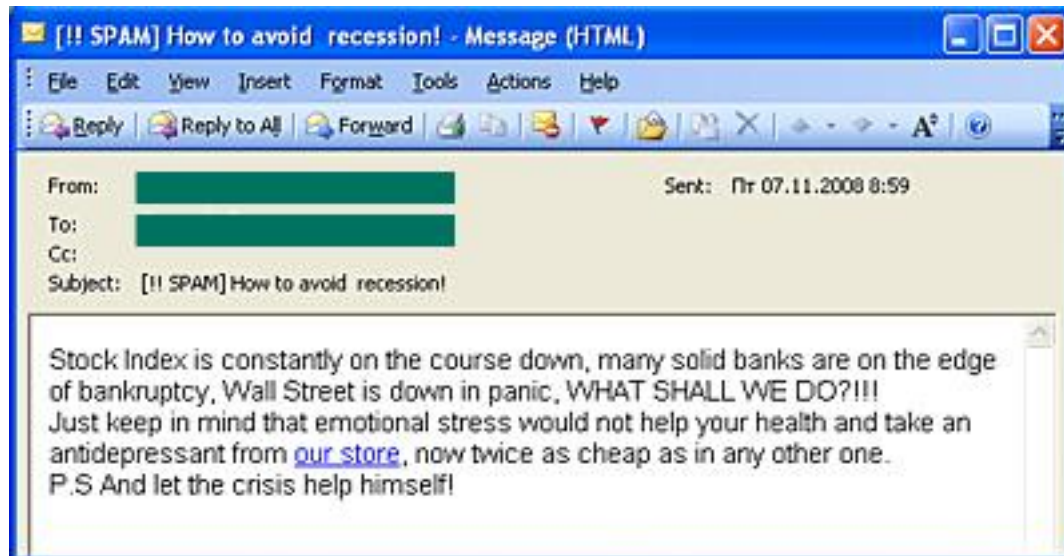
W listopadzie zmniejszyła się ilość spamu z kategorii „Treści dla dorosłych”, prawdopodobnie w wyniku zamknięcia firmy hostingowej McColo oraz trudności spamerów w znalezieniu nowego „domu” dla swoich centrów kontroli botnetów. Warto zauważyć, że w tej kategorii spamu dominują oszustwa. Strony pornograficzne, do których są przekierowywani użytkownicy klikający zawarte e-mailach odsyłacze, często proszą o wysłanie wiadomości tekstowej na krótki numer w celu obejrzenia zawartości. Mimo że oszuści obiecują, że koszt wiadomości tekstowej będzie minimalny (5 – 7 rubli), w rzeczywistości jest on znacznie wyższy (około 300 rubli). Spadek liczby tego typu wiadomości spamowych może wynikać z faktu, że użytkownicy Internetu zdali sobie sprawę z tego oszustwa i przestali chwytać tę przynętę.

Pojawienie się nowych kategorii spamu oraz przeprowadzane od dłuższego czasu masowe wysyłki pokazują, że w rosyjskim przemyśle spamowym działa kilka głównych graczy, którzy posiadają zasoby niezbędne do przeprowadzania tego typu operacji na dużą skalę.

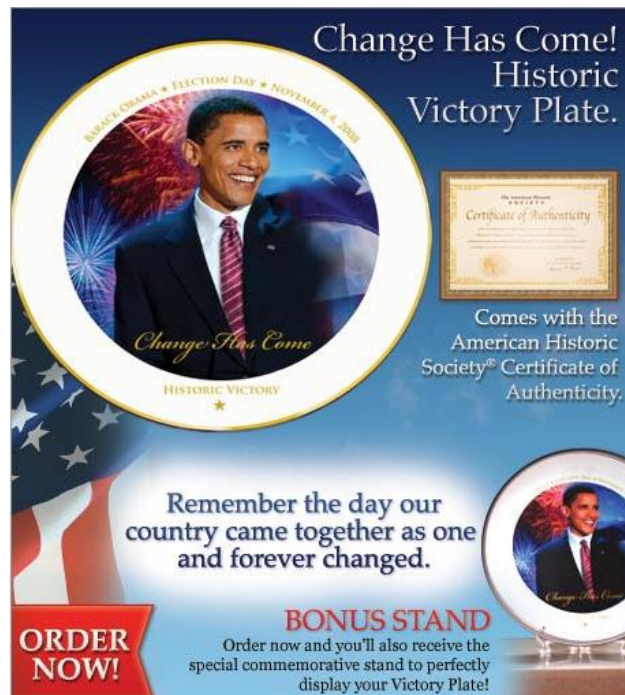
## Spam a globalne wydarzenia

Wiadomo, że odwoływanie się do globalnych wydarzeń jest dobrym sposobem skłonienia użytkowników Internetu do przeczytania wiadomości spamowych. W 2008 roku do najważniejszych wydarzeń wykorzystywanych w spamie należały: Mistrzostwa Świata, ame-

rykańskie wybory prezydenckie i oczywiście globalny kryzys finansowy. Interesujące jest to, że większość wiadomości e-mail, które nawiązywały do kryzysu, nie znalazła się w kategorii spamu „Osobiste finanse”. Wiadomości te nie reklamowały specjalnych ofert pożyczek ani nie promowały projektów typu „wzbogacić się szybko”. Większość wiadomości spamowych wykorzystujących kryzys reklamowało różne seminaria na temat tego, jak postępować w okresie kryzysu. Ponadto, kryzys stanowił stale powracający temat w wielu reklamach różnych towarów i usług.



Innym głównym tematem spamu w 2008 roku były wybory prezydenckie w Stanach Zjednoczonych. W czasie kampanii prezydenckiej (jak również przed i po niej) spamery nawiązywali do wyborów w celu reklamowania różnych towarów i usług oraz rozprzestrzeniania szkodliwych programów. Niemal każdy temat zawierał nazwisko Prezydenta Baracka Obamy. Nawet reklamy Viagry zawierały takie nagłówki, jak „Zwycięska mowa Baracka Obamy”. Inny spam reklamował pamiętki z wizerunkiem Obamy. Pisaliśmy o spamie, który w 2005 roku promował popiersia Putina. W 2008 roku spamery oferowali talerze pamiętkowe z portretem nowego amerykańskiego prezydenta.



## Wnioski

Globalny kryzys finansowy, który dotknął prawie wszystkie sektory gospodarki światowej, odcisnął swój ślad również na cyberprzestępczości. Spadek odnotowały rodzaje spamu bezpośrednio związane z realną gospodarką. Spamerzy zaczęli wykorzystywać technologie, które mogłyby im pomóc szybko zarobić pieniądze, takie jak oszukańczy spam wykorzystujący wiadomości tekstowe oraz zwiększający ruch na stronach pornograficznych.

Spadek odsetka spamu reklamującego towary i usługi świadczy o równoczesnym spadku zamówień otrzymywanych przez spamerów od realnych firm. Jednocześnie wzrost liczby „przestępczych” ataków spamowych wyraźnie świadczy o tym, że cyberprzestępcy zaczynają odczuwać spadek dochodów i szukają nowych sposobów zarobienia pieniędzy.

Trzeba pamiętać, że spam to zjawisko globalne, dlatego zmiany w jego strukturze – nawet przed dotarciem kryzysu do Rosji – mogą odzwierciedlać stan gospodarki. Jeżeli związek między strukturą spamu a procesami makroekonomicznymi okaże się silny, być może będziemy w stanie przewidzieć koniec kryzysu na podstawie obserwacji trendów w spamie.

Użytkownicy Internetu powinni pamiętać, że kryzys stworzył odpowiednie warunki do rozwoju phishingu, zwłaszcza phishingu skierowanego do klientów banków i użytkowników systemów płatności elektronicznej. Jeżeli chodzi o trendy przestępcze w spamie, możemy spodziewać się kolejnej fali spamu z kategorii „Treści dla dorosłych”.

W 2009 roku nie spodziewamy się spadku ilości spamu; wręcz przeciwnie, prawdopodobnie nastąpi wzrost ilości spamu przestępczego. Co więcej, w obecnych warunkach kryzysu dla wielu firm spam może stanowić jedyną dostępną metodę reklamy.

Biorąc pod uwagę niestabilność globalnej sytuacji gospodarczej, prognozy te odnoszą się do pierwszej połowy 2009 roku. Firma Kaspersky Lab nadal będzie śledziła rozwój wydarzeń dotyczących ewolucji spamu.