# NAJWIĘKSZE ZAGROŻENIA DLA BEZPIECZEŃSTWA W INTERNECIE W ROKU 2013

## RAPORT

FUNDACJA
bezpieczna
cyberprzestrzeń

# Spis Treści

# WSTĘP

Co roku, na jego zakończenie, oprócz podsumowań pojawiają się prognozy. Nie inaczej jest, jeśli chodzi o temat bezpieczeństwa w cyberprzestrzeni. Najważniejsze wydarzenia z dziedziny cyberbezpieczeństwa, w roku, który właśnie się skończył, to twarde dowody na to, że mówimy o rzeczach poważnych. Natomiast przewidywania, które znajdują się w tym raporcie, mają nas uczulić na to, co potencjalnie najgroźniejsze. Dla wielu zresztą tego typu opracowania są elementem poważnego planowania budżetów czy działań strategicznych, do czego zachęcamy.

Coroczna lektura raportów przygotowanych przez różne ośrodki zajmujące się bezpieczeństwem teleinformatycznym zainspirowała nas do stworzenia własnego raportu. Aby był on jak najbardziej solidny, oprócz własnej opinii, uwzględniliśmy w nim opinie wielu innych specjalistów z dziedziny bezpieczeństwa teleinformatycznego z naszego kraju, których uważamy za autorytety w tej dziedzinie. Tak powstała lista tego, co potencjalnie najgroźniejsze w roku 2013. Pojawiające się na przełomie roku tego typu raporty praktycznie niemalże w całości pochodzą z zagranicy. My zdecydowaliśmy się na prezentację głosu polskich specjalistów. Można dzięki temu sprawdzić, czy opinie rodzimych specjalistów odbiegają od opinii wyrażanych zagranicą. Zresztą specyfikę polską w niektórych przypadkach wyraźnie widać, jak chociażby w ocenie działań prawno-regulacyjnych czy występowania niektórych szczególnych zagrożeń technicznych, które mają swoją historię w polskiej cyberprzestrzeni.
Mamy nadzieję, że nasz raport jest ciekawą lekturą, a dla wielu stanie się pożytecznym materiałem, pomocnym w rozważaniach na temat tego, co nas czeka w najbliższych miesiącach.

**MIROSŁAW MAJ** Prezes Fundacji Bezpieczna Cyberprzestrzeń

# METODOLOGIA

W celu zebrania opinii eksperckich przygotowana została ankieta. Ankieta zawierała zestawienie potencjalnych zagrożeń w 2013 r. Lista tych zagrożeń powstała na podstawie innych podobnych ankiet oraz naszych własnych opinii co do jej kształtu. Dodatkowo lista mogła być uzupełniona przez propozycje eksperckie, w sytuacji, kiedy zdaniem eksperta istotne zagrożenie nie pojawiło się w zestawieniu. Uczestnicy ankiety poproszeni zostali o wyrażenie swoich opinii na temat prawdopodobieństwa powszechnego wystąpienia danego zagrożenia oraz poziomu niebezpieczeństwa w przypadku jego wystąpienia. Zestawienie zawierało 14 pozycji:

- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi (np: Stuxnet)
- Zagrożenia zawiązane z BYOD
- Phishing email i www
- Haktywizm
- Powstawanie botnetów opartych o platformy mobilne
- Zagrożenia w serwisach społecznościowych
- Zagrożenia dla platformy Android
- Zagrożenia dla platformy iOS
- Zagrożenia dla platformy Windows Phone/Mobile
- Zagrożenia typu ransom/scareware
- Wykorzystanie gier sieciowych w atakach
- Wycieki baz danych zawierających dane osobowe
- Ataki drive-by download
- Ataki na cloud-computing.

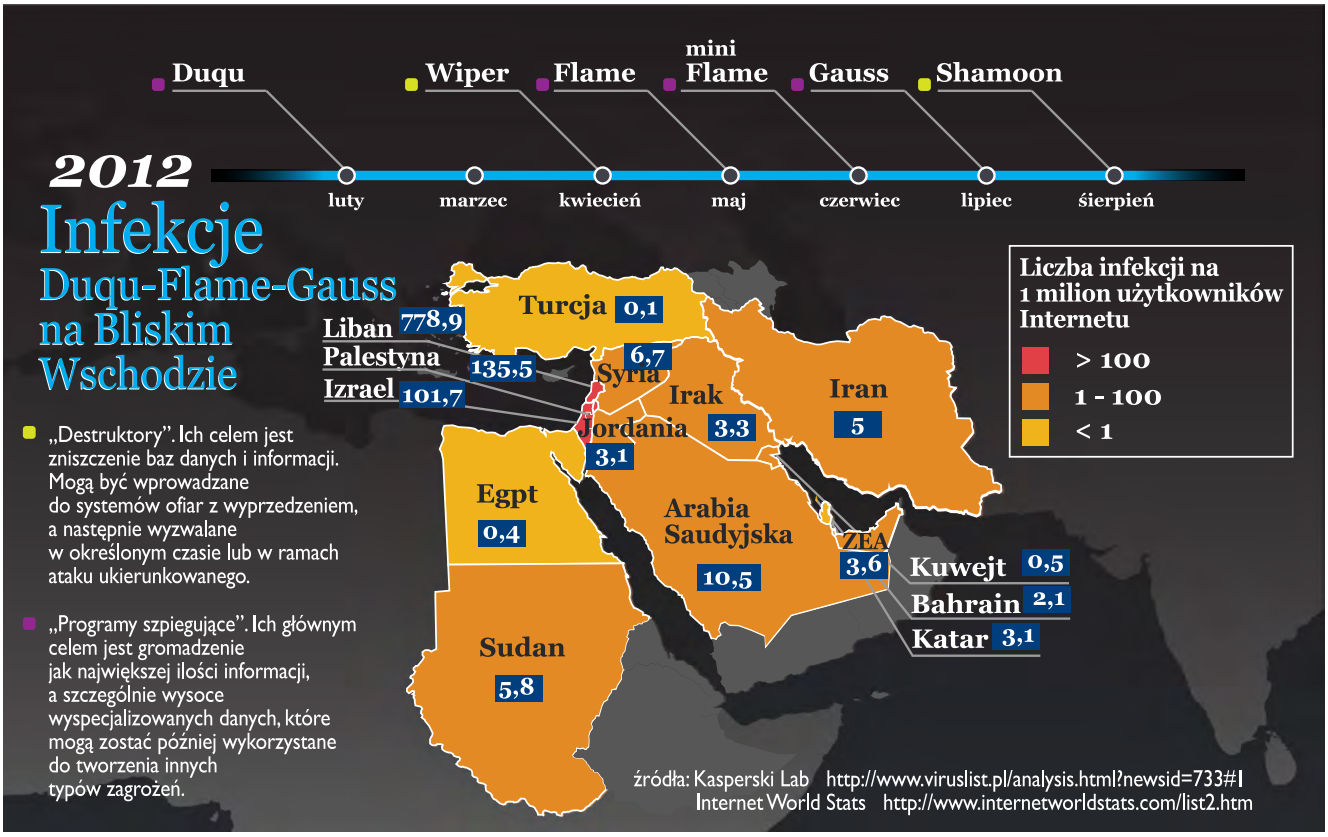
Odpowiedziom można było nadać wagi poprzez przypisanie punktacji od 1 (waga najmniejsza) do 5 (waga największa).
Na koniec każdy z ekspertów poproszony został o wyrażenie swojej opinii w postaci kilku zdań, na temat tego, czego możemy się spodziewać i czego najbardziej obawiać w 2013 roku. Większość z ekspertów zdecydowało się na przedstawienie swojej opinii.

# PRZEGLĄD NAJWAŻNIEJSZYCH WYDARZEŃ 2012 ROKU

Przed przystąpieniem do omówienia zagrożeń, które mogą nas spotkać w roku 2013 warto na chwilę powrócić do tych najważniejszych z zeszłego roku. Rok 2012 to między innymi sieciowe konflikty na poziomie międzynarodowym, ataki ukierunkowane, haktywizm. Z mijającego roku wszyscy powinni zapamiętać takie wirusy jak Flame i Gauss. Haktywiści uruchamiali coraz to kolejne operacje, z czego z pewnością w Polsce zapamiętamy ataki z drugiej połowy stycznia związane z konfliktem społecznym wokół ACTA i uciążliwymi atakami na serwisy rządowe oraz przemówieniem „Baśki" na stronie premiera rządu RP. Później w ciągu roku wielokrotnie słyszeliśmy o poważnych atakach, które nie omijały największych, czyli takich firm jak Sony, Oracle, Adobe, Microsoft czy Google. Doniesienia o atakach obalały mity na temat bezpieczeństwa niektórych systemów. Skutecznie zrobił to na przykład wirus Flashback, który w kwietniu zainfekował ponad 700 000 komputerów obsługiwanych przez system MacOS X. Wyznawcy poglądu „mam Maca więc jestem bezpieczny" musieli zrewidować swoje poglądy.

Prawdziwym majstersztykiem złośliwego kodu był pakiet wirusowy Flame. Długa jest lista jego funkcjonalności. Są to głównie funkcje szpiegowskie i z pewnością ten wirus wpisuje się w kategorię „wojny cybernetyczne", biorąc pod uwagę cele jego ataku. Istnieją też opracowania pokazujące jego podobieństwo do wcześniejszych wirusów Stuxnet i Duqu. A wiele śladów wskazuje na rządy Izraela i Stanów Zjednoczonych, jako jego autorów. Wirus działał od roku 2010, a kiedy pojawiły się pierwsze doniesienia o jego wykryciu, w dość szybkim czasie znikł z komputerów swoich ofiar. Co ciekawe, w historii o Flame jest też wątek polski. Zdaniem Kaspersky Lab część infrastruktury, która służyła do zarządzania znajdowała się w Polsce[1].

[1] „Dach płonie: walka z serwerami kontroli Flame'a" – http://www.viruslist.pl/weblog.html?weblogid=794




**Rysunek** – Mapa przedstawiająca infekcje wirusami Duqu, Flame, Gauss w regionie Bliskiego Wschodu.

Co jednak najważniejsze w tym wszystkim to to, że począwszy do Stuxneta, a później idąc przez Flame, Duqu i późniejszey Gauss, pojęcie „wojen cybernetycznych" z pozycji terminu w literaturze przeszło do fazy realnego zjawiska. Jeśli ktoś ma jeszcze wątpliwości po przytoczeniu powyższego zestawu, to może do niego dodać kasowanie danych na 30 000 komputerów światowego giganta w wydobyciu ropy naftowej – Saudi Aramco, czyli coś, co znamy pod nazwą wirusa Shamoon.

Omawiając najważniejsze wydarzenia roku 2012 nie można pominąć sprawy dynamicznego wzrostu zagrożeń dla platform mobilnych. A właściwie należałoby uczciwie stwierdzić, że chodzi przede wszystkim o system Android. Powodem tego jest oczywiście niezwykła popularność tego systemu (około 70% udziału w rynku), ale chyba jeszcze bardziej słabye mechanizmy weryfikacji oprogramowania, które pojawiają się w Android Market. To sytuacja zupełnie inna niż w przypadku dwóch innych systemów – iOS i Windows

Phone/Mobile. Tam ta kontrola jest znacznie bardziej restrykcyjna. Efekt jest widoczny gołym okiem. Wirusy na iOS i Windows Phone/Mobile łącznie oscylują wokół 1% wszystkich wirusów na platformy mobilne. Natomiast wirusy na Android to mniej więcej taki sam udział w liczbie wirusów, jak ich udział w rynku. Żeby uprzytomnić skalę zjawiska warto przywołać statystyki wspominanego już KasperskyLab mówiące o tym, że w 2012 roku odnotowano około 35 000 wirusów na Android. Krótko mówiąc, po blisko 10 latach ustawicznego „wywoływania wilka z lasu", biorąc pod uwagę systematyczne przewidywania co do wzrostu zagrożeń związanych z telefonami komórkowymi, „wilk z lasu wyszedł" i co gorsza jest coraz bardziej syty. Nie obyło się w 2012 roku również bez dużych wycieków danych osobowych. Co prawda nie było tak spektakularnie jak w 2011 roku, kiedy to atak na Sony skończył się wyciekiem danych o 70 milionach użytkownikach, ale wpadki – najpierw LinkedIn (6,4 mln rekordów), a później Dropbox (8 mln rekordów), podtrzymały złą passę.

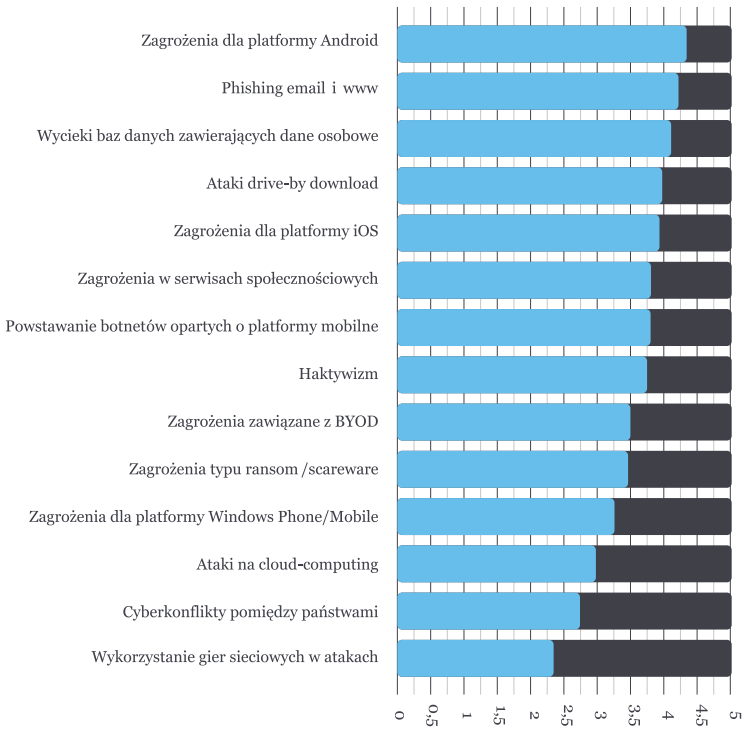
W 2012 roku kolejny raz potwierdziło się istotne zagrożenie związane z korzystaniem z Javy. W sierpniu pojawiły się masowe infekcje związane z krytyczną dziurą w Javie oraz równie powszechne związane z Adobe Flash Player.

Oprócz spektakularnych problemów z powszechnie używanym oprogramowaniem warto wspomnieć jeszcze o dwóch ciekawych przypadkach dotyczących sprzętu. Pierwszy z nich to pojawienie się na „rynku" urządzenia wartego 50$, dzięki któremu można otworzyć 4 miliony drzwi w kilku tysiącach hoteli na całym świecie, wliczając w to takie sieci hotelowe jak Hyatt, Marriott czy Holiday Inn. Łatwo sobie wyobrazić, jak bardzo kosztowne byłoby „załatanie" tej dziury w porównaniu do łatania dziur w oprogramowaniu.
Drugi ciekawy przypadek to historia z Brazylii, gdzie ofiarą ataku wirusa padło padło 4,5 mln właścicieli modemów.
Wszystko to poprzez jedną dziurę w modemowym firmware'rze i nielegalnej sieci 40 serwerów DNS.

# NAJWIĘKSZE ZAGROŻENIA W 2013 ROKU

Po tym szybkim podsumowaniu roku 2012 przejdźmy do prognoz dotyczących roku 2013. Zestaw, jaki zaproponowaliśmy do oceny, to zestawienie tego, co najczęściej się pojawia w dyskusji na temat tegorocznych zagrożeń, poparte naszą opinią na temat zagrożeń. Zresztą jeśli któryś z odpowiadających uznał, że ominęliśmy jego „faworyta", mógł sam go zgłosić. Większość kategorii wydaje się dość oczywista. Najpierw na wyniki dotyczące odpowiedzi na pytanie o te zagrożenia, które będą w dopiero co rozpoczętym roku najbardziej powszechne.

**Prawdopodobieństwo powszechnego wystąpienia wskazanego poniżej zagrożenia. Skala 1–5 (1 – najmniej prawdopodobne, 5 – najbardziej prawdopodobne).**



Na czoło klasyfikacji wybijają się trzy kategorie[2]:

- Zagrożenia dla platformy Android – **4,35**
- Phishing z wykorzystaniem poczty elektronicznej i serwisów WWW – **4,24**
- Wycieki baz danych zawierających dane osobowe – **4,12**

Te trzy pozycje to oczywiście kategorie różnego rodzaju. Jedna mówi o najbardziej narażonej na atak platformie, druga o metodzie, a trzecia o skutku. Teoretycznie więc moglibyśmy ją złożyć w całość, czyli na przykład phishingowy atak na platformie Android, w wyniku którego wyciekają dane osobowe. Choć akurat taki scenariusz nie jest chyba najbardziej prawdopodobny.

Z prognoz wynika, że nadchodzący rok może być związany z używaniem tego, co od lat jest już sprawdzone i niestety nadal zbiera spore plony, czyli z phishingiem oraz z najnowszym masowym zagrożeniem, które przy okazji rozwija się niezwykle dynamicznie, czyli z atakami na platformę Android. W ciągu kilku ostatnich lat, w rankingu zagrożeń ugruntowały również swoją pozycję „wycieki danych osobowych".

Na drugim biegunie powszechności zagrożeń mamy trzy pozycje, które w punktacji nie przekroczyły wartości 3 punktów. Są to, począwszy od najniżej notowanych:

- Wykorzystanie gier sieciowych w atakach – **2,35**
- Cyberkonflikty pomiędzy państwami – **2,76**
- Ataki na cloud-computing – **3,00**

Pierwsza i trzecia pozycja wydaje się, że nie budzi kontrowersji. Rzeczywiście jak dotąd gry sieciowe nie zostały masowo wykorzystane do propagacji zagrożeń. Jest to zresztą dość ciekawe, biorąc pod uwagę popularność gier sieciowych. Co prawda dwa lata temu mieliśmy olbrzymi wyciek danych użytkowników Sony PlayStation,

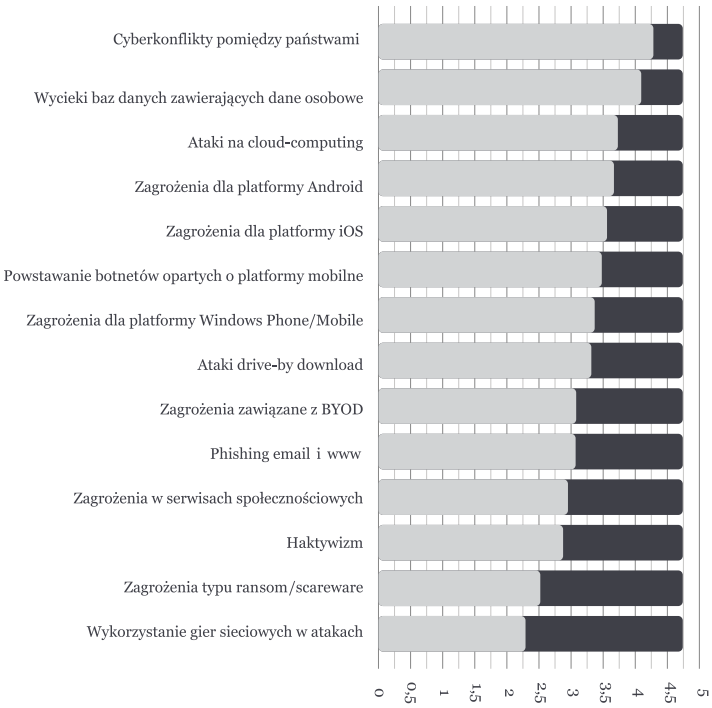
*Rok 2013 to nadal trwająca ekspansja technologii mbilnych i przenoszenia biznesu w "chmury". Najlepszy współczynnik ROI dla przestępcy jest tam, gdzie działają zasady Pareto i "low hanging fruits" (ang. nisko wiszące owoce). Z uwagi na popularność nowych urządzeń i innowacyjnych sposobów przetwarzania informacji uważam, że właśnie tam skoncentrują swoje działania. Działając reaktywnie nie zdołamy sobie z nimi poradzić na czas, a "ciemna strona" z tego korzysta. By się przed tym ustrzec powinniśmy działać pro-aktywnie z myślą o przyczynach występowania podatności wykorzystywanych przez przestępców.– **Przemysław Skowron** / WhiteCat Security*

*Zmiana celów ataków będzie podyktowana zmianami w technologii, głównym kierunkiem platformy mobilne, chmura, portale społecznościowe. Będziemy mieli do czynienia zarówno z prostymi atakami typu wysłanie SMS-ów premium bez wiedzy użytkowników, jak również z kradzieżami tożsamości synchronizowanych pomiędzy telefonem/tabletem a portalami i chmurą. Wyzwaniem będzie zabezpieczenie danych na nowych platformach.*
***– Tadeusz Włodarczyk** / PSE Operator SA*

[2] wszystkie wartości oceny odnoszą się do skali **1–5** (**1** – najmniejsze prawdopodobieństwo, **5** – największe prawdopodobieństwo).

ale to, co się wtedy stało, trudno nazwać atakiem na samą architekturę czy konfigurację związaną z grami. Od czasu do czasu pojawiają się więc informacje o zagrożeniach, ale wielkiego „bum!" jeszcze nie było. Prognozy eksperckie nie zapowiadają zmiany, aczkolwiek historia różnych prognoz pokazuje, że dość często ranking zagrożeń jest zdominowany przez coś, co wcześniej nie było prawie w ogóle brane pod uwagę. Tak było chociażby w 2010 roku ze Stuxnetem. Natomiast jeśli chodzi o zagrożenia związane z przetwarzaniem w chmurze, to powodem dość niskiej punktacji może być przekonanie, że w tym przypadku bezpieczeństwo dotyczy przede wszystkim zagadnień związanych z ciągłością działania, a największe problemy z tym związane nie dotyczą

**Poziom niebezpieczeństwa w przypadku wystąpienia podanego poniżej zagrożenia. Skala 1–5 (1 – najmniej groźne, 5 – najbardziej groźne).**




*W roku 2013 spodziewałbym się dynamicznego rozwoju zagrożeń związanych z platformami mobilnymi w związku z upowszechnieniem tzw. smartfonów oraz nowymi usługami świadczonymi przy ich użyciu (np. funkcje płatności zbliżeniowych itp.). Nie zniknie również dość powszechne zjawisko phishingu i próby wyłudzania danych za pomocą poczty elektronicznej czy też serwisów społecznościowych, na które to próby niestety szereg użytkowników wciąż jest podatny. Z globalnego punktu widzenia największe ryzyko niesie za sobą wystąpienie cyberkonfliktów na poziomie międzypaństwowym, które może prowadzić do zaognienia stosunków pomiędzy państwami i otwartych konfliktów zbrojnych. Groźne, lecz trudne do przeprowadzenia ze względu na rozproszoną architekturę, mogą być ataki na infrastrukturę związaną z usługami w chmurach obliczeniowych.*

*– **Maciej Miłostan** / PCSS, IChB PAN (PIONIER CERT), Politechnika Poznańska*

ataków sieciowych, a raczej odpowiedniego zaprojektowania i eksploatacji systemu oraz stosowaniem procedur ciągłości działania.

Pewne kontrowersje może budzić obecność w grupie najmniejszych zagrożeń ataków związanych z cyberkonfliktami pomiędzy państwami. Przecież od co najmniej 2 lat słyszymy non stop o tych przypadkach, w szczególności od czasu wspomnianego już Stuxneta. Warto jednak przypomnieć w tym miejscu, że w tej części ankiety eksperci odpowiadali na pytanie o powszechność występowania danego zagrożenia. Mimo dużego rozgłosu medialnego takich wirusów jak Flame, Duqu czy Gauss, warto pamiętać, że udokumentowana liczba infekcji tymi wirusami to raptem kilkanaście tysięcy przypadków, co, w porównaniu z wieloma innymi nawet pojedynczymi wirusami jest, liczbą wręcz znikomą.

O tym, że mimo wszystko prognozujący zagrożenia w 2013 nie bagatelizują tych związanych z cyberkonfliktami, świadczą wyniki odpowiedzi na drugie kluczowe pytanie ankiety, czyli na pytanie: „Jaki jest poziom niebezpieczeństwa w przypadku wystąpienia danego zagrożenia?". Tu zdecydowanym zwycięzcą zostało właśnie zagrożenie związane z występowaniem cyberkonfliktów. Pierwsza trójka zagrożeń o największych potencjalnych konsekwencjach wygląda następująco:

- Cyberkonflikty pomiędzy państwami – **4,18**
- Wycieki baz danych zawierających dane osobowe – **4,00**
- Ataki na cloud computing – **3,65**

Jak widać, doświadczenia związane z serią wirusów związanych z cyberkonfliktami, począwszy od Stuxneta, uzmysłowiła wszystkim, jak poważne mogą być konsekwencje ataku skierowanego na najważniejszą infrastrukturę. Zestaw zeszłorocznych ataków z wykorzystaniem funkcji destrukcyjnych (np.: wirusa

*Sądzę, że po przełamaniu pewnej bariery nastąpi jeszcze bardziej zdecydowany atak na platformy mobilne. Wydają się one z wielu względów wręcz idealnym celem ataku. Nie wykluczam jednak, że mimo dociekliwych analiz, w 2013 r. może być tak, że pojawi się coś, co zupełnie nas zaskoczy. Tak było w wielu przypadkach w przeszłości. Jeśli tak się stanie, to oczywiście ten rodzaj ataku będzie najgroźniejszy, ponieważ nikt na niego nie będzie przygotowany.*

***– Mirosław Maj** / Fundacja Bezpieczna Cyberprzestrzeń, ComCERT SA*

Shamoon) albo funkcji szpiegowskich (np.: wirusa Flame czy Gauss) tylko utwierdził przekonanie o wysokim ryzyku związanym z tego typu zdarzeniami.

Wysoka druga pozycja przypadków potencjalnych wycieków danych osobowych to z pewnością przejaw świadomości związanej z koniecznością ochrony danych osobowych i tego, jak poważne konsekwencje występują dla poszkodowanych w takich wyciekach. Często pojedynczy przypadek jest dopiero początkiem łańcucha feralnych zdarzeń, zresztą zazwyczaj „na prośbę" samego poszkodowanego, chociażby w związku z tym, że używa on tych samych danych autoryzacyjnych do wielu serwisów. Na przykład wyciek hasła do jednego serwisu społecznościowego, może być automatycznie „przekazaniem" hasła do innych serwisów społecznościowych, kont pocztowych a nawet serwisów bankowości elektronicznej.

Na dole rankingu zagrożeń o największych konsekwencjach znajdują się:

- Haktywizm – **2,82**
- Zagrożenia typu ransom/scareware – **2,47**
- Wykorzystanie gier sieciowych – **2,24**

Niska ocena zagrożeń związanych z haktywizmem w warunkach polskich to zapewne doświadczenia związane z naszymi doświadczeniami sprzed roku, czyli atakami na rządowe serwisy w czasie protestów społecznych związanych z próbą wprowadzenia ACTA. Ataki DDoS i podmiana strony premiera budzą raczej skojarzenia z atakami na reputację i prestiż, co wśród specjalistów technicznych nie budzi największych obaw. Zapewne gdyby w Polsce nastąpiła akcja będąca polską odmianą WikiLeaks i w sieci pojawiłyby się poufne informacje dotyczące działania ważnych służb państwowych, ocena zagrożenia związanego z haktywizmem byłaby bardziej alarmująca.

*W dzisiejszych czasach zarówno firmowe sieci jak i domowe komputery są wyposażone w szereg rozwiązań mających chronić użytkownika przed skutkami ataków komputerowych. W większości przypadków te rozwiązania (antywirusy, firewalle, itp.) mimo, że nie są idealne, sprawdzają się całkiem nieźle, pod warunkiem że: 1. regularnie aktualizujemy oprogramowanie – zwłaszcza przeglądarkę i jej wtyczki, bo to "w przeglądarce" spędzamy dziś przeważającą część naszego dnia. 2. zachowujemy zdrowy rozsądek – bo nawet najlepsze zabezpieczenia nie pomogą, jeśli atak skierowany jest w człowieka. Przestępcy zdają sobie z tego sprawę, dlatego od pewnego czasu coraz więcej ataków wykorzystuje socjotechnikę, wychodząc z założenia, że skoro nie możemy złamać sprzętu, złamiemy człowieka. A że człowiek jest najsłabszym ogniwem, na większość z nas znajdzie się odpowiednia metoda, co wspaniale pokazują coraz sprytniejsze ataki trojanów typu ZeuS czy Citadel. – **Piotr Konieczny** / Niebezpiecznik.pl*

Trzeba przyznać, dość zaskakująca jest niska ocena zagrożenia związanego z występowaniem oprogramowania typu ransom/scareware. Jest to zagrożenie, które praktycznie zawsze wiąże się z wymiernymi stratami finansowymi, czyli zakupem „oprogramowania antywirusowego", które jest wirusem albo zapłaceniem okupu na konto cyberprzestępców. Nie można też stwierdzić, że w warunkach polskich jest to zagrożenie egzotyczne, ponieważ w 2012 roku dość spore żniwa w Polsce zebrał tzw. „wirus policja".

*W roku 2013, poza najczęściej wymienianymi zagrożeniami związanymi z nowymi typami złośliwego oprogramowania dedykowanego na urządzenia mobilne, widzę co najmniej cztery typy zagrożeń, które powinny być bardzo poważnie brane pod uwagę przy planowaniu działań ochronnych: wykorzystanie serwisów społecznościowych do destabilizacji polityczne zwiększenie kontroli nad Internetem przez instytucje międzynarodowe i rządowe, brak skutecznych metod współpracy sektora publicznego (w szczególności rządowego) z sektorem prywatnym w propagowaniu najlepszych praktyk obrony przed atakami w cyberprzestrzeni i wreszcie brak klarownych kryteriów oceny i porównania skuteczności środków ochrony przed atakami sieciowymi, utrudniający ich wybór i zastosowanie.*
***– Robert Kośla** / Microsoft – Central and Eastern European Headquarters*

# INNE ZAGROŻENIA

Biorący udział w ankiecie mieli możliwość wskazania własnych typów zagrożeń, których możemy się spodziewać w 2013 roku, a które nie zostały uwzględnione w rankingu. Podali oni kilkanaście zagrożeń, które można pogrupować. Pierwsza grupa dotyczy obszaru finansów:

- Ataki na systemy giełdowe
- Ataki związane z płatnościami elektronicznymi (m.in. kradzieże danych kart kredytowych przy użyciu malware'u)
- Ataki na karty debetowe paypass i płatności z wykorzystaniem technologii NFC (ang. Near Field Communication – tj. komunikacji bliskiego zasięgu)

Druga dotyczy obszaru prawa, regulacji i dobrych praktyk:

- Zwiększenie „kontroli" nad Internetem przez instytucje międzynarodowe i rządowe
- Brak skutecznych metod współpracy sektora publicznego (w szczególności rządowego) z sektorem prywatnym w propagowaniu najlepszych praktyk obrony przed atakami w cyberprzestrzeni
- Brak klarownych kryteriów oceny i porównania skuteczności środków ochrony przed atakami sieciowymi, utrudniający ich wybór i zastosowanie
- Zamieszanie w przepisach skutkujące zamykaniem serwisów internetowych

Wreszcie eksperci wskazali kilka pozycji dotyczących różnych technik ataku:

- Ataki typu DDoS oparte o botnet
- Ataki socjotechniczne
- Szpiegostwo gospodarcze
- Ataki na systemy osadzone i przemysłowe (np. SCADA)

*Rok 2013 wprowadzi też duże zamieszanie formalno-prawne w Polsce i Europie, ponieważ wiele przepisów właśnie jest nowelizowanych, a użytkownicy cyberprzestrzeni nie nadążają za zmianami i popełniają błędy, które mogą być dla nich kosztowne. Przykładem jest nowelizacja polskiego prawa telekomunikacyjnego (cookie) i Ustawy o ochronie danych osobowych (zmiany z ABI, transferem danych i rejestracją zbiorów) oraz intensywne prace nad unijnym Rozporządzeniem dotyczącym ochrony danych osobowych.*

*– **Maciej Kołodziej** / FHU MatSoft, ComCERT SA*

Wszystkie te pozycje są bardzo ciekawe. Niektóre z nich pojawiają się w praktyce w liście rankingowej i właściwie są tylko uszczegółowieniem lub uogólnieniem konkretnej kategorii. Np.: „ataki DDoS oparte o botnet" to może być szczególna metoda wykorzystywana w różnych przypadkach, chociażby haktywizmu. Swoją drogą być może tej pozycji w Polsce szczególnie powinniśmy się obawiać biorąc pod uwagę bardzo niepokojące dane dotyczące poziomu bezpieczeństwa polskich komputerów. Na przykład w prestiżowym rankingu publikowanym przez amerykański zespół bezpieczeństwa – TeamCymru, od wielu tygodni nasz kraj zajmuje niechlubne pierwsze miejsce w rankingu największej aktywności botnetów i praktycznie nie wypada z TOP10 krajów, z których pochodzi szkodliwa aktywność teleinformatyczna[3]. Wskazana przez ekspertów pozycja „ataki socjotechniczne" to przypomnienie o tym, że dzisiejsze zagrożenia bardzo często związane są z tym elementem. Oprogramowanie typu ransom/scareware czy powszechne ataki phishingowe przez www i pocztę elektroniczną to bardzo charakterystyczny przykład ataków socjotechnicznych. Tego typu element występuje w wielu innych przypadkach, np: przy naciągnięciu ofiary do odwiedzenia infekującego serwisu internetowego, czyli przeprowadzeniu ataku typu drive-by download. Również większość ataków na platformy mobilne zawiera element socjotechniczny.

Co ciekawe, eksperci wskazali w swoich prognozach to, że na poziom bezpieczeństwa w Internecie bardzo duże znaczenie ma prawidłowe podejście do spraw prawodawstwa, regulacji i popularyzowania dobrych praktyk. Przekładając to na język naszego raportu – obawiają się, że tego zabraknie i jest to poważnym zagrożeniem. To ważny sygnał, który powinien wywołać działania po obydwu stronach „dialogu publiczno-prywatnego". Nasze krajowe doświadczenia jeśli chodzi o dialog w tej sprawie nie są najlepsze i warto odebrać ten głos jako obawę, że skutki tego mogą być groźne.

Na koniec warto też wspomnieć o prognozie dotyczącej potencjalnych ataków na systemy teleinformatycznej infrastruktury krytycznej. Poważnych przypadków tego typu jak dotąd w Polsce nie mieliśmy, ale ćwiczenia Cyber-EXE Polska 2012 dowiodły, że zagrożenia są realne i warto o tym pamiętać.

*Choć zwykle nie postrzega się tego jako zagrożenia technicznego, próby przejęcia kontroli politycznej nad Internetem również doprowadzą do pogorszenia technicznej jakości i dostępności usług w sieci. Są one przeważnie forsowane przez osoby nie rozumiejące funkcjonowania sieci, w sposób nietransparentny i w oparciu o tworzone ad hoc rozwiązania techniczne lub prawne. Dlatego mechanizmy takie jak "takedown notice" czy rejestry stron zakazanych należy również traktować jako ryzyko, zwłaszcza z punktu widzenia dostępności stron, zwłaszcza w krajach o niskiej kulturze legislacyjnej – takich jak Polska.* – **Paweł Krawczyk** / *OWASP*

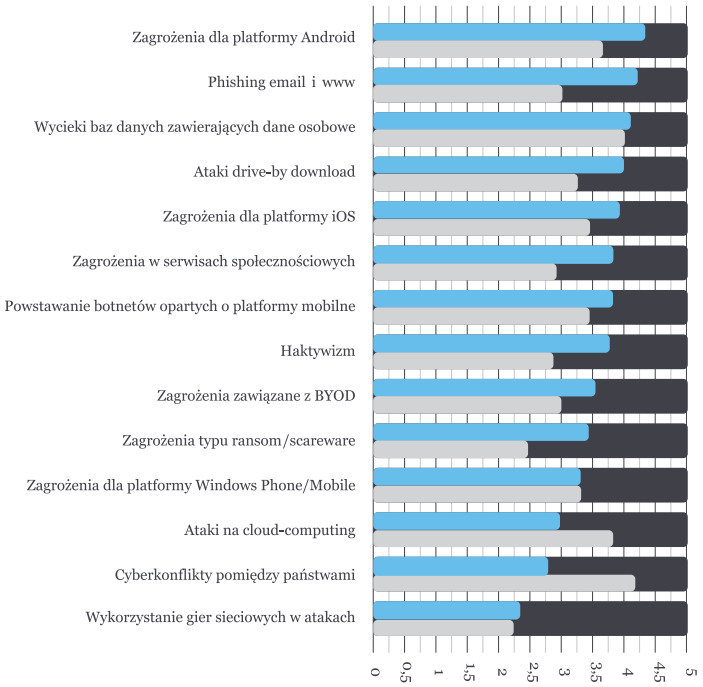
[3] http://www.team-cymru.org/Monitoring/Graphs/

# PODSUMOWANIE

Wyniki ankiety wskazują na to, że w nadchodzącym roku powinniśmy w szczególny sposób obawiać się zagrożeń związanych z atakami na platformy mobilne, a tak naprawdę przede wszystkim na platformę Android. Bardzo ważnym sygnałem dla wszystkich, którzy prowadzą serwisy internetowe i bazy danych dostępnych przez Internet jest to, aby zadbali o bezpieczeństwo danych osobowych swoich użytkowników. Wreszcie warto podkreślić, że mimo tego, że poważne cybernetyczne konflikty pomiędzy państwami nie muszą być powszechne, to ich konsekwencje mogą być bardzo poważne i mogą dotyczyć skutecznych ataków na teleinformatyczną infrastrukturę krytyczną. W tym przypadku warto swoje spojrzenie skierować na odpowiedzialnych za ochronę teleinformatycznej infrastruktury krytycznej, ponieważ te konsekwencje mogą być związane ze słabościami w systemie zabezpieczeń technicznych i organizacyjnych tych zasobów.

Przygotowany raport na temat prognoz dotyczących zagrożeń teleinformatycznych w 2013 r. jest najprawdopodobniej pierwszym tego typu raportem, na wyniki którego składają się głosy polskich specjalistów ds. bezpieczeństwa teleinformatycznego. Dotychczas przy analizie tego co może być groźne w nadchodzącym okresie korzystaliśmy z opinii innych podmiotów i specjalistów z zagranicy.

**Porównanie prawdopodobieństwa powszechnego wystąpienia i poziomu niebezpieczeństwa zagrożenia w 2013 r.**



# UCZESTNICY ANKIETY

**Adam Danieluk**
Dyrektor Departamentu Bezpieczeństwa IT
**First Data Polska SA**

**Przemysław Frasunek**
Dyrektor działu
**ATM Software sp. z o.o.**

**Adam Haertle**
IT Security Officer
**UPC Polska sp. z o.o.**

**Maciej Kołodziej**
Specjalista ds. Bezpieczeństwa Teleinformatycznego
**FHU MatSoft /ComCERT SA**

**Piotr Konieczny**
CISO
**Niebezpiecznik.pl**

**Robert Kośla**
Dyrektor Sektora Obronności i Bezpieczeństwa Narodowego
**Microsoft - Central and Eastern European Headquarters**

**Paweł Krawczyk**
Application security manager
**OWASP**

**Maciej Łopaciński**
Wiceprezes
**Agora TC Sp. z o.o.**

**Mirosław Maj**
Prezes Zarządu / CIO
**Fundacja Bezpieczna Cyberprzestrzeń / ComCERT SA**

**Marcin Marciniak**
Dziennikarz
**IDG Poland SA**

**Maciej Miłostan**
Specjalista ds. informatyki
**PCSS, ICHB PAN (PIONIER CERT) / Politechnika Poznańska**

**Michał Pawlak**
Kierownik Działu Bezpieczeństwa Teleinformatycznego
**Operator Gazociągów Przesyłowych GAZ-SYSTEM SA**

**Przemysław Skowron**
Menedżer ds. Badań i Rozwoju Bezpieczeństwa IT
**WhiteCat Security**

**Artur Ślubowski**
Information Security Officer
**RWE Polska**

**Zbigniew Świerczyński**
Adiunkt
**Wojskowa Akademia Techniczna**

**Tadeusz Włodarczyk**
Główny specjalista
**PSE Operator SA**

# ZAŁACZNIKI

| Prawdopodobieństwo powszechnego wystąpienia wskazanego poniżej zagrożenia. Skala 1–5 (1– najmniej prawdopodobne, 5 – najbardziej prawdopodobne). | 1 | 2 | 3 | 4 | 5 | Ocena średnia |
|---|---|---|---|---|---|---|
| Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi (np: Stuxnet). | 17,6% (3) | 35,3% (6) | 17,6% (3) | 11,8% (2) | 17,6% (3) | 2,76 |
| Zagrożenia zawiązane z BYOD. | 0,0% (0) | 11,8% (2) | 41,2% (7) | 29,4% (5) | 17,6% (3) | 3,53 |
| Phishing email and www. | 0,0% (0) | 0,0% (0) | 29,4% (5) | 17,6% (3) | 52,9% (9) | 4,24 |
| Haktywizm. | 0,0% (0) | 11,8% (2) | 23,5% (4) | 41,2% (7) | 23,5% (4) | 3,76 |
| Powstawanie botnet-ów opartych o platformy mobilne. | 5,9% (1) | 0,0% (0) | 23,5% (4) | 47,1% (8) | 23,5% (4) | 3,82 |
| Zagrożenia w serwisach społecznościowych. | 0,0% (0) | 5,9% (1) | 47,1% (8) | 5,9% (1) | 41,2% (7) | 3,82 |
| Zagrożenia dla platformy Android. | 0,0% (0) | 0,0% (0) | 17,6% (3) | 29,4% (5) | 52,9% (9) | 4,35 |
| Zagrożenia dla platformy iOS. | 0,0% (0) | 0,0% (0) | 29,4% (5) | 47,1% (8) | 23,5% (4) | 3,94 |
| Zagrożenia dla platformy Windows Phone/Mobile. | 0,0% (0) | 29,4% (5) | 29,4% (5) | 23,5% (4) | 17,6% (3) | 3,29 |
| Zagrożenia typu ransom/scareware. | 5,9% (1) | 5,9% (1) | 41,2% (7) | 29,4% (5) | 17,6% (3) | 3,47 |
| Wykorzystanie gier sieciowych w atakach. | 11,8% (2) | 52,9% (9) | 23,5% (4) | 11,8% (2) | 0,0% (0) | 2,35 |
| Wycieki baz danych zawierających dane osobowe. | 0,0% (0) | 0,0% (0) | 29,4% (5) | 29,4% (5) | 41,2% (7) | 4,12 |
| Ataki drive-by download. | 0,0% (0) | 0,0% (0) | 29,4% (5) | 41,2% (7) | 29,4% (5) | 4,00 |
| Ataki na cloud-computing. | 5,9% (1) | 23,5% (4) | 41,2% (7) | 23,5% (4) | 5,9% (1) | 3,00 |

**Tabela 1 –** Wyniki ankiety dotyczącej prawdopodobieństwa powszechnego wystąpienia ZAGROŻENIA.

| Poziom niebezpieczeństwa w przypadku wystąpienia podanego poniżej zagrożenia. Skala 1–5 (1– najmniej groźne, 5 – najbardziej groźne). | 1 | 2 | 3 | 4 | 5 | Ocena średnia |
|---|---|---|---|---|---|---|
| Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi (np: Stuxnet). | 5,9% (1) | 11,8% (2) | 0,0% (0) | 23,5% (4) | 58,8% (10) | 4,18 |
| Zagrożenia zawiązane z BYOD. | 0,0% (0) | 23,5% (4) | 52,9% (9) | 23,5% (4) | 0,0% (0) | 3,00 |
| Phishing email and www. | 0,0% (0) | 23,5% (4) | 58,8% (10) | 11,8% (2) | 5,9% (1) | 3,00 |
| Haktywizm. | 11,8% (2) | 35,3% (6) | 17,6% (3) | 29,4% (5) | 5,9% (1) | 2,82 |
| Powstawanie botnet-ów opartych o platformy mobilne. | 0,0% (0) | 23,5% (4) | 17,6% (3) | 52,9% (9) | 5,9% (1) | 3,41 |
| Zagrożenia w serwisach społecznościowych. | 5,9% (1) | 35,3% (6) | 23,5% (4) | 35,3% (6) | 0,0% (0) | 2,88 |
| Zagrożenia dla platformy Android. | 0,0% (0) | 17,6% (3) | 23,5% (4) | 41,2% (7) | 17,6% (3) | 3,59 |
| Zagrożenia dla platformy iOS. | 0,0% (0) | 23,5% (4) | 23,5% (4) | 35,3% (6) | 17,6% (3) | 3,47 |
| Zagrożenia dla platformy Windows Phone/Mobile. | 0,0% (0) | 23,5% (4) | 29,4% (5) | 41,2% (7) | 5,9% (1) | 3,29 |
| Zagrożenia typu ransom/scareware. | 17,6% (3) | 23,5% (4) | 52,9% (9) | 5,9% (1) | 0,0% (0) | 2,47 |
| Wykorzystanie gier sieciowych w atakach. | 23,5% (4) | 41,2% (7) | 23,5% (4) | 11,8% (2) | 0,0% (0) | 2,24 |
| Wycieki baz danych zawierających dane osobowe. | 0,0% (0) | 11,8% (2) | 17,6% (3) | 29,4% (5) | 41,2% (7) | 4,00 |
| Ataki drive-by download. | 0,0% (0) | 29,4% (5) | 35,3% (6) | 17,6% (3) | 17,6% (3) | 3,24 |
| Ataki na cloud-computing. | 5,9% (1) | 11,8% (2) | 17,6% (3) | 41,2% (7) | 23,5% (4) | 3,65 |

**Tabela 2 –** Wyniki ankiety dotyczącej poziomu niebezpieczeństwa w przypadku WYSTĄPIENIA ZAGROŻENIA




FUNDACJA BEZPIECZNA CYBERPRZESTRZEŃ
ul. Tytoniowa 20, 04-228 Warszawa
tel: +48 22 112 0 800
e-mail: kontakt@cybsecurity.org

Raport: Największe zagrożenia dla bezpieczeństwa w Internecie w roku 2013.

www.cybsecurity.org