OS X i iOS vs. malware

Jakub Zadrożny

1 Wstęp

Szacuje się, że niemal jedna trzecia wszystkich komputerów na świecie jest zainfekowana pewnym rodzajem złośliwego oprogramowania [1]. Działalność takiego oprogramowania może mieć przykre dla użytkownika konsekwencje - odpowiedni trojan jest przecież w stanie wykraść od nas numery kart kredytowych, dane personalne, hasła do bankowości internetowej itd. Doskonałym rozwiązaniem byłoby więc stworzenie sprzętu odpornego na to zagrożenie. Jednak czy jest to w ogóle możliwe?

Z pewnością wszyscy zainteresowani technologicznymi trendami ostatnich lat doskonale pamiętają kampanię reklamową *Get a Mac* firmy Apple z lat 2006-2009. W wielu materiałach stworzonych na jej potrzeby producent Maców chwali się, że jego sprzęt - w odróżnieniu od komputerów PC - nie jest podatny na działanie typowego malware'u [2]. Przekaz tej kampanii był na tyle silny, że w opinii społecznej powszechne stało się poczucie solidnego bezpieczeństwa ich systemu OS X. Tak powszechne, że odnalezienie Maca, na którym zainstalowany jest program antywirusowy mogłoby okazać się trudniejsze niż przypuszczamy. Jednak czy OS X jest rzeczywiście *bezpieczny*? A może jest to tylko kolejny marketingowy mit stworzony by mydlić oczy nieświadomym konsumentom? Poza tym, sama kampania liczy już sobie ponad 7 lat, więc nawet jeśli wówczas Maci były odporne na wirusy, to czy są i dziś?

2 Bezpieczeństwo dawniej

Historia malware'u dedykowanego dla OS X liczy już sobie wiele (jak na standardy software'owe) lat. Przez długi okres hakerom nie udawało się jednak stworzyć poważnego, globalnego zagrożenia dla użytkowników systemu OS X. Oto krótka historia trzech najgłośniejszych przykładów złośliwego oprogramowania ze świata Apple do roku 2008.

2.1 Renepo [3]

Według korporacji ESET pierwszy malware napisany na OS X pojawił się już w 2004 roku. Otrzymał on nazwę *Renepo* i dawał atakującemu szereg możliwości, łącznie z backdoorami i szpiegowaniem zainfekowanej maszyny. *Renepo* nigdy nie stanowił rzeczywistego zagrożenia, ponieważ nie przemieszczał się przez internet, a do przeprowadzenia ataku wymagał fizycznego dostępu do komputera ofiary. Udało mu się jednak pokazać, że system operacyjny od Apple nie

Instytut Informatyki Uniwersytetu Wrocławskiego, 2016–2017
Esej przygotowany w ramach zajęć *Kultura bezpieczeństwa komputerowego*

posiada żadnej magicznej zapory chroniącej go przed tego typu złośliwym oprogramowaniem i że w przyszłości należy spodziewać się gorszych ataków.

2.2 Leap [4]

Jak czytamy na blogu *naked security* firmy Sophos - kolejny wykryty malware na OS X był już prawdziwym wirusem, tzn. potrafił rozsyłać swoje kopie przez internet i automatycznie infekować kolejne urządzenia. Został wykryty w 2006 roku i otrzymał nazwę *Leap*. Aby doszło do zakażenia naszego komputera, musielibyśmy wykonać kilka naprawdę nieodpowiedzialnych kroków:

1. Odebrać dowolną drogą (email, iChat lub podobne) plik *latestpics.tgz*.
2. Rozpakować otrzymane archiwum.
3. W otrzymanym folderze zobaczylibyśmy plik imitujący zdjęcie, który musielibyśmy otworzyć.

Ponadto jeśli użytkownik, który wykonał te czynności nie był administratorem, to infekcja nie doszłaby do skutku. Wirusem *Leap* nie dało się zatem przypadkowo zarazić, bo nawet gdyby ktoś wysłał nam plik *latestpics.tgz* to nadal musielibyśmy go sami otworzyć. Sam wirus zawierał natomiast błędy w implementacji i w przypadku skutecznej infekcji nie powodował praktycznie żadnych skutków ubocznych w systemie, a zdaniem analityków prawdopodobnie napisany był bardziej jako proof-of-concept niż rzeczywisty atak [13].

2.3 RSPlug [5]

Wykryty w listopadzie 2007 roku trojan *RSPlug* był pierwszym złośliwym oprogramowaniem na OS X wypuszczonym w celu zarobkowym. Była to konstrukcja bardziej zaawansowana niż *Leap* i w przypadku skutecznej infekcji mógł nieświadomego użytkownika narazić na nieprzyjemne konsekwencje (w odróżnieniu od poprzednika). Przypadkowe zarażenie tym wirusem było dla przeciętnego użytkownika wysoce nieprawdopodobne, a dla użytkownika ostrożnego w zasadzie niemożliwe. Oto co musielibyśmy zrobić, aby złapać *RSPlug'a*:

1. Otworzyć link do strony pornograficznej, który był zwykle rozsyłany spamowym mailem.
2. Na tej stronie zostalibyśmy poproszeni o pobranie specjalnego kodeka, bez którego odtworzenie materiału byłoby niemożliwe.
3. Plik z kodekiem należało pobrać z tej samej strony, a następnie zamontować w systemie i uruchomić instalator.
4. W trakcie instalacji musielibyśmy dodatkowo podać hasło administratora.

Po skutecznej infekcji wirus zmieniał na komputerze adresy serwerów DNS tak, by przekierowywały one użytkownika na strony wybrane przez przestępców, gdzie Ci mogli z łatwością uprawiać np. *phishing*. Proces zarażania tym wirusem był jednak tak skomplikowany i nieprawdopodobny, że ciężko uznać go za prawdziwe niebezpieczeństwo.

Znając działanie trzech powyższych (wówczas najgroźniejszych) wirusów, możemy powiedzieć, że przed 2008 rokiem przemysł malware'u na OS X był dopiero w powijakach, a przypadki, które wykryli eksperci dość prymitywne. Szanse na przypadkowe złapanie któregoś z takich robaków były znikome. Same wirusy nie wykorzystywały żadnej luki w systemie OS X, a

jedynie naiwność użytkownika go obsługującego. Zatem twórcy kampanii reklamowej *Get a Mac* nie odbiegli znacząco od prawdy twierdząc, że problem złośliwego oprogramowania nie dotyczy ich sprzętu - wirusy na Maci wprawdzie istniały, jednak w porównaniu z ich odpowiednikami na komputery PC, były wtedy w zasadzie nieszkodliwe.

3 Postępy hakerów

Zdaniem ekspertów jedną z przyczyn ograniczonej obecności hakerów na platformie OS X była jego popularność. Udział Macintoshy w rynku był wówczas niewielki, przez co zdecydowana większość cyberprzestępców decydowała się atakować komputery pod kontrolą Windowsa. Coraz częściej pojawiały się jednak głosy, że wkrótce sytuacja ulegnie zmianie, bo wraz z nowymi klientami Maci przyciągną do siebie także hakerów. Ponadto przypadki wirusów takich jak *Renepo*, *Leap* i *RSPlug* pokazywały, że OS X powoli zaczynał już wchodzić w krąg zainteresowania twórców malware'u.

3.1 Scareware i kolejne trojany [4]

W 2008 pojawił się na OS X pierwszy scareware, czyli oprogramowanie wyłudzające od użytkowników opłaty za usługi, których w rzeczywistości nie świadczyło. Później pojawiły się w sieci aplikacje takie jak *MacDefender* podszywające się pod programy antywirusowe i żądające od użytkownika opłat licencyjnych. Ponadto cyberprzestępcy zaczęli umieszczać trojany (wykradające dane i hasła, lub instalujące backdoory w systemie) m.in. w pirackich wersjach software'u - np. pakietu iWork, czy aplikacji Adobe Photoshop. Dalej kontynuowana była również praktyka żądania instalacji niestandardowych kodeków wideo dostępnych jedynie na podejrzanych stronach.

Mimo coraz szerszej gamy zagrożeń czyhających na właścicieli Maców, przypadkowe wpadnięcie w pułapkę złośliwego oprogramowania było wciąż mało prawdopodobne. Wymagało z reguły nie tylko odwiedzania podejrzanych zakątków internetu, ale także zlecania im instalacji niezaufanego oprogramowania. Prawdziwe problemy zaczęły się dopiero kilka lat później, a zagrożenie jakie stworzyły dobrze obrazują dwa poniższe przykłady.

3.2 Flashback [6]

Początki trojana *Flashback* sięgają 2011 roku, kiedy to został wykryty przez firmę Intego [14]. Początkowo uznano, że nie stwarza on większego zagrożenia, gdyż jedynym sposobem na jego złapanie było uruchomienie zainfekowanego programu podającego się za instalator Flash Playera. Można uznać, że ostrożny internauta nie dałby się łatwo nabrać na taki trik. Po niecałym roku mechanizm infekcji został jednak przez twórców *Flashbacka* udoskonalony tak, by móc instalować trojana na Macu bez jakiejkolwiek zgody ani wiedzy użytkownika. Wykorzystali oni do tego niezałataną dotychczas przez Apple podatność Javy. Proces wyglądał następująco:

1. Użytkownik próbował połączyć się ze znajomą mu stroną, nad którą kontrolę przejęli hakerzy.
2. Taka zhakowana strona przekierowywała go na serwer przestępców, który następnie próbował wykorzystać wspomnianą lukę bezpieczeństwa.
3. Jeśli mu się powiodło, to automatycznie przerzucał instalator wirusa na dysk użytkownika i uruchamiał go. W przeciwnym wypadku próbował dokonać ataku jedną z bardziej tradycyjnych metod - podając się za instalator Flasha lub wtyczkę od Apple.

Po udanej infekcji instalator sprawdzał, czy na komputerze ofiary zainstalowane jest oprogramowanie antywirusowe i jeśli takie wykrył, to przerywał proces atak, aby uniknąć wykrycia. Jeśli natomiast system nie był chroniony, to instalator kończył swoją pracę podłączając komputer ofiary do botnetu atakujących. Głównym celem, dla którego stworzono *Flashbacka*, było wzbogacenie się jego twórców poprzez przekierowywanie użytkowników na strony reklamodawców.

Przykład *Flashbacka* jest w świecie malware'u na OS X niezwykle istotny. Przypadkowe złapanie tego wirusa było znacznie bardziej prawdopodobne niż w przypadku jego poprzedników, bo dzięki wykorzystaniu luki bezpieczeństwa system mógł zostać zainfekowany bez wiedzy i (choćby nieświadomej) zgody użytkownika. Ponadto poprawna infekcja mogła zostać przeprowadzana przez instalator nie posiadający nawet uprawnień administratora naszej maszyny, a sam trojan był w stanie ominąć wbudowane zabezpieczenie systemu OS X - *XProtect*. Te cechy złożyły się na sukces, jaki odniósł *Flashback* - według szacunków rosyjskiego dostawcy oprogramowania antywirusowego Dr. Web potwierdzonych przez firmę Kaspersky Lab ponad 600 000 komputerów Mac zostało zainfekowanych przez tego właśnie wirusa, pozwalając jego twórcom uformować pokaźny botnet [15, 16]. Jak napisał Broderick Ian Aquilino z F-Secure: "Flashback był nie tylko najbardziej zaawansowanym, ale także najskuteczniejszym malware'em na OS X, jaki dotąd widzieliśmy". Ten przypadek tylko potwierdził tezę, że złośliwe oprogramowanie na OS X zaczęło już wtedy poważnie doganiać swoich Windowsowych konkurentów, a wkrótce należało spodziewać się dalszej eskalacji problemu.

3.3 Rootpipe [7]

Odkryty w 2014 roku przez szwedzkiego analityka bezpieczeństwa Emila Kvarnhammara z Truesec *Rootpipe* nie był wirusem, ani trojanem, a czymś, co mogłoby hakerom pozwolić stworzyć zagrożenie znacznie większe niż *Flashback*. Był poważną luką bezpieczeństwa w systemie OS X Yosemite, która pozwalała programowi przekroczyć uprawnienia użytkownika, który go uruchomił. Po jej wykorzystaniu proces mógł bez weryfikacji hasła uzyskać najwyższy poziom dostępu znany jako poziom root'a (dający pełną kontrolę nad urządzeniem). Potencjalny wirus wykorzystujący tą podatność systemu operacyjnego mógłby zatem z łatwością wyrządzić szkody większe niż dotychczasowe i to bez znajomości hasła administartora.

Blisko rok po odkryciu tej podatności, bo dopiero w lipcu 2015 roku, Apple wydało bezpłatną aktualizację systemu OS X dostępną dla wszystkich użytkowników niwelującą to zagrożenie. I chociaż bezpośredni problem zniknął, to przypadek *Rootpipe'a* uświadomił opinii publicznej, że w systemie OS X znajdują się już błędy tak samo niebezpieczne, jak u jego konkurentów. Powszechne przekonanie o odporności OS X na wirusy stanęło pod dużym znakiem zapytania - przecież komuś może udać się połączyć najgroźniejsze cechy *Flashback'a* i *Rootpipe'a* i stworzyć wirusa infekującego Maci bez alarmowania użytkownika i uzyskującego dostęp root'a bez znajomości hasła administratora.

4 Bezpieczeństwo obecnie

Wraz z wzrostem popularności OS X wzrosła również ilość celującego w niego malware'u. Nie jest więc dziwne, że rok 2015 został przez wielu ekspertów okrzyknięty najgorszym w historii OS X pod względem grasujących w sieci zagrożeń. Zaskakujące mogą okazać się jednak ustalenia grupy analityków *Bit9 + Carbon Black*, według których w samym tylko roku 2015 wykryto aż pięciokrotnie więcej przykładów złośliwego oprogramowania niż łącznie w latach 2010-2014 [12]. W ciągu trwających 10 tygodni badań udało im się zebrać 180 przykładów pochodzących z lat 2010-2014 i aż 948 z samego 2015 roku. Z ich ustaleń wynika również, że cyberprzestępcy atakujący system OS X przyjęli technikę podobną do tych, którzy celują w Windows - wypuszczają

znaczne ilości mniej zaawansowanych wirusów, licząc, że w ogromnej już bazie użytkowników OS X i tak uda im się zainfekować odpowiednio wiele maszyn.

4.1 Epidemia adware'u [8]

Jak pisze portal *How-To-Geek* w ostatnich latach wybuchła epidemia tzw. *adware'u* i *spyware'u*, czyli oprogramowania do bombardowania użytkownika reklamami i śledzenia jego aktywności. Dawniej zainfekowanie tego typu malware'em następowało głównie na skutek nadmiernego zaufania podejrzanym stronom, a zachowując zdrowy rozsądek i ostrożność, mogliśmy w spokoju przeglądać internet, nie narażając się na łapanie wirusów. Jednak obecnie, chcąc zainstalować nawet zaufane i powszechnie znane oprogramowanie jak Open Office, czy VLC Player, prawdopodobnie trafimy w sieci na instalator, który poza żądanym programem zaopatrzy nasz komputer również w kilka "dodatków" w postaci wirusów śledzących i wstrzykujących reklamy w każde możliwe miejsce. Mniej zaawansowane z nich będą widoczne w pewnym miejscu w systemie (np. jako rozszerzenia przeglądarki) i stosunkowo łatwe do usunięcia, jednak inne zaszyją głęboko w ukrytych folderach, do których przeciętny użytkownik nie ma absolutnie potrzeby zaglądać. Większość takich programów nie jest tworzona, by wyrządzać użytkownikom poważne szkody (poza uniemożliwieniem im korzystania z przeglądarki), jednak należy mieć na uwadze, że mogą one przechwytywać dane, które przepływają przez naszą przeglądarkę - być może również te, na których poufności nam zależy.

4.2 KeRanger [9]

W ekosystemie Apple coraz częściej pojawiają się również doniesienia o zagrożeniach znacznie poważniejszych niż *adware*. Wykryty w marcu bieżącego roku *KeRanger* to pierwszy przykład w pełni funkcjonalnego *ransomware'u* na OS X. *Ransomware* to atak nie tylko groźniejszy, ale i bardziej skomplikowany niż *adware*. Skutki jego działań mogą być wyjątkowo nieprzyjemne - potencjalne ofiary narażone są na znaczne straty pieniężne lub utratę zawartości swoich dysków.

KeRanger był w rzeczywistości trojanem, a dostawał się na komputer ofiary wraz z instalatorem programu *Transmission* - klienta BitTorrent. Program ten posiadał certyfikat bezpieczeństwa, więc jego instalacja mogła przebiec z pominięciem wbudowanego zabezpieczenia OS X - Gatekeepera. Po instalacji wirus przesypiał kilka dni, po czym rozpoczynał szyfrowanie plików na dysku ofiary. Gdy skończył, informował ją o tym, że jej pliki są zaszyfrowane i przez to obecnie niedostępne. Opisywał również jedyny sposób, w jaki można było pliki odzyskać - należało zakupić narzędzie do rozszyfrowania od hakerów za 1 BTC (równowartość około 400$).

KeRanger posiadał dwie cechy, które doskonale obrazują, jak groźne potrafią być współczesne wirusy na OS X. Po pierwsze, jego instalacja przebiegała bez zaalarmowania użytkownika - równolegle z instalacją faktycznego oprogramowania, które użytkownik mógł rzeczywiście chcieć uruchomić, i to oszukując *Gatekeeper'a*. Po drugie, jego działania stwarzały poważne niebezpieczeństwo dla ofiar - 400$ okupu lub utrata zawartości swojego dysku. Należy również wspomnieć, że *KeRanger* to dopiero pierwszy wykryty przypadek funkcjonalnego *ransomware* na OS X, a kolejne mogą zostać jeszcze udoskonalone.

5 iOS

Pojawienie się na rynku mobilnych systemów operacyjnych (głównie Androida i iOS) stworzyło wiele nowych możliwości dla hakerów. Urządzenia działające pod ich kontrolą przechowują przecież ogromne ilości naszych danych. Prawie każdy posiada dziś smartfon, w którym przechowuje

listę swoich kontaktów, korespondencję, zdjęcia, i przez który łączy się z internetem podając swoje hasła do portali społecznościowych, banków itd. Sposób, w jaki korzystamy ze smartfonów, naturalnie czyni je niezwykle cennym łupem dla hakerów. Jak to więc możliwe, że iOS jest wciąż uważany przez wielu ludzi za bezpieczny i czy jego użytkownicy rzeczywiście nie muszą obawiać się infekcji?

Jest kilka powodów, przez które można sądzić, że ryzyko zakażenia systemu iOS jest niewielkie. Po pierwsze - podobnie jak w przypadku OS X - większość hakerów działa w celach czysto zarobkowych, zatem na cel wybierają oni najczęściej systemy z ogromnymi bazami użytkowników. Ponieważ to Android opanował znaczną większość (w 2016 roku aż 85%) rynku smartfonów [20], to właśnie on przyciągana najwięcej przestępców. Po drugie infrastruktura iOS jest dużo bardziej hermetyczna niż systemów desktopowych, a Apple zarezerwowało sobie m.in. prawo do kontrolowania zbioru aplikacji, które użytkownicy mogą uruchamiać na swoich urządzeniach. Domyślnie iOS dopuszcza jedynie instalowanie oprogramowania dostępnego w AppStore, a zanim aplikacja tam trafi musi pozytywnie przejść proces weryfikacji, w którym specjaliści mogą przyjrzeć się, czy program nie przemyca po cichu złośliwego kodu.

Z roku na rok przybywa jednak urządzeń z iOS'em, a wraz z nimi do ekosystemu Apple napływają i hakerzy tworzący malware. Oczywiście pozostaje im do sforsowania jeszcze kilka przeszkód, w tym proces weryfikacji AppStore, jednak mając odpowiednią motywację w postaci rosnącej bazy użytkowników, coraz usilniej poszukują oni luk w systemie i coraz częściej próbują przemycić wirusy zaszyte tak głęboko w aplikacjach, że ich nosiciele pozytywnie przechodzą proces weryfikacji. Pierwsze przypadki złośliwego oprogramowania atakujące urządzenia bez *jailbreaka* pojawiły się w 2014 roku. Przypadkowa infekcja nimi była jednak wysoce nieprawdopodobna, gdyż wymagała stosowania certyfikatów dla przedsiębiorstw, których większość użytkowników nie ma potrzeby używać [18]. Malware będący realnym zagrożeniem pojawił się stosunkowo niedawno, a poniższe przykłady obrazują współczesną skalę problemu.

5.1 XcodeGhost [10]

Pod koniec 2015 roku deweloperzy z Chin ujawnili istnienie złośliwej wersji oprogramowania Xcode służącego do tworzenia aplikacji na systemy iOS i OS X. Spreparowana wersja została umieszczona na jednym z chińskich portali i następnie pobrana przez niektórych deweloperów z tamtego kraju. Sama złośliwa wersja Xcode'a nie wpływała w żaden sposób na system dewelopera, jednak przy kompilacji stworzonych przy jej pomocy aplikacji wstrzykiwała malware do docelowej aplikacji tak, by wyglądał on jak normalne komponenty dostarczane przez Apple. W rezultacie, wiele z tych aplikacji pozytywnie przeszło proces weryfikacji i zostało dopuszczonych do obrotu w AppStore. Zainfekowane nimi urządzenia docelowe były wcielane do ogromnego botnetu, wysyłały do swojego Command And Control dane pozyskane z urządzeń i wyłudzały od użytkowników informacje np. poprzez phishing [17].

Jak donosi firma FireEye wykryto ponad 4000 zainfekowanych przy pomocy *XcodeGhost* aplikacji dostępnych w AppStore. [19]. Liczba użytkowników narażonych na działanie złośliwego kodu mogła być ogromna, głównie z powodu aplikacji takich jak *WeChat*, które cieszą się w Azji dużą popularnością. Przykład *XcodeGhost'a* pokazuje, że nawet proces weryfikacji, choć z pozoru zdolny do całkowitego wyeliminowania zagrożenia, nie jest niestety idealny i że bezpieczeństwo użytkowników systemu nie powinno zależeć wyłącznie od wewnętrznej "policji" AppStore.

5.2 Pegasus [11]

Zaledwie kilka miesięcy temu Ahmed Mansoor - aktywista działający na rzecz praw człowieka w Zjednoczonych Emiratach Arabskich - dostał na swój telefon wiadomość tekstową odsyła-

jącą go do strony internetowej rzekomo zawierającej dowody na nielegalne przetrzymywanie i torturowanie więźniów w Emiratach. Zamiast otworzyć otrzymany link, Mansoor przekazał go do grupy badawczej Citizen Lab. Po dokładnym przebadaniu specjalistom udało się ustalić, że gdyby otworzył on otrzymany link jego system zostałby zjailbreakowany, a na urządzeniu zostałoby zainstalowane niezwykle rozbudowane oprogramowanie szpiegujące.

Zdaniem firmy Lookout ten atak był najbardziej zaawansowanym ze wszystkich dotąd obserwowanych na iOS. *Pegasus* (taką nazwę otrzymał wirus) potrafił zjailbreakować iOS użytkownika bez jego interakcji dzięki wykorzystaniu aż trzech poważnych podatności systemu, z których nikt nie zdawał sobie sprawy (zero-day attack). Sam proces infekcji był prostą odmianą *phishingu*: ofiara otrzymywała link do podejrzanej strony wiadomością tekstową, otwierała go i ładowała stronę razem z wirusem, który następnie wykorzystywał podatności systemu, by dokonać jailbreaka i instalował oprogramowanie szpiegujące. Istotny jest fakt, że po załadowaniu strony proces przebiegał po cichu i niewidocznie - tak, by użytkownik nie zorientował się, że jego urządzenie zostało zainfekowane. Samo szpiegowanie mogło być natomiast dostosowane przez atakujących do potrzeb, jednak przeważnie obejmowało całą komunikację ofiary (w postaci wiadomości, połączeń, maili, komunikatorów), jej hasła i historię lokalizacji.

Wraz z wydaniem wersji iOS 9.3.5 Apple załatało wszystkie trzy podatności, które umożliwiały atakującym włamanie na urządzenia. Nie wiadomo jednak jak długo ten wirus krążył po sieci, ani jak wiele urządzeń zdołał zainfekować. Jego istnienie uświadomiło społeczności użytkowników iOS, że stworzenie naprawdę groźnego spyware'u, który infekuje urządzenie bez wiedzy użytkownika i wysyła jego poufne dane do hakerów, jest niestety możliwe i że być może nadszedł czas, by odstąpić od przekonania, że iOS jest odporny na malware.

6 Podsumowanie

W czasach słynnej kampanii *Get a Mac*, w której Apple chwaliło się odpornością swojego systemu na złośliwe oprogramowanie, sytuacja użytkowników OS X była dość komfortowa - w sieci czyhało na nich stosunkowo niewiele zagrożeń, a potencjalna infekcja mogła nastąpić praktycznie tylko w wypadku zupełnie nieodpowiedzialnego postępowania użytkownika. Nawet w przypadku zarażenia, szkody wyrządzane przez wirusy takie jak *Leap*, czy *RSPlug* były niewielkie i z reguły nie pociągały za sobą poważnych konsekwencji. Od tamtych lat minęło jednak naprawdę sporo czasu, a sytuacja zmieniła się diametralnie - tak, że nawet sam producent odstąpił od reklamowania swoich produktów odpornością na malware.

Również dzisiaj OS X posiada wbudowane mechanizmy obronne takie jak np. Gatekeeper czy XProtect, które prawdopodobnie czynią zabezpieczenie się przed zagrożeniem łatwiejsze niż w przypadku np. Windowsa. Jednak powstanie wirusów tak powszechnych jak *Flashback* i tak groźnych jak *KeRanger*, trwająca epidemia wszechobecnych instalatorów z adware'em i spyware'em, podatności takie jak *Rootpipe* i statystki alarmujące o niesamowicie szybkim wzroście obecności Macowego malware'u nie pozwalają już absolutnie twierdzić, że system OS X jest bezpieczny i odporny na złośliwe oprogramowanie. Dzięki zamkniętej architekturze trochę lepiej wygląda sytuacja systemu iOS, chociaż i tutaj nie jest bezpiecznie. Ostatnie doniesienie o atakach takich jak *XcodeGhost* i szczególnie groźny *Pegasus* pokazują, że wirusy wycelowane w iOS stają się z biegiem czasu coraz bardziej powszechne i zaawansowane, a przypadkowe zarażenie jednym z nich nie jest już fikcją, jak do roku 2014, tylko realnym zagrożeniem.

Niestety nie można liczyć na to, że kiedykolwiek z systemów OS X i iOS zostaną wyeliminowane wszystkie podatności, bo, jak twierdzą programiści, każdy software pisany przez ludzi obarczony jest różnego rodzaju lukami i błędami, których nieustannie poszukują hakerzy. Ponadto im lepszą pozycję na rynku zdobywa Apple i jego produkty, tym więcej przestępców przyciąga do swojego ekosystemu. Możemy zatem przypuszczać, że w kolejnych latach czeka

nas tylko dalsza eskalacja wystarczająco poważnego już problemu.

Literatura

[1] April Adams. *How Infected Are We?*. TopTenReviews, 2014. http://www.toptenreviews.com/software/security/best-antivirus-software/how-infected-are-we.html

[2] *Get a Mac*. Wikipedia. https://en.wikipedia.org/wiki/Get_a_Mac

[3] Graham Cluley. *10 years of Mac OS X malware*. We Live Security, 2014. http://www.welivesecurity.com/2014/04/10/10-years-of-mac-os-x-malware/

[4] Graham Cluley. *History of Mac malware: 1982 – 2011*. Naked Security, 2011. https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/#2011

[5] Graham Cluley. *Mac OS X RSPlug Trojan horse: in pictures*. Naked Security, 2007. https://nakedsecurity.sophos.com/2007/11/01/mac-os-x-rsplug-trojan-horse-in-pictures/

[6] Broderick Ian Aquilino. *Flashback OS X Malware*. F-Secure Corporation, 2012. https://www.f-secure.com/weblog/archives/Aquilino-VB2012.pdf

[7] Magnus Aschan. *Swedish hacker finds 'serious' vulnerability in OS X Yosemite*. Macworld, 2014. http://www.macworld.com/article/2841965/swedish-hacker-finds-serious-vulnerability-in-os-x-yosemite.html

[8] Lowell Heddings. *Mac OS X Isn't Safe Anymore: The Crapware / Malware Epidemic Has Begun*. How-To Geek, 2015. http://www.howtogeek.com/210589/mac-os-x-isnŹt-safe-anymore-the-crapware-malware-epidemic-has-begun/

[9] Claud Xiao, Jin Chen. *New OS X Ransomware KeRanger Infected Transmission BitTorrent Client Installer*. Palo Alto Networks, 2016. http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

[10] Paul Ducklin. *Apple's App Store hit by the XCodeGhost of malware present*. Naked Security, 2015. https://nakedsecurity.sophos.com/2015/09/22/apples-app-store-hit-by-the-xcodeghost-of-malware-present/

[11] Max Bazaliy, Michael Flossman, Andrew Blaich, Seth Hardy, Kristy Edwards, Mike Murray. *Technical Analysis of Pegasus Spyware*. Lookout, 2016. https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

[12] *2015: The Most Prolific Year In History For OS X Malware*. Bit9 + Carbon Black, 2015. https://assets.documentcloud.org/documents/2459197/bit9-carbon-black-threat-research-report-2015.pdf

[13] Andrew Welch. *New MacOS X trojan/virus alert*. Abrosia Software Inc., 2006. http://www.ambrosiasw.com/forums/index.php?showtopic=102379

[14] Peter James. *Mac Flashback Trojan Horse Masquerades as Flash Player Installer Package*. The Mac Security Blog, 2011. https://www.intego.com/mac-security-blog/intego-security-memo-september-26-2011-mac-flashback-trojan-horse-masquerades-as-flash-p

[15] *Doctor Web exposes 550 000 strong Mac botnet*. Dr. Web, 2012. http://news.drweb.com/show/?i=2341&lng=en&c=14

[16] Chloe Albanesius. *Kaspersky Confirms Widespread Mac Infections Via Flashback Trojan.* PCMag, 2012. http://www.pcmag.com/article2/0,2817,2402715,00.asp

[17] Joe Rossignol. *What You Need to Know About iOS Malware XcodeGhost.* MacRumors, 2015. http://www.macrumors.com/2015/09/20/xcodeghost-chinese-malware-faq/

[18] Claud Xiao. *YiSpecter: First iOS Malware That Attacks Non-jailbroken Apple iOS Devices by Abusing Private APIs.* Palo Alto Networks, 2015. http://researchcenter.paloaltonetworks.com/2015/10/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis/

[19] *Protecting Our Customers From XcodeGhost.* FireEye, 2015. https://www.fireeye.com/blog/executive-perspective/2015/09/protecting_our_custo.html

[20] *Smartphone OS Market Share.* IDC, 2016. http://www.idc.com/prodserv/smartphone-os-market-share.jsp