Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Czym jest złośliwe oprogramowanie

Wstęp

Z całą pewnością słyszałeś o wirusach, robakach internetowych, trojanach i podobnych zagrożeniach. Tego rodzaju oprogramowanie jest używane przez przestępców do infekowania i przejmowania kontroli nad komputerami i urządzeniami mobilnymi. Dziś wszystkie te rodzaje określa się jedną nazwą - złośliwe oprogramowanie, lub z ang. malware. W tym wydaniu biuletynu wyjaśnimy, czym jest malware, kto i dlaczego tworzy tego rodzaju oprogramowanie oraz co możesz zrobić, aby uchronić się przed infekcją.

Redaktor gościnny

Lenny Zeltser zajmuje się zabezpieczeniami IT w firmie NCR Corp. oraz prowadzi wykłady poświęcone walce ze złośliwym oprogramowaniem w Instytucie SANS. Jest aktywnym użytkownikiem Twittera (**@lennyzeltser**) oraz prowadzi blog poświęcony bezpieczeństwu, **blog.zeltser.com**.

Czym jest złośliwe oprogramowanie

W uproszczeniu złośliwe oprogramowanie zwane też malware, to program komputerowy napisany specjalnie w celu wykonywania szkodliwych działań. Termin malware pochodzi z j. angielskiego ze złożenia dwóch słów: malicious (złośliwe) oraz software (oprogramowanie). To co chcą osiągnąć przestępcy wykorzystujący złośliwe oprogramowanie to instalacja go na Twoich urządzeniach mobilnych i komputerach. Gdy już to im się uda, mogą przejąć nad nimi całkowitą kontrolę. Wiele osób tkwi w błędzie uważając, że problem złośliwego oprogramowania dotyczy tylko komputerów z systemami Windows. W związku z tym, że system Windows jest jednym z najbardziej rozpowszechnionych, stał się także najpopularniejszym celem ataków. Należy jednak pamiętać, że malware może zaatakować dowolne urządzenie, a odsetek infekcji na urządzeniach przenośnych takich jak smartfony i tablety ciągle rośnie. Pamiętaj, że każdy jest potencjalnym celem. Im więcej urządzeń zostanie zainfekowanych, tym więcej są w stanie zarobić przestępcy, których w większości przypadków nie obchodzi, kto padnie ich ofiarą.

Kto i dlaczego tworzy złośliwe oprogramowanie

Złośliwe oprogramowanie nie jest już tworzone przez hobbystów, czy domorosłych hackerów, ale przez doświadczone zespoły programistów działających na zlecenie grup przestępczych, które mają określone cele. Są nimi kradzież poufnych informacji, gromadzenie danych o loginach i hasłach, wysyłanie SPAMu, ataki typu DDoS, wymuszanie oraz kradzież tożsamości i danych osobowych. Jednym z przykładów takiego oprogramowania jest Cryptolocker, którego celem jest zaszyfrowanie wszystkich danych na dysku twardym komputera, a następnie żądanie okupu za ich odtworzenie.

Ludźmi, którzy tworzą, rozpowszechniają i zyskują na złośliwym oprogramowaniu mogą być pojedyncze jednostki działające na własną rękę, zorganizowane grupy przestępcze lub nawet organizacje rządowe. Dodatkowo, tak jak wspomnieliśmy wcześniej, tworzeniem nowoczesnego złośliwego oprogramowania

Czym jest złośliwe oprogramowanie

zajmują się zespoły programistów specjalnie zatrudniane do tego celu. Oferują one nawet usługi swoim "klientom" polegające na utrzymaniu i serwisowaniu oprogramowania, które wytworzą. Przestępcy, po nabyciu takiego "produktu" starają się zainfekować nim jak największą liczbę komputerów, tworząc botnety, które później wykorzystują do zarabiania pieniędzy. Zainfekowane komputery połączone w botnet, to armia, która może być wykorzystana do najróżniejszych celów, odsprzedana albo wynajęta innym grupom przestępczym.

Najlepszą ochronę przed złośliwym oprogramowaniem zapewni zaktualizowane oprogramowanie, program antywirusowy z aktualną bazą sygnatur oraz czujność.

Jak się chronić

Typowym krokiem w celu ochrony jest zainstalowanie oprogramowania antywirusowego od jednego z zaufanych dostawców. Antywirus ma za zadanie w porę wykryć i zatrzymać infekcję. Jednakże antywirusy nie są panaceum i nie zatrzymają ani nie usuną wszystkich rodzajów złośliwego oprogramowania. Przestępcy starają się ciągle je ulepszać i wyposażać w coraz bardziej wyrafinowany zestaw ataków, który omija antywirusowe zabezpieczenia.Twórcy antywirusów odpowiadają na takie działania, również starając się ulepszać swoje produkty. Prowadzi to do swoistego wyścigu zbrojeń, w którym niestety przestępcy coraz częściej są górą. W związku z tym pamiętaj, że antywirus wykryje i usunie większość złośliwego oprogramowania, ale nowsze wersje mogą nie zostać przez niego usunięte. Dlatego nie można polegać wyłącznie na antywirusie, należy podjąć dodatkowe kroki aby się chronić.

Po pierwsze upewnij się, że system operacyjny oraz aplikacje mają włączone automatyczne aktualizacje. Im bardziej aktualne oprogramowanie, tym trudniej przestępcom uzyskać dostęp do Twojego komputera lub urządzenia przenośnego poprzez wykorzystanie w nim podatności.

Po drugie, pamiętaj, że jesteś najlepszym zabezpieczeniem przed złośliwym oprogramowaniem, jakie może mieć Twój komputer. Przestępcy często wykorzystują inżynierię społeczną, czyli mówiąc prosto, chcą Cię oszukać i nakłonić, abyś sam zainstalował wirusa na swoim komputerze. Typowym przykładem są ataki phishingowe. Wykorzystują one korespondencję elektroniczną, która jest próbą podszycia się pod zaufaną instytucję, np. bank, urząd lub usługodawcę. Taki fałszywy email może nakłaniać do kliknięcia w odnośnik, który zamiast na stronę banku prowadzi na stronę WWW, która będzie próbowała zainfekować Twój komputer. Innym przykładem może być email od firmy kurierskiej z załącznikiem, np. fakturą, która po otwarciu zainstaluje niechciane oprogramowanie.

Inżynieria społeczna to nie tylko ataki z wykorzystaniem poczty elektronicznej. Możliwe jest, że przestępcy wykorzystają także inne technologie, np. zwykły telefon. Przestępca może do Ciebie zadzwonić i podszyć się pod pracownika linii wsparcia, np. firmy Microsoft. Będzie usiłował przekonać Cię, że Twój

Czym jest złośliwe oprogramowanie

komputer jest zainfekowany, co jest oczywiście kłamstwem. Kolejnym krokiem w oszustwie będzie przekonanie Cię do udostępnienia Twojego komputera w celu sprawdzenia lub kupna i zainstalowania oprogramowania, które rzekomo usunie wirusa. W rzeczywistości to ono właśnie jest jakimś rodzajem złośliwego oprogramowania. Zachowaj zdrowy rozsądek. Jeśli email lub rozmowa telefoniczna brzmi dziwnie, podejrzanie lub obiecuje "gruszki na wierzbie", to najprawdopodobniej jest próbą oszustwa.

Ostatecznie najlepszą ochroną przed złośliwym oprogramowaniem pozostaje utrzymywanie aktualnego systemu operacyjnego i wszystkich zainstalowanych aplikacji oraz posiadanie programu antywirusowego zaufanego producenta z aktualną bazą sygnatur. Bądź zawsze czujny i nie daj się namówić na zainfekowanie własnego komputera.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Źródła

OUCH Email i ataki phishingowe:

www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

OUCH Bezpieczny komputer w siedmiu krokach:

www.securingthehuman.org/resources/newsletters/ouch/2012#december2012

Plakat "Jesteś na celowniku":

http://www.securingthehuman.org/resources/posters

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz