Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- Czym jest złośliwe oprogramowanie
- Kto tworzy złośliwe oprogramowanie
- Jak się chronić

Czym jest złośliwe oprogramowanie

Wstęp

Z całą pewnością słyszałeś o wirusach, robakach internetowych, trojanach, oprogramowaniu szyfrującym 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 najważniejsze: 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). Przestępcy starają się zainstalować złośliwe oprogramowanie na Twoim komputerze, aby przejąć nad nim kontrolę oraz uzyskać dostęp do potrzebnych im danych. Gdy już im się to uda, mogą szpiegować Twoją aktywność w Internecie, kraść hasła lub prywatne pliki a także użyć Twojego systemu do ataku na inne osoby. Złośliwe oprogramowanie potrafi nawet uniemożliwić Ci dostęp do Twoich własnych plików, doprowadzając do tego, że będziesz musiał zapłacić przestępcy za odzyskanie kontroli nad własnymi danymi.

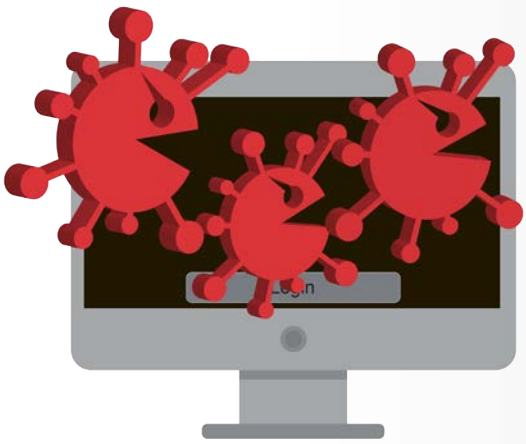
Wiele osób tkwi w błędzie uważając, że problem złośliwego oprogramowania dotyczy tylko komputerów z systemami Windows. W związku z tym, że system Windows jest jednym z najbardziej rozpowszechnionych, stał się także najpopularniejszym celem ataków. Należy jednak pamiętać, że malware może zaatakować dowolne urządzenie, a odsetek infekcji na urządzeniach przenośnych takich jak smartfony i tablety ciągle rośnie. Pamiętaj, że 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 działające na zlecenie grup przestępczych, mających 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. Ludźmi, którzy tworzą, rozpowszechniają i zyskują na złośliwym oprogramowaniu mogą

Czym jest złośliwe oprogramowanie

być pojedyncze jednostki działające na własną rękę, zorganizowane grupy przestępcze lub nawet organizacje rządowe. Dodatkowo, tak jak wspomnieliśmy wcześniej, tworzeniem nowoczesnego złośliwego oprogramowania zajmują się zespoły programistów specjalnie zatrudniane do tego celu. Oferują one nawet usługi swoim "klientom" polegające na utrzymaniu i serwisowaniu oprogramowania, które wytworzą.



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 swoje programy 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. Dlatego nie można polegać wyłącznie na antywirusie, należy podjąć dodatkowe kroki aby się chronić:

- Przestępcy bardzo często infekują komputery oraz urządzenia mobilne wykorzystując podatności w zainstalowanych na nich aplikacjach. Im nowsza wersja używanego oprogramowania, tym mniejsza szansa na istnienie podatności a tym samym mniejsze możliwości przejęcia systemu przez cyberprzestępców. Pamiętaj, aby zadbać o to, by Twój system operacyjny oraz zainstalowane na nim aplikacje były zawsze aktualne. Najlepiej jeśli od razu włączysz automatyczne aktualizacje.
- Popularnym ostatnio sposobem infekcji urządzeń mobilnych, stało się tworzenie przez przestępców fałszywych aplikacji, rozpowszechnianie ich w Internecie i zachęcanie ludzi do ściągnięcia i zainstalowania ich. Pamiętaj, żeby zawsze pobierać programy z zaufanych źródeł! Jeżeli ściągasz aplikacje mobilne, warto sprawdzić datę ich publikacji oraz upewnić się, że zostały pobrane przez dużą liczbę użytkowników i posiadają pozytywne oceny.
- Korzystając z komputera, staraj się używać konta z ograniczonymi uprawnieniami. Nie korzystaj z kont nie posiadających ograniczeń czyli najczęściej "Administratora" albo "roota". Wprowadza to dodatkową ochronę, ograniczając złośliwemu oprogramowaniu możliwość zainstalowania się samemu.
- Często wykorzystywanym sposobem ataku jest także próba przekonania Cię do zainstalowania złośliwego oprogramowania własnoręcznie. Do tegu celu przestępcy wykorzystują 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. Jeżeli wiadomość wygląda podejrzanie, jest zbyt piękna aby mogła być prawdziwa,

Czym jest złośliwe oprogramowanie

dotyczy przesyłek, których nie zamiawiałeś to mogłeś paść ofiarą ataku. Bądź uważny! Zdrowy rozsądek jest Twoją najlepszą formą obrony.

- Staraj się regularnie wykonywać kopie zapasowe swoich plików. Najlepsze do tego celu będa zewnętrzne serwery lub nośniki danych, które pracują w trybie offline. Pozwoli to chronić Twoje dane w sytuacji gdy padniesz ofiarą oprogramowania szyfrującego (ransomware). Kopie zapasowe są wtedy niezbędne i mogą stać się jedynym sposobem na odzyskanie utraconych w drodze infekcji plików.

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 namówić się 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

Phishing i oszustwa w e-mailach:	https://securingthehuman.sans.org/ouch/2015#december2015
Socjotechnika:	https://securingthehuman.sans.org/ouch/2014#november2014
Bezpieczne aplikacje mobilne:	https://securingthehuman.sans.org/ouch/2015#january2015
Zabezpiecz swój nowy tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Backup i odzyskiwanie danych:	https://securingthehuman.sans.org/ouch/2015#august2015

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Paweł Jacewicz, Małgorzata Dębska, Przemysław Zielony