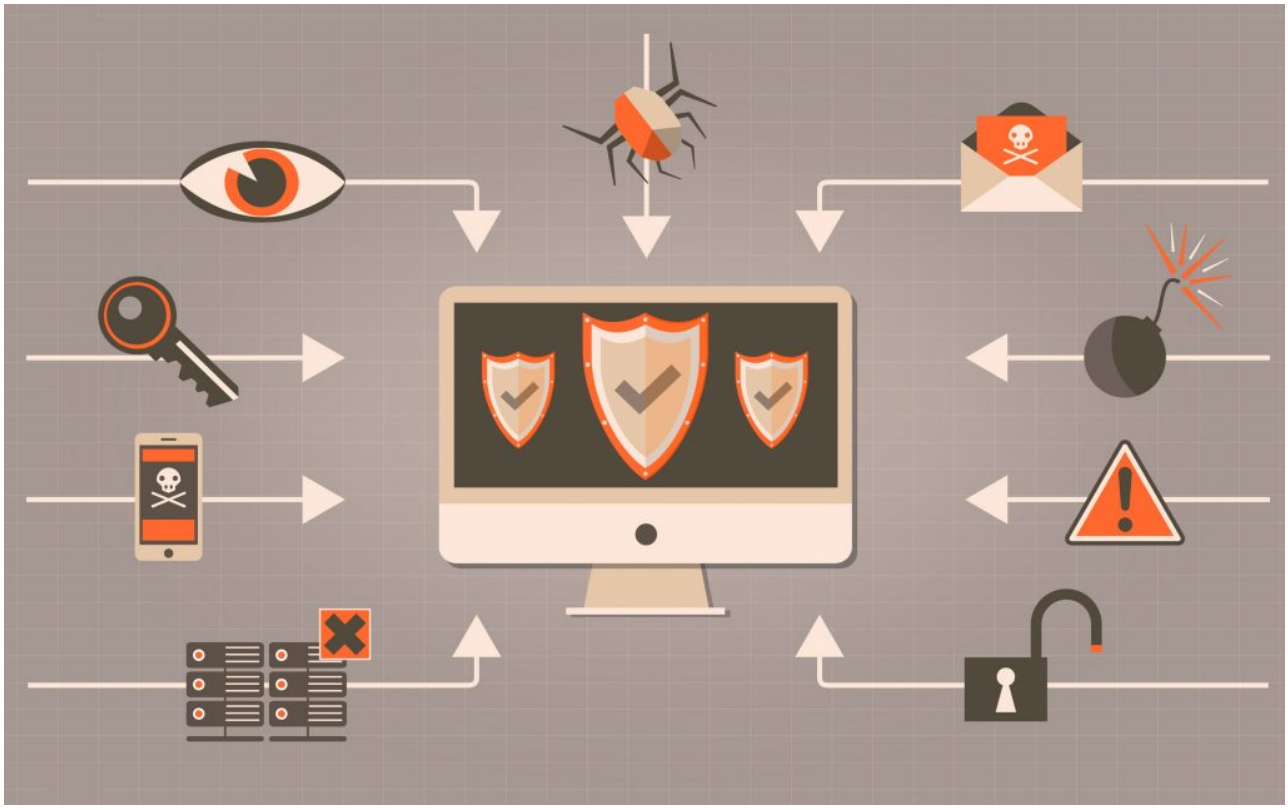
Oprogramowanie złośliwe, szkodliwe, malware…. Czyli wracamy do Was z naszą autorską serią Cyber Poradnik i dziś piszemy o najczęściej stosowanych metodach przeprowadzania ataków cybernetycznych.

Nawet nie wiecie jak razem z całą ekipą S.M.S. tęskniliśmy za tą serią. Dlatego postanowiliśmy wrócić i znów popularyzować wiedzę na temat cyberbezpieczeństwa. Chcemy dalej mieć swój wkład w rozwój społeczeństwa cyfrowego, które jest świadome zagrożeń i nie boi się korzystać z nowych technologii. Więc wszystkie ręce na pokład i ze zdwojonymi siłami powracamy z naszym ukochanym Cyber Poradnikiem.

Ostatnim razem pisaliśmy o najprostszych metodach oszustw w Internecie – czyli oddziaływaniu na podświadomość ludzką za pomocą socjotechniki. Wtedy też obiecaliśmy, że w ramach Cyber Poradnika pojawi się wpis taki jak ten. Dotrzymujemy więc słowa i tym numerem postanowiliśmy nieco skomplikować oraz wrzucić Was na trochę głębszą wodę. Jednocześnie obiecujemy, że po dzisiejszej lekturze nie będziecie mieli najmniejszych problemów z tym tematem. Mianowicie dziś chcemy przybliżyć Wam kwestie związane z oprogramowaniem złośliwym.

Co to jest oprogramowanie złośliwe?



Najczęściej cyberatak dokonywany jest poprzez zastosowanie wektora ataku, za pośrednictwem którego cyberprzestępca ma możliwość uzyskania dostępu do danych uwierzytelniających bądź do komputera lub serwera sieciowego w celu realizacji działalności przestępczej. W głównej mierze rolę wektora ataku pełnią urządzenia USB, załączniki do poczty elektronicznej, strony internetowe, okna dialogowe, komunikatory, itd.

Do najczęściej stosowanych metod ataku można zaliczyć instalację złośliwego oprogramowania, częściej określanym mianem malware. Termin ten to zbitek wyrazowy angielskich słów malicious (złośliwy) i software (oprogramowanie). Malware można określić jako oprogramowanie, którego celem jest uzyskanie dostępu i przejęcie kontroli nad urządzeniem cyfrowym w celach przestępczych. Dokonywane jest zazwyczaj w celu kradzieży danych uwierzytelniających, pieniędzy lub rozpowszechnienia oprogramowania na inne komputery.

Do oprogramowania złośliwego zaliczyć można wirusy komputerowe (najczęściej robaki komputerowe i konie trojańskie), programy szpiegujące, adware (oprogramowanie reklamowe), scareware (oprogramowanie zastraszające; czasem określane jako rougeware, czyli oprogramowanie fałszywe), ransomware oraz inne.

Kto i po co tworzy malware?

Obecnie najczęściej stworzenia oprogramowania złośliwego podejmują się wyspecjalizowane grupy bądź zespoły programistów. Coraz rzadziej spotkamy się z tym, aby malware został przygotowany przez laika lub pierwszego lepszego programistę. Cyberprzestępcy tworzący oprogramowanie tego typu mają ściśle określone cele. Przede wszystkim skoncentrowani są na kradzieży danych – zarówno tych poufnych jak i osobowych, które w dzisiejszych czasach są jednym z najbardziej cenionych produktów na (również czarnym) rynku. Poprawnie zainstalowany malware może umożliwić również gromadzenie danych dostępowych takich jak loginy i hasła, wysyłanie spamu, przeprowadzanie ataków DDoS czy kradzież tożsamości.

Jak się bronić przed atakami?

Pierwszą linią ochrony przed oprogramowaniem złośliwym może stać się instalacja oprogramowania antywirusowego pochodzącego z zaufanego źródła od jednego z renomowanych dostawców tego typu rozwiązań. Antywirus może w porę zatrzymać rozprzestrzenianie się malware'u na naszym urządzeniu oraz skutecznie je usunąć. Jednak umówmy się – program antywirusowy nie jest metodą pozwalającą nam na 100% pewności co do zabezpieczeń naszego systemu. Oczywiście będzie w stanie powstrzymać część oprogramowania złośliwego, ale nie będzie on „lekarstwem" na wszystko. Mimo, że antywirusy są ulepszane na każdym kroku, to również cyberprzestępcy starają się ulepszać swój malware w taki sposób, aby omijać powstałe zabezpieczenia. Dodatkowo większość programów antywirusowych ma jeden poważny mankament nie sprawdza pliku a jego sumę kontrolną (czyli liczby uzyskanej za pomocą specjalnego algorytmu, która ma zapewnić integralność danych). Znaczy to, ze wystarczy czasem zmienić nazwę pliku, aby jego suma kontrolna została zmieniona. Przez taki zabieg antywirus nie rozpoznaje już danego pliku jako niezaufany. Często cyberprzestępcy

przed np. wysłaniem każdego maila phishingowego starają się obejść zabezpieczenia zmieniając złośliwy plik w ten sposób, aby miał inną sumę kontrolną. Dlatego oprócz instalacji odpowiedniego programu antywirusowego zalecamy również podjęcie dodatkowych środków ochrony:

- Przede wszystkim zwróć uwagę czy robisz regularne aktualizacje systemu oraz programatorów/aplikacji, które masz zainstalowane na swoim urządzeniu. Przestępcy, którzy starają się zainfekować użytkownika oprogramowaniem malware najczęściej wykorzystują podatności i luki w zabezpieczeniach, które mogą zostać wykryte podczas korzystania z danego programu. Regularne aktualizacje pozwalają na doinstalowywanie wszelkich najnowszych poprawek od producenta i mogą dać ci pewność, że nie zostaniesz zaatakowany za pośrednictwem tego wektora ataku.
- Kolejna rada jest prosta – włącz myślenie, bądź nieufny i rób research . Instaluj aplikacje i programy pochodzące wyłącznie z pewnych źródeł. Nie sugeruj się kolorowymi, zachęcającymi do instalacji reklamami, ale rób własny rekonesans. Sprawdzaj opinie o danym produkcie, czytaj komentarze innych użytkowników na jego temat, dowiedz się, czy twórca danej aplikacji jest zaufany. Ta sama porada tyczy się przeglądania stron www – odwiedzaj tylko te, które mają aktualne certyfikaty SSL, nie zarzucają Cię milionem wyskakujących okienek reklamowych oraz są pewne.
- Na pewno pamiętasz, że kiedy pisaliśmy o phishingu wspominaliśmy o przesyłaniu fałszywych maili i plików za pośrednictwem poczty elektronicznej. Jest to kolejny popularny wektor ataku przestępców chcących zainfekować Cię malware. Przesyłając Ci fałszywy mail oraz nakłaniając do ściągnięcia załączonego do niego pliku, zachęcają Cię do samodzielnej instalacji oprogramowania złośliwego na twoim urządzeniu. Poprzez ściągnięcie podejrzanego pliku dochodzi do zainfekowania Twojego urządzenia. Dlatego znów powtarzamy – uważaj na to co ściągasz oraz sprawdzaj czy możesz zaufać nadawcy wiadomości.
- Może zdarzyć się tak, ze padniesz ofiarą oprogramowania szyfrującego jak np. ransomware (o którym więcej opowiemy w kolejnym numerze Cyber Poradnika). Wtedy możesz utracić dostęp zarówno do swojego urządzenia jak i danych na nich zawartych. Dlatego w takim przypadku jedyną deską ratunku będzie kopia zapasowa, którą wykonałeś wcześniej (bo jesteśmy pewni, że jako świadomy użytkownik i nasz czytelnik na pewno regularnie robisz kopie, prawda?). Dzięki zachowaniu kopii swoich plików masz szansę na odzyskanie chociaż części straconych danych oraz możesz mieć możliwość odtworzenia tego, do czego utraciłeś dostęp.

Malware brzmi groźnie, ale zdecydowanie nie zachęcamy Cię do strachu przed nim. Dzięki odpowiednim metodom zabezpieczania siebie i swoich danych, mądrym decyzjom, które

podejmujesz w Internecie oraz odpowiedniej wiedzy możesz mieć pewność, że nie dasz się nabrać na sztuczki cyberprzestępców i nie zostaniesz ofiarą malware.

Po lekturze Cyber Poradnika wpadnij na nasze profile w mediach społecznościowych (Facebook oraz Twitter) , gdzie możemy dalej podyskutować na temat bezpieczeństwa w sieci.

Czytałeś już nasze wcześniejsze numery **Cyber Poradnika**? Jeśli nie to serdecznie zachęcamy Cię do ich lektury i podnoszenia świadomości nt. cyberbezpieczeństwa.

Cyber Poradnik nr 1 – Bezpieczne zakupy

Cyber Poradnik nr 2 – Co zrobić, gdy padniesz ofiarą cyberprzestępcy?

Cyber Poradnik nr 3 – Phishing

Cyber Poradnik nr 4 – Użytkownik w podróży

Cyber Poradnik nr 5 – Socjotechnika w cyberatakach – co powinieneś wiedzieć i jak się przed nią bronić?