Bitdefender

Złośliwe oprogramowanie – najgroźniejsze rodzaje

06.06.2023

Eksperci do spraw cyberbezpieczeństwa z firmy Bitdefender od wielu lat ostrzegają internautów, że złośliwe oprogramowanie jest niebezpieczne nie tylko dla firm i instytucji publicznych, lecz także dla zwykłych użytkowników sieci. Coraz częściej możemy się spotkać z kampaniami hakerskimi, które są skierowane właśnie przeciwko osobom prywatnym. Pomimo tego, że historia wirusów oraz złośliwego oprogramowania ma już kilkadziesiąt lat i przez ten czas bardzo się rozwinęły, to ich najniebezpieczniejsze typy pozostają takie same. Dlatego w tym artykule przedstawimy przykłady najgroźniejszych rodzajów złośliwego oprogramowania oraz sposoby obrony przed nimi.

Typy złośliwego oprogramowania

Złośliwe oprogramowanie możemy klasyfikować na podstawie wielu czynników, takich jak sposób rozprzestrzeniania się, sposób działania i skutków, które wywołuje na urządzeniach ofiary. Poniżej wymieniamy najpopularniejsze typy złośliwego oprogramowania, na jakie może się

natknąć użytkownik sieci.

Ransomware

Nasze zestawienie rozpoczniemy od najprawdopodobniej najbardziej medialnego zagrożenia, jakim jest ransomware. Zasada działania tego złośliwego oprogramowania polega na tym, że po zainfekowaniu systemu szyfruje dane ofiary i nadaje komunikat, który głosi, iż użytkownik otrzyma dostęp do swoich danych po tym, jak zapłaci odpowiedni okup.

Ransomware jest najczęściej rozprzestrzeniane za pomocą kampanii phishingowych. Hakerzy przygotowują fałszywe maile, w których podszywają się pod banki, ZUS i inne instytucje rządowe i zachęcają użytkowników sieci do kliknięcia w niebezpieczny link lub załączają do wiadomości zainfekowany plik. Gdy internauta otworzy plik, następuje jego detonacja i zainfekowanie systemu. Ransomware jest uważany za jeden z najgroźniejszych programów, ponieważ odkodowanie zaszyfrowanych danych bez pomocy deszyfratora jest praktycznie niemożliwe.

Oprogramowanie szpiegujące – spyware

Oprogramowanie szpiegujące spyware uchodzi za bardzo groźne, ponieważ bardzo trudno je wykryć i usunąć. Jego podstawowym zadaniem jest infiltracja środowiska użytkownika, kradzież cennych danych i przekazanie ich niepowołanym osobom trzecim. Spyware to bardzo uniwersalne oprogramowanie. Jego różne warianty mogą działać

praktycznie na wszystkich urządzeniach, które mają stałe połączenie z siecią. Za ich pomocą hakerzy mogą zbierać niezwykle cenne dane, takie jak aktywność ofiary w sieci i informacje o tym, jakie klawisze wciskał użytkownik komputera. Dzięki tym danym hakerzy mogą w bardzo prosty sposób odkryć wszystkie loginy i hasła swojej ofiary.

Wśród spyware możemy rozróżnić trzy najpopularniejsze typy. Pierwszym są trojany, czyli złośliwe oprogramowanie, które najczęściej „podszywa się" pod inne pliki, a następnie infekuje system użytkownika. Przez cały okres swego działania umożliwia hakerom zdalne kontrolowanie komputera ofiary. Trojany niezwykle trudno wykryć i tylko skuteczny antywirus jest w stanie usunąć je z urządzenia, które zostało nim zainfekowane.

Kolejnym typem oprogramowania szpiegującego są keyloggery. Monitory systemu to narzędzia, które pozwalają hakerom na śledzenie aktywności swojej ofiary. Za pomocą keyloggerów mogą oni poznać historię przeglądarki użytkownika, którego obserwują, czytać jego wiadomości mailowe i konwersacje na czatach, a także monitorować ciągi klawiszy, które wcisnął podczas korzystania z urządzenia.

Kolejnym niezwykle popularnym typem oprogramowania szpiegującego są infostealery, których podstawowym zadaniem jest kradzież danych z dysku ofiary i przesyłanie ich cyberprzestępcom. Za pomocą infostealerów hakerzy najczęściej starają się zdobyć informacje na temat wykonywanych płatności online śledzonego użytkownika. Infostealery są jednym z najgroźniejszych typów złośliwego oprogramowania, ponieważ na skutek ich działania ofiary mogą stracić

nie tylko cenne dane, lecz także swoje środki materialne.

Robaki - worms

Robaki to specyficzny rodzaj złośliwego oprogramowania, który charakteryzuje się tym, że bardzo szybko infekuje sieci i „przeskakuje" z jednego komputera na drugi. Co ciekawe, zainfekowanie systemu robakami nie skutkuje jakimiś wielkimi wyciekami lub utratą danych, lecz bardzo negatywnie wpływa na wydajność maszyn – do tego stopnia, że jakakolwiek praca na nich jest niemożliwa. W wypadku zainfekowania komputera przez robaki jedyną szansą na powrót do „normalnej" pracy komputera jest przeskanowanie go za pomocą skutecznego antywirusa.

Jak uniknąć złośliwego oprogramowania?

„Najważniejszym elementem ochrony przed złośliwym oprogramowaniem jest przestrzeganie podstawowych zasad cyberbezpieczeństwa. Użytkownicy sieci powinni zawsze korzystać ze skutecznego systemu antywirusowego, a także unikać otwierania wszelkiego rodzaju podejrzanych linków. Warto także wyposażyć się w zaporę firewall oraz dostęp do prywatnej sieci VPN" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/zlosliwe-oprogramowanie-najgrozniejsze-rodzaje/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy

Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 06.06.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.