Statystyki zagrożeń w pierwszej połowie 2018 roku, sporo niebezpiecznych

W obecnych czasach w większości przypadków złośliwe oprogramowanie rozprzestrzenia się w sieci pliki wykonywalne stają się coraz mniej powszechnym problemem. Już w pierwszej połowie roku eksperci ds. zabezpieczeń firmy G DATA zauważyli specyficzną tendencję zagrożeń, które mogłyby okazać się niebezpieczne dla urządzeń. Podobnie jak ma to miejsce w kontekście przemysłu IT, rozwój obecnie występujących grup złośliwego oprogramowania podlega znacznym zmianom. Pokazują to najnowsze analizy laboratorium zabezpieczeń G DATA SecurityLabs: dziewięć na dziesięć najszerzej rozpowszechnionych zagrożeń czyhających na użytkowników komputerów w poprzednich latach nie znalazło się w pierwszej połowie 2018 roku w grupie dziesięciu najczęściej wykrywanych zagrożeń. 70% z nich stanowią oprogramowania PUP, a 30% - malware. Poza tym, ataki coraz częściej są przeprowadzane za pośrednictwem stron internetowych, a nie jak to miało miejsce w przeszłości, wyłącznie poprzez pliki wykonywalne.

- Zgodnie z tradycyjnym podejściem, złośliwe oprogramowanie rozprzestrzenia się głównie za pośrednictwem plików wykonywalnych. Obserwujemy jednak wyraźny wzrost liczby ataków przeprowadzanych za pośrednictwem stron internetowych, a niektóre z nich w ogóle nie wykorzystują plików mówi Ralf Benzmüller, Główny Przedstawiciel G DATA Security Labs Ataki za pośrednictwem makr w dokumentach biurowych również są powszechne i skłaniają użytkowników do interakcji. Najkrótszy w historii cykl rozwoju złośliwego oprogramowania pokazuje, że użytkownicy zyskają kompletną ochronę wyłącznie dzięki proaktywnym technologiom od G DATA Security Labs.

Przedstawione dane liczbowe oparte są na statystykach zebranych przez G DATA Security Labs. Informacje zbiera inicjatywa informowania o złośliwym oprogramowaniu Malware Information Initiative (MII), w ramach której klienci G DATA mogą dobrowolnie przesyłać do firmy dane statystyczne na temat zidentyfikowanych oraz udaremnionych zagrożeń, co umożliwia przeprowadzenie dokładniejszej analizy bieżących próbek pod kątem obecnie panujących zagrożeń.

Rok 2018 do tej pory pod znakiem Cryptojackingu

Cryptojacking tajemnicze kopanie kryptowalut, z reguły Monero zyskał szczególne znaczenie w pierwszej połowie roku. Zwłaszcza w pierwszym kwartale, na wielu stronach internetowych ukrywano Cryptominer pobierający skrypty na komputer użytkownika i prowadzący do przeciążenia procesora. Jednak w niektórych przypadkach funkcje kopania walut można odkryć także w takich plikach wykonywalnych, jak gra Abstractionism dostarczana za pośrednictwem platformy Steam.

Nie zawsze pozostaje jasne, czy użytkownicy wyrazili wcześniej zgodę na tego typu działanie. Z tego powodu G DATA klasyfikuje kopanie kryptowalut po części jako złośliwe oprogramowanie w przypadku, gdy działaniu jednoznacznie przyświecają niecne zamiary a w niektórych przypadkach jako Potencjalnie Niechciany Program (PUP). Trzy narzędzia do kopania krypto walut znajdują się pośród dziesięciu najpowszechniejszych zagrożeń w formie złośliwego oprogramowania, a aż cztery takie narzędzia pośród dziesięciu najczęściej wykrywanych PUPów. Nowością jest to, iż Web Assembly w postaci kodu bajtowego jest wykorzystywany nie tylko w narzędziach do kopania kryptowalut działających za pośrednictwem stron internetowych, ale także w złośliwym oprogramowaniu. Web Assembly to dodatek do Javascript, obecnie obsługiwany przez wszystkie popularne przeglądarki. Przy pomocy Web Assembly web developerzy są w stanie osiągnąć znacznie krótszy czas ładowania oraz szybsze wykonanie kodu w ten sposób standard webowy staje się idealną technologią dla kopania monet.

Co istotne z technicznego punktu widzenia, coraz częściej złośliwe oprogramowanie wykorzystuje mniej znane funkcje systemu Windows w celu wykonywania złośliwych poleceń przy pomocy skryptów wierszy poleceń. Dla przykładu: eksperci z firmy G DATA z powodzeniem wykorzystali heurystyczne wykrywanie próbek złośliwego oprogramowania Voiv do blokowania licznych ataków wykorzystujących zaplanowane zadania w systemie Windows w celu wprowadzania zmian do systemu. Złośliwe oprogramowanie ukrywa się, podając się za proces związany z działaniem przeglądarki. W zależności od wersji, wykonuje różne rodzaje kodu za pośrednictwem różnych silników skryptujących, które na przykład same aktualizują złośliwe oprogramowanie bądź ładują jego dodatkowe moduły.

Rzekome wsparcie techniczne umarło. Niech żyje rzekome wsparcie techniczne

Zwłaszcza w miesiącach letnich eksperci firmy G DATA zauważyli powrót do dobrze już znanej metody oszustwa opartego na rzekomym wsparciu technicznym. Użytkownik widzi zajmujące cały ekran wyskakujące okienko z informacją, że jego komputer został zainfekowany przez złośliwe oprogramowanie i konieczne jest jego odpłatne naprawienie. W tym celu należy zadzwonić pod numer rzekomej infolinii. Rozmówcy zazwyczaj podają się za pracowników firmy Microsoft i wywierają presję psychiczną na użytkowniku. Płatności zazwyczaj należy dokonać za pośrednictwem karty przedpłaconej iTunes. Tim Berghoff, Specjalista ds. Zabezpieczeń w firmie G DATA skorzystał w zeszłym roku z okazji i odbył tego typu rozmowę z oszustem. Berghoff przedstawia bieżące doniesienia oraz wskazówki od G DATA o tym, jak radzić sobie z oszustami.

Wtyczki Adobe Flash to kolejny powszechny problem w kontekście zabezpieczeń. Luka z 2017 roku (CVE-2017-3077) uplasowała się na siódmej pozycji w rankingu udaremnionych zagrożeń wykrytych wśród klientów G DATA. W tym wypadku zmodyfikowany obraz w formacie PNG jest wykorzystywany po to, by wprowadzić złośliwy kod do komputera użytkownika i wykorzystać istniejące luki. Po utworzeniu tego rodzaju punktu wyjścia dla ataku powstaje możliwość załadowania kolejnych porcji złośliwego kodu. G DATA zaleca, by przestać korzystać z Adobe Flash Playera i odinstalować go. Jeśli nie wyobrażasz sobie takiego rozwiązania pamiętaj, by zawsze niezwłocznie instalować aktualizacje.

Gracze, miejcie się na baczności!

Czwartą i ósmą pozycję w rankingu zajmują przypadki wykrycia generycznego złośliwego oprogramowania ukrywające się pod postacią scrackowanych wersji gier. Twórcy złośliwego oprogramowania często ukrywają swoje dzieła w grach, nie tylko na komputerach z systemem Windows, jako że wiele dzieci nie zdaje sobie sprawy z potencjalnych zagrożeń. W szczególności jeśli chodzi o system Android, gry dedykowane dla dzieci znajdują się na celowniku oszustów. Firma G DATA niedawno ostrzegała o pojawiających się fałszywych wersjach gry Fortnite na system Android.
Jeśli chodzi o wykrywanie Potencjalnie Niechcianych Programów (PUP), poza Monero Miners nadal istnieją programy, które modyfikują ustawienia przeglądarki bez zgody użytkownika na przykład zmieniają stronę startową lub domyślną przeglądarkę bądź instalują irytujące paski narzędzi. Open Candy i Mindspark -Framework, ukryte głównie w instalatorach darmowego oprogramowania, które są w tym kontekście znane od lat. Nadal krążą po sieci, a rozwiązania od G DATA skutecznie je wykrywają. Co interesujące, oprogramowanie sklasyfikowane jako PUP, takie jak Win32.Application.DownloadGuide.T, które obecnie rozpoznaje również maszyny wirtualne, stara się w tym wypadku uniknąć wykrycia przez programy antywirusowe poprzez przyjęcie mniej agresywnej strategii działania.

Liczba odpartych ataków nieznacznie spada

Informacje o atakach udaremnionych w minionym półroczu docierają do nas odrobinę rzadziej niż w roku ubiegłym. Było to szczególnie widoczne w drugim kwartale
2018 roku.

Dane Statystyczne pokazują również, że w zakresie złośliwego oprogramowania sytuacja znacząco różni się w poszczególnych krajach. Większość udaremnionych ataków złośliwego oprogramowania i PUPów została w pierwszej połowie 2018 roku odnotowana w Turcji, zostawiając daleko w tyle Izrael, który uplasował się na drugiej pozycji. W Turcji rozwiązania zabezpieczające od G DATA pow=strzymały zwłaszcza ataki przy pomocy dobrze znanych narzędzi do crackowania oprogramowania systemu Windows.

Liczba nowo powstających przykładów złośliwego oprogramowania również nieznacznie zmalała w pierwszej połowie roku w porównaniu z rokiem ubiegłym. Łącznie laboratoria G DATA wykryły 2 396 830 nowych przykładów złośliwego oprogramowania za szkodliwe. Średnio wykrywano dziennie 13 000 nowych próbek złośliwego oprogramowania, co daje 9 na minutę. Benzmüller w ten sposób komentuje dane liczbowe: Przewidujemy, że w drugiej połowie roku liczba nowych przykładów złośliwego oprogramowania znów wzrośnie. W tym roku rekord prawdopodobnie nie zostanie pobity, chociaż indywidualne ataki stają się coraz bardziej wyrafinowane i ściśle ukierunkowane .