Port USB – niesławna przystań piratów, nie tylko z Karaibów

Jakub Kralka,
Product Manager Axence

Ten kto myśli, że w temacie ataków wykorzystujących porty USB napisano już wszystko, niech koniecznie przeczyta niniejszy artykuł. Technika ta nie tylko nie przechodzi do lamusa, ale wciąż ewoluuje, dlatego warto stosować skuteczne metody zapobiegania. Edukacji nigdy dość!

Prymitywny acz skuteczny

Atak wykorzystujący port USB można porównać z przecięciem przewodów hamulcowych w samochodzie. Nie wymaga dużo sprytu, może go wykonać niemal każdy, jest bardzo tani i zabójczo skuteczny. Wielu nosicieli niszczycielskiego kodu można kupić w Internecie za kilka dolarów[1]. Jak działają? W większości imitując inne urządzenia (podatność BadUSB). Oprogramowanie kontrolera USB odpowiadające za właściwe rozpoznanie komponentu w systemie, po zabiegach hakera może „przedstawiać się" komputerowi jako klawiatura i przechwytywać wpisywane dane (keylogging). Może także wpisywać zaprogramowane ciągi znaków, co w praktyce pozwala na wykonanie dowolnego kodu z uprawnieniami zalogowanego użytkownika. Niektórym zmodyfikowanym urządzeniom USB wystarczy 30 sekund, by zdobyć dane logowania do komputera i to nawet, gdy ten jest zablokowany[2]. To jeszcze nie koniec. Jako karta sieciowa zmutowany pendrive jest w stanie przekierować nasz ruch sieciowy.

Obrażający inteligencję przeciwnika

Pendrive znaleziony pod biurkiem lub na korytarzu firmy jest nie lada gratką. Tajemnica jego zawartości kusi nie tylko szeregowych pracowników. Niewiele osób potrafi się oprzeć tej pokusie i zanieść znalezisko do działu IT. Sytuacja komplikuje się zwłaszcza jeśli USB stick jest markowy i ma dużą pojemność. To tak jak znaleźć stówę na ulicy. Trzeba tylko sprawdzić co się na nim znajduje, sformatować i mamy dodatkowy storage na prywatne zdjęcia i filmy, których w cyfrowym świecie nigdy dość. Po co czekać, lepiej zrobić to na firmowym laptopie… Podobny scenariusz zadziałał pewnego dnia w fabryce broni jądrowej w Iranie, gdzie za pomocą podrzuconego pendrive'a zdestabilizowano pracę wirówek wzbogacających uran (patrz Stuxnet[3]).

[1] https://sekurak.pl/poison-tap-za-20-zlotych-wykrada-ciastka-z-zablokowanych-kompow/

[2] http://http://www.centrumxp.pl/Aktualnosci/16523,Kradziez-danych-logowania-za-pomoca-USB-PC-i-Mac-wciaz-niezabezpieczone.aspx

[3] https://niebezpiecznik.pl/post/stuxnet/

Dlaczego to wciąż działa?

Czemu ataki USB są nadal tak popularne i skuteczne? Otóż edukacja nt. bezpieczeństwa sieciowego, jeśli jest w ogóle w prowadzona w firmach, bazuje na najnowszych przykładach ataków. Pracownicy mają więc szansę dowiedzieć się jak rozpoznawać phishing oraz czym jest oprogramowanie ransomware, nie mają jednak świadomości, że zagrożenie może przyjść od najmniej spodziewanej strony. Kto by pomyślał, że ładując e-papierosa przez USB możemy wpuścić do firmy groźnego robaka[4]? Ładowanie telefonów, podłączanie wiatraczków czy lampek z Chin do portów w naszych służbowych komputerach jest na porządku dziennym. Niewiadomego pochodzenia tanie gadżety z Państwa Środka to jednak nie jedyne „niepewne" produkty. Do dnia obecnego nie została wyjaśniona międzynarodowa afera, do której doszło na szczycie G20 organizowanym w Sankt Petersburgu w 2013 roku, gdzie jako gadżet w tzw. „welcome packu" uczestnicy otrzymywali wielofunkcyjną ładowarkę z wgranym właśnie złośliwym oprogramowaniem[5]. To bardzo niebezpieczna gra. Gdy cyberprzestępca chce przeprowadzić atak APT (ang. Advanced Persistent Threat), bo dane na których mu zależy są bardzo cenne, stworzy exploita, którego nie rozpozna oprogramowanie antywirusowe. Jeśli w firmie jest sprzętowy sandbox, istnieje szansa na złapanie intruza, lecz to wciąż nieczęsty widok w serwerowniach polskich firm. Ponadto ataki wykorzystujące podatność BadUSB, opisane na samym początku, uciekną nawet z piaskownicy, ponieważ nie wykorzystują żadnych plików na komputerze ofiary.

O czym zapominamy?

Bruce Schneier – amerykański kryptograf i specjalista z zakresu bezpieczeństwa teleinformatycznego – stwierdził, że „bezpieczeństwo to proces, nie produkt[6]" i w 100% się z nim zgadzamy. Proces zabezpieczania sieci praktycznie nigdy się nie kończy i nigdy nie można być całkowicie pewnym, że jakakolwiek sieć jest bezpieczna. Wg raportu Cisco z 2016 roku 55% badanych uważa, że sposób zachowania się pracowników jest jednym z dwóch największych zagrożeń dla bezpieczeństwa danych i ustępuje tylko zagrożeniom ze strony zorganizowanych grup cyberprzestępczych (62%). Jedna i druga grupa bardzo często posługuje się nośnikami danych USB do stworzenia szkód, awarii lub do wyprowadzenia danych z naszych komputerów.

Najczęstsze zagrożenia

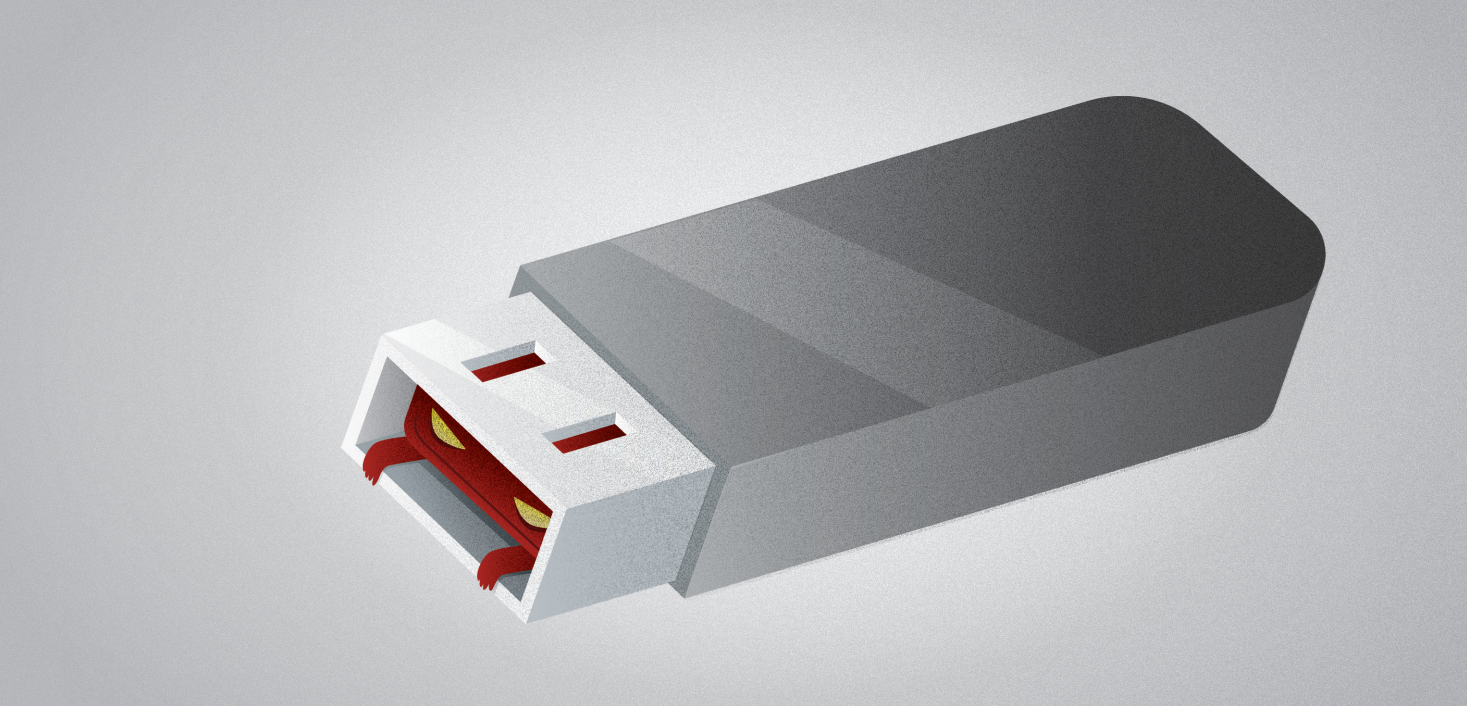
Istnieje wiele przykładów ataków z wykorzystaniem niezabezpieczonych portów USB, jednak najczęstsze to:

- Social Engineering: wykorzystuje typowy USB, który zawiera pliki HTML. Jest to atak typu phishing i wydobywa od użytkowników ich loginy i hasła w momencie operacji na plikach znajdujących się na nośniku.
- HID (Human Interface Device) spoofing: odpowiednio spreparowane nośniki USB używają wyspecjalizowanego kodu do oszukania komputera, aby uwierzyć, że klucz USB to klawiatura. Ta fałszywa klawiatura naciśnie klawisze, gdy tylko urządzenie jest podłączone do komputera. Naciśnięcia klawiszy to zestaw poleceń, które naruszają komputer ofiary. Dzięki takiemu zabiegowi hakerzy mogą uzyskać pełen dostęp do stacji roboczej użytkownika.
- 0-day: przykład ataku, który wykorzystuje lukę w sterowniku USB do bezpośredniej kontroli nad komputerem, gdy tylko zostanie podłączony. Może mieć miejsce w momencie znalezienia przez hakerów luki w oprogramowaniu sterownika urządzenia USB jeszcze przed wprowadzeniem patcha przez producenta sprzętu.

[4] https://www.theguardian.com/technology/2014/nov/21/e-cigarettes-malware-computers

[5] https://niebezpiecznik.pl/post/rosjanie-wreczali-politykom-zainfekowane-ladowarki-i-pendrivey-na-szycie-g20/

[6] https://www.schneier.com/crypto-gram/archives/2000/0515.html



Zabetonować porty

Jak zabezpieczyć się przed wirusami infekującymi sieć przez porty USB? Rozwiązanie jest bardzo proste. Polecają je stosować nawet sami twórcy złośliwego kodu, przynajmniej ci, którzy piszą go dla sportu. Nie wszystkie rozwiązania typu end-point security jednak tę funkcjonalność zapewniają. Chodzi wprost o blokowanie portów USB. Co jednak zrobić, gdy w sieci mamy kilkaset końcówek? Przyda się narzędzie, które pozwoli na stworzenie reguł dla blokowania portów w organizacji, a następnie umożliwi ich szybkie wdrożenie na wszystkich komputerach w sieci. Zadanie to realizuje Moduł DataGuard w Axence nVision®. Z jego pomocą można zarządzać dostępem urządzeń przenośnych (zapis, uruchomienie, odczyt) do firmowej sieci, eliminując ryzyko zarażenia robakami wyposażonymi w instrukcje automatycznej instalacji. Możliwa jest centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory. Dodatkowo korzystając z DataGuard organizacja może ograniczyć wyciek strategicznych danych za pośrednictwem pamięci masowych oraz urządzeń mobilnych. Krajobraz zagrożeń jest szeroki, należy jednak pamiętać o tym, co jest z pozoru oczywiste, by nie dać się złapać. Warto pokazywać też powyższe przykłady pracownikom.