Jak rozumiemy pojęcie cyberatak ?

Głównym celem cyberataków są firmy i instytucje, gdzie po pomyślnym jego przeprowadzeniu, Hakerzy żądają okupu za skradzione dane, które nie powinny być ujawnione publicznie. Ponadto mimo żądanego okupu są jeszcze inne przyczyny cyber ataktów. Są to między innymi jak np. niszczenie reputacji danej marki, doprowadzanie firm do bankructwa, zagrażanie bezpieczeństwu państw, tworzeniu konfliktów i wzbudzanie u ludzi buntu itd.

Techniki cyberataku

- szkodliwe oprogramowanie (malware) – najbardziej popularna broń hakerów i obejmuje m. in. wirusy, robaki, trojany, rootkity. Generalnie, gdy użytkownik wykona interakcję z danym złośliwym programem w postaci binarki/pliku wykonywalnego to malware zaczyna uruchamiać swój złośliwy kod i zablokować dostęp do danych na dysku, wykraść informacje i uniemożliwić działanie systemu.
- oprogramowanie szantażujące (ramsomware) – szkodliwe oprogramowanie, które grozi ofiarom cyberataku opublikowaniem wrażliwych informacji niejawnych oraz blokuje dostęp do systemu do czasu opłacenia okupu w postaci kryptowaluty.
- phishing – ma postać w postaci e-mail z pozoru pochodzącego z zaufanego źródła lub strony internetowej, użytkownik otwiera zainfekowany link/plik i podejmuje czynności tj. podawanie własnych chronionych informacji.
- MitM – polega na wykradaniu danych przepływających między dwoma stronami użytkownik – punkt dostępu do sieci.
- Atak DDoS – zalewanie systemu wzmożonym ruchem w celu uniemożliwienia właściwego funkcjonowania systemu.
- SQL Injection – wstrzyknięcie złośliwego kodu do bazy SQL w celu kierowaniu zapytań bazodanowych do serwera pozyskania chronionych informacji.
- „wykorzystanie luki w dniu zerowym” – jest to metoda polegająca na wprowadzeniu szkodliwego oprogramowania poprzez słabe punkty zabezpieczeń systemu, o których producent lub użytkownik oprogramowania nie wie. W zasadzie to odnosi się do faktu, że programiści tworzący kod mieli zero dni na wyeliminowanie tego słabego punktu. Łatając „dziury” systemowe po jakimś czasie są wykrywane przez hakerów nowe i tak w kółko. Zazwyczaj dany system jest bezpieczny do czasu wykrycia nowego backdoora.

Skrócona historia ataków

W zasadzie tych ataków było sporo, ale wymienię poszczególny, główny, który zdarzył się na Ukrainie. Firma Linkos Group odpowiedzialna za poprawki i wszelkie aktualizacje do oprogramowania do programu księgowości o nazwie MEDoc. Był to program do rozliczania się z podatków. Korzystało z niego ponad 90% krajowych firm. Późniejsze analizy przeprowadzone przez firmę ESET (twórcy dość popularnego antywirusa pod system Windows oraz urządzenia mobilne) wskazały, że 80% ataków zostały przeprowadzone w kierunku Ukrainy. Atak nastąpił

przed dniem Ukraińskiego Dnia Konstytucji (27 czerwca 2017 roku), gdzie pracownicy zostawili swoje puste biura z włączonymi komputerami, dając tym wielkie pole do popisu przeprowadzenia cyberataku hakerom. Aczkolwiek złośliwe oprogramowanie lekko uciekło spod kontroli i ucierpiały w tym jeszcze ukraińskie ministerstwa, banki, metra, przedsiębiorstwa handlowe tj. supermarkety, stacje benzynowe itd. Następnie rozrosło się to na skalę światową co wspomniałem wcześniej te firmy, które są widoczne na prezentacji.

Jeżeli chodzi o Polskę to tego dnia o godzinie 13 zostały odnotowane ataki na sektory logistyczne oraz spółki usługowo-handlowe. Atak ten był na tyle poważny, że pierwszy raz w Polsce miało spotkanie Rządowego Zespołu Zarządzania Kryzysowego ze współpracą wraz z CERT-em (Zespół Reagowania na Incydenty Internetowe) o szkoleniach pracowników frmy w kwestiach wykonywania kopii bezpieczeństwa danych oraz podstawowej ochronie prze tego typu atakami, czyli mw. przeprowadzanie aktualizacji systemu. Firmy polskie, które zostały dotknięte tym atakiem to: Firma Raben, InterCars, TNT, Modelez, Saint-Gobain.

Ogólne straty tym atakiem są liczone mln USD. Np. Maersk oszacował stratę na około 200-300 mln USD, Fedex na 400 mln USD, Saint-Gobain 384 mln, Merck na 870 mln. Według wyceny Białego Domu w USA wartość szkód jaką przyniósł ten atak szacuje się na 10 mld USD.

Co to jest Wiper ?

Niby to żądało okupu, ale tak naprawdę po opłaceniu na dysk ofiary został wyczyszczony oraz nadpisany losowymi danymi, które były nie do odzyskania. Reasumując algorytm Wipera działał w taki sposób, że najpierw przeszukiwał formaty plików, które mógł je wyczyścić, następnie przeszukiwał wszystkie foldery na dysku komputera wraz z podłączonymi urządzeniami zewnętrznymi, na koniec czyścił sektory na dysku (wymazywał pliki). Statystycznie Wiper wykonywał swoje działanie w 75 %, ale większość plików i tak nie była do odzyskania, ponieważ została nadpisana losowymi danymi.

Skład Wipera

- Exploit EternalBlue – exploit (program mający na celu wykorzystanie błędów w oprogramowaniu), zostało opracowane przez NSA (amerykańską agencję bezpieczeństwa). Pierwszy raz wykorzystane przez grupę hakerów pod nazwą Shadow Brokers. Działanie jego było takie, że udostępniało ono publiczne luki systemowe, które były ukierunkowane na zapory korporacyjne, oprogramowanie antywirusowe oraz wszelkie produkty/usługi Microsoftu. Wykorzystywał lukę w protokole Microsoft Server Message Block w wersji 1 i dzięki temu zyskiwał dostęp do zdalnego wykonywania operacji na komputerze ofiary. Haker mógł używać trzech poleceń: ping, kill, exec.
- Mimikatz – w połączeniu z wymienionym wcześniej exploitem. Typowe narzędzie open-sourceowe, które zbiera i wykorzystuje poświadczenia w systemie Windows. Jest to tzw. „szwajcarski hakerski scyzoryk”, ponieważ ono wykrada wrażliwe dane tj. hasła, co za tym idzie, że umożliwia całkowity dostęp do urządzenia. W dość szybkim czasie została wydana łatka na exploita Ethernal Blue, ale łącząc oba te narzędzia były

one nie do pokonania. Twórca Mimikatza stwierdził to takimi słowami. Cytuję : „Możesz zainfekować komputery, które nie są załatane, a następnie możesz pobrać hasła z tych komputerów, aby zainfekować inne komputery, które są załatane”.

Przebieg ataku

- MEDoc – tak jak wspomniałem w oprogramowaniu do księgowości został znaleziony backdoor prowadzący do kontroli nad danym oprogramowaniem. Hakerzy wstrzyknęli złośliwy kod, który pobierał i uruchamiał malware o nazwie NotPetya, podczas gdy użytkownicy pobierali uaktualnienie z serwera upd.me-doc.ua Następnie złośliwy kod wywołany w tle zaczynał szyfrować MFT (Master File Table to ukryty plik, w którym zawarte są pełne informacje o ścieżce dostępu, datach edycji, utworzenia pliku na danej partycji, jest on bardzo ważny, ponieważ definiuje on tablicę plików). Następnie zaczęto szyfrowanie głównej partycji rozruchowej systemu operacyjnego (zazwyczaj to MBR w Windows, zapisywał część losowymi danymi). Wywołanie ponownego uruchomienia i fałszywy skan plików na dysku wbudowanym programem chkdsk (skan plików) w Windows. Wyświetlenie takiego samego komunikatu o opłaceniu okupu za zaszyforwane pliki jak w przypadku wirusa Petyi.

Na koniec chciałbym zadać wam pytanie jakie były oskarżenia od kogo do kogo za spowodowane te szkody ? Czy ktoś wie ? :)

Jak zwykle odwieczny mały konflikt polityczny nie będzie się kończył. Biały Dom w USA oskarżał Rosję za ten atak. Niby z wydanego oświadczenia wynika, że rosyjskie wojsko przeprowadziło najbardziej niszczycielski oraz kosztowny atak w historii według USA. Państwo stawiało też fakt na konflikt między Rosją i Ukrainą na linii Kreml-Kijów. Ukraińska firma od cyberbezpieczeństwa ISSP oraz słowacki ESET wykryły zależność między ataki, jakie podejmowała grupa hakerska Sandworms lub Telebots.

Natomiast Rosja oskarżyła cztery państwa xD : Wielką Brytanię, Kanadę, Australię, Nową Zelandię.