Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- Wstęp
- Aktualizacje
- Kopie Zapasowe
- Phishing

Nauka Płynąca z WannaCry

Wstęp

W ostatnim czasie, w mediach pojawiła się niepokojąca informacja o nowym ataku przestępców nazwanym "WannaCry". "WannaCry" zainfekował ponad 200 000 komputerów, uniemożliwiając prawidłowe funkcjonowanie wielu instytucji, w tym szpitali w Wielkiej Brytanii. Atak zyskał niechlubną sławę z kilku powodów. Pierwszym z nich było jego szybkie rozprzestrzenianie się między komputerami dzięki wykorzystaniu znanej podatności systemu Windows. Drugim, było wykorzystanie złośliwego oprogramowania typu ransomware, powodującego zaszyfrowanie plików zarażonego komputera, co oznacza całkowite zablokowanie dostępu do dokumentów. Sposobem na odzyskanie plików jest przywrócenie ich kopii zapasowej lub zapłacenie okupu atakującemu w wysokości 300 dolarów, co niekoniecznie gwarantuje ich odszyfrowanie. Trzecim, a jednocześnie najważniejszym powodem jest to, że ten atak nigdy nie powinien dojść do skutku. Podatność komputerów z systemem Windows, którą wykorzystywał "WannaCry" była dobrze znana przez Microsoft, a aktualizacja łatająca tę podatność została udostępniona kilka miesięcy wcześniej. Mimo wszystko wiele organizacji nie zainstalowało tych aktualizacji lub korzystały z komputerów opartych na starym systemie operacyjnym Windows XP, który nie jest już wspierany przez Microsoft. Poniżej przedstawiamy trzy kroki, które dadzą Ci pewność, że ataki podobne do "WannaCry" nie spowodują szkód również na twoim komputerze.

Redaktor gościnny

Dr Johannes Ullrich jest kierownikiem działu badań Instytutu Technologii SANS oraz założycielem DShield.org. Jest odpowiedzialny za **SANS Internet Storm Center**, monitorujący zagrożenia w cyberprzestrzeni. Naucza bezpieczeństwa aplikacji web (**DEV522**), wykrywania włamań (**SEC503**) oraz IPv6(**SEC546**).

Aktualizacje

Po pierwsze, zawsze bądź pewny, że komputery, urządzenia mobilne, aplikacje oraz inne urządzenia mające dostęp do internetu są aktualne. Przestępcy stale szukają nowych podatności w oprogramowaniu używanym przez twoje urządzenie. Kiedy znajdą podatność, używają specjalnych programów do przejęcia urządzenia. W tym samym czasie firma, która wyprodukowała oprogramowanie dla Twojego urządzenia usilnie stara się załatać te podatności wypuszczając aktualizacje. Jeśli instalujesz na bieżąco aktualizacje, sprawiasz, że o wiele ciężej będzie przejąć twoje urządzenie. Jest to najbardziej przygnębiający fakt w odniesieniu do rozprzestrzeniania się "WannaCry". Aktualizacja, która zapobiegała rozprzestrzenianiu się tego wirusa została opublikowana przez Microsoft prawie dwa miesiące wcześniej niż nastąpił atak. Gdyby instytucje stale aktualizowały komputery, atak ten nigdy nie osiągnąłby tak dużej skali. Jeśli tylko jest to możliwe pozostaw opcję automatycznej aktualizacji włączoną. Zasada ta dotyczy właściwie każdej technologii, która ma dostęp do internetu jak na przykład telewizorów, routerów

Nauka Płynąca z WannaCry

domowych, konsoli do gier lub nawet samochodu. Jeśli system operacyjny lub urządzenie jest na tyle stare, że nie jest już dłużej wspierane w zakresie aktualizacji bezpieczeństwa, jak np. Windows XP, wymień je na nowe.

Kopie zapasowe

W pewnych przypadkach, ataki ransomwarem mogą zainfekować aktualny system. Dlatego bardzo ważne jest tworzenie kopii zapasowej (ang. backup). Kopie zapasowe to kopie plików, umieszczane w innym miejscu niż twój komputer lub urządzenie mobilne. Jeśli utracisz dane na nośniku źródłowym, możesz odzyskać te dane z kopii zapasowej. Niestety, wiele osób nie wykonuje regularnie kopii zapasowych pomimo tego, że wykonuje się je łatwo i nie wymagają dużych nakładów finansowych. Kopie można tworzyć na dwa sposoby: na nośniku fizycznym lub używając rozwiązań w chmurze. Każde z tych podejść ma swoje zalety oraz wady. Jeśli nie jesteś pewny, którą metodę wybrać, możesz zawsze używać obu.

Kluczem do ochrony przed atakami takimi jak WannaCry są trzy drobne kroki: aktualizacja oprogramowania, czujność oraz kopie zapasowe systemu.

Nośnikami fizycznymi są urządzenia, które możesz podłączyć do zewnętrznych portów USB lub sieci w domu i pracy. Ich zaletą jest szybkie tworzenie kopii dużych zbiorów danych, zaś wadą jest możliwość przeniesienia złośliwego oprogramowania np. ransomwaru również na kopie zapasowe. Jeśli tworzysz kopie na nośnikach fizycznych, pamiętaj by znajdowały się one w bezpiecznym i odseparowanym miejscu. Pamiętaj o prawidłowym oznaczeniu odpowiednich kopii, tak by nie było w przyszłości problemu z ich przywróceniem.

Rozwiązania oparte na chmurze to serwisy online zapisujące dane w internecie. Zazwyczaj instalowane jest dla nich dedykowane oprogramowanie obsługujące cały proces. Zaletami rozwiązań w chmurze jest ich prostota w użyciu. Dodatkowo, jeśli zostaniesz zainfekowany ransomwarem, zazwyczaj infekcja ta nie ma dostępu do plików kopii zapasowej w chmurze. Do minusów należy zaliczyć długi czas przesyłania dużych partii danych. Pamiętaj o sprawdzeniu ustawień prywatności oraz bezpieczeństwa kopii w chmurze. Wybierając konkretną usługę sprawdź czy jest ona bezpieczna, czy dane są szyfrowane oraz czy posiada silne uwierzytelnianie.

Phishing

Pamiętaj, przestępcy stale udoskonalają i zmieniają metody ataku. Do zaatakowania i zarażenia ofiary, często korzystają z innej metody ataku, którą jest Phishing. Polega ona na między innymi na wysłaniu tak spreparowanej wiadomości email, by

Nauka Płynąca z WannaCry

zachęcić ofiarę do otwarcia złośliwego załącznika lub odwiedzenia fałszywej strony internetowej. Jeśli atak się powiedzie, Twój komputer może zostać zarażony. “WannaCry” nie używał tej metody ataku, jednak jest ona powszechna w przypadku innych rodzin ransomwaru. Dodatkowo, można być pewnym, że autorzy “WannaCry” w najbliższych miesiącach poprawią swoje metody ataku oraz użyją ich, tak by zarazić jeszcze więcej komputerów. Kluczem do ochrony przed atakami opierającymi się na wiadomościach mailowych jest zdrowy rozsądek. Jeśli wiadomość wydaje się być podejrzana, sformułowana w niejasny sposób lub jej treść brzmi zbyt pięknie, aby mogła być prawdziwa, z dużym prawdopodobieństwem będzie to wiadomość phishingowa.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.

Odwiedź securingthehuman.sans.org/ouch/archives i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.

WWW: http://www.cert.pl

Twitter: @CERT_Polska

Facebook: http://facebook.com/CERT.Polska

Źródła

Co to jest Malware ?:	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Kopie zapasowe:	https://securingthehuman.sans.org/ouch/2015#august2015
Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Bezpieczne korzystanie z chmury:	https://securingthehuman.sans.org/ouch/2016#november2016

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski

