RANSOMWARE PETYA NIE ZASZKODZIŁ POLSKIEJ GOSPODARCE [KOMENTARZ EXATELA]

O wektorach ataku, zagrożeniu dla systemów Windows 10, podobieństwach i różnicach między WannaCry a Petya oraz sposobach ochrony pisze dla cyberdefence24.pl Tomasz Wodziński Kierownik Security Operations Center (SOC) Exatel

Analizy wskazują, że inicjalnym wektorem ataku na Ukrainie była aktualizacja oprogramowania firmy M.E.DOC. Instalacja tego typu nie wymagała interakcji użytkowników. I tak, około godziny 11.00 program sam się pobrał i zainfekował systemy, wymuszając restart komputera o godzinie 14.35.

Jednocześnie, korzystając z techniki ARP sniffing, szukał ofiar w sieci wewnętrznej. Jeden z modułów zawierał program do kradzieży haseł, tzw. keylogger, który następnie sprawdzał, czy któreś z wykradzionych haseł nie jest takie samo jak hasło administratora komputera sąsiadującego lub administratora domenowego.

Drugim zarejestrowanym wektorem ataku były e-maile phishingowe z dokumentem DOC. Dokument Worda miał ukryty ładunek złośliwy, ściągający kod wykonywalny z serwera Command&Control. W obu wypadkach oprogramowanie wykorzystywało tą samą podatność opierającą się na błędzie w usługach udziałów sieciowych (dysków sieciowych) w systemach Windows. Podatność ta w wielu organizacjach była załatana, bo stosowna poprawka została wcześniej dostarczona do wszystkich systemów po atakach ransomware WannaCry 12 maja 2017 roku.

Czytaj też: Petya - WannaCry na sterydach. Kolejny globalny atak ransomware [AKTUALIZACJA]

Wczorajszy atak ransomware był bardzo ciekawy z punktu widzenia jego złożoności i pomysłu. Szyfrowanie dysku wykonywało się zaraz po ponownym uruchomieniu systemu. Kodowany był cały dysk lub – jeśli oprogramowanie nie miało możliwości pozyskania uprawnień administratora– szyfrowały się pliki w katalogach, do których użytkownik miał dostęp.

Co do bezpieczeństwa Windows 10 – użytkownicy posiadający wszystkie poprawki byli odporni na mechanizmy rozsiewania poprzez sieć wewnętrzną. Jednak zgodnie z naszą wiedzą ransomware Petya w wersji dystrybuowanej przez aktualizator M.E.DOC korzystał z podwyższonych uprawnień. Nie miał więc problemu z ominięciem zabezpieczeń systemu Windows 10.

Petya i WannaCry działały z wykorzystaniem tej samej podatności. W przypadku majowego ataku WannaCry jedyną podatnością była ta dotycząca udziałów sieciowych, tzw. samba. Czerwcowy atak Petya wykorzystywał już trzy różne podatności, miał dwa alternatywne sposoby infekowania (wektory ataku). Jest znacznie bardziej zaawansowany i dużo lepiej przemyślany w aspekcie początkowej infekcji. Znacznie gorzej wymyślony został sposób monetyzacji, który chwilę po godzinie 23.00 polskiego czasu przestał działać, a zainfekowani użytkownicy pozostali z zaszyfrowanymi dyskami.

Czytaj też: Służby na bieżąco monitorują zagrożenie cyberatakami

Aktualne analizy i fakt wykorzystania oprogramowania M.E.DOC wskazują, że głównym celem ataku była Ukraina. Nie do końca wiadomo, czy efekt końcowy, czyli atak DDoS na infrastrukturę na Ukrainie, był zamierzony, czy też był efektem ubocznym ataku.

Podobnie jak WannaCry ten ransomware nie zaszkodził polskiej gospodarce w dużym stopniu. Są firmy, które mają oddziały na Ukrainie lub prowadzą interesy z firmami ukraińskimi. Dlatego też posiadają połączenia przez systemy informatyczne. Te firmy, jeżeli nie stosowały dobrych praktyk w aspekcie bezpieczeństwa i segmentacji sieci, mogły zostać narażone na skutki ataku.

Obroną przed tego typu atakami powinno być:

zmniejszenie dostępności kont z uprawnieniami administratora,

zwiększenie nacisku na szkolenie pracowników z zakresu świadomości cyberzagrożeń,

zmniejszenie ilości oprogramowania do niezbędnego minimum potrzebnego do pracy,

wdrożenia polityki white listowania aplikacji oraz listy dopuszczonego oprogramowania,

przegląd infrastruktury sieciowej i wprowadzenia szczegółowej segmentacji sieci,

uruchomienie systemów antymalware.

Jednak należy pamiętać, że atakujący zmienia swoje taktyki. Dlatego należy nieustannie monitorować swoją infrastrukturę oraz obserwować całe otoczenie. To trudne zadanie. Dlatego zawsze można się wspomóc wyspecjalizowanymi usługami takimi jak Security Operations Center Exatela.

Ciężko jednoznacznie wskazać winnego. Szczególnie, że większość śladów zostało dobrze zatartych. Potencjalnych autorów jest wielu, jak choćby organizacje przestępcze przedstawiające się na cyberrabunki. W sieci krążą też informacje o zorganizowanych grupach powiązanych z rządami takich czy innych państw.

Wydawać by się mogło, że nie wyciągnięto żadnych wniosków z WannaCry. Tak jednak nie jest. Jednak, jak to bywa w cyberbezpieczeństwie, zarówno przez obrońców, jak i atakujących. Swoista „pomysłowość" działania złośliwego kodu tzw. TTP, różnorodność metod i wektorów ataku znacząco utrudniło jego powstrzymanie. Monitoring i analiza bieżąca systemów w dużym stopniu mogłaby tu pomóc, ale często w organizacjach brak jest wyspecjalizowanych pracowników mogących takie działania prowadzić. Brak jest też woli ze strony zarządzających, którzy nie doceniają wagi cyberbezpieczeństwa w obecnych czasach.

Tomasz Wodziński - Kierownik Security Operations Center (SOC) Exatel