aut. Adam Lelonek 20.02.2018

CYBERATAK NA UKRAINIE DWA LATA „POZA RADARAMI”: NOWY MALWARE VERMIN [ANALIZA]

Na koniec stycznia zespół identyfikacji zagrożeń Palo Alto Networks Unit 42 odkrył nową rodzinę złośliwego oprogramowania (malware), napisanego z wykorzystaniem platformy programistycznej Microsoft .NET Framework. Sami autorzy nazwali ją VERMIN. Jest to zdalne narzędzie zarządzania, czyli tzw. RAT (Remote Access Tool). Zidentyfikowane zagrożenie jest określane jest też jako zaawansowana wersja złośliwego oprogramowania szpiegującego QuasarRAT. Całe zajście skomentowali dla CyberDefence24.pl Kamil Gapiński z Fundacji Bezpieczna Cyberprzestrzeń i Maciej Ostasz z Fundacji Centrum Analiz Propagandy i Dezinformacji.

Oprogramowanie pobierało dane z zainfekowanych komputerów. Było również w stanie kasować i pobierać pliki, zmieniać nazwy plików i folderów, a także pobierać zapis audio oraz wideo. Zespół Palo Alto Networks dostał informację na ten temat od innego badacza, który przekazał im dokument spreparowany w taki sposób, aby udawać oficjalny komunikat ukraińskiego ministerstwa obrony. Miał on być zainfekowaną przynętą, która po otwarciu instalowała malware'a. W trakcie prac nad identyfikacją złośliwego oprogramowania okazało się, że było ono wykorzystywane od końca 2015 roku. Wiele z ataków nie miało nawet „przynęt” w postaci interesujących dokumentów. Dropper ze złośliwym oprogramowaniem udawał chociażby ikonkę aplikacji do przeglądania dokumentów programu Microsoft Word.

Malware wykorzystywał protokół komunikacyjny do wymiany wiadomości pomiędzy aplikacjami SOAP (Simple Object Access Protocol). Z jego pomocą ustanowiony został zabezpieczony system komunikacji C&C (Command and Control). Po zainfekowaniu oprogramowanie weryfikowało czy w systemie ofiary był zainstalowany język rosyjski. Gdy urządzenie nie było ustawione na język rosyjski, poprzez specjalnie skonstruowaną przystawkę komunikacyjną pozwalającą na analizę, komunikację i instalację oprogramowania w tle (po za interfejsem użytkownika, w sposób w którym nic nie dzieje się na pulpicie), uruchamiano funkcjonalność złośliwego oprogramowania. Część ekspertów zwraca uwagę, że podobne zachowanie może sugerować, że atakujący nie chcieli atakować własnych rodaków. Jest to jednak jedynie teoria.

Aplikacja po zainstalowaniu na danym urządzeniu wykonywała analizę oprogramowania przetwarzając informacje takie jak: nazwę urządzenia, nazwę użytkownika, adres IP i obecność oprogramowania antywirusowego, a następnie wysyłała je na serwer w celu weryfikacji zebranych danych. W momencie gdy analiza tych ostatnich wykazywała zainstalowany program antywirusowy na danym komputerze, nie był instalowany keylogger, tj. oprogramowanie rejestrujące klawisze naciskane przez użytkownika.

Istota ataku

Zdaniem eksperta Fundacji Bezpieczna Cyberprzestrzeń Kamila Gapińskiego całe zajście związane jest z kampanią, którą należy zakwalifikować do zagrożeń typu ATP. „Hakerzy zastosowali znane wcześniej

narzędzia, ale wprowadzono tez nowe – autorskie. Sposób ataku, czyli połączenie wyrafinowanych elementów socjotechniki w warstwie dostarczenia pliku oraz zaawansowanej eksploatacji podatności systemów dobrze wpisuje się w tego rodzaju ataki. **Dużo do myślenia daje fakt, że zdalne wykonywanie poleceń na zainfekowanych komputerach miało miejsce przez ostatnie dwa lata – czas ten pozwolił na zbudowanie botnetu o stosunkowo dużym potencjale. Z punktu widzenia funkcjonalności malware'u należy odnotować przede wszystkim proces targetowania. Otóż atak jest wyraźnie skierowany na stacje robocze użytkowników posługujących się językiem ukraińskim i rosyjskim. Widać to zarówno w fazie kampanii phishingowej i już podczas próby uruchomienia malware'a na komputerze.** Funkcja ta jednak nie działała poprawnie, wiec można podejrzewać, ze ładunek był dopiero w fazie testowania. Niezależnie od tego, cyberprzestępcy, po skutecznym uzyskaniu dostępu do środowiska ofiary, mieli właściwie nieograniczone możliwości w zakresie operacji na systemie".

Jak dodaje ekspert: „materiał dowodowy wskazuje na to ze autorom kampanii zależało na przejęciu i prawdopodobnie eksfiltracji danych z ukraińskich komputerów. Zwróćmy uwagę, że pliki-pułapki, czyli dokumenty tekstowe, są napisane w języku ukraińskim, takie też mają nazwy. Gdyby jednak pominąć kwestie geopolityki czy atrybucji mamy właściwie do czynienia z kampanią jakich dziesiątki w branży cyberbezpieczeństwa".

Eksperci podkreślają przy tym, że ostateczne cele atakujących nie są znane. Podobnie jak na chwilę obecną nie można określić jakie dane i w jakich ilościach zostały wykradzione. Zagraniczni komentatorzy podkreślają jednak, że wszystko wskazuje na to, iż był to skoordynowany atak przeciwko stronie ukraińskiej.

Eskalacja cyberataków na Ukrainie?

Ekspert IT Fundacji Centrum Analiz Propagandy i Dezinformacji Maciej Ostasz podkreśla, że to systematyczne, stałe działania, więc o eskalacji nie może być mowy. Jak twierdzi: „**od czasu deklaracji chęci przystąpienia przez Ukrainę do UE, stała się ona buforem komunikacyjnym między Wspólnotą a Azją. Do najważniejszych aspektów z tym związanych należy fizyczna komunikacja drogą lądową oraz translacja kontenerów informacyjnych. Jeżeli chodzi o bufor komunikacyjny to element, który można porównać do właściwości Jedwabnego Szlaku, z tą różnicą że informatyczne zasoby Ukrainy są wykorzystywane do obsługi całego procesu przetwarzania informacji.** Tu jedną ze składowych części, jest również integracja i unifikacja danych, przesyłanych od klientów azjatyckich do europejskich – czyli wspomniana wcześniej translacja i dostosowanie do rozwiązań stosowanych w tej części świata".

To często niedoceniany element. Jak zauważa Ostasz: „niejednokrotnie dane te są kluczowe w procesie handlowym, a co za tym idzie, cennym źródłem informacji. Chęć ich pozyskania przez stronę rosyjską jest tu oczywista i ma kilka aspektów. Jednym z nich to chęć pozyskania ważnych informacji i przygotowania ofert handlowych z zaniżonymi cenami w celu przejęcia kontrahentów. Drugi to obniżenie zaufania do usług IT na Ukrainie. Tu trzeba jasno powiedzieć, że ma to na celu przejęcie zleceniodawców oraz doprowadzenie do stagnacji usług IT na ukraińskim rynku. Brak specjalistów w tak ważnej dziedzinie mógłby spowodować kryzys teleinformatyczny w całym kraju".

Bardzo istotny będzie tu jeszcze kontekst całego systemu technologii informacyjno-komunikacyjnych (Information and Communication Technologies, ITC). Zdaniem eksperta, ze względu na wciąż niski stopień zabezpieczeń infrastruktury ITC na terenie Ukrainy oraz fakt znajomości tych rozwiązań technologicznych przez stronę rosyjską, ale również chińską, która stosuje podobne rozwiązania, grupom hakerskim łatwo jest poruszać się w takim środowisku oraz wprowadzać złośliwe oprogramowanie do sieci. „Stąd też taka skala zainfekowanych komputerów złośliwym oprogramowaniem i innymi infekcjami. **Mogłoby się to oczywiście zmienić, pojawia się tu**

jednak pytanie kiedy Ukraina będzie w stanie zainwestować kilkanaście miliardów dolarów w sprawną wymianę krytycznych elementów infrastruktury teleinformatycznej, a oprócz tego skoordynować to z wprowadzeniem radykalnych i restrykcyjnych ustaw dotyczących zarządzania i korzystania z sieci Internet, a co za tym idzie, podejścia do IT na szczeblu administracji publicznej, która jest obecnie najbardziej narażona na straty i utratę informacji".

Wiązałoby się to oczywiście także z licznymi szkoleniami dla pracowników oraz wymianą większości sprzętu w urzędach i budynkach rządowych. Na co zwraca uwagę Ostasz, nie chodzi tylko o komputery, ale również o drukarki i wszystkie stare urządzenia, które posiadają cechy, które obecnie można spotkać w urządzeniach Internetu Rzeczy (IoT). „W przypadku kiedy urządzenie posiada nawet jedną cechę z długiej listy właściwości powinno zostać poddane analizie bezpieczeństwa i w przypadku niespełnienia wymogów wycofane z eksploatacji" – dodaje.

Można też wspomnieć, że w kontekście podobnych działań, istotna jest atrybucja ataku. Środowisko eksperckie podkreśla, że odkryty malware komunikował się z serwerami w domenach „.ru". Jak zauważa Ostasz, nie musi to jednak automatycznie oznaczać, że to działanie Rosjan. Równie dobrze może być to inny podmiot, niż rosyjski.

Czy cyberataki na Ukrainie mogą wpłynąć na cyberbezpieczeństwo Zachodu?

W ocenie Macieja Ostasza eskalacja działań w sferze cyber miałaby wpływ na zachodnie bezpieczeństwo w jednej sytuacji – wykorzystania ukraińskiej infrastruktury do cyberataku na inny kraj lub organizację. Na chwilę obecną nie ma jednak takiego ryzyka – „cyfrowe kanały komunikacyjne z Ukrainą są stale monitorowane w celu uniknięcia takiej sytuacji. Analiza przepływu danych jest realizowana zarówno w protokołach http jak i ftp w Sieci Internet jak i TOR. Oczywiście analizowanie informacji przesyłanych w darknecie nie jest prostym tematem, ale póki co nie ma dużego zagrożenia, aby Ukraina mogła zostać wykorzystana na zasadzie «konia trojańskiego»".

Jeżeli chodzi o outsourcing zachodnich firm usług i pracowników sektora IT na Ukrainie, to również nie ma większego powodu do obaw – każde państwo stoi przed takimi samymi wyzwaniami i geografia nie ma zbyt dużego wpływu na kwestie ryzyka. „Obecnie rynek IT jest jedną z najdynamiczniejszych gałęzi przemysłu i tu nie ma mowy o opieraniu swoich działań na pojedynczych punktach działalności. Jeżeli dana firma zleca zewnętrznej firmie usługi IT, liczy się z tym że coś może pójść nie tak. Dla poprawienia poziomu bezpieczeństwa stosuje się system kooperacji, co eliminuje takie problemy" – mówi Ostasz.

Jego zdaniem każda firma korzystająca z informatyków z innego państwa musi posiadać odpowiednie zaplecze w swojej infrastrukturze, pozwalające na kontynuowanie określonych procesów. Jeżeli natomiast podobne ryzyko operacyjne nie zawarło takiej możliwości, to oczekuje się na możliwość powtórnego skorzystania z usług lub poszukuje nowych usługodawców. Tak wygląda sytuacja w momencie kiedy usługa IT jest produktem. Jeżeli natomiast produktem jest oprogramowanie lub rozwiązanie cyfrowe zagrożenie może urosnąć do maksimum. „Takim przykładem może być jeden z producentów pendrive'ów, który to na rynek wypuścił ponad milion sztuk zainfekowanych urządzeń. Firma zewnętrzna, która przygotowywała oprogramowanie do pamięci została zaatakowana przez grupę hakerów, która wprowadziła zmiany w oprogramowaniu i zaimplementowała w jego kod złośliwe oprogramowanie. Produkt ten został rozesłany po całym świecie i był sprzedawany, a po jakimś czasie okazało się że infekuje komputery złośliwym oprogramowaniem. Ten przykład pokazuje co mogłoby się stać w przypadku gdy rozwiązania softwareowe zostałyby zmodyfikowane przez osoby trzecie. Problem ten nie dotyczy tylko Ukrainy, ale każdego państwa w którym tworzy się oprogramowanie. Oczywiście w obecnej sytuacji geopolitycznej prawdopodobieństwo takiej infekcji po stronie ukraińskiej jest wysokie, niemniej jednak firmy korzystające z usług zewnętrznych, nauczyły

się przez ostatnią dekadę, że każde nowe rozwiązanie, które ma pojawić się na rynku jest testowane w izolowanych warunkach w celu wykluczenia takiej sytuacji”.

Jak podsumowuje Ostasz – nie ważne gdzie tworzone jest oprogramowanie. Najważniejszym aspektem jest to, w jaki sposób dane są dystrybuowane oraz jaka jest polityka bezpieczeństwa danego producenta czy dostawcy usług. To od nich zależy skuteczność danego ataku.