NASK

http://www.nask.pl/pl/aktualnosci/wydarzenia/wydarzenia-2019/1567,SISSDEN-system-wczesnego-ostrzegania-w-internecie-dziala-w-ponad-100-krajach.html
2019-06-20, 10:20

SISSDEN - system wczesnego ostrzegania w internecie działa w ponad 100 krajach

Prawie 250 sensorów w ponad 100 krajach na całym świecie – ponad dwukrotnie więcej niż zakładano – działa w ramach sieci pozyskiwania i wymiany informacji o cyberzagrożeniach SISSDEN. W kwietniu europejski projekt koordynowany przez Państwowy Instytut Badawczy NASK się kończy, ale specjaliści z instytutu już prowadzą działania, aby utrzymać oferowane przez system funkcjonowanie non profit, czyli m.in. przekazywanie istotnych danych o zarejestrowanych atakach.

Głównym celem trwającego od maja 2016 r. projektu SISSDEN, finansowanego z programu ramowego UE Horyzont 2020, było stworzenie jak najszerszej sieci czujników, zbierających informacje o zagrożeniach w cyberprzestrzeni. Umożliwiają one analizowanie szkodliwego oprogramowania, wykrywanie nowych wirusów pojawiających się w sieci oraz namierzanie serwerów, które kontrolują botnety lub zarządzają użyciem ransomware. Efektem tych działań są konkretne informacje o zagrożeniach, dostarczane m.in. agencjom rządowym, CERT-om i innym organizacjom odpowiadającym za bezpieczeństwo oraz operatorom sieci.

Wszystko jest na dobrej drodze, żeby projekt zakończył się sukcesem. Udało się zbudować dużo większą sieć sensorów, niż zakładaliśmy na etapie wniosku. Zebraliśmy sporo danych i zrobiliśmy bardzo interesujące analizy, które spotkały się z dużym zainteresowaniem w środowisku – mówi koordynator projektu dr inż. Adam Kozakiewicz, kierownik Zakładu Metod Bezpieczeństwa Sieci i Informacji w NASK. - Od maja 2018 do początku kwietnia 2019 zebraliśmy prawie 1 800 000 zdarzeń. W tej chwili rejestrujemy 250-300 zdarzeń na sekundę. Dr Kozakiewicz szacuje, że można tu mówić o dziesiątkach gigabajtów danych dziennie.

Istniejąca sieć sensorów monitoruje prawie 1000 adresów IP. Dane z SISSDEN-a trafiają w tej chwili do tysięcy jednostek, m.in. za pośrednictwem sieci dystrybucji organizacji pozarządowej ShadowServer. Dzięki takiemu automatycznemu powiadamianiu możliwe jest szybkie reagowanie na zagrożenia.

Sieć składająca się głównie z tzw. honeypotów, czyli wirtualnych serwerów, które stanowią pułapki na działania przestępców, obejmuje już praktycznie cały świat, ale wciąż trwają prace nad rozszerzeniem jej zasięgu. Pokryta jest większość Europy, Stany Zjednoczone i spora część Azji. Sensory znajdują się w Afryce i Ameryce Południowej. W tej chwili eksperci poszukują jeszcze serwerów m.in. na Bałkanach, gdzie dostępność tego typu usług jest mniejsza. Chcieliby też zwiększyć pokrycie np. Chin, krajów posowieckich, Indii czy Pakistanu.

Informacje z kolejnych krajów będą przydatne na dalszym etapie działań, po zakończeniu projektu SISSDEN. "Kiedy skończy się finansowanie projektu SISSDEN, trzeba będzie na nowo zastanowić się nad tym, jak konstruować sieć sensorów, nie w sensie technicznym, ale gdzie i ile sensorów umieścić. W tej chwili już widzimy, że w niektórych miejscach mamy te sensory rozlokowane wręcz za gęsto, a utrzymanie tak wielu sensorów nie byłoby efektywnym wykorzystaniem środków, które można by przeznaczyć na trudniejsze miejsca" – uważa kierownik projektu.

Sensory honeypotowe to nie jedyne źródło informacji dla ekspertów z NASK. Korzystają oni również z tzw. sandboxów, czyli kontrolowanych środowisk do uruchamiania złośliwego oprogramowania. Prowadzone są też analizy spamu. Dużo danych dostarcza również tzw. darknet, czyli przestrzeń nieużywanych adresów IP należących do NASK, na której teoretycznie żaden ruch nie powinien mieć miejsca. W praktyce okazuje się, że jego obserwowanie w połączeniu z innymi analizami może prowadzić do wielu interesujących wniosków. "95 proc. tego ruchu można zaklasyfikować jako potencjalnie złośliwy, reszta są to pomyłki - ktoś źle gdzieś wpisał adres IP" – tłumaczy pracujący przy projekcie kierownik Zespołu Metod Bezpieczeństwa Sieci Piotr Bazydło. Specjaliści z NASK podkreślają, że ogromna ilość danych pozyskiwanych w ramach SISSDEN-u wykracza poza możliwości analityczne założone w projekcie.

Jednym z najważniejszych wniosków, jaki nasuwa się ekspertom, jest fakt, że analizowanie danych w tak szerokiej skali daje duże możliwości prognozowania potencjalnie groźnych zdarzeń. "Prowadzenie bieżącej analizy takich danych umożliwia czasem zauważenie nowych zjawisk na długo przed tym, jak zaczną one być problematyczne. Oprócz reagowania post factum - dzięki temu, że widzimy, jakie

zaszły ataki i skąd przyszły - mamy też możliwość zauważenia, że zaczyna się dziać coś nowego, zanim zdarzy się coś groźnego" – podkreśla koordynator projektu, przytaczając przykład zeszłorocznych ataków DDoS na błędnie skonfigurowane serwery Memcached, które – jak wykazały późniejsze analizy – dałoby się przewidzieć z kilkudniowym wyprzedzeniem.

W związku z pozytywnym wynikiem projektu specjaliści z NASK już prowadzą działania mające na celu utrzymanie funkcjonowania systemu na dotychczasowej zasadzie non profit. "O ile nasi partnerzy zamierzają komercjalizować wyniki, o tyle my planujemy po zakończeniu projektu utrzymać oferowane przez system działania non profit" – mówi dr Kozakiewicz. Wymaga to nowego finansowania i nowego projektu, ale pracownicy NASK zamierzają dalej rozwijać to, co do tej pory wypracowali, w ramach kolejnych projektów, m.in. w ogłoszonym niedawno europejskim konsorcjum SPARTA, angażującym czołowe podmioty w działania na rzecz cyberbezpieczeństwa. Chcemy odgrywać dużą rolę także na arenie międzynarodowej jako poważny gracz w środowisku cyberbezpieczeństwa" – deklaruje dr Kozakiewicz.

Projekt SISSDEN (Secure Information Sharing Sensor Delivery event Network) jest realizowany przez osiem instytucji: instytut badawczy NASK - lider konsorcjum, Montimage EURL (Francja), Cyberdefcon Ltd. (Wielka Brytania), Universitaet des Saarlandes (Niemcy), Deutsche Telekom AG (Niemcy), Eclexys Sagl (Szwajcaria), Poste Italiane – Società per Azioni (Włochy), Stichting The Shadowserver Foundation Europe (Holandia). Przedsięwzięcie jest finansowane w ramach programu ramowego UE Horyzont 2020, umowa nr 700176. Budżet całego projektu wynosi 6 341 775,00 EUR (w tym dofinansowanie z KE: 4 912 692,50 EUR). Prace zaplanowano na trzy lata, projekt kończy się 30 kwietnia 2019 r.