CERT Polska i SKW ostrzegają przed działaniami rosyjskich szpiegów

cert.pl/posts/2023/04/kampania-szpiegowska-apt29/

Zespół CERT Polska oraz Służba Kontrwywiadu Wojskowego zaobserwowały kampanię szpiegowską łączoną z działaniami rosyjskich służb specjalnych. Celem kampanii było nielegalne pozyskiwanie informacji z ministerstw spraw zagranicznych oraz placówek dyplomatycznych, w większości znajdujących się w państwach należących do NATO i Unii Europejskiej.

Wiele elementów zaobserwowanej kampanii, takich jak infrastruktura, wykorzystane techniki oraz narzędzia, częściowo lub całkowicie pokrywa się z opisywanymi w przeszłości aktywnościami grupy określanej przez Microsoft mianem „NOBELIUM", zaś przez Mandiant jako „APT29". Grupa ta wiązana jest m.in. z kampanią zwaną „SOLARWINDS", narzędziami „SUNBURST", „ENVYSCOUT" i „BOOMBOX", a także licznymi innymi kampaniami o charakterze wywiadowczym.

Działania wykryte oraz opisane przez CERT Polska i SKW wyróżniają się jednak na tle poprzednich wykorzystaniem unikalnego, nieodnotowanego wcześniej publicznie oprogramowania. Nowe narzędzia były używane równolegle i niezależnie od siebie lub też kolejno, zastępując starsze rozwiązania, których skuteczność spadała. Pozwalało to sprawcom na utrzymanie ciągłości działań.

„Zacieśnianie współpracy między krajowymi podmiotami obserwującymi aktywność grup sponsorowanych przez obce państwa jest kluczowe dla bezpieczeństwa Polski. Dzięki bliskiej współpracy analityków CERT Polska i Służby Kontrwywiadu Wojskowego połączono elementy widziane z różnych perspektyw. Dało to efekt w postaci raportu zawierającego analizę nigdy wcześniej nie opisywanych narzędzi i z pewnością przyczyni się do zwiększenia ich wykrywalności" – podkreślił Janusz Cieszyński, Minister Cyfryzacji.

Publikujemy i ostrzegamy

Należy podkreślić, że w momencie publikacji raportu kampania realizowana przez rosyjską grupę wywiadowczą nie tylko nadal trwa, ale ma też charakter rozwojowy. Dlatego CERT Polska oraz SKW rekomendują wszystkim podmiotom, które mogą znajdować się w obszarze zainteresowania tej grupy, wdrożenie mechanizmów mających na celu podniesienie bezpieczeństwa wykorzystywanych systemów informatycznych i zwiększenie wykrywalności ataków. **Przykładowe zmiany konfiguracyjne oraz mechanizmy detekcji zostały zaproponowane w rekomendacjach.**

Podstawowym celem publikacji raportu jest zatem zakłócenie trwającej kampanii szpiegowskiej oraz umożliwienie wykrycia, analizy oraz śledzenia opisywanych działań zarówno poszkodowanym podmiotom, jak i przedstawicielom branży cyberbezpieczeństwa.

Przebieg obserwowanej kampanii

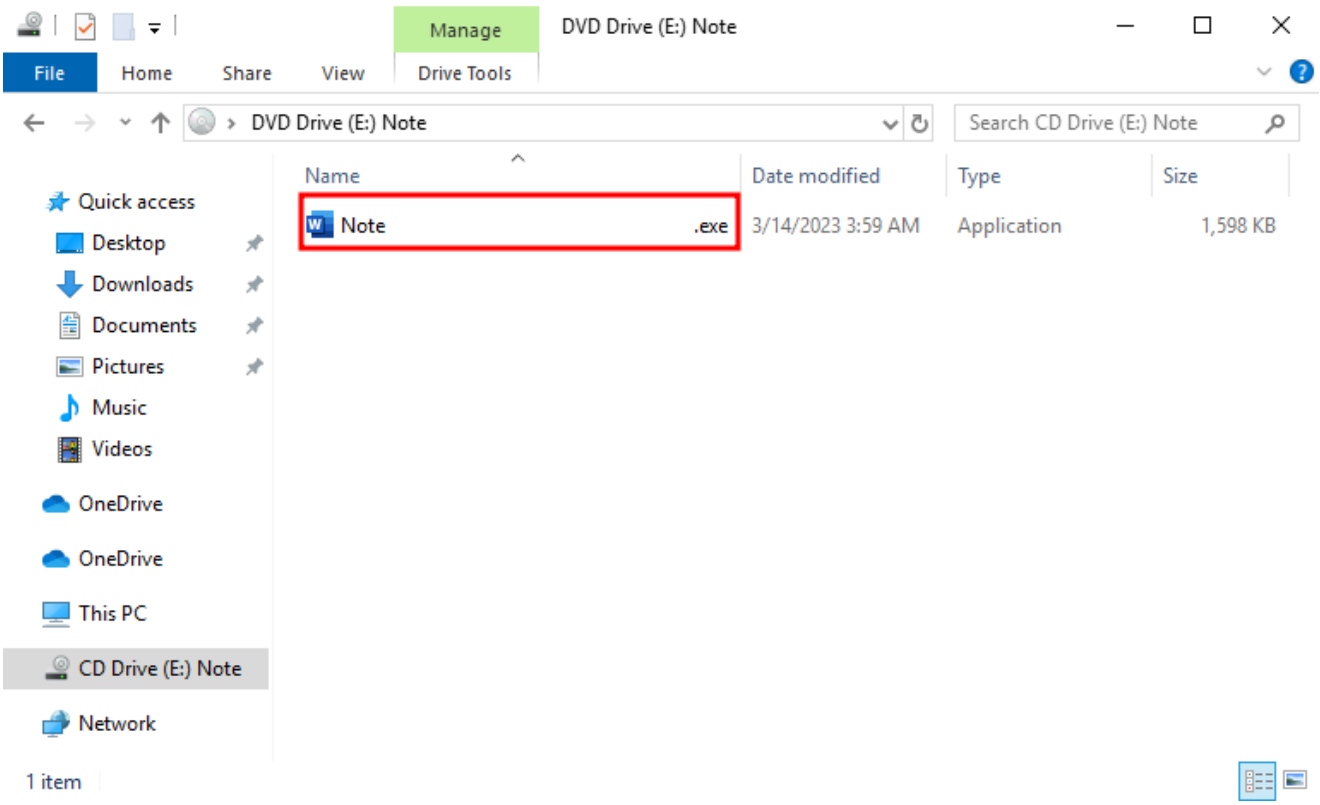
We wszystkich zaobserwowanych przypadkach sprawcy korzystali z techniki spear phishingu. Do wyselekcjonowanych pracowników placówek dyplomatycznych wysyłane były wiadomości e-mail podszywające się pod ambasady krajów europejskich. Korespondencja zawierała zaproszenie na spotkanie lub do wspólnej pracy nad dokumentami. W treści wiadomości lub w załączonym dokumencie PDF zawarty był link kierujący rzekomo do kalendarza ambasadora, szczegółów spotkania lub pliku do pobrania.

Przykładowa wiadomość email podszywająca się pod polską ambasadę i nakłaniająca do kliknięcia w złośliwy link.

W rzeczywistości odnośnik kierował do przejętej strony, na której umieszczony był charakterystyczny dla tej grupy skrypt. Korzystał on z techniki „HTML Smuggling” – przy jej użyciu złośliwy plik jest odkodowywany w momencie otwarcia strony, a następnie pobierany na urządzenie ofiary. Skrypt wyświetlał również stronę internetową, której treść miała utwierdzić ofiarę w przekonaniu, że pobrała prawidłowy załącznik.

Strona podszywająca się pod polską ambasadę sugerująca możliwość pobrania kalendarza ambasadora.

Sprawcy wykorzystywali różne techniki, aby nakłonić potencjalne ofiary do uruchomienia pobranego złośliwego oprogramowania. Jedną z nich był plik skrótu udający dokument, w rzeczywistości uruchamiający ukrytą bibliotekę DLL. Zaobserwowano również technikę „DLL Sideloading", polegającą na użyciu podpisanego pliku wykonywalnego do załadowania i wykonania złośliwego kodu zawartego w dołączonej bibliotece DLL. Na późniejszym etapie kampanii nazwa pliku wykonywalnego zawierała dodatkowo wiele spacji, aby utrudnić zauważenie rozszerzenia exe.



Widok po uruchomieniu przez ofiarę pliku obrazu przy domyślnych ustawieniach eksploratora Windows.

Rekomendacje

CERT Polska oraz SKW stanowczo rekomendują wszystkim podmiotom mogącym znajdować się w obszarze zainteresowania rosyjskiej grypy szpiegowskiej wdrożenie zmian, które skutecznie przeciwstawią się mechanizmom dostarczenia używanym w opisywanej kampanii. Sektory, które szczególnie powinny rozważyć wdrożenie zaleceń to:

1. Podmioty rządowe;
2. Podmioty dyplomatyczne, ministerstwa spraw zagranicznych, ambasady, personel dyplomatyczny i pracujący w podmiotach międzynarodowych;
3. Organizacje międzynarodowe;
4. Organizacje pozarządowe.

Szczegółowe rekomendacje zmian konfiguracyjnych oraz dokładny opis przebiegu kampanii szpiegowskiej znajduje się na stronie https://www.gov.pl/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami-specjalnymi.