**Północnokoreańscy hakerzy zaatakowali rosyjskie firmy?**

**W ciągu dwóch ostatnich tygodni analitycy firmy Check Point monitorowali podejrzaną aktywność wymierzoną w rosyjskie firmy, która stanowi dotąd niespotykaną relację pomiędzy atakującym a ofiarą. Po raz pierwszy w historii zaobserwowano coś, co wyglądało na skoordynowany atak Korei Północnej na cele znajdujące się na terytorium Rosji. Pomimo tego, że powiązanie ataków z konkretną grupą hakerską jest problematyczne, analiza ujawnia istotne powiązania z taktyką, technikami i narzędziami używanymi przez północnokoreańską grupę APT - Lazarus.**

Jak informują specjaliści Check Pointa, odkrycia dokonano podczas śledzenia wielu złośliwych dokumentów pakietu Office, które zostały zaprojektowane i wykonane specjalnie pod kątem rosyjskich ofiar. Po ich bliższych oględzinach udało nam się powiązać je z wczesnym etapem scenariusza ataku, który finalnie prowadził do zaktualizowanego wariantu wszechstronnego backdoora grupy Lazarus nazwanego przez US-CERT [KEYMARBLE](https://www.us-cert.gov/ncas/analysis-reports/AR18-221A).

Czasami nazywany Hidden Cobra (ang. Ukryta Kobra), Lazarus jest jedną z najaktywniejszych grup APT. Niesławna grupę, będącą organizacją sponsorowaną przez północnokoreański rząd, uważa się za odpowiedzialną za kilka z największych włamań internetowych ostatniej dekady. Mowa tu między innymi o [zhakowaniu Sony Pictures Entertainment](https://en.wikipedia.org/wiki/Sony_Pictures_hack), [oszustwo bankowe w Bangladeszu](https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/) oraz wiele innych poważnych operacji, takich jak kradzież kryptowalut o wartości wielu milionów dolarów z przynajmniej pięciu różnych [giełd kryptowalutowych](https://www.coindesk.com/north-korean-hacking-group-lazarus-stole-571-million-in-cryptos-report) na całym świecie.

Pomimo tego, że czas trwania kampanii pokrywa się z doniesieniami z zeszłotygodniowego [raportu](https://blog.alyac.co.kr/2105) ESTsecurity na temat kampanii “Operation Extreme Job”, której ofiarami były południowokoreańskie firmy związane z bezpieczeństwem, zaobserwowano inne taktyki, techniki i procedury zastosowane w tych dwóch operacjach.

W społeczności cyberbezpieczeństwa od dłuższego czasu panuje przekonanie, że Lazarus jest podzielony na co najmniej dwa oddziały: pierwszy nazywa się Andariel i skupia głównie na atakach na południowokoreański rząd i organizacje, a drugi to Bluenoroff, którego głównym celem jest monetyzacja i kampanie szpiegowskie.

Różnice pomiędzy dwoma kampaniami przeprowadzanymi w tym samym czasie zdaje się potwierdzać teorię o wielu oddziałach.

Incydent ten stanowi jednakże nietypowy wybór ofiary północnokoreańskich hakerów. Zwykle ich ataki odzwierciedlają geopolityczne napięcia pomiędzy Koreą Północną a krajami takimi jak USA, Japonia czy Korea Południowa. W tym przypadku jednak, celem były rosyjskie organizacje.

**Przebieg ataku**

Podczas analiz eksperci Check Pointa spotkali się z dwoma różnymi scenariuszami infekcji. Główny scenariusz składa się z trzech kroków:

1. Pobranie pliku ZIP zawierającego dwa dokumenty: niezainfekowanego dokumentu PDF oraz złośliwego dokumentu Word zawierającego makra.

2. Złośliwe makra pobiera skrypt VBS z konta Dropbox, po czym następuje uruchomienie pobranego skryptu.

3. Skrypt VBS pobiera plik CAB z serwera dropzone, rozpakowuje plik EXE z backdoorem korzystając z windowsowego narzędzia expand.exe, a następnie uruchamia go.

Początkowo, scenariusz składał się ze wszystkich powyższych kroków, ale w którymś momencie atakujący zdecydowali się pomijać drugi krok i makra w dokumencie Word zostały zmodyfikowane, aby bezpośrednio pobierać i uruchamiać backdoora Lazarus z etapu trzeciego.