Bitdefender

Rosyjska grupa hakerska APT29 wykorzystała systemy wymiany informacji do ataków na rządy krajów europejskich

20.03.2023

Niedawno zauważono, że powiązana z Rosją hakerska grupa APT29 wykorzystuje legalne europejskie systemy wymiany informacji do przeprowadzania ataków na jednostki rządowe. Organizacja cyberprzestępcza, znana również jako The Dukes, Cosy Bear, SVR Group i NOBELIUM, rozpoczęła bezwzględną kampanię wymierzoną w systemy komunikacyjne i organizacje dyplomatyczne krajów europejskich.

Rosyjska grupa hakerska APT29 przeprowadza nową kampanię phishingową

Sprawcy wysyłali do swoich celów e-maile z treściami typu spear

phishing, zawierające linki do dokumentów z niebezpiecznymi, złośliwymi plikami.

Aby skłonić ofiary do kliknięcia w niebezpieczny link i zainfekować ich urządzenia, rosyjscy hakerzy wykorzystali jako przynętę między innymi harmonogram na rok 2023 jednego z ambasadorów Polski oraz legalne systemy, takie jak eTrustEx i LegisWrite. Cyberprzestępcy umieścili nawet złośliwy plik na oficjalnej stronie internetowej biblioteki, prawdopodobnie przejętej na początku tego roku.

Kampania przeciwko krajom Unii Europejskiej

„LegisWrite to program do edycji, który umożliwia bezpieczne tworzenie, poprawianie i wymianę dokumentów między rządami w Unii Europejskiej" — czytamy w poradniku bezpieczeństwa firmy Blackberry. „Użycie LegisWrite w charakterze wabika wskazuje, że cyberprzestępca stojący za tą przynętą bierze na cel organizacje państwowe w Unii Europejskiej".

Wejście w jeden z tych niebezpiecznych linków spowodowałoby pobranie pliku HTML na maszynę ofiary. Po analizie specjaliści do spraw cyberbezpieczeństwa ujawnili, że pliki były iteracją trojanów NOBELIUM i EnvyScout – śledzonego jako ROOTSAW.

EnvyScout po pobraniu wykorzystuje techniki przemytu HTML, aby upuścić dodatkowy plik IMG lub ISO na zainfekowane maszyny. Zawartość plików graficznych zawierała różne zaszyfrowane ciągi

znaków, które miały na celu dalsze rozprzestrzenianie się infekcji, pozwalając sprawcom zbierać informacje, przenosić je do centrum dowodzenia i utrwalać na komputerach ofiar.

„Od ponad roku obserwujemy znaczący wzrost liczby cyberataków przeprowadzanych przez rosyjskich hakerów. Celem coraz częściej stają się nie tylko firmy komercyjne, lecz także podmioty o krytycznym znaczeniu dla funkcjonowania państwa oraz instytucje rządowe. Niestety trend ten jest nie tylko widoczny w naszym kraju, lecz także na całym szeroko pojętym Zachodzie" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/rosyjska-grupa-hakerska-apt29/

Data udostępnienia: 20.03.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia

bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.