Bitdefender

Nowa kampania hakerska z wykorzystaniem złośliwej aplikacji NullMixer

30.03.2023

Zespół Security Affair zaobserwował wzmożoną aktywność cyberprzestępców, którzy obrali za cel internautów we Włoszech i Francji i atakują ich za pomocą złośliwej aplikacji NullMixer.

Nowa niebezpieczna kampania skierowana jest głównie przeciwko urządzeniom z systemami operacyjnymi Windows, w tym Windows 10 Professional, Enterprise i Server. Ponadto eksperci znaleźli ofiary wśród użytkowników systemu Windows Embedded, co wskazuje, że złośliwe oprogramowanie przedostało się również do urządzeń IoT.

Nowa kampania hakerska

Złośliwe oprogramowanie NullMixer jest znane z upuszczania szeregu niebezpiecznych komponentów na docelowe systemy, w tym programów kradnących lub szpiegujących, programów do pobierania i trojanów

bankowych. Po uzyskaniu dostępu do punktów końcowych przestępcy kradną poufne dane i sprzedają je na czarnym rynku.

Sprawcy wykorzystują różne techniki rozprzestrzeniania szkodliwego oprogramowania, takie jak metody socjotechniczne i zatruwanie SEO. Podczas niedawnej kampanii NullMixer hakerzy zachęcali administratorów systemów do pobierania zainfekowanych wersji popularnych narzędzi do konserwacji komputerów PC z backdoorem. Dzięki temu uzyskali możliwość przejęcia urządzeń niczego nie spodziewających się użytkowników sieci.

„Pakiet NullMixer zawiera nowe polimorficzne moduły zewnętrznych dostawców usług MaaS i PPI na rynkach podziemnych, a także fragmenty kontrowersyjnego, potencjalnie powiązanego z Koreą Północną kodu PseudoManuscript" – czytamy w raporcie technicznym Security Affair .

NullMixer – nowa złośliwa aplikacja

Raport Security Affair głosi, że kampania NullMixer naruszyła ponad 8 000 maszyn w ciągu zaledwie 30 dni, „ze szczególnym naciskiem na cele w Ameryce Północnej, Włoszech i Francji".

Specjaliści do spraw cyberbezpieczeństwa wskazują również, że złośliwe oprogramowanie wykorzystuje podstawowe techniki unikania obrony, takie jak sprawdzanie obecności kontrolerów wideo używanych przez struktury emulacji i wspólne nazwy użytkowników ustanawiane

przez procedury emulacji AV lub sandboxy.

Badacze zauważyli kolejną wskazówkę, która może pomóc w zlokalizowaniu i zneutralizowaniu cyberniebezpieczeństwa. Złośliwe oprogramowanie NullMixer unika wykonywania procedur kradzieży, jeśli zaatakowana maszyna ma ustawiony język systemu krajów WNP (poza Ukrainą), czyli Azerbejdżanu, Armenii, Białorusi, Kazachstanu, Kirgistanu, Mołdawii, Rosji, Tadżykistanu, Turkmenistanu i Uzbekistanu.

„Oprogramowanie szpiegowskie i trojany są niezwykle niebezpieczne nie tylko dla wielkich korporacji i instytutów o znaczeniu krytycznym dla funkcjonowania państwa, lecz także dla zwykłych użytkowników sieci. Zainfekowanie naszego urządzenia może skutkować utratą naszych środków z konta bankowego, a nawet kradzieżą naszej cyfrowej tożsamości. Dlatego, aby tego uniknąć, warto korzystać ze skutecznego antywirusa i dodatkowych modułów ochronnych, takich jak XDR i MDR” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/nowa-kampania-hakerska-nullmixer/

Data udostępnienia: 30.03.2023
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.