CYBERPRZESTĘPCY OPUBLIKOWALI POUFNE DOKUMENTY FIRM PO ATAKU RANSOMWARE

Cyberprzestępcy opublikowali poufne dokumenty firm takich jak Boeing, Lockheed-Martin i SpaceX po cyberataku z użyciem oprogramowania szyfrującego na ich kontrahenta, który odmówił zapłacenia okupu - podaje serwis The Register.

Wśród dokumentów, jakie w internecie opublikowali cyberprzestępcy, znalazły się m.in. formularze do dokonywania płatności, specyfikacje techniczne systemów wojskowych (przypadek Lockheed-Martin) oraz inne poufne informacje. Za ich wyciek odpowiedzialna jest grupa hakerska operująca ransomware DoppelPaymer szyfrującym komputery działające w oparciu o system Windows.

Kontrahent, który został zaatakowany przez hakerów i odmówił zapłaty okupu, to firma Visser Precision zajmująca się projektowaniem oraz produkcją elementów przemysłowych. Dostarcza ona części dla koncernów takich jak Boeing, Tesla, SpaceX, Honeywell, czy Joe Gibbs Racing. Termin płatności upłynął w marcu tego roku. Gang atakujący z użyciem DoppelPaymera, jak przypomina The Register, z reguły żąda od swoich ofiar kwot sięgających tysięcy lub nawet milionów dolarów.

Rzecznik firmy Lockheed-Martin odpowiadając na pytania serwisu dotyczące sytuacji poinformował, iż spółka zdaje sobie sprawę z tego, iż jej dane zostały opublikowane i stosuje "standardowe procedury reagowania na możliwe cyberincydenty w ramach jej łańcucha dostaw". Koncern poinformował też, iż w sposób ciągły inwestuje w cyberbezpieczeństwo i wykorzystuje "wiodące w branży praktyki bezpieczeństwa" celem ochrony wrażliwych danych.

Firma Visser Precision, z której cyberprzestępcy pozyskali opublikowane dane, nie odpowiedziała na pytania The Register w związku ze sprawą.

Serwis podkreśla jednak, że to nie pierwszy przypadek, kiedy gang odpowiedzialny za ransomware DoppelPaymer publikuje wykradzione przez siebie dane ofiar, które nie zapłaciły żądanego okupu. Celem publikacji jest przede wszystkim wywarcie efektu psychologicznego. Jak ocenia The Register, ujawnienie danych poszkodowanych firm ma uświadomić kolejnym ofiarom, jakie ryzyko wiąże się z niezapłaceniem żądanego przez hakerów okupu.

Eksperci z branży cyberbezpieczeństwa, podobnie jak organy ścigania zgadzają się, iż uleganie żądaniom cyberprzestępców nie jest dobrym wyjściem z sytuacji. Znacznie lepiej przed skutkami ataków ransomware zabezpiecza robienie zapasowych kopii danych i przechowywanie ich offline, a także właściwe zabezpieczanie swojej infrastruktury teleinformatycznej - oceniają.