Grupul Lazarus revine cu o noua campanie de spionaj în industria de aparare (Kaspersky)

Grupul Lazarus, unul dintre cei mai prolifici spioni din mediul cibernetic, deruleaza de la începutul anului 2020, o noua campanie ce vizeaza industria de aparare, informeaza Kaspersky, pe baza unei analize realizate recent.

Conform cercetatorilor, de la începutul anului 2020, industria de aparare a fost vizata de un atac de tip backdoor personalizat, numit ThreatNeedle, un backdoor care se deplaseaza lateral prin retelele infectate colectând informatii importante.

"Lazarus este unul dintre cei mai prolifici actori de amenintare de astazi. Activ cel putin din 2009, Lazarus a fost implicat în campanii de ciberspionaj pe scara larga, campanii de ransomware si chiar atacuri împotriva pietei criptomonedelor. În timp ce în ultimii ani s-au concentrat asupra institutiilor financiare, la începutul anului 2020, se pare ca au adaugat industria de aparare la "portofoliul" lor", sustin expertii,

Potrivit sursei citate, primele indicii referitoare la aceasta campanie au aparut pentru prima data când specialistii Kaspersky au fost contactati de o companie victima ca sa reactioneze la atac si au descoperit ca organizatia în cauza suferise un atac de tip backdoor personalizat (un tip de malware care permite controlul complet, de la distanta, asupra dispozitivului).

Pâna în prezent, organizatii din peste 12 tari au fost afectate, noteaza compania de securitate cibernetica.

"Infectia initiala avea loc prin spear phishing; tintele primeau e-mailuri care contineau fie un atasament Word rau intentionat, fie un link ce face legatura cu serverele companiei. De multe ori, e-mailurile sustineau ca sunt necesare actualizari urgente legate de pandemia globala si pretindeau ca provin de la un centru medical respectat. Odata ce documentul rau intentionat era deschis, malware-ul era accesat si trecea la urmatoarea etapa a procesului de implementare. Programul malware ThreatNeedle utilizat în aceasta campanie apartine unei familii de malware cunoscuta sub numele de Manuscrypt, care apartine grupului Lazarus si a fost descoperita anterior atacând afacerile cu criptomonede. Odata instalat, ThreatNeedle este capabil sa obtina controlul complet al dispozitivului victimei, ceea ce înseamna ca poate face orice, de la manipularea fisierelor pâna la executarea comenzilor primite", au explicat specialistii.

Raportul acestora releva faptul ca una dintre cele mai interesante tehnici din aceasta campanie a fost capacitatea grupului de a fura date atât din retelele IT de birou (o retea care contine computere cu acces la internet), cât si din reteaua restrictionata a unei centrale (una care contine active critice si computere cu date foarte sensibile, fara acces la internet). #Conform politicilor companiei, între aceste doua retele nu se transferau informatii. Cu toate acestea, administratorii se puteau conecta la ambele retele pentru a le întretine. Lazarus a reusit sa obtina controlul statiilor de lucru ale administratorilor si apoi a creat un gateway rau intentionat pentru a ataca reteaua restrictionata si pentru a fura si extrage date confidentiale de acolo", sustin reprezentantii companiei.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) este un proiect global lansat de Kaspersky în 2016 pentru a coordona eforturile vânzatorilor de sisteme de automatizare, ale proprietarilor si operatorilor de instalatii industriale si ale cercetatorilor în domeniul securitatii IT pentru a proteja organizatiile industriale de atacurile cibernetice.