Kaspersky avertizeaza asupra virusului “Sunburst” care ataca dispozitivele clientilor IT ai companiilor

Un nou malware, botezat "Sunburst", utilizat de infractorii cibernetici împotriva clientilor IT a unor companii din domeniu a fost descoperit în luna decembrie a anului trecut, informeaza Kaspersky, într-un comunicat transmis, luni, AGERPRES.

Noua amenintare a fost identificata dupa ce, pe data de 13 decembrie 2020, FireEye, Microsoft si SolarWinds au anuntat descoperirea unui atac cibernetic sofisticat asupra lantului de aprovizionare.

În acest sens, si expertii Kaspersky au gasit diferite asemanari la nivel de cod între Sunburst si versiunile cunoscute ale backdoor-urilor Kazuar - tipul de malware care ofera acces de la distanta la dispozitivele victimelor.

"În timp ce studiau backdoor-ul Sunburst, expertii Kaspersky au descoperit o serie de caracteristici similare cu cele ale unui Kazuar identificat anterior, un backdoor scris folosind reteaua .NET, raportat pentru prima data de Palo Alto în 2017 si utilizat în atacurile cibernetice de spionaj din întreaga lume. Multiple similitudini la nivel de cod sugereaza o legatura între Kazuar si Sunburst, desi natura acesteia este, înca, nedeterminata. Similitudinile dintre Sunburst si Kazuar includ algoritmul de generare UID al victimei, algoritmul de inactivitate (sleeping algorithm) si utilizarea extinsa a hash-ului FNV-1a", explica specialistii.

Potrivit expertilor, aceste fragmente de cod nu sunt 100% identice si sugereaza ca între Kazuar si Sunburst poate exista o legatura, dar natura acestei relatii nu este înca clara. Dupa ce malware-ul Sunburst a fost lansat pentru prima data, în februarie 2020, Kazuar a continuat sa evolueze, iar variantele din 2020 sunt si mai asemanatoare, în anumite privinte, cu Sunburst.

"Legatura identificata nu scoate la iveala cine a fost în spatele atacului SolarWinds, însa ofera mai multe informatii care pot ajuta cercetatorii sa avanseze în aceasta investigatie. Consideram ca este important ca si alti cercetatori din întreaga lume sa investigheze aceste asemanari si sa încerce sa descopere mai multe informatii despre Kazuar si originea Sunburst, malware-ul folosit în bresa SolarWinds. Din experienta trecuta, de exemplu analizând atacul WannaCry, stim ca în primele zile au existat foarte putine indicii care sa îl lege de grupul Lazarus. În timp, însa, au aparut tot mai multe dovezi care ne-au permis sa facem legatura între grup si atac cu mai mare încredere. Cercetarile suplimentare pe aceasta tema sunt cruciale pentru a pune cap la cap informatiile", comenteaza Costin Raiu, directorul echipei globale de cercetare si analiza Great a Kaspersky.

Specialistii în securitate cibernetica sustin ca, desi asemanarile între Kazuar si Sunburst sunt relevante, ar putea exista o multime de motive pentru existenta lor, inclusiv faptul ca Sunburst este dezvoltat de acelasi grup care dezvolta si Kazuar, atacatorii din spatele Sunburst folosind Kazuar ca punct de inspiratie.

Un alt motiv poate fi reprezentat de mutarea unuia dintre dezvoltatorii Kazuar în echipa Sunburst sau faptul ca ambele grupuri din spatele Sunburst si Kazuar au obtinut malware din aceeasi sursa.