CyberArk : Cyberattaques contre lâ□□Ukraine, analyse.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 28/2/2022 13:00:00

Outre les attaques militaires sur son sol, lâ□□Ukraine fait Ã©galement face actuellement Ã des cyberattaques massives.

Lavi Lazarovitz, Head of Security Research chez CyberArk, analyse ci-dessous ces campagnes malveillantes imputÃ©es au malware HermeticWiper:

Â« Le CyberArk Labs a suivi l'Ã©mergence du logiciel malveillant de type "wiper", surnommÃ© HermeticWiper, qui cible l'infrastructure ukrainienne. Jusqu'Ã prÃ©sent, notre Ã©quipe a identifiÃ© quelques caractÃ©ristiques spÃ©cifiques qui rendent ce malware unique, notamment le fait que les attaques ont Ã©tÃ© trÃ¨s ciblÃ©es et que les infections observÃ©es jusqu'Ã prÃ©sent s'appuient sur des identitÃ©s compromises pour se dÃ©placer latÃ©ralement, ce qui conduit potentiellement Ã un fort ancrage initial en raison de leur nature.

Plus prÃ©cisÃ©ment, la distribution de ce malware ne semble pas tirer parti des vulnÃ©rabilitÃ©s de la supply chain, ou tout autre technique de "super propagation", ce qui signifie que l'infection ne s'Ã©tendra pas rapidement Ã d'autres zones gÃ©ographiques.

Dans un cas Ã©tudiÃ©, le ransomware s'est dÃ©ployÃ© en utilisant la stratÃ©gie de groupe d'Active-Directory, ce qui signifie que les cybercriminels avaient un accÃ¨s Ã privilÃ¨ges Ã AD. Ce scÃ©nario est plus couramment utilisÃ© dans les incidents ciblÃ©s, opÃ©rÃ©s par des humains ; comme ce fut dans le cas dans lâ□□attaque contre lâ□□entreprise Kaseya.

Il est important de noter que le wiper utilise des privilÃ¨ges Ã©levÃ©s sur l'hÃ´te compromis pour le rendre "non bootable", en remplaÃ§ant les enregistrements et les configurations de dÃ©marrage, en effaÃ§ant les configurations des pÃ©riphÃ©riques et en supprimant les sauvegardes automatiques.

Il semble que le wiper soit configurÃ© pour ne pas chiffrer les contrÃ´leurs de domaine - c'est-Ã -dire pour maintenir le domaine en fonctionnement et permettre au ransomware d'utiliser des identifiants valides pour s'authentifier auprÃ¨s des serveurs et chiffrer ceux-ci. Cela met encore plus en Ã©vidence que les cybercriminels utilisent des identitÃ©s compromises pour accÃ©der au rÃ©seau et/ou se dÃ©placer latÃ©ralement. Â»