Severity

High

Analysis Summary

BlackCat — aka AlphaVM & AlphaV — is a Ransomware family that is deployed as a part of a Ransomware as a Service (RaaS). It is written in the Rust programming language and can run on Windows, Linux-based operating systems (Debian, Ubuntu, ReadyNAS, Synology), and VMWare ESXi. This ransomware first appeared in November 2021. The majority of the group's victims have been in the United States, although BlackCat and its associates have also targeted organizations in Europe, the Philippines, and other regions. Construction and engineering, retail, transportation, commercial services, insurance, machinery, professional services, telecommunication, auto components, and medicines are among the targeted sectors of BlackCat ransomware. This ransomware can be set to encrypt files using either the AES or ChaCha20 algorithms. It can destroy volume shadow copies, terminate programs and services, and stop virtual machines on ESXi servers to maximize the quantity of ransomed data.

Recently, the Federal Bureau of Investigation (FBI) of the United States published a flash report stating that BlackCat ransomware had compromised at least 60 organizations globally since its inception in November.

Indicators Of Compromise

IP

- 89[.]44[.]9[.]243
- 37[.]120[.]238[.]58
- 45[.]153[.]160[.]140
- 94[.]232[.]41[.]155
- 142[.]234[.]157[.]246
- 152[.]89[.]247[.]207
- 23[.]106[.]223[.]97
- 45[.]134[.]20[.]66
- 198[.]144[.]121[.]93
- 139[.]60[.]161[.]161
- 185[.]220[.]102[.]253
- 89[.]163[.]252[.]230
- 146[.]0[.]77[.]15

MD5

- 861738dd15eb7fb50568f0e39a69e107
- 20855475d20d252dda21287264a6d860
- 82db4c04f5dcda3bfcd75357adf98228
- 91625f7f5d590534949ebe08cc728380
- a3cb3b02a683275f7e0a0f8a9a5c9e07
- 173c4085c23080d9fb19280cc507d28d
- 817f4bf0b4d0fc327fdfc21efacddaee

SHA-256

- 7d8671c91a02bfbff8b89a76501b9be017a66a8bba624ed4fe2c7f81b9380ac9
- 1b90e6f959db883fb4a036dac06242be724a7637708058e2c439e2250222d6d1
- 8ee191b51b853addc862307c8f641bd251a8b7dd88263d228453bb06882f2464
- 3c300726a6cdd8a39230f0775ea726c2d42838ac7ff53bfdd7c58d28df4182d5
- 31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc
- 731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161

- f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb

SHA-1

- e96950f2b7a9c1cdd542ab5bce025303a0b032f9
- 04589618b18ed1e073768bd5669127aaf916c4f1
- b310f72d967b265fb82cdee21ad75b3c7b90bc20
- bf1b0ab5a2c49bde5b5dbe828df3e69af5d724c2
- d241df7b9d2ec0b8194751cd5ce153e27cc40fa4
- a186c08d3d10885ebb129b1a0d8ea0da056fc362
- 8917af3878fa49fe4ec930230b881ff0ae8d19c9

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.