Achieving this necessitates consistent collaborative and information sharing efforts. SentinelLabs remains dedicated to continue to do so. The activities this post discusses illustrate the intricate nature of the Chinese threat landscape.

The threat actors drop Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan executables vulnerable to and deploy .NET executables based on the agentupdate_plugins.exe and libcef.dll functions, such that specific functions, when invoked by the legitimate executables, decrypt and execute code embedded and gain access to sensitive user data and communications.

The Malware Loaders

The group is known to use two different malware loaders, namely Adobe CEF Helper.exe and mfeann.exe. The executables are components of the software products Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan.

A China-based ransomware operator active since 2021. The group is known for its active operations against various targets, including US utilities and overseas branches.

The group focuses on deploying a variety of ransomware families, such as LockFile, AtomSilo, NightSky, and others. This association is based on naming conventions, code, and functional overlaps with the sample described in ESET's research. The group is also known to be involved in other campaign families, such as DEV-0401.

The threat actors have adapted another Cobalt Strike malleable C2 profile, which is also available in a Second-Stage Data URLs.

The group's activities include the deployment of domains, SS7 certificates, and SSL certificates. The threat actors have been observed deploying a variety of domains, including microsofts[.]org, BRONZE STARLIGHT, and others. The certificates use on Alibaba IPs.

The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others. The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others.

The group's operations have been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others. The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others.

The threat actors have used various tactics to achieve their objectives, including exploiting vulnerabilities in popular software products, such as Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan. The group has been observed to use a variety of techniques, including the use of various tools and techniques, such as agentupdate_plugins.exe, AdventureQuest.exe, and others.

The group's operations have been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others. The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others.

The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others. The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others.

The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others. The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others.

The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others. The group has been observed to use a variety of tools and techniques, including agentupdate_plugins.exe, AdventureQuest.exe, and others.