Incident Report: Ragnar Locker

Summary:

This report details the tactics, techniques, and procedures (TTPs) employed by the Ragnar Locker ransomware gang, as documented by various cybersecurity research organizations. Ragnar Locker, active since December 2019, has targeted organizations in the energy, critical manufacturing, financial services, government, and information technology sectors. The ransomware gang is part of a larger ransomware family, working with multiple ransomware variants and threat actor groups.

Attack Details:

The Ragnar Locker gang gains initial access to target networks through two primary methods: brute-forcing passwords for the Remote Desktop Protocol (RDP) service or purchasing stolen RDP credentials on the black market.

Once the attackers gain access to the network, they exploit a vulnerability in the Windows COM Aggregate Marshaler (CVE-2017-0213) to elevate their privileges to administrator-level access. This is achieved by running a specially crafted application designed to exploit the vulnerability.

If the privilege escalation attempt is unsuccessful, the attackers resort to using Group Policy Modification and PowerShell to move laterally across the network, infecting other computers. They use the Microsoft Installer (msiexec.exe) to pass parameters to a remote web server, which hosts a malicious MSI package. The package contains an old version of Oracle VirtualBox and a stripped-down Windows XP virtual disk image (VDI) that includes the Ragnar Locker ransomware.

Before deploying the ransomware, the attackers perform various reconnaissance and defense evasion techniques. They check the system language settings and terminate the ransomware process if the machine's default language matches one on the Commonwealth of Independent States (CIS) list. The attackers also use a batch script to stop various security-related processes and services, disable Windows AutoPlay notifications, delete volume shadow copies, and enumerate local and network drives to be accessed by the ransomware.

The attackers then run the VirtualBox VM and load the Windows XP image containing the ransomware. The VM is configured to map all local drives as read/writable, allowing the ransomware to encrypt files on the host system. Before encrypting files, the ransomware steals sensitive data and exfiltrates it to one or more servers, in case the victim refuses to pay the ransom.

The Ragnar Locker ransomware encrypts files using the Salsa20 algorithm, with the encrypted key data and a signature appended to the end of each file. The ransomware code is protected with obfuscation techniques, such as junk code and encryption, to evade detection by security software.