Ransomware deploys virtual machines to hide itself from antivirus software

By Catalin Cimpanu

Published: 2020-05-22 · Archived: 2026-04-05 22:38:05 UTC

The operators of the RagnarLocker ransomware are installing the VirtualBox app and running virtual machines on computers they infect in order to run their ransomware in a "safe" environment, outside the reach of local antivirus software.

This latest trick has been spotted and detailed today by UK cyber-security firm Sophos and shows the creativity and great lengths some ransomware gangs will go to avoid detection while attacking a victim.

What's RagnarLocker?

Avoiding detection is crucial because RagnarLocker is not your typical ransomware gang. They're a group that carefully selects targets, avoiding home consumers, and goes after corporate networks and government organizations only.

Sophos says the group has targeted victims in the past by abusing internet-exposed RDP endpoints and has compromised MSP (managed service provider) tools to breach companies and gain access to their internal networks.

On these networks, the RagnarLocker group deploys a version of their ransomware -- customized per each victim -- and then demands an astronomical decryption fee in the tune of tens and hundreds of thousands of US dollars.

Because each of these carefully planned intrusions represents a chance to earn large amounts of money, the RagnarLocker group has put a primer on stealth and has recently come up with a novel trick to avoid detection by antivirus software.

The virtual machine trick

The "trick" is actually pretty simple and clever when you think of it.

Instead of running the ransomware directly on the computer they want to encrypt, the RagnarLocker gang downloads and installs Oracle VirtualBox, a type of software that lets you run virtual machines.

The group then configures the virtual machine to give it full access to all local and shared drives, allowing the virtual machine to interact with files stored outside its own storage.

The next step is to boot up the virtual machine, running a stripped-down version of the Windows XP SP3 operating system, called MicroXP v0.82.

The final phase is to load the ransomware inside the virtual machine (VM) and run it. Because the ransomware runs inside the VM, the antivirus software won't be able to detect the ransomware's malicious process.

From the antivirus software's point of view, files on the local system and shared drives will suddenly be replaced with their encrypted versions, and all the file modifications appear to come from a legitimate process -- namely the VirtualBox app.

Mark Loman, director of engineering and threat mitigation at Sophos told ZDNet today that this is the first time he's seen a ransomware gang abuse virtual machines during an attack.

"In the last few months, we've seen ransomware evolve in several ways. But, the Ragnar Locker adversaries are taking ransomware to a new level and thinking outside of the box," he added.

An overview of the entire RagnarLocker ransomware, including its VM trick, is available in Sophos' recent report.

Editorial standards
