Maze Ransomware Adopts Ragnar Locker Virtual-Machine Approach

4 minute read

Author:
Tara Seals

Share this article:

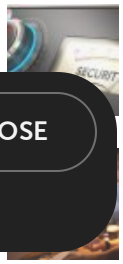
INFOSEC INSIDER

Securing Your Move to the Hybrid Cloud
August 1, 2022

Why Physical Security Maintenance Should Never Be an Afterthought
July 25, 2022

Conti's Reign of Chaos: Costa Rica in the Crosshairs
July 20, 2022

How War Impacts Cyber Insurance
July 12, 2022



Maze continues to adopt tactics from rival cybercrime gangs.

The operators of the Maze ransomware have added a fresh trick to their bag of badness: Distributing ransomware payloads via virtual machines (VM). It's a "radical" approach, according to researchers, meant to help the ransomware get around endpoint defense.

That's according to researchers with Sophos Managed Threat Response (MTR), who said that the threat actors were recently seen distributing the malware in the form of a VirtualBox virtual disk image (a VDI file). The VDI file itself was delivered inside of a Windows MSI file, which is a format used for installation, storage and removal of programs.

In order to set up the VM on the target, "the attackers also bundled a stripped down, 11-year-old copy of the VirtualBox hypervisor inside the .MSI file, which runs the VM as a 'headless' device, with no user-facing interface," researchers said, in a Thursday posting.

The VM would run as a trusted application, which helps the ransomware conceal itself. Also, most endpoint solutions only have visibility into physical drives, not VMs – virtual environments usually require their own separate security monitoring solution.

"Since the...ransomware application runs inside the virtual guest machine, its process and behaviors can run unhindered, because they're out-of-reach for security s

'legitimate' VboxHeadless.exe process, the VirtualBox virtualization software."

In employing the strategy, the Maze authors are taking a page from the Ragnar Locker ransomware, according to Sophos' analysts, who uncovered the latter using the same technique earlier this year.

"In an earlier attack, Ragnar Locker also deployed a virtual machine in an attempt to bypass protection measures," Sophos researchers explained. In that attack, they added, "Ragnar Locker was deployed inside an Oracle VirtualBox Windows XP virtual machine. The attack payload was a 122 MB installer with a 282 MB virtual image inside—all to conceal a 49 KB ransomware executable."

Technical Details

In the Maze ransomware incident, the attack payload was a 733 MB installer with a 1.9 GB Windows 7 virtual image inside (uncompressed) — concealing a 494 KB ransomware executable.

The file sizes are much larger than the Ragnar Locker approach. The Maze infection routine included an installer for both the 32-bit and 64-bit versions of VirtualBox 3.0.4 inside of the MSI file, for one (the VirtualBox version dates back to 2009 and is still branded with its then-publisher's name, Sun Microsystems). And, the threat actors chose to use Windows 7.

"Using a virtual Windows 7 machine instead of XP significantly increases the size of the virtual disk, but also adds some new functionality that wasn't available in the Ragnar Locker version," according to the Sophos writeup.

The root of the virtual disk contains three files associated with the Maze ransomware: preload.bat, vrun.exe (the VM itself) and a file just named payload (with no file extension), which is the actual Maze DLL payload.

"The preload.bat file (shown below) modifies the computer name of the virtual machine, generating a series of random numbers to use as the name, and joins the virtual machine to the network domain of the victim organization's network using a WMI command-line function," explained Sophos analysts.

For persistence, the malware also adds a file named startup_vrun.bat to the Windows Start menu.

"The script copies the same three files found on the root of the VM disk (the vrun.exe and payload DLL binaries, and the preload.bat batch script) to other disks, then issues a command to shut down the computer immediately," according to the analysis. "When someone powers the computer on again, the script executes vrun.exe."

When the MSI file first runs, the VM creates the C:\SDRSMLINK\ folder location, which acts as a clearinghouse for specific folders the malware wants to track – Maze does so using symbolic links (symlinks), which act as shortcuts to folders on the local hard drive. This folder is shared with the rest of the network.

Ultimately, a batch script called starter.bat is used launch the ransomware payload from within the VM.

Recon Before Deployment

Sophos researchers said that telemetry analysis revealed t

"The attackers had spent days preparing to launch the ransomware by building lists of IP addresses inside the target's network, using one of the target's domain controller servers and exfiltrating data to cloud storage provider Mega.nz," researchers explained.

Also, the VM was apparently configured in advance by someone who was intimately familiar with the victim's network, they said.

The threat actors initially demanded a $15 million ransom from the target of the attack. The target did not pay the ransom, according to Sophos.

The [virtual machine's] configuration file (micro.xml) maps two drive letters that are used as shared network drives in this particular organization, presumably so it can encrypt the files on those shares as well as on the local machine," according to the analysis.

Meanwhile, the operators behind the Maze ransomware have been busy in 2020, usually going after very high-profile fish. In June Maze attacked a U.S. military contractor involved in the maintenance of the country's Minuteman III nuclear arsenal. In April they hit IT services giant Cognizant, causing service disruptions; Cognizant, a Fortune 500 company, employs close to 300,000 people. The malware was also behind the December cyberattack on the City of Pensacola, Fla., which shut down the city's computer networks and affected its systems. Other targets have included Allied Systems and Pitney Bowes.

The Maze operators continue to evolve their tactics as well. For instance, they often now carry out "double

a dedicated web page, which lists the identities of their

non-cooperative victims and regularly publishes samples of the stolen data. This so far includes details of dozens of companies, including law firms, medical service providers and insurance companies, that have not given in to their demands.

"The Maze threat actors have proven to be adept at adopting the techniques demonstrated to be successful by other ransomware gangs, including the use of extortion as a means to extract payment from victims," Sophos researchers concluded. "As endpoint protection products improve their abilities to defend against ransomware, attackers are forced to expend greater effort to make an end-run around those protections."

Malware