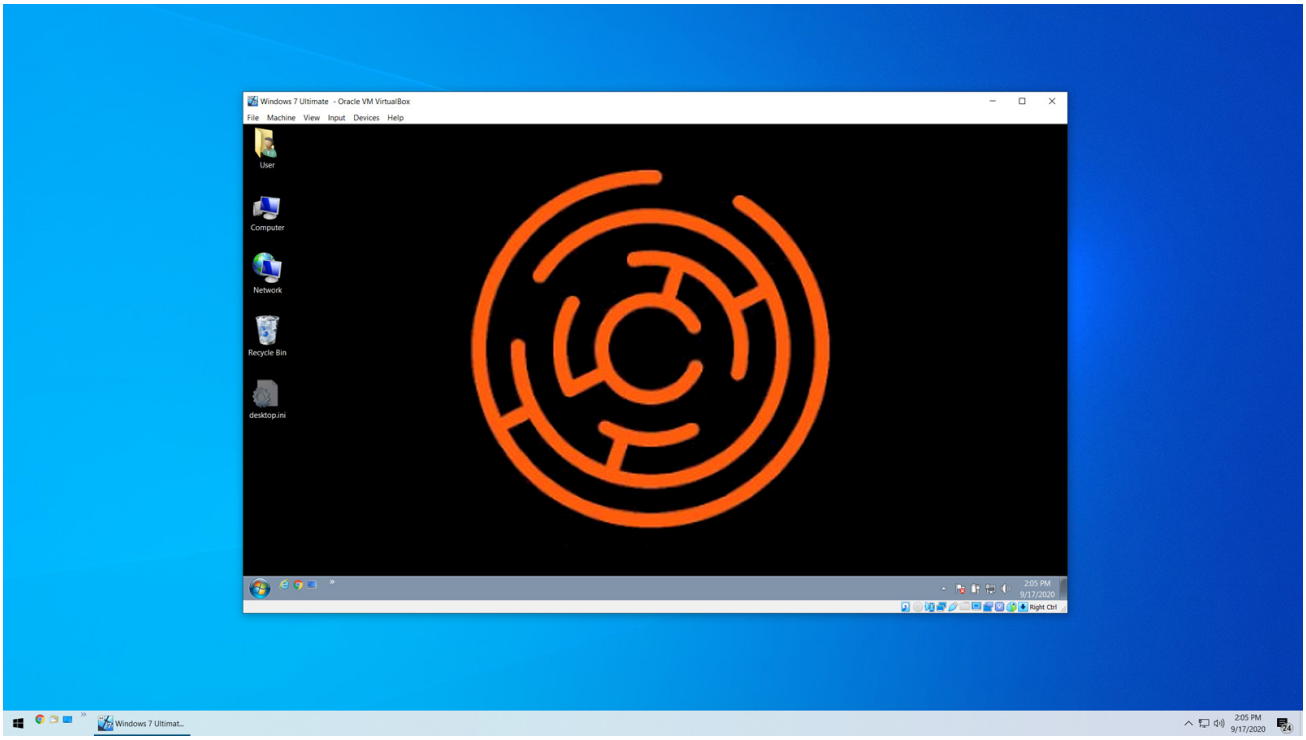
Maze ransomware now encrypts via virtual machines to evade detection

bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/

Lawrence Abrams

By
Lawrence Abrams

- September 17, 2020
- 02:24 PM
- 6



The Maze ransomware operators have adopted a tactic previously used by the Ragnar Locker gang; to encrypt a computer from within a virtual machine.

In May, we previously reported that Ragnar Locker was seen encrypting files through VirtualBox Windows XP virtual machines to bypass security software on the host.

The virtual machine would mount a host's drives as remote shares and then run the ransomware in the virtual machine to encrypt the share's files.

As the virtual machine is not running any security software and is mounting the host's drives, the host's security software could not detect the malware and block it.

Maze now uses virtual machines to encrypt computers

While performing an incident response for one of their customers, Sophos discovered Maze had attempted to deploy their ransomware twice but were blocked by Sophos' Intercept X feature.

For the first two attempts, the Maze attacker attempted to launch various ransomware executables using scheduled tasks named 'Windows Update Security,' or 'Windows Update Security Patches,' or 'Google Chrome Security Update.'

After the two failed attacks, Sophos' Peter Mackenzie told BleepingComputer that the Maze threat actors tried a tactic previously used by the Ragnar Locker ransomware.

In their third attack, Maze deployed an MSI file that installed the VirtualBox VM software on the server along with a customized Windows 7 virtual machine.

Once the virtual machine was started, like the previous Ragnar Locker attacks, a batch file called startup_vrun.bat batch file would be executed that preps the machine with the Maze executables.

```
@echo off
ping -n 6 127.0.0.1>nul
start explorer \\VBOXSVR\1\
if exist C:\vrun.exe goto o
:a
if exist \\VBOXSVR\1\builder\vrun\vrun.exe goto b
ping -n 2 127.0.0.1>nul
goto a
:b
copy /y \\VBOXSVR\1\builder\vrun\vrun.exe C:\vrun.exe
copy /y \\VBOXSVR\1\builder\vrun\payload C:\payload
copy /y \\VBOXSVR\1\builder\vrun\preload C:\preload.bat
C:\preload.bat
shutdown /s /f /t 1
exit
:o
C:\vrun.exe
```

SOPHOSlabs

Batch file to launch Maze ransomware on VM

The machine is then shut down, and once restarted again, will launch vrun.exe to encrypt the host's files.

As the virtual machine is performing the encryption on the host's mounted drives, security software could not detect the behavior and stop it.

The SophosLabs researchers note that this is an expensive attack method in terms of disk size compared to Ragnar Locker's previous attacks.

As Ragnar Locker's VM attack utilized Windows XP, the total footprint was only 404 MB in size. As Maze used Windows 7, the footprint was much larger at a total of 2.6 GB.

This attack illustrates how ransomware operations monitor the tactics of their competitors and adopt them as necessary.

It should also be noted that Ragnar Locker is part of the 'Maze Cartel,' so it is possible that Ragnar offered help to Maze in this attack method.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Hive ransomware ports its Linux VMware ESXi encryptor to Rust

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

SpiceJet airline passengers stranded after ransomware attack

- Maze
- Ragnar Locker
- Ransomware
- Virtual Machine
- VirtualBox

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 
  zakish7 - 1 year ago
  -
  -
  This wouldn't work if sharing was disabled in VM's settings right?
- 
  qwertyanon - 1 year ago
  -
  -
  probably not, we should ask them to disable it when they launch the vm. :p
- 
  Lawrence Abrams - 1 year ago
  -
  -
  It's a customized VM installation. They control the settings.

- 
  zakish7 - 1 year ago
  -
  -
  Appreciate the reply -- my bad, didn't notice the payload was an entire VM :)

- 
  testa - 1 year ago
  -
  -
  So the way to protect from VM attacks is to disable virtualization in BIOS right if you don't use VM?

  Maybe anti-virus could be implemented to read contents inside VM disks. 7-zip can read them and extract just fine unless encrypted

- 
  jasonanwe - 1 year ago
  -
  -
  Disable Windows (MSI) Installer via GPO (i.e., Enable 'Turn off Windows Installer'). Then only those with admin rights can install (and no one should be primarily working from an ID with admin rights). Guide: https://www.top-password.com/blog/turn-off-windows-installer-to-block-msi-package/

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: