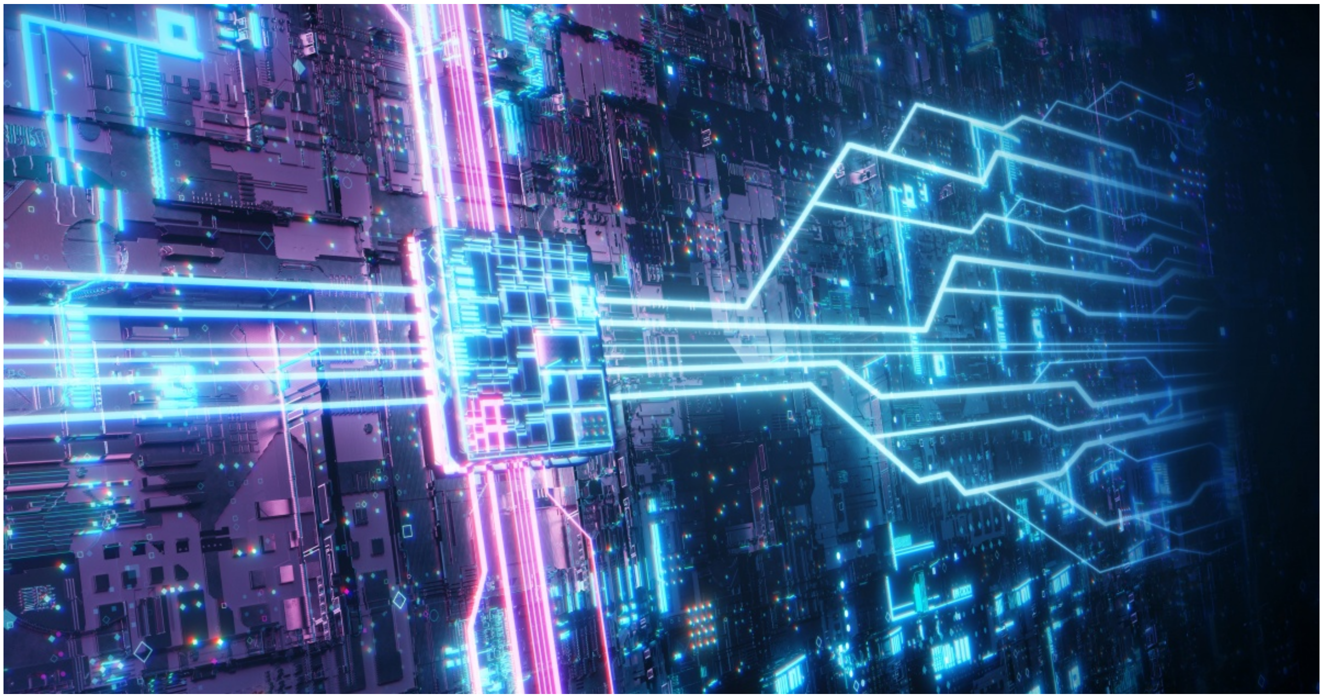
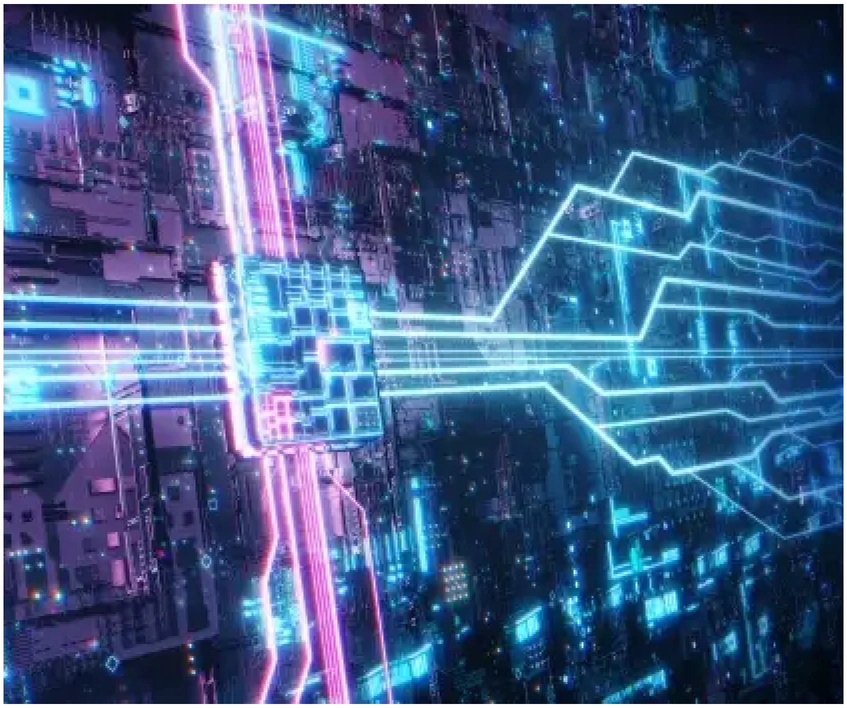
Ransomware: Growing Number of Attackers Using Virtual Machines

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-virtual-machines





Threat Hunter TeamSymantec

Tactic hides ransomware payload and lowers the risk of discovery while encryption process is underway.

Symantec has found evidence that an increasing number of ransomware attackers are using virtual machines (VMs) in order to run their ransomware payloads on compromised computers. The motivation behind the tactic is stealth. In order to avoid raising suspicions or triggering antivirus software, the ransomware payload will "hide" within a VM while encrypting files on the host computer.

The tactic is a recent development, having been documented by Sophos in connection with RagnarLocker last year. In that case, ransomware was run from inside an Oracle VirtualBox Windows XP VM.

VirtualBox usage

During a recent investigation into an attempted ransomware attack, Symantec discovered that the attackers had installed a VirtualBox VM on some compromised computers. Unlike the previously documented RagnarLocker attacks, which involved Windows XP, the VM in this case appeared to be running Windows 7.

The VM was delivered to the target via a malicious installer file that used various file names, including:

- fuckyou.msi
- fuck.msi
- aa51978f.msi
- s3c.msi

The installer created a file called runner.exe, which was a Golang (Go) executable compiled from the following source file:

```
C:/builder/runner/main.go
```

Apart from standard Go libraries, it used the go-ps library for process enumeration. Embedded strings used by the executable, such as file names, process names, and commands, were obfuscated using four-byte XOR keys. Each string was encrypted using a unique key.

This executable depended on multiple other files that were expected to be present in the same directory. Its main purpose was to install a VirtualBox VM in a headless mode.

When executed, runner.exe performed following actions:

- It checked if it was running on Active Directory (AD) controller based on whether the *C:\Windows\SYSVOL* directory was present. It exited if the check proved true.
- It used a function named russianDetect to check if it was running on a system using a Russian keyboard layout (0x0419). It exited if the check proved true. Checks such as this are a common feature of targeted ransomware attacks.
- It enumerated running processes and services and terminated any that were present on blacklists (procBlacklist, servicesBlacklist) using *taskkill.exe* and *sc.exe.*

The executable then dropped, executed, and deleted a file called starter.bat with the following content in order to mount a recovery partition:

> *mountvol E:\ \\?\Volume{<ID>}*

It then decrypted and dropped VirtualBox.xml, a VirtualBox configuration file, and micro.xml, a VM configuration file (see appendix). It created an SDRSMLINK directory and linked system files to that directory, e.g:

> *cmd /C mklink /j "%SYSTEMROOT%\SDRSMLINK\Program Files" "%SYSTEMROOT%\Program Files"*

It also adjusted the "<SharedFolders>" section in micro.xml to reflect files and directories linked in CSIDL_WINDOWS\SDRSMLINK. It then initialized VirtualBox components:

It enumerated and cleared Windows system logs using WEvtUtil.exe:

Symantec did not obtain a VM image, but what likely occurred next was that the ransomware payload was located on the VM's disk and auto started once the operating system was fully booted. The VM likely had access to the host computer’s files and directories (via "SharedFolders" set up by runner.exe), allowing it to encrypt files on the host computer.

Conti or Mount Locker?

While the payload running in the VM was not identified, there were reasonably strong indicators that it was Conti. A username and password combination (nuuser/[email protected]) used in these attacks was previously associated with older Conti activity, dating from April 2021.

However, on the same computer that the VM was deployed on, Symantec also observed Mount Locker being deployed, raising the question as to whether the payload was actually Mount Locker. Since the main purpose of running a payload on a VM is to avoid detection, it doesn’t make much sense for the attacker to also deploy the payload on the host computer.

One possible explanation is that the attacker is an affiliate operator with access to both Conti and Mount Locker. They may have attempted to run a payload (either Conti or Mount Locker) on a virtual machine and, when that didn’t work, opted to run Mount Locker on the host computer instead.

Obfuscating malicious activity

Ransomware operators are continually refining their tactics in a bid to stay one step ahead of detection. Many are now heavily relying on legitimate and dual-use tools in order to stage attacks on targeted networks. The ransomware payload itself is often the stage of the attack most likely to raise red flags and, by hiding it in a virtual machine, there is an expectation that it may not be discovered. Organizations should exercise increased vigilance in relation to the unauthorized installation of virtual machines on their networks.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

- 2eae8e1c2e59527b8b4bb454a51b65f0ea1b0b7476e1c80b385f579328752836 - Installer
- 9f801a8d6b4801b8f120be9e5a157b0d1fc3bbf6ba11a7d202a9060e60b707d8 - runner.exe
- e5291bae18b0fa3239503ab676cacb12f58a69eb2ec1fd3d0c0702b5a29246cb - VirtualBox
- d89bd47fb457908e8d65f705f091372251bae3603f5ff59afb2436abfcf976d8 - Mountlocker
- 8f247e4149742532b8a0258afd31466f968af7b5ac01fdb7960ac8c0643d2499 - Mountlocker

Appendix

VirtualBox.xml - VirtualBox configuration file

Micro.xml - virtual machine configuration file

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?