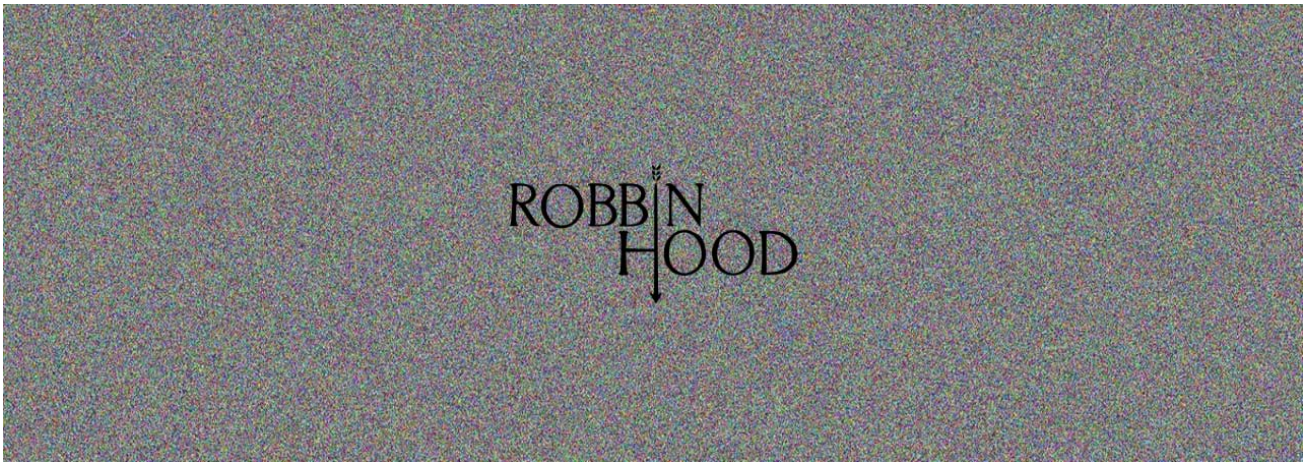
Ransomware Exploits GIGABYTE Driver to Kill AV Processes

bleepingcomputer.com/news/security/ransomware-exploits-gigabyte-driver-to-kill-av-processes/

Lawrence Abrams

By
Lawrence Abrams

- February 6, 2020
- 12:37 PM
- 0



The attackers behind the RobbinHood Ransomware are exploiting a vulnerable GIGABYTE driver to install a malicious and unsigned driver into Windows that is used to terminate antivirus and security software.

When performing a network-wide compromise, ransomware attackers need to push out a ransomware executable as quickly as possible and to as many systems as they can to avoid being detected.

One protection that can get in their way of a successful attack, though, is antivirus software running on a workstation that removes the ransomware executable before it can be executed.

To overcome this hurdle, the operators behind the RobbinHood Ransomware are utilizing a custom antivirus killing package that is pushed out to workstations to prepare it for encryption.

Using trusted drivers to terminate security processes

Most Windows security software processes are protected from being terminated by regular processes and can only be terminated by Kernel drivers, which have the highest permission possible in Windows.

To better secure Windows, Microsoft added a driver signature enforcement policy that prevents the installation of Windows Kernel drivers unless they have been cosigned by Microsoft.

This prevents attackers and malware from installing their malicious drivers that can gain kernel-level privileges without first being reviewed by Microsoft.

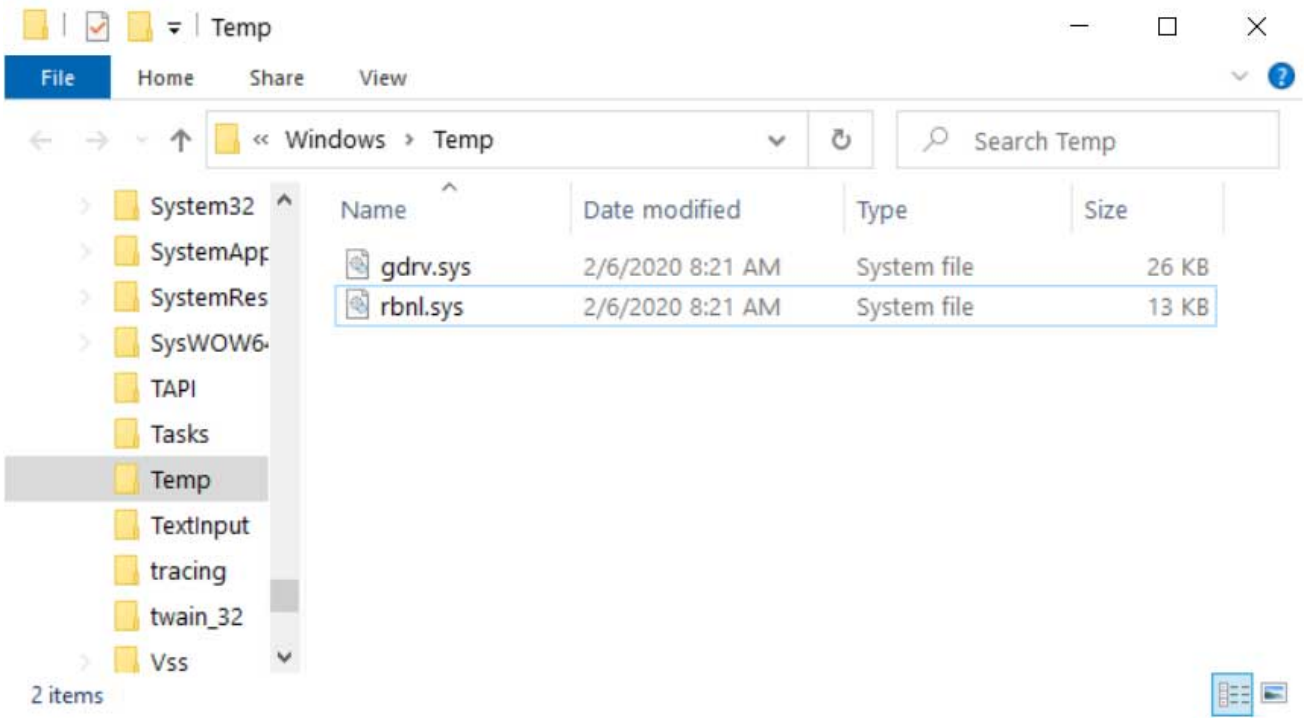
In a new report, Sophos researchers have seen the RobbinHood attackers installing a known vulnerable GIGABYTE driver that has been cosigned by Microsoft and exploiting its vulnerability to disable Microsoft's driver signature enforcement feature.

Once disabled, they can install a custom malicious kernel driver that is used to terminate antivirus and security software processes.

"In this attack scenario, the criminals have used the Gigabyte driver as a wedge so they could load a second, unsigned driver into Windows," Sophos' report explains. "This second driver then goes to great lengths to kill processes and files belonging to endpoint security products, bypassing tamper protection, to enable the ransomware to attack without interference."

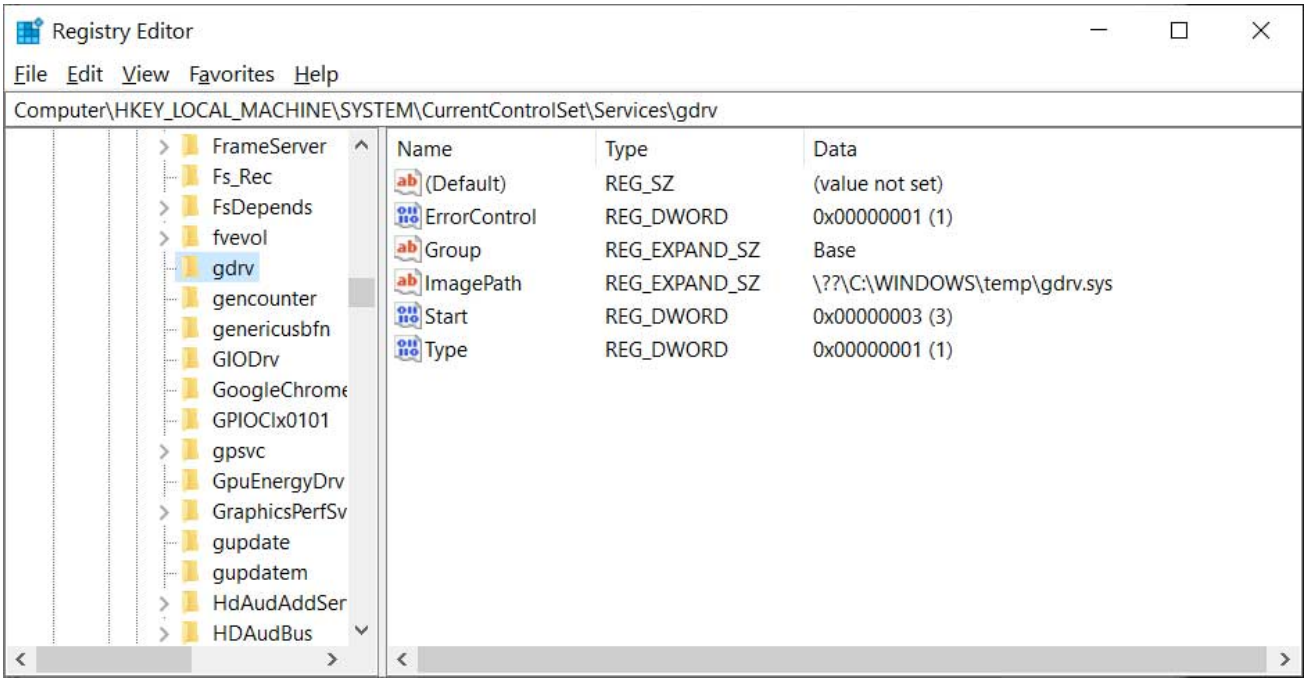
The attack starts with the operators deploying an executable named Steel.exe to exploit the CORE-2018-0007 vulnerability in the GIGABYTE gdrv.sys driver.

When executed, Steel.exe extracts the ROBNR.EXE executable to the C:\Windows\Temp folder. This will cause two drivers to be extracted to the folder; the vulnerable GIGABYTE gdrv.sys driver and the malicious RobbinHood driver called rbnl.sys.



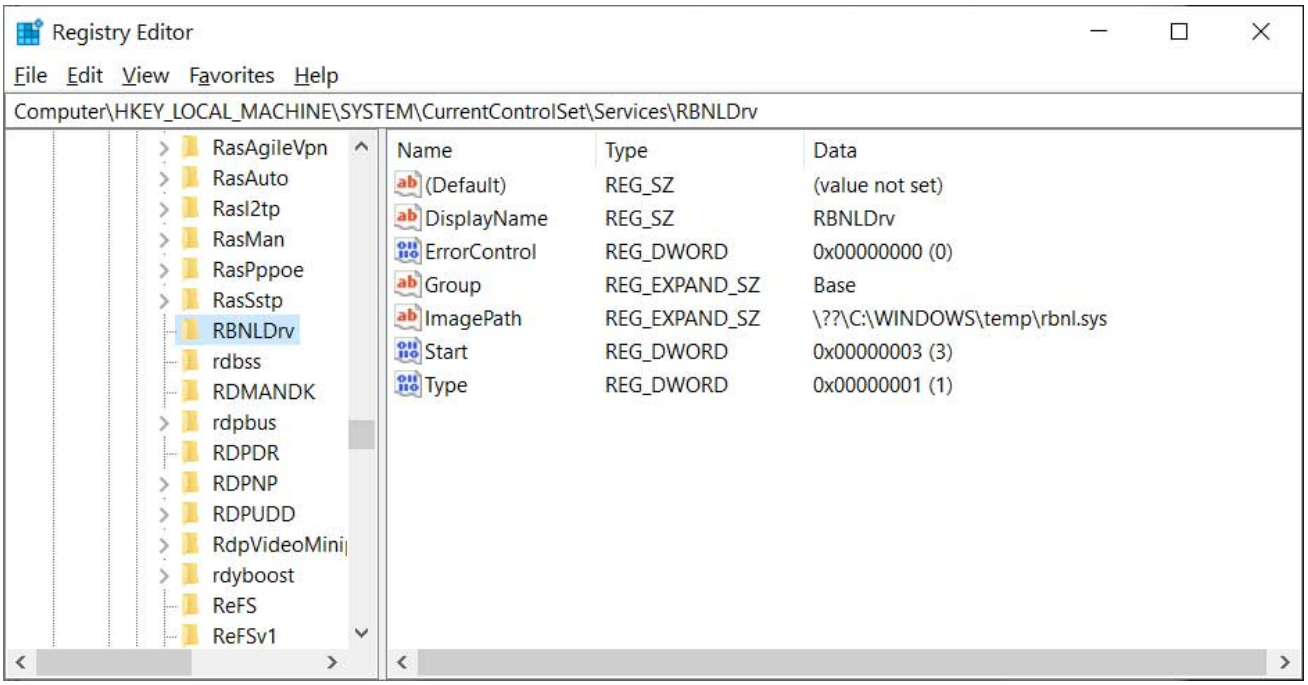
Drivers in the Windows Temp Folder

ROBNR will now install the GIGABYTE driver and exploit it to disable Windows driver signature enforcement.



Installed vulnerable GIGABYTE gdrv.sys driver

Once driver signature enforcement is disabled, ROBNR can now install the malicious rbnl.sys driver, which will be used by Steel.exe to terminate and delete antivirus and security software.



Installed RobbinHood driver that kills processes

The Steel.exe program will read the list of processes that should be terminated and services whose files should be deleted from a file called **PLIST.TXT**. It will then look for each of the listed processes or files and either terminate or delete them.

```
__int64 __fastcall SuperKillFile(wchar_t *FileName)
{
  wchar_t *fileName; // rbx@1

  fileName = FileName;

  KillFileTrick1_ZwDeleteFile(FileName);
  KillFileTrick2_ZwSetInformationFile(fileName);
  KillFileTrick3_Irp(fileName);
  KillFileTrick4(fileName);
  KillFileTrick5(fileName, 1);
  KillFileTrick6(fileName);
  KillFileTrick7(fileName);
  return 0i64;
}
```

Code used by the driver to delete files

Source: Sophos

At this time, Sophos has told BleepingComputer that they have been unable to gain access to the PLIST.TXT file and do not know what processes and services are being targeted.

When Steel.exe has finished terminating security software, the ransomware will now be able to encrypt a computer without fear of being detected.

With the high payouts of network-wide ransomware attacks, attackers are investing a lot of resources into new and innovative methods to bypass security software and protections in Windows.

As these attacks cannot take place without a network first being compromised, the best way to protect yourself is to make the network less vulnerable.

This includes performing phishing recognition training, making sure security updates are installed, and removing access to Internet exposed services like Remote Desktop Services.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

- Driver
- GIGABYTE
- LoLBin
- Ransomware
- RobbinHood
- Security Software

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

You may also like: