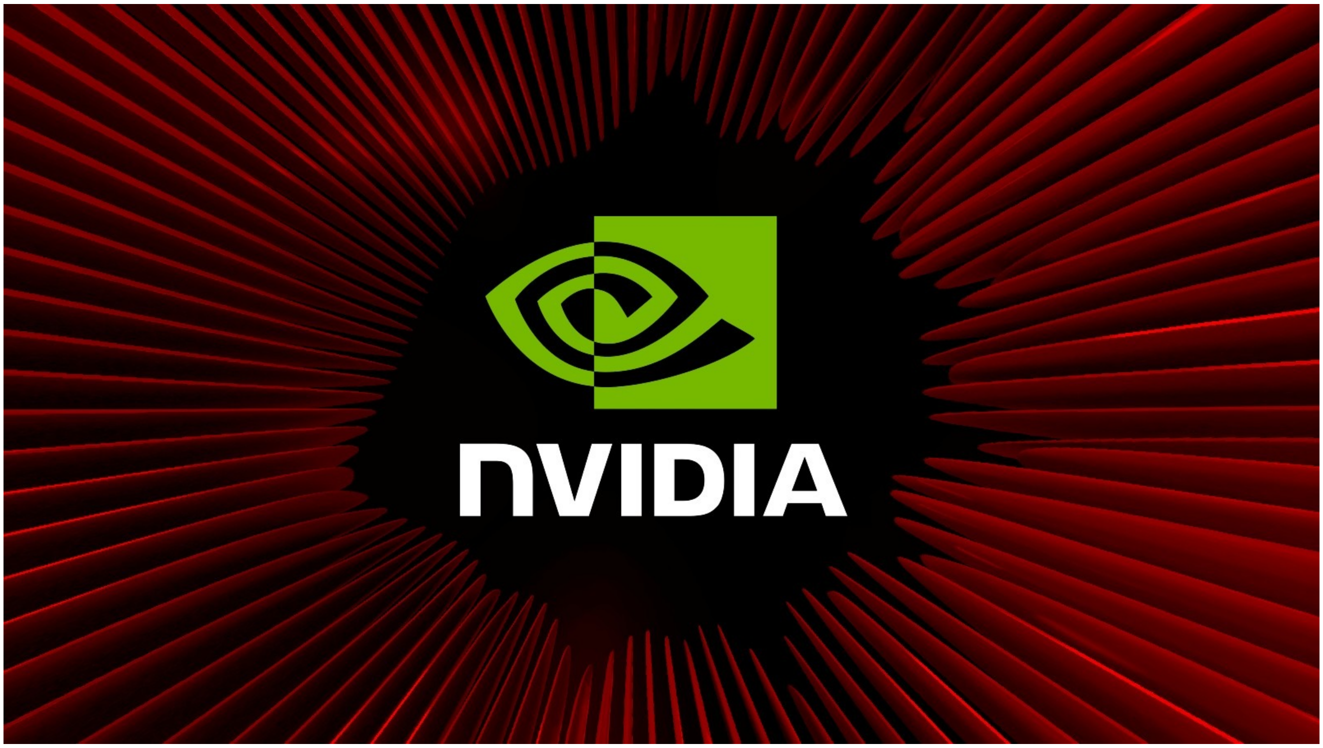
Malware now using NVIDIA's stolen code signing certificates

bleepingcomputer.com/news/security/malware-now-using-nvidias-stolen-code-signing-certificates/

Lawrence Abrams

By
Lawrence Abrams

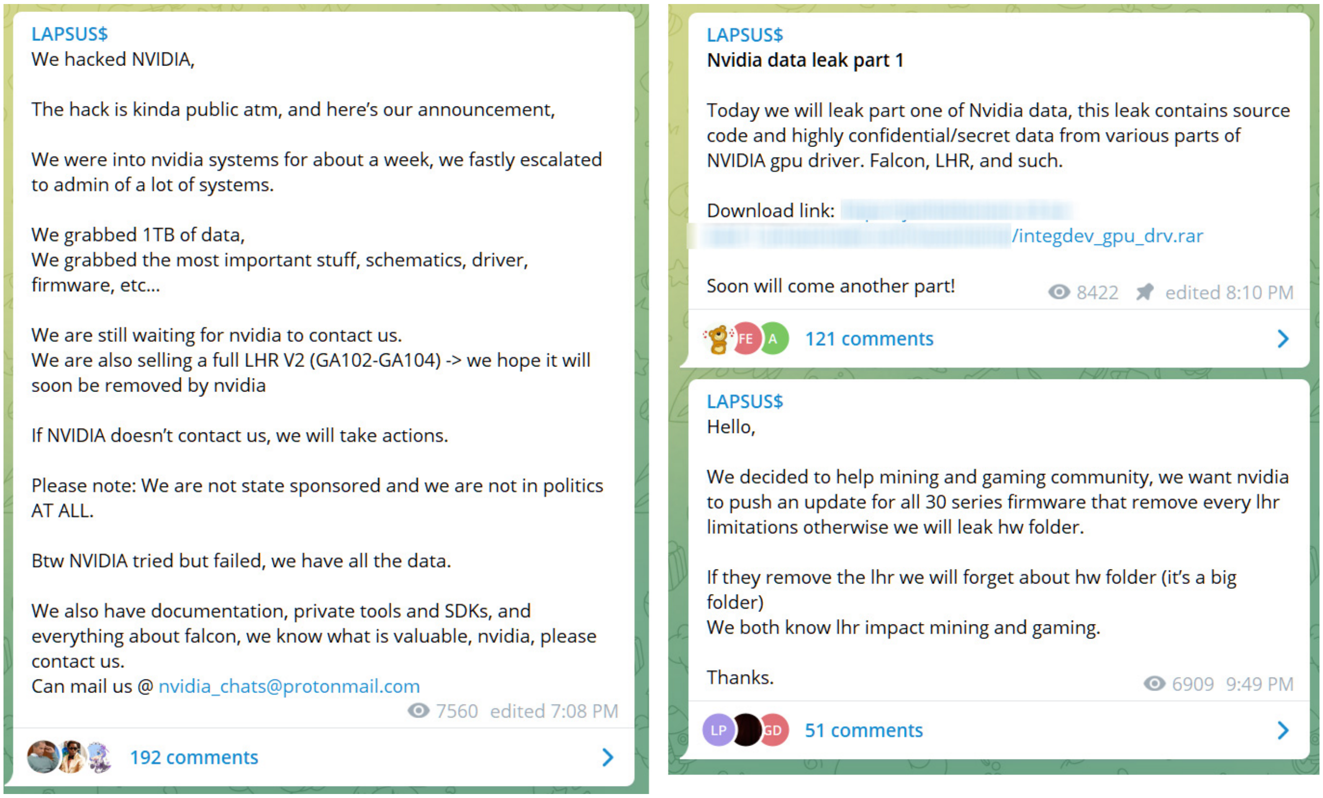
- March 5, 2022
- 03:45 PM
- 4



Threat actors are using stolen NVIDIA code signing certificates to sign malware to appear trustworthy and allow malicious drivers to be loaded in Windows.

This week, NVIDIA confirmed that they suffered a cyberattack that allowed threat actors to steal employee credentials and proprietary data.

The extortion group, known as Lapsus$, states that they stole 1TB of data during the attack and began leaking the data online after NVIDIA refused to negotiate with them.



LAPSUS$
We hacked NVIDIA,

The hack is kinda public atm, and here's our announcement,

We were into nvidia systems for about a week, we fastly escalated to admin of a lot of systems.

We grabbed 1TB of data,
We grabbed the most important stuff, schematics, driver, firmware, etc...

We are still waiting for nvidia to contact us.
We are also selling a full LHR V2 (GA102-GA104) -> we hope it will soon be removed by nvidia

If NVIDIA doesn't contact us, we will take actions.

Please note: We are not state sponsored and we are not in politics AT ALL.

Btw NVIDIA tried but failed, we have all the data.

We also have documentation, private tools and SDKs, and everything about falcon, we know what is valuable, nvidia, please contact us.
Can mail us @ nvidia_chats@protonmail.com

7560 edited 7:08 PM

192 comments

LAPSUS$
Nvidia data leak part 1

Today we will leak part one of Nvidia data, this leak contains source code and highly confidential/secret data from various parts of NVIDIA gpu driver. Falcon, LHR, and such.

Download link: [redacted]/integdev_gpu_drv.rar

Soon will come another part!

8422 edited 8:10 PM

121 comments

LAPSUS$
Hello,

We decided to help mining and gaming community, we want nvidia to push an update for all 30 series firmware that remove every lhr limitations otherwise we will leak hw folder.

If they remove the lhr we will forget about hw folder (it's a big folder)
We both know lhr impact mining and gaming.

Thanks.

6909 9:49 PM

51 comments

Lapsus$ messages about the NVIDIA attack

The leak includes two stolen code-signing certificates used by NVIDIA developers to sign their drivers and executables.

> As part of the #NvidiaLeaks, two code signing certificates have been compromised. Although they have expired, Windows still allows them to be used for driver signing purposes. See the talk I gave at BH/DC for more context on leaked certificates: https://t.co/UWu3AzHc66 pic.twitter.com/gCrol0BxHd
>
> — Bill Demirkapi (@BillDemirkapi) March 3, 2022

A code-signing certificate allows developers to digitally sign executables and drivers so that Windows and end-users can verify the file's owner and whether they have been tampered with by a third party.

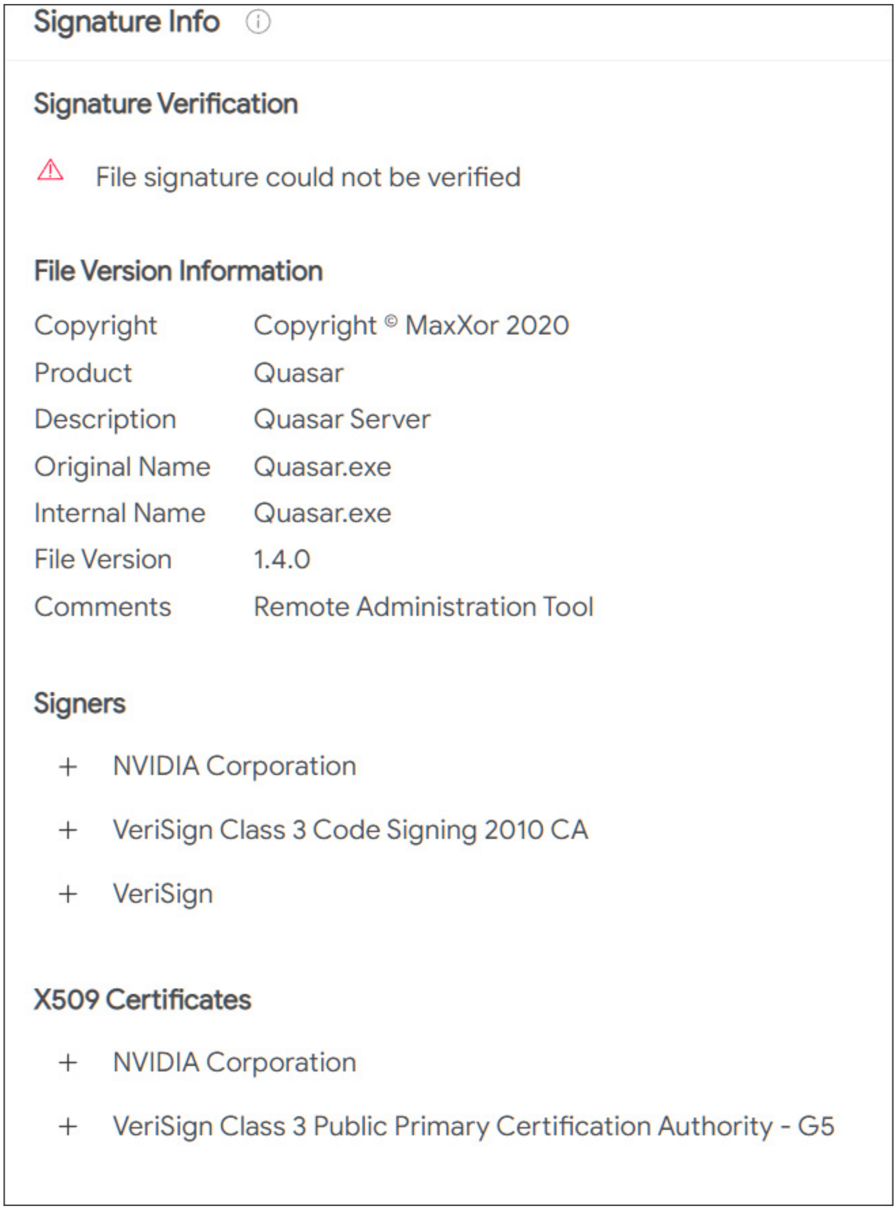
To increase security in Windows, Microsoft also requires kernel-mode drivers to be code signed before the operating system will load them.

NVIDIA certificates used to sign malware

After Lapsus$ leaked NVIDIA's code-signing certificates, security researchers quickly found that the certificates were being used to sign malware and other tools used by threat actors.

According to samples uploaded to the VirusTotal malware scanning service, the stolen certificates were used to sign various malware and hacking tools, such as Cobalt Strike beacons, Mimikatz, backdoors, and remote access trojans.

For example, one threat actor used the certificate to sign a Quasar remote access trojan [VirusTotal], while someone else used the certificate to sign a Windows driver [VirusTotal].



Signature Info

Signature Verification

⚠ File signature could not be verified

File Version Information

Copyright	Copyright © MaxXor 2020
Product	Quasar
Description	Quasar Server
Original Name	Quasar.exe
Internal Name	Quasar.exe
File Version	1.4.0
Comments	Remote Administration Tool

Signers

+ NVIDIA Corporation
+ VeriSign Class 3 Code Signing 2010 CA
+ VeriSign

X509 Certificates

+ NVIDIA Corporation
+ VeriSign Class 3 Public Primary Certification Authority - G5

Quasar RAT signed by NVIDIA certificate

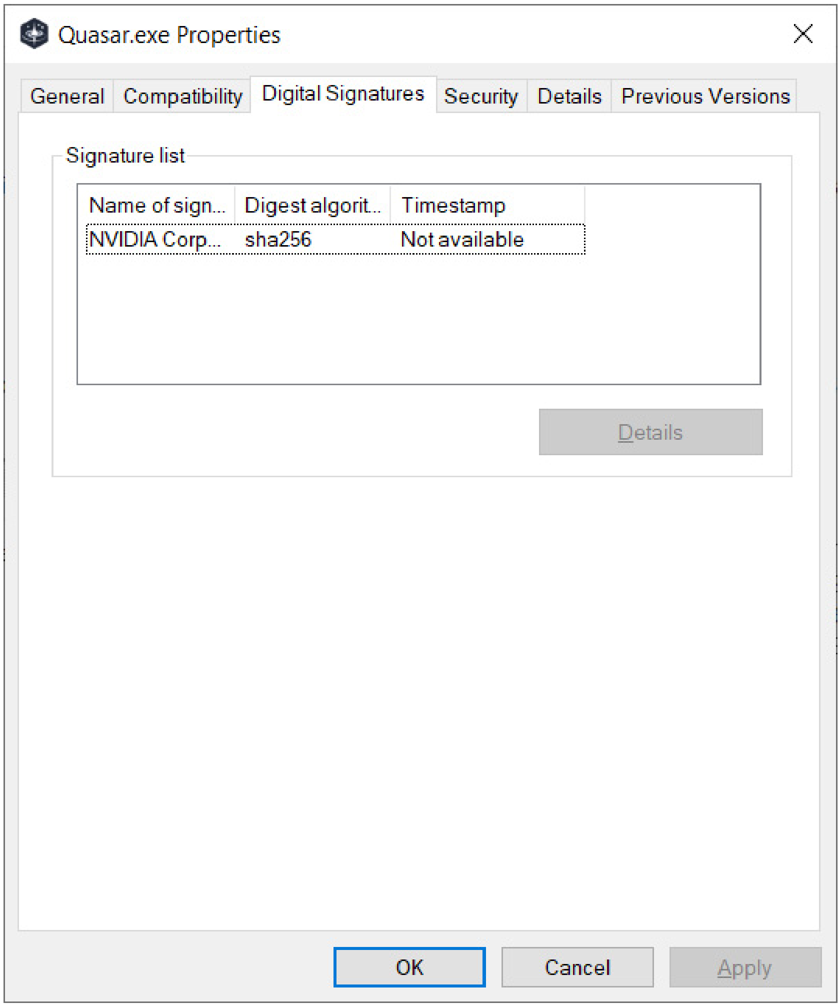
Security researchers Kevin Beaumont and Will Dormann shared that the stolen certificates utilize the following serial numbers:

```
43BB437D609866286DD839E1D00309F5
14781bc862e8dc503a559346f5dcc518
```

Some of the files were likely uploaded to VirusTotal by security researchers but others appear to be used by threat actors for malware campaigns [1, 2].

While both stolen NVIDIA certificates are expired, Windows will still allow a driver signed with the certificates to be loaded in the operating system.

Therefore, using these stolen certificates, threat actors gain the advantage of making their programs look like legitimate NVIDIA programs and allowing malicious drivers to be loaded by Windows.



Name of sign...	Digest algorit...	Timestamp
NVIDIA Corp...	sha256	Not available

Signed Quasar RAT sample

To prevent known vulnerable drivers from being loaded in Windows, David Weston, director of enterprise and OS security at Microsoft, tweeted that admins can configure Windows Defender Application Control policies to control what NVIDIA drivers can be loaded.

> WDAC policies work on both 10-11 with no hardware requirements down to the home SKU despite some FUD misinformation i have seen so it should be your first choice. Create a policy with the Wizard and then add a deny rule or allow specific versions of Nvidia if you need
>
> — David Weston (DWIZZZLE) (@dwizzzleMSFT) March 3, 2022

However, using WDAC is not an easy task, especially for non-IT Windows users.

Due to the potential for abuse, it is hoped that the stolen certificates will be added to Microsoft's certificate revocation list in the future to prevent malicious drivers from loading in Windows.

However, doing so will cause legitimate NVIDIA drivers to be blocked as well, so we will likely not see this happening soon.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

New RansomHouse group sets up extortion market, adds first victims

NVIDIA fixes ten vulnerabilities in Windows GPU display drivers

NVIDIA has open-sourced its Linux GPU kernel drivers

NVIDIA fined for failure to disclose cryptomining sales boost

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.