

Lapsus\$ Ransomware Gang – A Malware in Disguise

blog.checkpoint.com/2022/03/07/lapsus-ransomware-gang-uses-stolen-source-code-to-disguise-malware-files-as-trustworthy-check-point-customers-remain-protected/

March 7, 2022

07/03/2022

Lapsus\$ Ransomware gang uses stolen source code to disguise malware files as trustworthy. Check Point customers remain protected

Background

A ransomware gang named Lapsus\$, which took responsibility for last week's breach on the giant chip firm NVidia, claims it has now managed to breach the Korean manufacturer Samsung, and published 190GB of sensitive data online.

Breaches to major companies aren't a new thing, though in this case the attacker has not just stolen credentials or business related content, it went directly to the crown jewel, which is the source code of some of the companies' proprietary firmware.

Supply chain attacks have grown to unprecedented sizes in recent years

Having possession and controls over such source codes might create a massive supply chain reaction, which can lead to numerous organizations and machines being infected and harmed as both, NVidia's and Samsung's firmware and hardware are massively distributed globally.

The scenario, later described in details, enables malware to enter machines, even if these are supposedly protected by security technology, by having stolen certificates signed and verified as legitimate and trustworthy, when in fact there are malware in disguise.

As well as being one of the top trends in the global cyber security landscape globally, supply chain attacks have increased in numbers and reach over the past year, , even compromising major organizations like US government departments, such as homeland security offices.

In their official public response, NVidia announced: "We have no evidence of ransomware being deployed on the NVIDIA environment or that this is related to the Russia-Ukraine conflict. However, we are aware that the threat actor took employee passwords and some NVIDIA proprietary information from our systems and has begun leaking it online."

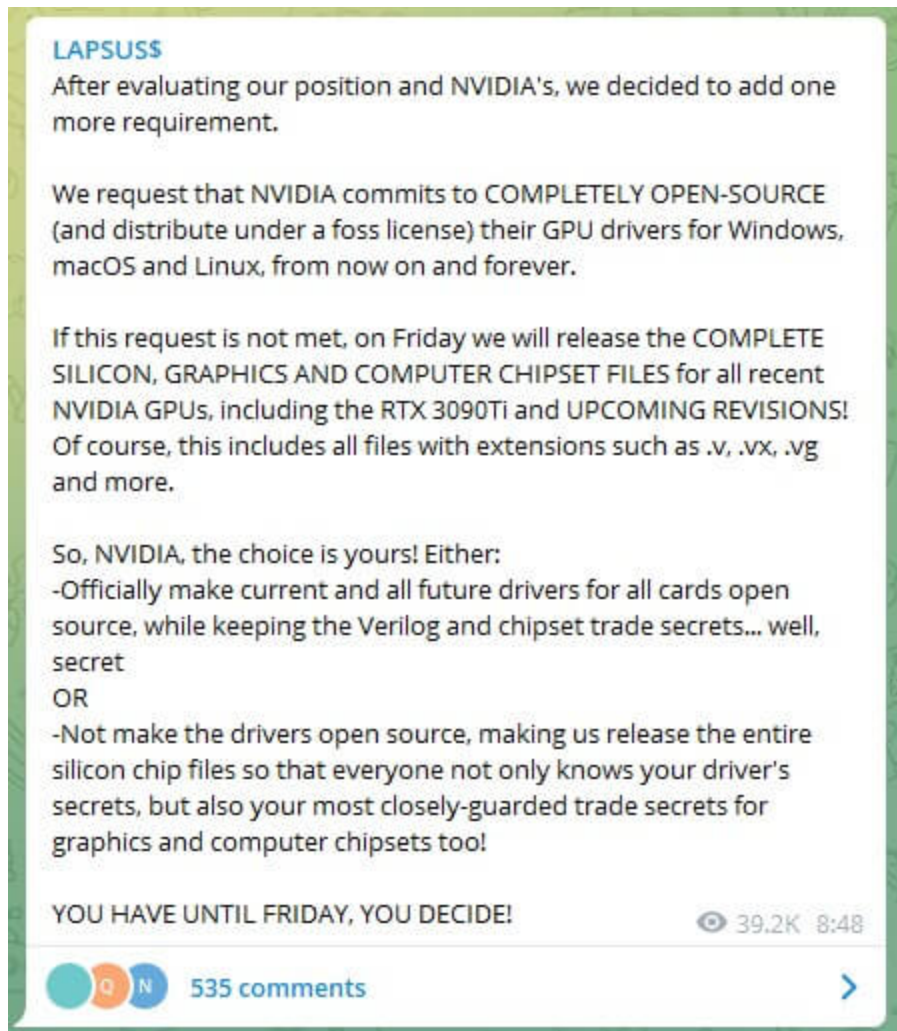
Samsung officially responded and confirmed the breach on Monday, March 7th: “There was a security breach relating to certain internal company data,” said a Samsung official. “According to our initial analysis, the breach involves some source code relating to the operation of Galaxy devices, but does not include the personal information of our consumers or employees. Currently, we do not anticipate any impact to our business or customers”

What do we know on the recent breaches by Lapsus\$?

Through an official notice, NVidia acknowledged that they became aware of “a cyber security incident, which impacted IT resources. Lapsus\$ claimed responsibility and were asking Nvidia to remove its lite hash rate (LHR) feature. The LHR was created to limit Ethereum mining capabilities in its RTX 30 series graphics cards, as the cryptomining community depleted the stock in early 2021. The group is also asking Nvidia to open-source its GPU drivers for macOS, Windows, and Linux devices.

Failing to meet their demands, Lapsus\$ threatened to publish NVidia’s source code, which is used in drivers and firmware. Yet, the gang did not stop there. On March 5th they published nearly 190GB of sensitive data obtained from the Korean technology giant, Samsung.

The group first published a snapshot of C/C++ instructions on Samsung’s software followed with a description of the upcoming leak, stating that it included confidential Samsung’s source code




Source: Telegram

In a later official confirmation, Samsung did confirm that almost 200GB of confidential data which includes source code for various technologies and algorithms for biometric unlock operations has been breached.



How can stolen signed certificates deliver malware?

As part of the NVidia's leak were indeed two stolen code-signing certificates used by NVidia developers to sign their drivers and executables.

According to different sources, attackers already started using this code signing certificates to sign malware so it will appear to be dependable and go through Windows' screening to be loaded and executed.

 **Bill Demirkapi**
@BillDemirkapi

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: youtu.be/1H9tEfKjFXs?t=...

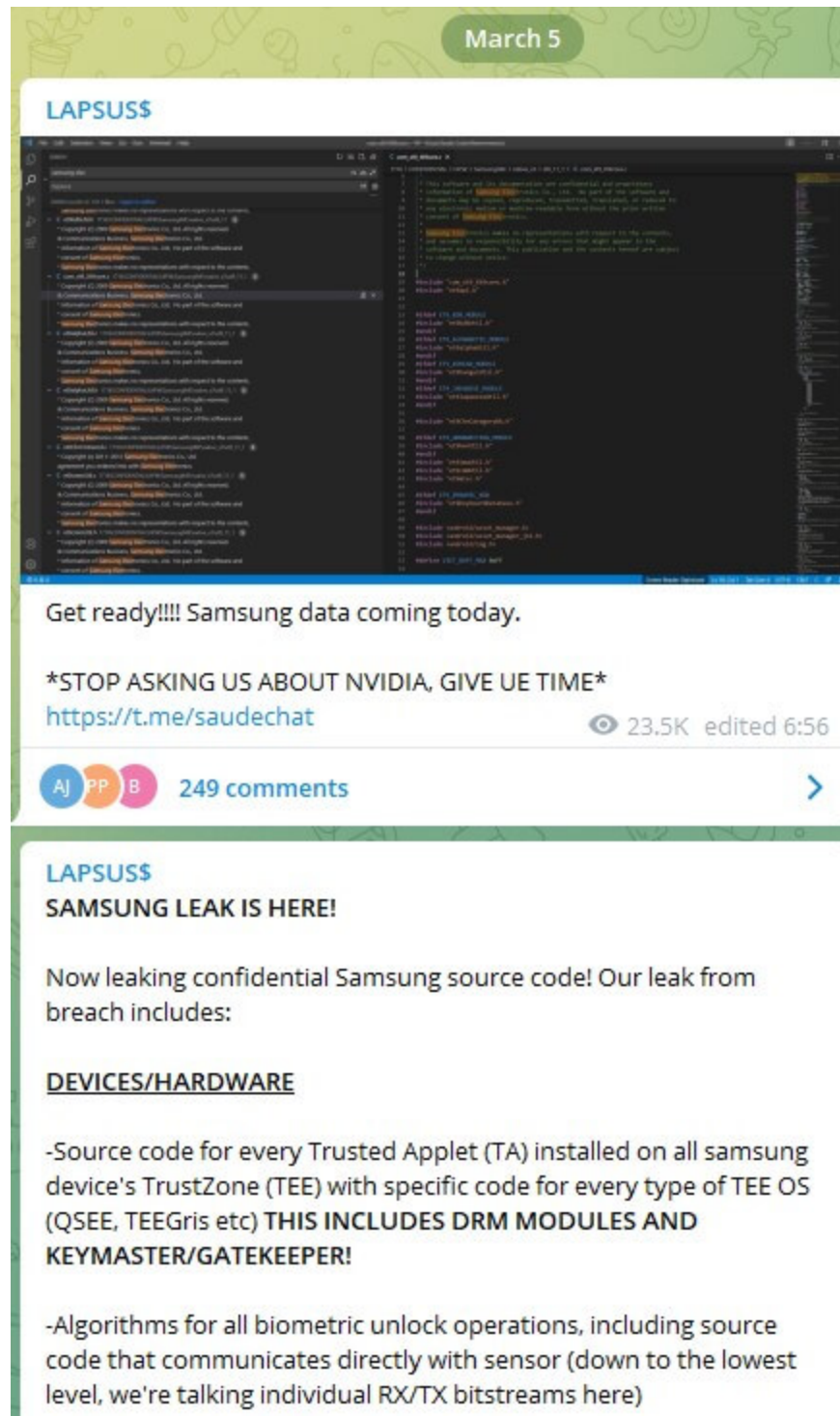
Issued to: NVIDIA C	Issued to: NVIDIA C
Issued by: VeriSign C	Issued by: VeriSign C
Valid from 9/1/2011	Valid from 7/27/2011
 You have a private key	 You have a private key

4:31 AM · Mar 4, 2022

624 Reply Share

Source: Twitter

Code signing certificate actually enables a digital signature on executables and drivers to allow them and mark them as “cleared”. Using these stolen certificates, attackers are practically disguising files and executables as legitimate and might bypass security means, allowing malware to be uploaded to Windows.



Source: Telegram

The Samsung leak also allegedly includes bootloader source code for recent Samsung's devices, algorithms for all biometric unlock operations, source code for Samsung's activation servers, the full source code used to authenticate Samsung accounts, and secret Qualcomm source code.

Check Point Research's (CPR) teams are constantly monitoring the situation in search for additional potential threats that might surface. We will update accordingly.

Prevention first – What you need to do to remain protected

Organizations should be mainly concerned about malware penetration into their corporate network via the aforementioned stolen certificates.

Unfortunately, some security solutions in the market still expose organizations to this supply chain threat, as they seem to automatically revoke the stolen certificates, most probably since they consider the vendor who produced the certificate as trusted by default.

To keep your entire IT infrastructure safe, we recommend ensuring your network security gateways, as well as your endpoint device security solutions, have been updated with the appropriate protection against the stolen certificates. We also recommend that you download software updates from the formal vendor website and update your entire workforce to do the same.

Check Point's customers remain protected

Check Point's customers gain preemptive protection from any supply chain attack that may arise from the stolen certificates.

Unfortunately, some security solutions in the market still expose organizations to this supply chain threat, as they seem to automatically approve the stolen certificates, even though they've already been revoked, most probably since they consider the vendor who produced the certificate as trusted by default.

Whether you're using Check Point to secure your network cloud or workforce, you gain accurate prevention against the threat mentioned above through Check Point ThreatCloud. ThreatCloud combines 60+ threat prevention and AI technologies with globally-shared threat intelligence derived from hundreds of millions of sensors worldwide, and enriched with insights from Check Point Research.

The products below leverage Check Point ThreatCloud's threat emulation service, an innovative zero-day sandboxing technology, to detect and block these stolen certificates from penetrating. This process is fully automated and does not require any action by the user.

More specifically:

- **Check Point Quantum security gateways** will protect your network and data centers from malware.
- **Check Point Harmony Endpoint**, complete endpoint protection, and EDR solution will protect your employees from downloading malicious files or executables to work laptops and PCs and prevent data leak and lateral movement of malware to other systems.
- **Check Point Harmony Mobile**, the industry's leading Mobile Threat Defense solution, will prevent employees from downloading malicious files and applications and therefore prevent the compromise of sensitive business data.