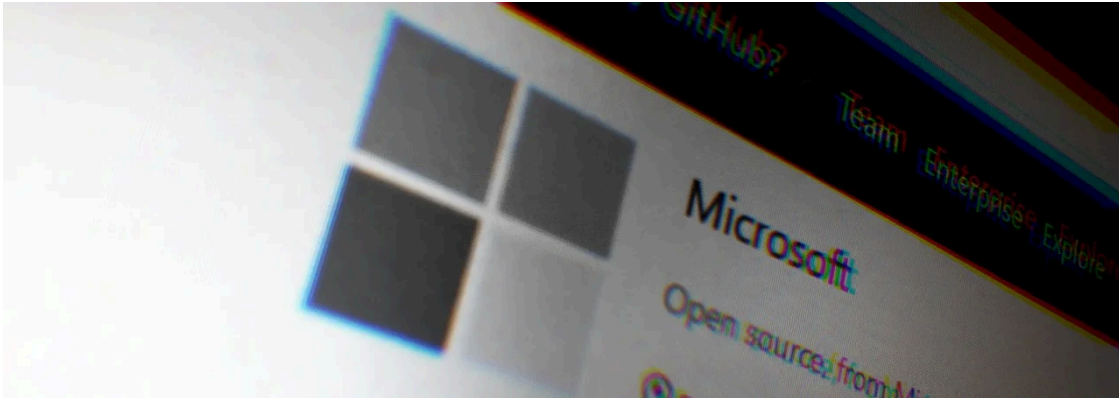


# Microsoft's GitHub account hacked, private repositories stolen

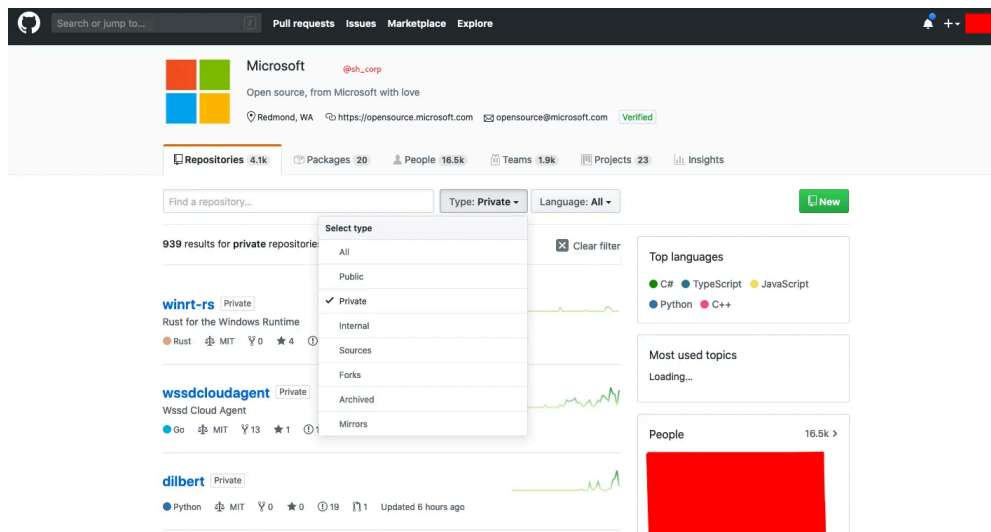
By Lawrence Abrams

Published: 2020-05-07 · Archived: 2026-04-05 19:24:33 UTC



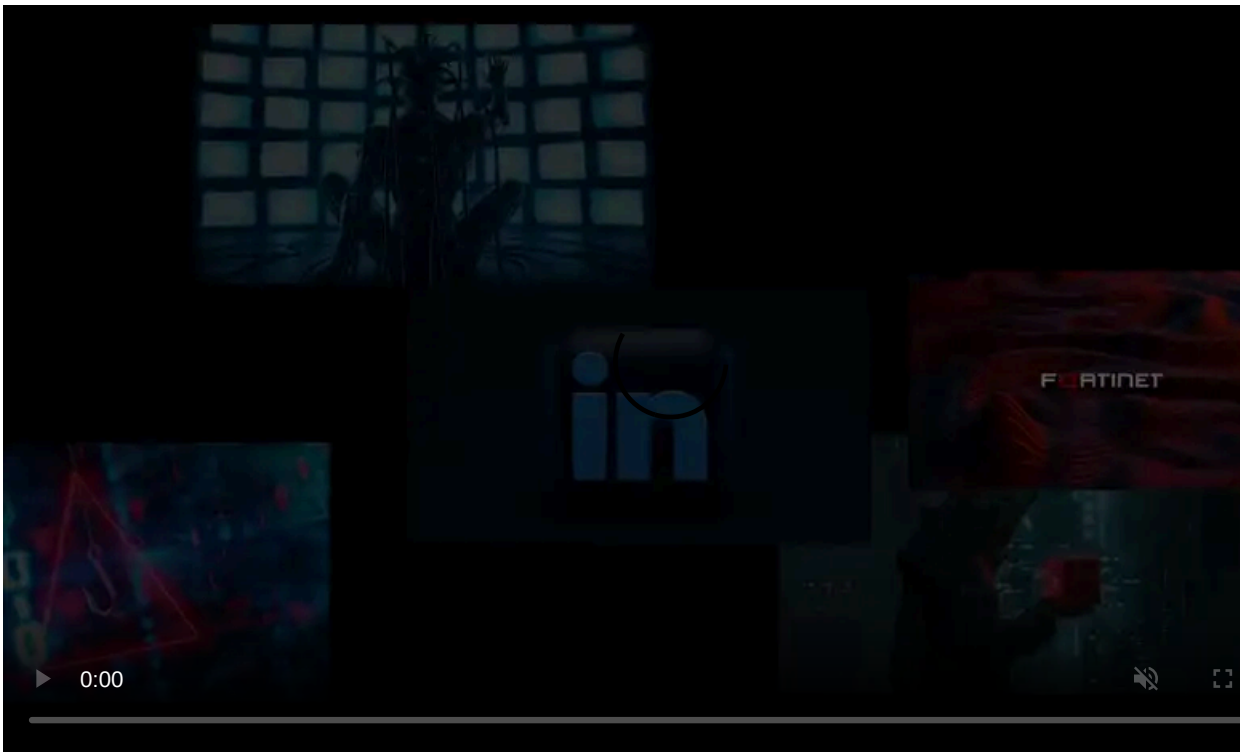
A hacker claims to have stolen over 500GB of data from Microsoft's private GitHub repositories, BleepingComputer has learned.

This evening, a hacker going by the name Shiny Hunters contacted BleepingComputer to tell us they had hacked into the Microsoft GitHub account, gaining full access to the software giant's 'Private' repositories.



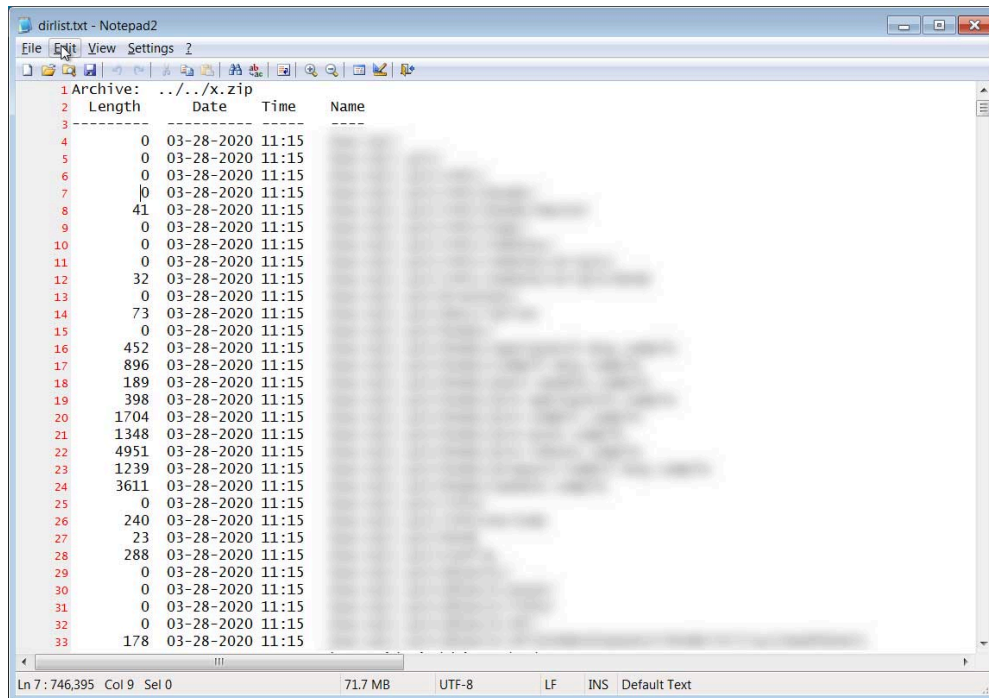
## Actor's proof of access to Microsoft's private GitHub repos

The individual told us that they then downloaded 500GB of private projects and initially planned on selling it, but has now decided to leak it for free



Visit Advertiser website [GO TO PAGE](#)

Based on the file stamps in full directory listing of the leaked files, the breach may have occurred on March 28th, 2020.



Leaked data listing showing the breach date

Shiny Hunters told BleepingComputer that they no longer have access to Microsofts GitHub account.

## Private repositories leaked

As a teaser, the hacker offered 1GB of files on a hacker forum for registered members to use site 'credits' to gain access to the leaked data.

As some of the leaked files contain Chinese text or references to latelee.org, other threat actors on the forum do not feel that the data is real.

Based on the full directory listing of the stolen data and and source code from private repositories that was sent to BleepingComputer by the hacker, the stolen files appear to be mostly code samples, test projects, an eBook, and other generic items.

Some private repositories look a bit more interesting such as ones named some 'wssd cloud agent', a The Rust/WinRT language projection', and a 'PowerSweep' PowerShell project.

Overall, from what was shared, there does not appear to be anything significant for Microsoft to worry about, as it did not contain more sensitive code for software like Windows or Office.

Cyber intelligence firm Under the Breach, who also saw the leak on the hacker forum, shares BleepingComputer's opinion that there is not much to worry about.

They did express concern that private API keys or passwords could have accidentally been left behind in some of the private repositories like other developers have done in the past.

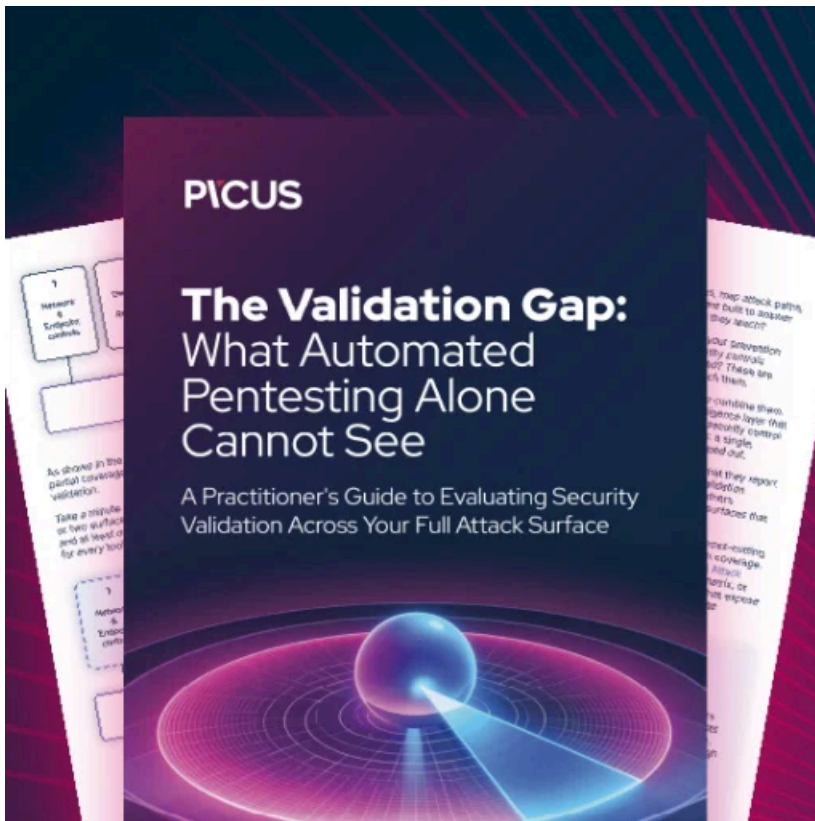


Since publishing this story, a Microsoft employee who wished to remain anonymous has told BleepingComputer that the stolen data is legitimate.

Other employees who had previously denounced the leak as fake, have since deleted their tweets.

Microsoft has told BleepingComputer that they are "aware of these claims and are investigating."

**Update 5/8/20:** Updated to include info that the breach was confirmed as legitimate by MS employee and statement from Microsoft.



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/microsofts-github-account-hacked-private-repositories-stolen/>