MUST READ: Software developer jobs are growing again. But the top skills companies want are changing

Hacker gains access to a small number of Microsoft's private GitHub repos

Hack considered harmless as the hacker did not gain access to the source code of any major Microsoft apps.

By Catalin Cimpanu for Zero Day | May 8, 2020 -- 02:12 GMT (19:12 PDT) | Topic: Security

A hacker has gained access to a Microsoft employee's GitHub account and has downloaded some of the company's private GitHub repositories.

The intrusion is believed to have taken place in March, and came to light this week when the hacker announced plans to publish some of the stolen projects on a hacking forum.

While *ZDNet* has confirmed with multiple Microsoft employees that at least a small portion of the stolen files are authentic, we have been told that the hacker did not gain access to the source code of any major Microsoft core projects, such as Windows and Office.

Microsoft employees who commented on the leak have told *ZDNet* that such major projects are hosted internally at Microsoft and not on the company's public GitHub portal.

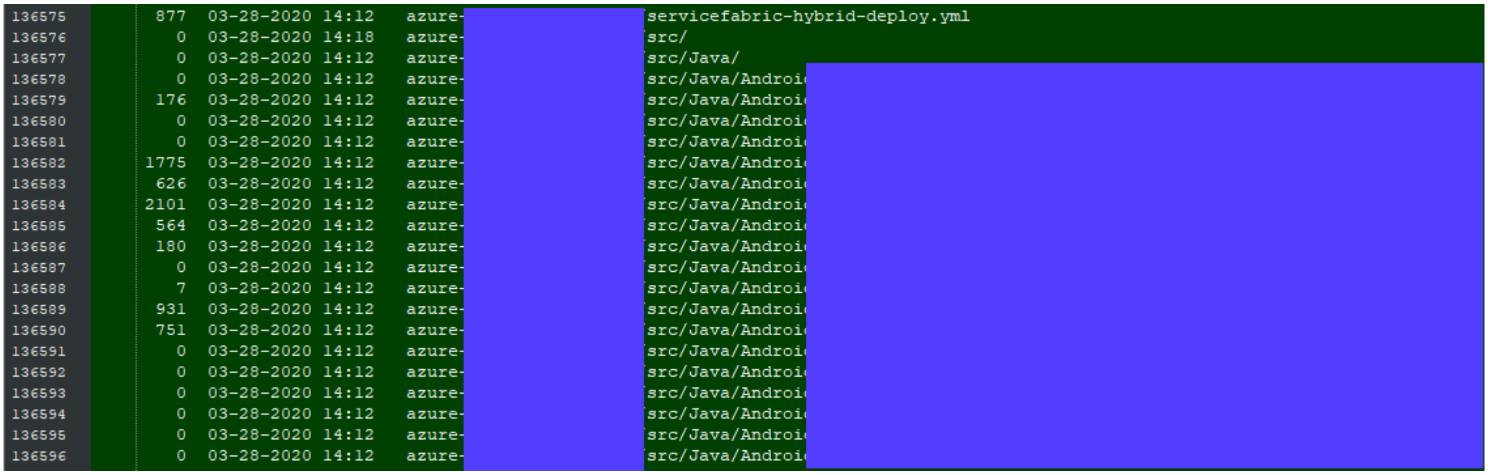
The number of private repos believed to have been acquired by the hacker is believed to be around 1,200.

A Microsoft spokesperson told *ZDNet* earlier today that the company is investigating the incident, but did not want to comment further.

NOTHING OF ACTUAL IMPORTANCE LEAKED

With the help of cyber-security firms Nightlion Security (https://www.nightlion.com/) and Under the Breach (https://underthebreach.com/), *ZDNet* has obtained copies of files the hacker shared online this week.

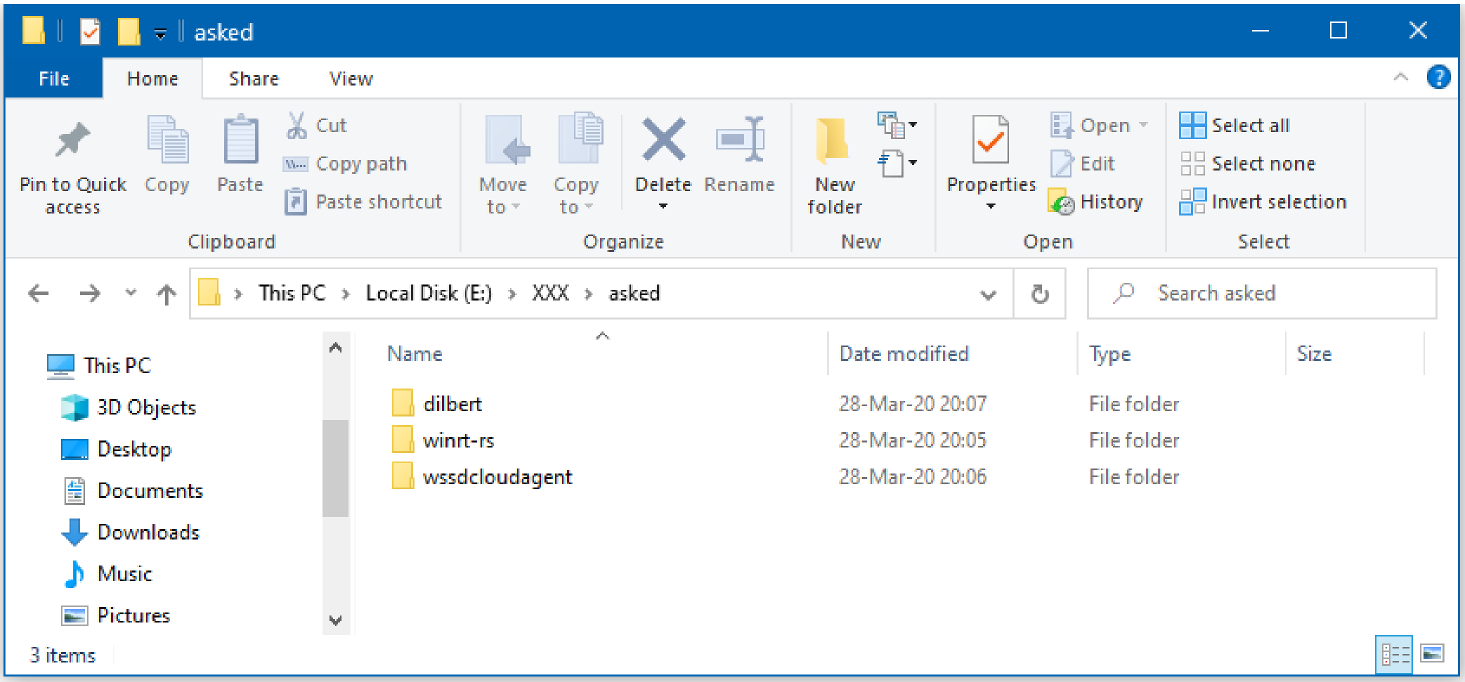
This includes a list of all the files and directories downloaded from Microsoft's private GitHub repositories.



```
136575       877  03-28-2020 14:12   azure-[redacted]servicefabric-hybrid-deploy.yml
136576         0  03-28-2020 14:18   azure-[redacted]src/
136577         0  03-28-2020 14:12   azure-[redacted]src/Java/
136578         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136579       176  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136580         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136581         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136582      1775  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136583       626  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136584      2101  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136585       564  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136586       180  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136587         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136588         7  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136589       931  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136590       751  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136591         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136592         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136593         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136594         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136595         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
136596         0  03-28-2020 14:12   azure-[redacted]src/Java/Androi[redacted]
```

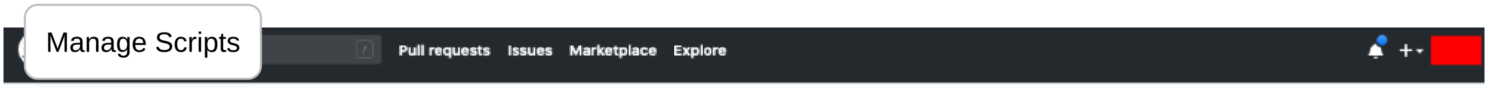
Image: ZDNet

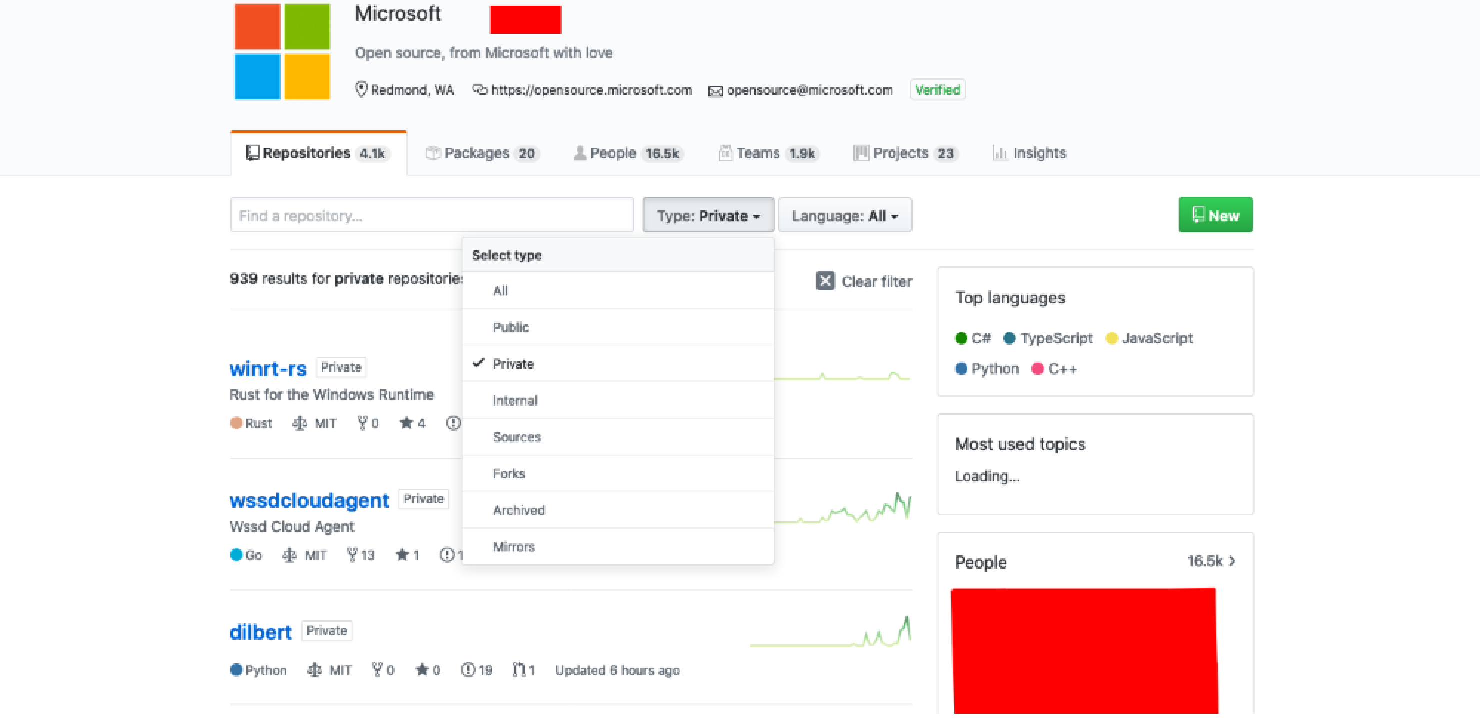
We also received three projects, including full source code, of private Microsoft projects.



Name	Date modified	Type	Size
dilbert	28-Mar-20 20:07	File folder	
winrt-rs	28-Mar-20 20:05	File folder	
wssdcloudagent	28-Mar-20 20:06	File folder	

Image: ZDNet





Microsoft [redacted]

Open source, from Microsoft with love

Redmond, WA · https://opensource.microsoft.com · opensource@microsoft.com · Verified

Repositories 4.1k · Packages 20 · People 16.5k · Teams 1.9k · Projects 23 · Insights

Find a repository... · Type: Private ▾ · Language: All ▾ · New

Select type: All · Public · ✓ Private · Internal · Sources · Forks · Archived · Mirrors

939 results for private repositorie · Clear filter

winrt-rs Private
Rust for the Windows Runtime
Rust · MIT · 0 · ★ 4

wssdcloudagent Private
Wssd Cloud Agent
Go · MIT · 13 · ★ 1 · 1

dilbert Private
Python · MIT · 0 · ★ 0 · 19 · 1 · Updated 6 hours ago

Top languages
● C# ● TypeScript ● JavaScript ● Python ● C++

Most used topics
Loading...

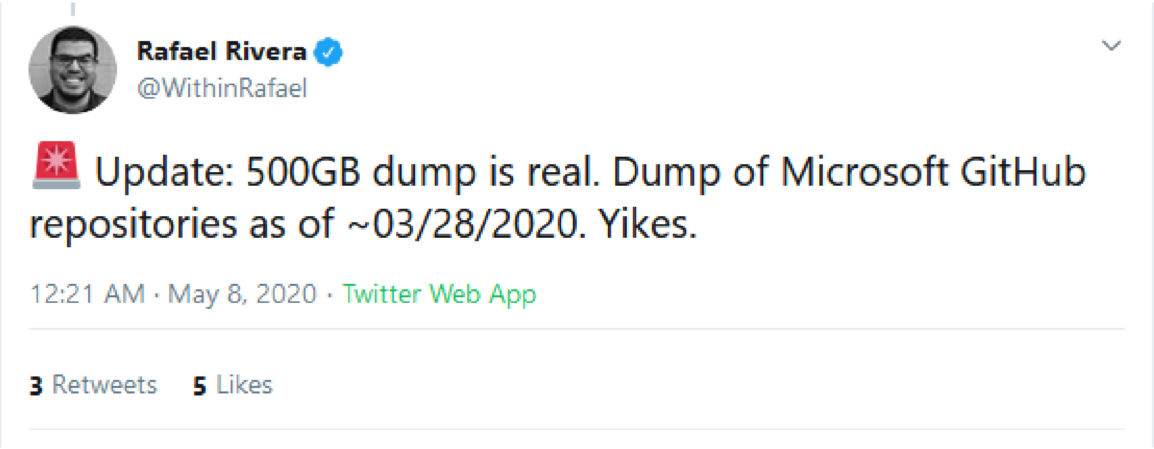
People 16.5k ›

[redacted]

Image: ZDNet

This reporter and *ZDNet*'s Microsoft writer Mary Jo Foley (https://www.zdnet.com/meet-the-team/us/mary-jo-foley/) have spoken yesterday and today with multiple Microsoft software engineers on the promise of anonymity. Sources have now confirmed that files and directories included on the list shared by the hacker did indeed contain projects that were stored in Microsoft's GitHub account as private repositories.

Other Microsoft employees made their assessment public, also confirming the leak's authenticity.



Rafael Rivera ✓
@WithinRafael

🚨 Update: 500GB dump is real. Dump of Microsoft GitHub repositories as of ~03/28/2020. Yikes.

12:21 AM · May 8, 2020 · Twitter Web App

3 Retweets **5** Likes

Image: ZDNet

Manage Scripts

Microsoft engineers who initially told us yesterday that "the leak was a scam" have now walked back their comments as news of the leak spread inside the company, and some employees confirmed its partial authenticity.

Employees who commented publicly on the leak as being a scam have also deleted their tweets.

A NOTHINGBURGER?

We say "partial authenticity" because a large portion of the files and directories listed by the hacker do not appear to be Microsoft-related projects, or are open-source projects that have been public for years and have no affiliation to Microsoft. It is unclear how these GitHub repositories got on the hacker's list.

ZDNet was told that none of the authentic Microsoft projects obtained by the hacker are even remotely sensitive. Internal policy is that the Microsoft GitHub account is to be used to host and share open-source projects and documentation. The Microsoft GitHub account is also used to host private projects that are to be made available under an open-source license in the future.

Furthermore, some employees said that their own private projects hosted on Microsoft's official GitHub account were not included in the list of files obtained by the hacker, which means the threat actor only gained access to only a fraction of the non-sensitive information stored in Microsoft's account.

The only sensitive issue might be that some projects could contain access tokens and API credentials that may now have to be revoked.

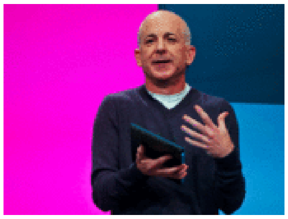
Under the Breach, which had direct contact with the hacker, has told ZDNet today that the attacker has now lost access to Microsoft's private GitHub repositories, as Microsoft staff appears to have identified the compromised employee GitHub account.

The hacker behind this incident is the same individual behind the Tokopedia hack (https://www.zdnet.com/article/hacker-leaks-15-million-records-from-tokopedia-indonesias-largest-online-store/) that ZDNet disclosed on Saturday.

A *ting by Mary Jo Foley.*

A brief history of Microsoft's Surface: Missteps... (/pictures/the-history-of-microsofts-surface/)

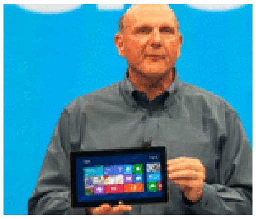
SEE FULL GALLERY (/pictures/the-history-of-microsofts-surface/)


(/pictures/the-history-of-

(/pictures/the-history-of-

(/pictures/the-history-of-

(/pictures/the-history-of-


(/pictures/the-history-c

1 - 5 of 22

NEXT > ()

SECURITY

Microsoft August 2020 Patch Tuesday fixes 120 vulnerabilities, two zero-days (https://www.zdnet.com/article/microsoft-august-2020-patch-tuesday-fixes-120-vulnerabilities-two-zero-days/)

Ransomware: These warning signs could mean you are already under attack (https://www.zdnet.com/article/ransomware-these-warning-signs-could-mean-you-are-already-under-attack/)

Best security keys in 2020: Hardware-based two-factor authentication for online protection (https://www.zdnet.com/article/best-security-keys/)

Best password managers for business in 2020: 1Password, Keeper, LastPass, and more (https://www.zdnet.com/article/best-password-managers/)

Cyber security 101: Protect your privacy from hackers, spies, and the government (https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/)

White hat hacker reveals the real job of an infosec pro (ZDNet YouTube) (https://www.youtube.com/watch?v=HiqPehsO53o)

Top 6 cheap home security devices in 2020 (CNET) (https://www.cnet.com/how-to/top-cheap-home-security-devices-in-2020-amazon-echo-smart-cam-wyze/?ftag=CMG-01-10aaa1b)

What are IT pros concerned about in the new normal? (TechRepublic) (https://www.techrepublic.com/article/what-are-it-pros-concerned-about-in-the-new-normal-security-and-flexibility/?ftag=CMG-01-10aaa1b)

RELATED TOPICS: MICROSOFT SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

By Manage Scripts Zero Day | May 8, 2020 -- 02:12 GMT (19:12 PDT) | Topic: Security

SHOW COMMENTS

MORE RESOURCES

Information Security Certification Training Bundle - ZDNet Academy

Training from ZDNet Academy

READ NOW

ZD Academy - Become an Ethical Hacker Bonus Bundle

Tr Manage Scripts cademy

TIGER LAKE, WILLOW COVE AND MORE

Intel's complex buffet of products: Will customers understand?

JUST IN

Apple mercilessly mocked by Epic where it hurts

2 hours ago

Manage Scripts

ebook joins The Linux Foundation as a platinum member

urs ago

Epic lawsuit vs. Apple's 30% App Store cut aims for leverage, pressure, and a better deal

2 hours ago

The 10 best smartphones of 2020: 5G powers the top contenders

2 hours ago

AWS quantum computing service Braket now generally available

3 hours ago

Open source takes on earthquake early warning project

4 hours ago

Notebook sales soared in Q2, with Lenovo and HP claiming half the market

5 hours ago

Apple reportedly developing digital service bundles for iOS 14

6 hours ago

TODAY ON ZDNET

SPECIAL FEATURE

Back to virtual school: Education embraces remote learning

How Atlassian sees remote work as a two-fold opportunity

6 hours ago by Larry Dignan in Innovation

Manage Scripts

Down but not out: How Boston's pro sports teams can still win in a pandemic

6 hours ago by Vala Afshar in Digital Transformation

FBI and NSA expose new Linux malware Drovorub, used by Russian state hackers

7 hours ago by Catalin Cimpanu in Security

Oracle brings the Autonomous Database to JSON

7 hours ago by Tony Baer (dbInsight) in Big Data Analytics

Manage Scripts

Time to update your iPhone again - iOS 13.6.1 is out

8 hours ago by Adrian Kingsley-Hughes in iPhone

VIDEO

Nothing Note-worthy about Samsung's new phones

Introducing the ARM processor (again): What you should know about it now

8 hours ago by Scott Fulton III in ARM

Intel shows off Tiger Lake and Willow Cove. Now it must make sure c nderstand the products

Manage Scripts

9 hours ago by Tiernan Ray in Intel

Lenovo ThinkPad X1 Carbon (8th Gen) review: Flagship ultraportable maintains the quality

9 hours ago by Sandra Vogel in Laptops

Google: We'll test hiding the full URL in Chrome 86 to combat phishing

10 hours ago by Liam Tung in Enterprise Software

Manage Scripts

Balancing budget pressures in a time of budget cuts

10 hours ago by Tonya Hall in Banking

GALLERY

Working from home on a laptop? Check out these external monitors

LOAD MORE

Collection

Coronavirus: Business and technology in a pandemic

How Atlassian sees remote work as a two-fold opportunity

Balancing budget pressures in a time of budget cuts

Surface Duo: The wrong device at the wrong time for the wrong price?

Defence to build up Royal Australian Navy's capabilities with autonomous systems

NSW government trials QR code scanner for COVID-19 contact tracing

Monash University takes game-like approach to capsule endoscopy

Manage Scripts

Collection

Small Business TV

Wyndham Hotels & Resorts tackled technical debt, cloud, hybrid cloud in a hurry [Cloud TV]

HSBC charts out its move to the cloud [Cloud TV]

How Brinker International thinks through cloud, data, Apple iPads [Cloud TV]

Why security is the top barrier in enterprise cloud adoption [Hybrid Cloud TV]

How New Belgium Brewing evaluated managed vs. private cloud [Hybrid Cloud TV]

With Red Hat, IBM to become the leading hybrid cloud provider

Manage Scripts