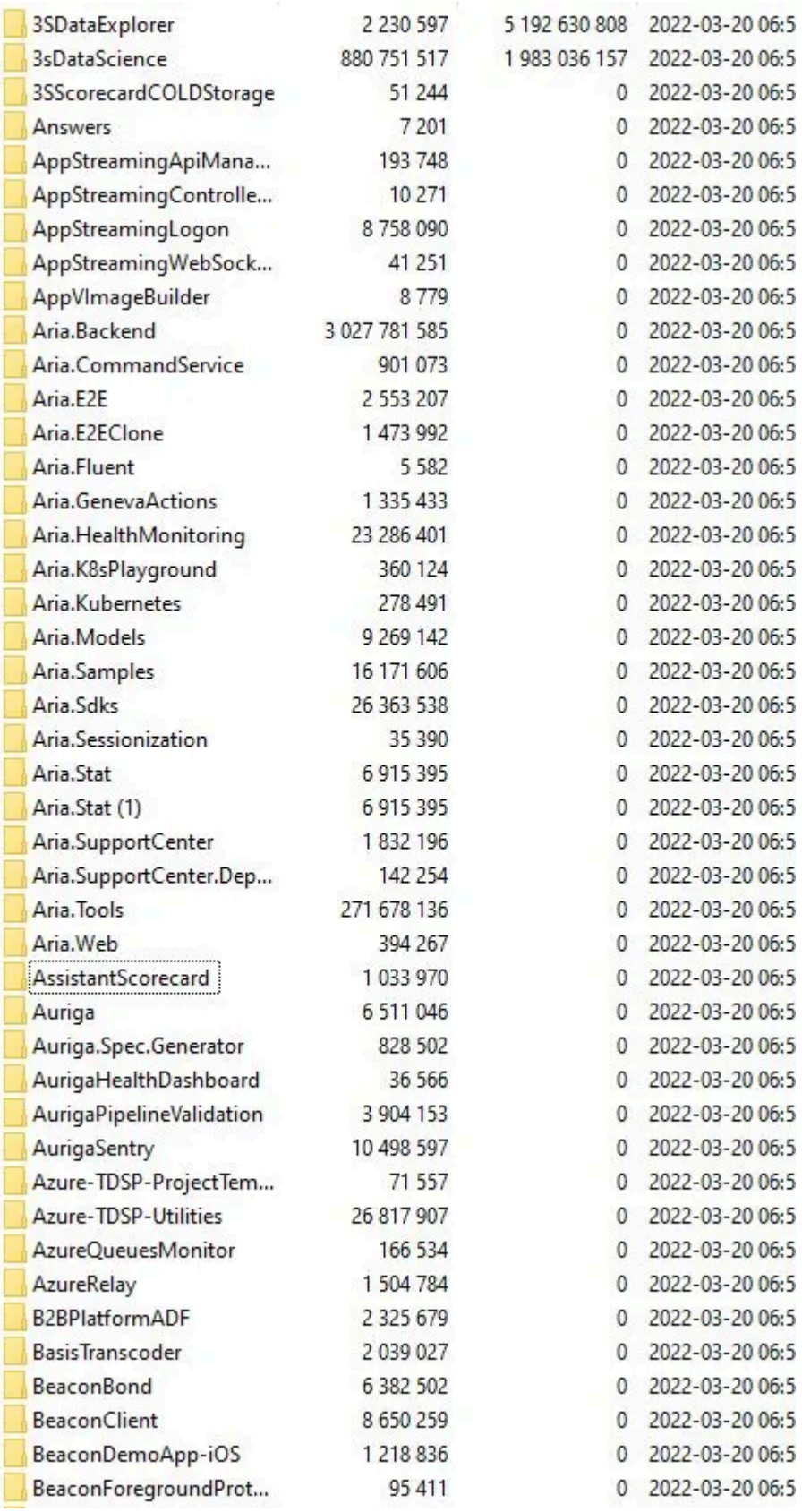
It’s official, Lapsus$ gang compromised a Microsoft employee’s account

By Pierluigi Paganini

Published: 2022-03-23 · Archived: 2026-04-06 01:07:54 UTC



3SDataExplorer	2 230 597	5 192 630 808	2022-03-20 06:5
3sDataScience	880 751 517	1 983 036 157	2022-03-20 06:5
3SScorecardCOLDStorage	51 244	0	2022-03-20 06:5
Answers	7 201	0	2022-03-20 06:5
AppStreamingApiMana...	193 748	0	2022-03-20 06:5
AppStreamingControlle...	10 271	0	2022-03-20 06:5
AppStreamingLogon	8 758 090	0	2022-03-20 06:5
AppStreamingWebSock...	41 251	0	2022-03-20 06:5
AppVImageBuilder	8 779	0	2022-03-20 06:5
Aria.Backend	3 027 781 585	0	2022-03-20 06:5
Aria.CommandService	901 073	0	2022-03-20 06:5
Aria.E2E	2 553 207	0	2022-03-20 06:5
Aria.E2EClone	1 473 992	0	2022-03-20 06:5
Aria.Fluent	5 582	0	2022-03-20 06:5
Aria.GenevaActions	1 335 433	0	2022-03-20 06:5
Aria.HealthMonitoring	23 286 401	0	2022-03-20 06:5
Aria.K8sPlayground	360 124	0	2022-03-20 06:5
Aria.Kubernetes	278 491	0	2022-03-20 06:5
Aria.Models	9 269 142	0	2022-03-20 06:5
Aria.Samples	16 171 606	0	2022-03-20 06:5
Aria.Sdks	26 363 538	0	2022-03-20 06:5
Aria.Sessionization	35 390	0	2022-03-20 06:5
Aria.Stat	6 915 395	0	2022-03-20 06:5
Aria.Stat (1)	6 915 395	0	2022-03-20 06:5
Aria.SupportCenter	1 832 196	0	2022-03-20 06:5
Aria.SupportCenter.Dep...	142 254	0	2022-03-20 06:5
Aria.Tools	271 678 136	0	2022-03-20 06:5
Aria.Web	394 267	0	2022-03-20 06:5
AssistantScorecard	1 033 970	0	2022-03-20 06:5
Auriga	6 511 046	0	2022-03-20 06:5
Auriga.Spec.Generator	828 502	0	2022-03-20 06:5
AurigaHealthDashboard	36 566	0	2022-03-20 06:5
AurigaPipelineValidation	3 904 153	0	2022-03-20 06:5
AurigaSentry	10 498 597	0	2022-03-20 06:5
Azure-TDSP-ProjectTem...	71 557	0	2022-03-20 06:5
Azure-TDSP-Utilities	26 817 907	0	2022-03-20 06:5
AzureQueuesMonitor	166 534	0	2022-03-20 06:5
AzureRelay	1 504 784	0	2022-03-20 06:5
B2BPlatformADF	2 325 679	0	2022-03-20 06:5
BasisTranscoder	2 039 027	0	2022-03-20 06:5
BeaconBond	6 382 502	0	2022-03-20 06:5
BeaconClient	8 650 259	0	2022-03-20 06:5
BeaconDemoApp-iOS	1 218 836	0	2022-03-20 06:5
BeaconForegroundProt...	95 411	0	2022-03-20 06:5

Microsoft confirmed that Lapsus$ extortion group has hacked one of its employees to access and steal the source code of some projects.

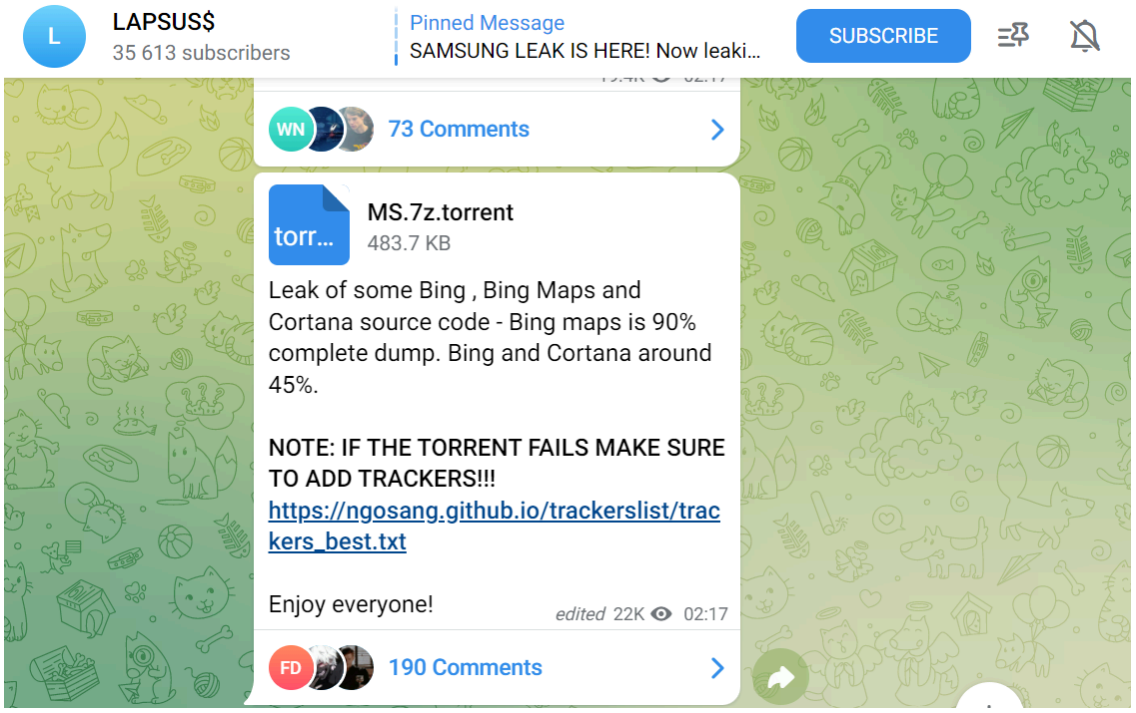
Microsoft confirmed that Lapsus$ extortion group has hacked one of its employees to access and steal the source code of some projects.

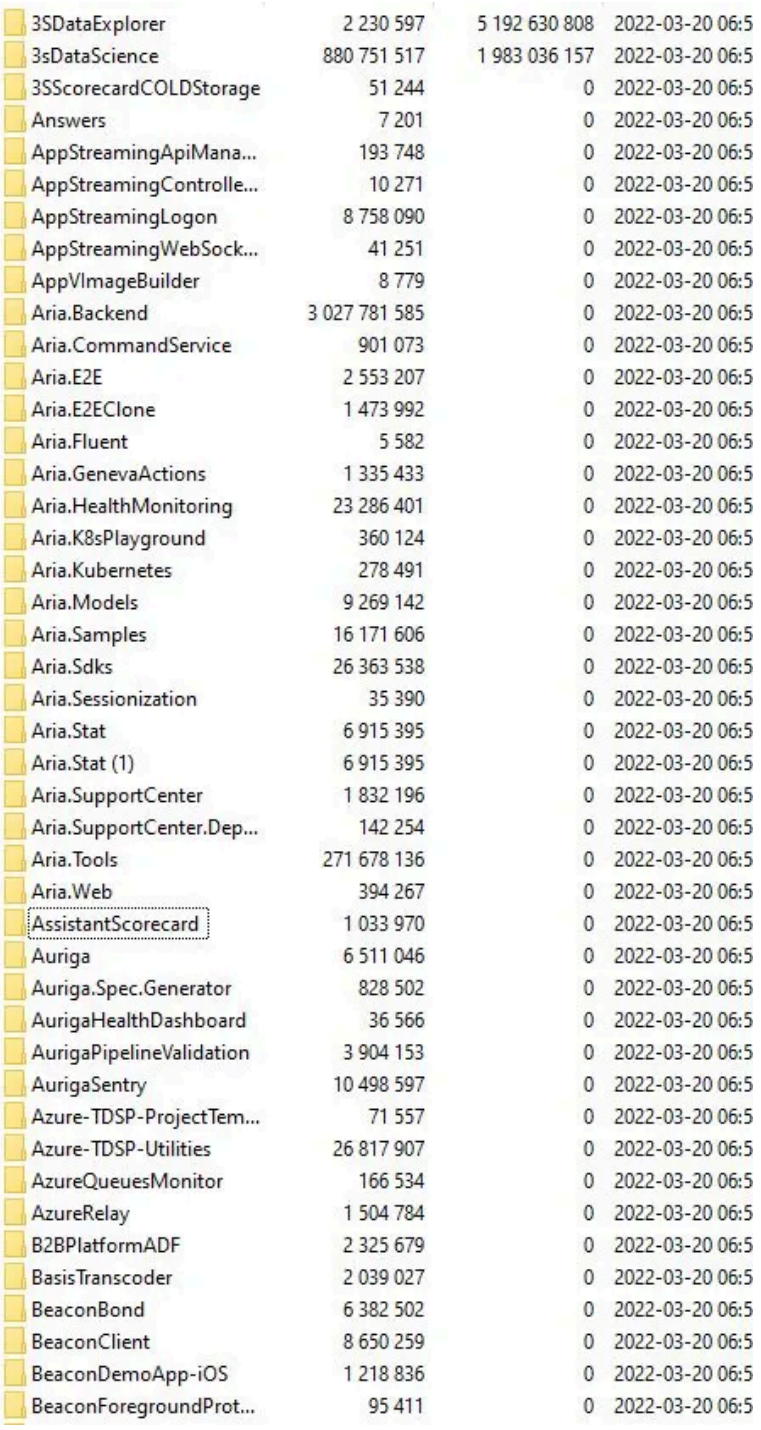
Yesterday the cybercrime gang leaked 37GB of source code stolen from Microsoft's Azure DevOps server.

On Sunday, the Lapsus$ gang announced to have compromised Microsoft's Azure DevOps server and shared a screenshot of alleged internal source code repositories.

The gang claims to have leaked the source code for some Microsoft projects, including Bing and Cortana.

On March 22, 2022 night the group shared a torrent for a 7zip archive containing 9 GB of Microsoft source code. The uncompressed archive contains 37GB of source code allegedly belonging to hundreds of Microsoft projects, including for Bing, Cortana, and Bing Maps.





3SDataExplorer	2 230 597	5 192 630 808	2022-03-20 06:5
3sDataScience	880 751 517	1 983 036 157	2022-03-20 06:5
3SScorecardCOLDStorage	51 244	0	2022-03-20 06:5
Answers	7 201	0	2022-03-20 06:5
AppStreamingApiMana...	193 748	0	2022-03-20 06:5
AppStreamingControlle...	10 271	0	2022-03-20 06:5
AppStreamingLogon	8 758 090	0	2022-03-20 06:5
AppStreamingWebSock...	41 251	0	2022-03-20 06:5
AppVImageBuilder	8 779	0	2022-03-20 06:5
Aria.Backend	3 027 781 585	0	2022-03-20 06:5
Aria.CommandService	901 073	0	2022-03-20 06:5
Aria.E2E	2 553 207	0	2022-03-20 06:5
Aria.E2EClone	1 473 992	0	2022-03-20 06:5
Aria.Fluent	5 582	0	2022-03-20 06:5
Aria.GenevaActions	1 335 433	0	2022-03-20 06:5
Aria.HealthMonitoring	23 286 401	0	2022-03-20 06:5
Aria.K8sPlayground	360 124	0	2022-03-20 06:5
Aria.Kubernetes	278 491	0	2022-03-20 06:5
Aria.Models	9 269 142	0	2022-03-20 06:5
Aria.Samples	16 171 606	0	2022-03-20 06:5
Aria.Sdks	26 363 538	0	2022-03-20 06:5
Aria.Sessionization	35 390	0	2022-03-20 06:5
Aria.Stat	6 915 395	0	2022-03-20 06:5
Aria.Stat (1)	6 915 395	0	2022-03-20 06:5
Aria.SupportCenter	1 832 196	0	2022-03-20 06:5
Aria.SupportCenter.Dep...	142 254	0	2022-03-20 06:5
Aria.Tools	271 678 136	0	2022-03-20 06:5
Aria.Web	394 267	0	2022-03-20 06:5
AssistantScorecard	1 033 970	0	2022-03-20 06:5
Auriga	6 511 046	0	2022-03-20 06:5
Auriga.Spec.Generator	828 502	0	2022-03-20 06:5
AurigaHealthDashboard	36 566	0	2022-03-20 06:5
AurigaPipelineValidation	3 904 153	0	2022-03-20 06:5
AurigaSentry	10 498 597	0	2022-03-20 06:5
Azure-TDSP-ProjectTem...	71 557	0	2022-03-20 06:5
Azure-TDSP-Utilities	26 817 907	0	2022-03-20 06:5
AzureQueuesMonitor	166 534	0	2022-03-20 06:5
AzureRelay	1 504 784	0	2022-03-20 06:5
B2BPlatformADF	2 325 679	0	2022-03-20 06:5
BasisTranscoder	2 039 027	0	2022-03-20 06:5
BeaconBond	6 382 502	0	2022-03-20 06:5
BeaconClient	8 650 259	0	2022-03-20 06:5
BeaconDemoApp-iOS	1 218 836	0	2022-03-20 06:5
BeaconForegroundProt...	95 411	0	2022-03-20 06:5

Microsoft has now confirmed that the attackers have compromised the account of one of its employees gaining limited access to source code repositories. The company pointed out that customer code or data was not compromised as a result of unauthorized access.

“This week, the actor made public claims that they had gained access to Microsoft and exfiltrated portions of source code. No customer code or data was involved in the observed activities. Our investigation has found a single account had been compromised, granting limited access. Our cybersecurity response teams quickly engaged to remediate the compromised account and prevent further activity.” reads the post published by Microsoft. “Microsoft does not rely on the secrecy of code as a security measure and viewing source code does not lead to elevation of risk.”

Microsoft team launched an investigation immediately after the Lapsus$ gang, tracked by the company as DEV-0537, claimed to have hacked the company.

Microsoft's post detailed the Lapsus gang's tactics, techniques, and procedures (TTPs), below are some of the methods that they used to compromise user identities to gain initial access to an organization:

- Deploying the malicious Redline password stealer to obtain passwords and session tokens
- Purchasing credentials and session tokens from criminal underground forums
- Paying employees at targeted organizations (or suppliers/business partners) for access to credentials and MFA approval
- Searching public code repositories for exposed credentials

The threat actors used the compromised credentials and/or session tokens to access the target networks through internet-facing systems and applications (i.e. virtual private network (VPN), remote desktop protocol (RDP), virtual desktop infrastructure (VDI) including Citrix, or Identity providers (including Azure Active Directory, Okta)).

The gang also uses session replay attacks to compromise the accounts that are protected with MFA, in some cases, they also continuously trigger MFA notifications until the user allowed them to log in. In at least one attack, the group also used a SIM swap attack to bypass 2FA.

"Once DEV-0537 obtained access to the target network using the compromised account, they used multiple tactics to discover additional credentials or intrusion points to extend their access including:

- *Exploiting unpatched vulnerabilities on internally accessible servers including JIRA, Gitlab, and Confluence*
- *Searching code repositories and collaboration platforms for exposed credentials and secrets.*

They have been consistently observed to use AD Explorer, a publicly available tool, to enumerate all users and groups in the said network." continues the analysis.

Lapsus$ gang set up a dedicated infrastructure in known virtual private server (VPS) providers and leverages NordVPN for data exfiltration using VPN egress points that were geographically like their targets to avoid detection. Data stolen from the targeted organization were also used for future extortion or public release.

Microsoft provides the following recommendations to protect against threat actors:

- Strengthen MFA implementation
- Require Healthy and Trusted Endpoints
- Leverage modern authentication options for VPNs
- Strengthen and monitor your cloud security posture
- Improve awareness of social engineering attacks
- Establish operational security processes in response to DEV-0537 intrusions

Over the last months, the Lapsus$ gang compromised other prominent companies such as NVIDIA, Samsung, Ubisoft, Mercado Libre, and Vodafone.

On Thursday, March 10, the group announced they're starting to recruit insiders employed within major technology giants and ISPs, such companies include Microsoft, Apple, EA Games and IBM. Their scope of interests includes – major telecommunications companies such as Claro, Telefonica and AT&T.

Notably, the actors are looking to buy remote VPN access and asking potential insiders to contact them privately via Telegram, they then reward them by paying for the access granted.

Follow me on Twitter: **@securityaffairs** and **Facebook**

[adrotate banner="9"]	[adrotate banner="12"]

Pierluigi Paganini

(SecurityAffairs – hacking, Microsoft)

[adrotate banner="5"]

[adrotate banner="13"]
