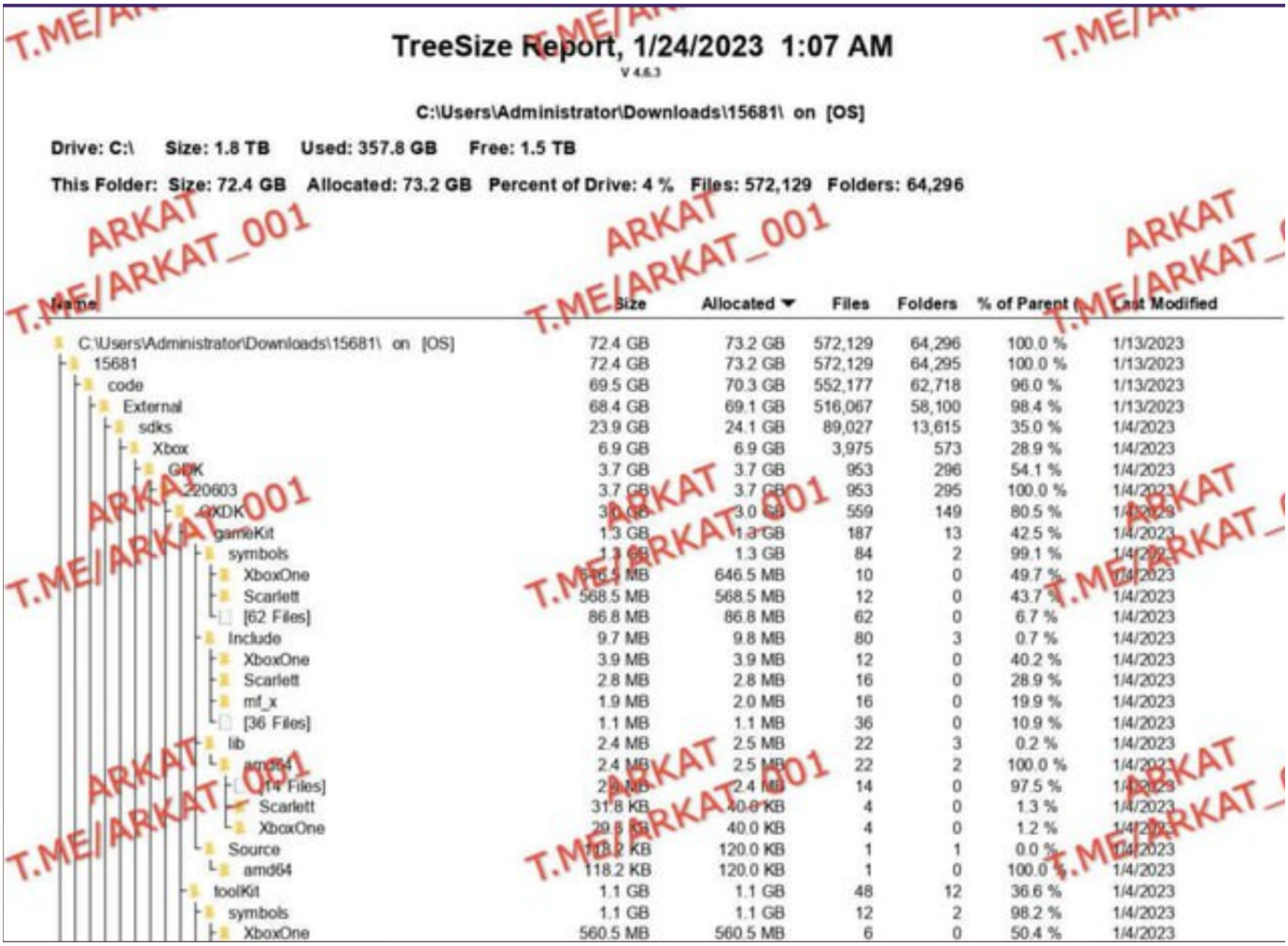
Riot Games Jan 2023 Social Engineering Attack

Incident Name	Riot Games Jan 2023
Date of Incident	January 20th, 2023
Summary	Riot Games is an American video game developer and publisher, most famous for the games League of Legends and Valorant. The company reported on January 20th via their Twitter page that their development environment had been compromised in a social engineering attack. They do not believe player data or personal information was compromised. However, as a result of this attack, the company is unable to release content, which will impact their future patching release cycles for their popular games. Further details on the attackers' methods and Riot Games' response to this hack will be released by Riot Games in the future.
24/01/2022 Update	On January 24th, Riot Games released an update and stated that the attacker had managed to exfiltrate source code for their games League of Legends, Teamfight Tactics, and a legacy anti-cheat platform. The company confirmed that while no personal data was compromised in this attack, the source code breach would impact future releases and increase the likelihood of cheats emerging in the game. The company also revealed that they had received a $10 million ransom demand from the hacker. The online magazine Motherboard obtained a copy of this ransom note from the Telegram channel the hacker set up to communicate with Riot Games employees. In the note, the hacker provides proof that they have the source code and states that if the ransom is paid, they will delete all data from their servers and provide information on how they were able to breach Riot Games. The company, however, is refusing to pay the ransom.
25/01/2022 Update	On the January 25th, VX-Underground posted on Twitter that they had spoken with the individual responsible who revealed how the breach happened. The hacker stated that that they socially engineered a Riot Games employee via SMS in order to gain access to the company's network.
Potential Key Social Engineering/OSINT Themes	• Recon - Riot Games employee information harvested. The hacker leveraged an exposed employee phone number to conduct a social engineering attack. • Smishing - In this form of attack, the attacker sends a phishing SMS message to the target which prompts them to click on a malicious URL that looks like a legitimate domain. Once the user clicks, they are prompted to enter their valid credentials which the hacker can then use to gain unauthorized access. Note: We have made assumptions based on information currently available and official confirmation from Riot Games on how the attack unfolded is required.
Remediations	• User social engineering awareness training • Identify and block newly registered domains similar to your org's. This way if used in an attack (e.g., user clicking), the request to domain is blocked. • Monitor for expiring domains which could be leveraged for the above. • Securely configure MFA on all accounts, using physical FIDO2 compliant tokens as another factor of authentication where possible. • Regularly review any external facing components to understand exposure. Allow those that are trusted, remove those that are not, and ensure MFA is securely configured for all accounts. • Ensure DNS DMARC settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party. • Regularly audit employee access to one of least privilege (including offboarding). • Regularly audit 3rd party access to one of least privilege. • Monitor and remove sensitive information disclosure.
Industry	Video Games

Actor	TBC
Motivations	Financial Gain
Related Hacks	• Rockstar 2022 • 2k Games
Breach Notice/Company Notice	https://twitter.com/riotgames/status/1616548651823935488 https://twitter.com/riotgames/status/1617900236172857345?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1617900236172857345%7Ctwgr%5E6fb3dd13ff6fd5e3ad02cee59dab550d042e55e2%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.bleepingcomputer.com%2Fnews%2Fsecurity%2Friot-games-receives-ransom-demand-from-hackers-refuses-to-pay%2F
Other Sources	https://securityaffairs.com/141171/cyber-crime/riot-games-hacked.html https://www.bleepingcomputer.com/news/security/riot-games-hacked-delays-game-patches-after-security-breach/ https://www.bleepingcomputer.com/news/security/riot-games-receives-ransom-demand-from-hackers-refuses-to-pay/ https://twitter.com/vxunderground/status/1618105539191504896?cxt=HHwWgIDQicaa1fQsAAAA https://twitter.com/vxunderground/status/1618116503550984193?cxt=HHwWgoDU9eCY2vQsAAAA https://www.vice.com/en/article/qjky8d/hackers-demand-dollar10m-from-riot-games-to-stop-leak-of-league-of-legends-source-code
Attachment	Screenshot from the hacker showing evidence of the acquired files.



TreeSize Report, 1/24/2023 1:07 AM

V 4.6.3

C:\Users\Administrator\Downloads\15681\ on [OS]

Drive: C:\ Size: 1.8 TB Used: 357.8 GB Free: 1.5 TB

This Folder: Size: 72.4 GB Allocated: 73.2 GB Percent of Drive: 4 % Files: 572,129 Folders: 64,296

Name	Size	Allocated	Files	Folders	% of Parent	Last Modified
C:\Users\Administrator\Downloads\15681\ on [OS]	72.4 GB	73.2 GB	572,129	64,296	100.0 %	1/13/2023
15681	72.4 GB	73.2 GB	572,129	64,295	100.0 %	1/13/2023
code	69.5 GB	70.3 GB	552,177	62,718	96.0 %	1/13/2023
External	68.4 GB	69.1 GB	516,067	58,100	98.4 %	1/13/2023
sdks	23.9 GB	24.1 GB	89,027	13,615	35.0 %	1/4/2023
Xbox	6.9 GB	6.9 GB	3,975	573	28.9 %	1/4/2023
GDK	3.7 GB	3.7 GB	953	296	54.1 %	1/4/2023
220603	3.7 GB	3.7 GB	953	295	100.0 %	1/4/2023
GXDK	3.0 GB	3.0 GB	559	149	80.5 %	1/4/2023
gameKit	1.3 GB	1.3 GB	187	13	42.5 %	1/4/2023
symbols	1.3 GB	1.3 GB	84	2	99.1 %	1/4/2023
XboxOne	646.5 MB	646.5 MB	10	0	49.7 %	1/4/2023
Scarlett	568.5 MB	568.5 MB	12	0	43.7 %	1/4/2023
[62 Files]	86.8 MB	86.8 MB	62	0	6.7 %	1/4/2023
Include	9.7 MB	9.8 MB	80	3	0.7 %	1/4/2023
XboxOne	3.9 MB	3.9 MB	12	0	40.2 %	1/4/2023
Scarlett	2.8 MB	2.8 MB	16	0	28.9 %	1/4/2023
mf_x	1.9 MB	2.0 MB	16	0	19.9 %	1/4/2023
[36 Files]	1.1 MB	1.1 MB	36	0	10.9 %	1/4/2023
lib	2.4 MB	2.5 MB	22	3	0.2 %	1/4/2023
amd64	2.4 MB	2.5 MB	22	2	100.0 %	1/4/2023
[4 Files]	2.3 MB	2.4 MB	14	0	97.5 %	1/4/2023
Scarlett	31.8 KB	40.0 KB	4	0	1.3 %	1/4/2023
XboxOne	29.5 KB	40.0 KB	4	0	1.2 %	1/4/2023
Source	118.2 KB	120.0 KB	1	1	0.0 %	1/4/2023
amd64	118.2 KB	120.0 KB	1	0	100.0 %	1/4/2023
toolKit	1.1 GB	1.1 GB	48	12	36.6 %	1/4/2023
symbols	1.1 GB	1.1 GB	12	2	98.2 %	1/4/2023
XboxOne	560.5 MB	560.5 MB	6	0	50.4 %	1/4/2023