## 

Dete of Incident         January 20th, 2023           Summary         Riot Games is an American video game developer and publicher, most further page that her if development reported on January 20th via hier' Triviter page that her if development reported on January 20th via hier' Triviter page that her if development reported on January 20th via hier' Triviter page that her if development reported on January 20th via hier' Triviter page that her if development release contract, which will impact ther influture pachting release cortex, the company is unable to release on the trade that that been compromised in a social engineering adata, the contrapany is unable to release or the release of the release of the tirge path. The torget that the attracker's 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 attracker had managed to exfiltret ocompany on immed that which and immediate was compromised in this attrack, the source code breach word impact future releases and increase the likelihood of cheats energing in the game. The company also company confirmed that which experson that beacher provides proof that they had received a 310 million ransom demand from the hacker. The company also communicate with Riot Games employees in the nergen enhance in the release at up to communicate with Riot Games menoposes. In the note, the hacker provides proof that they had received a social engineering attrack.           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 state that that they socially engineered as a reported to gain access to the company's insthey.           Fotential Key Social m	Incident Name	Riot Games Jan 2023
Legends and Valorant. The company reported on January 20th via their Twitter page that their devilopment had been compromised in a social engineering attack. They do not believe player data or release content, which will impact their future patching release cycles for their popular games.24/01/2022 UpdateFurther details on the attackers' methods and Riot Games' response to this hack will be released by Riot Games in the future.24/01/2022 UpdateOn January 24h, Riot Games released an update and stated that the attacker and managed to exfilinate company is unable to company confirmed that while no personal increase the likelihood of chasts and a legacy anti-cheat platform. The company confirmed that while no personal data was compromised in this attack, the 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 activate the the three releases and increase the likelihood of cheats emerging in the game. The company also revealed that they hod releaved a \$10 memand from the facker. The online magazine were shown and they were able to breach Riot Games. The company, however, is refusing to pay the ransom.25/01/2022 UpdateOn the January 25th, VX-Underground posted on Twitter that they had spoken with the individual responsible who revealed how the breach happened. The hacker leveraged an exposed employee information harvested. The hacker leveraged an exposed employee information harvested. The hacker leveraged an exposed employee they hone number to conduct a social engineering attack, the algumate domain. Once the user clicks, they are prompted to enter their valid credentials which the hacker can then use to gain unauthorized access. Noce-We have made assumptions based on information currently available and official confirmation from Riot Games on how the attack unfolded is	Date of Incident	January 20th, 2023
source code for their games League of Legends, Teamfight Tacics, 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 zet 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 the hacker zet 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 the restores and provide information on how they were able to breach Riot Games. The company, however, is reflusing to pay the ransom.25/01/2022 UpdateOn 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 information harvested. The hacker leveraged an exposed employee phone number to conduct a social engineering attack.Fotential Key Social Engineering/OSINT Themes• Recon - Riot Games employee information harvested. The hacker leveraged an exposed employee phone number to cick on a malicious URL that looks like a legitimate domain. Once the user cicks, they are prompted to enter their valid credentials which the hacker can then use to gain unauthorized accessRemediations• User social engineering awareness training • I their form of a tatack, the attacker sends a phishing SINS message to the target which prompts them to clic	Summary	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
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. 	24/01/2022 Update	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
Engineering/OSINT Themes       Record = Note Games employee imployee access to one of least privilege (including offboarding).         Remediations       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 amployee access to one of least privilege (including offboarding).         • Regularly audit 3rd party access to one of least privilege.	25/01/2022 Update	responsible who revealed how the breach happened. The hacker stated that that they socially engineered a
<ul> <li>Oser social engineering awareness training</li> <li>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.</li> <li>Monitor for expiring domains which could be leveraged for the above.</li> <li>Securely configure MFA on all accounts, using physical FIDO2 compliant tokens as another factor of authentication where possible.</li> <li>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.</li> <li>Ensure DNS DMARC settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party.</li> <li>Regularly audit employee access to one of least privilege (including offboarding).</li> <li>Regularly audit 3rd party access to one of least privilege.</li> <li>Monitor and remove sensitive information disclosure.</li> </ul>		<ul> <li>phone number to conduct a social engineering attack.</li> <li>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.</li> <li>Note: We have made assumptions based on information currently available and official confirmation from</li> </ul>
Industry Video Games	Remediations	<ul> <li>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.</li> <li>Monitor for expiring domains which could be leveraged for the above.</li> <li>Securely configure MFA on all accounts, using physical FIDO2 compliant tokens as another factor of authentication where possible.</li> <li>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.</li> <li>Ensure DNS DMARC settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party.</li> <li>Regularly audit employee access to one of least privilege (including offboarding).</li> <li>Regularly audit 3rd party access to one of least privilege.</li> </ul>
	Industry	Video Games

Actor	TBC
Motivations	Financial Gain
Related Hacks	Rockstar 2022     Zk 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://twitter.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.

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

ARKAT 001 ARKAT 001 C.Users'Administrator/Downloads/15681\ on IOS	ARKAT_001 ARKAT_001 TMESize Allocated Tiles Folders % of Parent ( 72.4 GB 73.2 GB 572,129 64,296 100.0 %					ARKAT	
T NATE ARM	TMESIZO	Allocated ¥	Files	Folders	% of Parent	A East Modified	
C:\Users\Administrator\Downloads\15681\ on [OS]	72.4 GB	73.2 GB	572,129	64,296	100.0 %	1/13/2023	
H1 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	
H Xbox	6.9 GB	6.9 GB	3,975	573	28.9 %	1/4/2023	
H GOK	3.7 GB	- 3.7 GB	953	296	54.1 %	1/4/2023	
A 220603 01	3.7 GBV	3.7 GB	1 953	295	100.0 %	1/4/2023/ 2	
ANT - AKDKOV	30.00	3.0	559	149	80.5 %	1/412028	
anneKit	13 GB	1.3 GB	187	13	42.5 %	1/4/2023 VA	
symbols	1368	1.3 GB	84	2	99.1 %	1/4/202	
XboxOne	1646.5 MB	646.5 MB	10	0	49.7 %	A 114 2023	
MEI Scarlett	568.5 MB	568.5 MB	12	0	43.7 9	1/4/2023	
L [62 Files]	86.8 MB	86.8 MB	62	0	6.7 %	1/4/2023	
-1 Include	9.7 MB	9.8 MB	80	3	0.7 %	1/4/2023	
F≡ XboxOne	3.9 MB	3.9 MB	12	0	40.2 %	1/4/2023	
-I Scarlett	2.8 MB	2.8 MB	16	0	28.9 %	1/4/2023	
-1 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	
Ib .	2.4 MB	- 2.5 MB	22	3	0.2 %	1/4/2023	
A PILL ACTON	2.4 MB	2.5 MB	1 22	2	100.0 %	1/4/2023	
Files	2000	24 148	14	0	97.5 %	1/02/28	
Scarlett	31.8 KB	1 0.0 KB	4	0	1.3 %	1/4/2023 1 4	
XboxOne	29 5 KB	40.0 KB	4	0	1.2 %	1/4/2023	
Source	ATTR KB	120.0 KB	1	1	0.0 %	A 114 2023	
La amd64	T. 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	
+1 symbols	1.1 GB	1.1 GB	12	2	98.2 %	1/4/2023	
L XboxOne	560.5 MB	560.5 MB	6	0	50.4 %	1/4/2023	