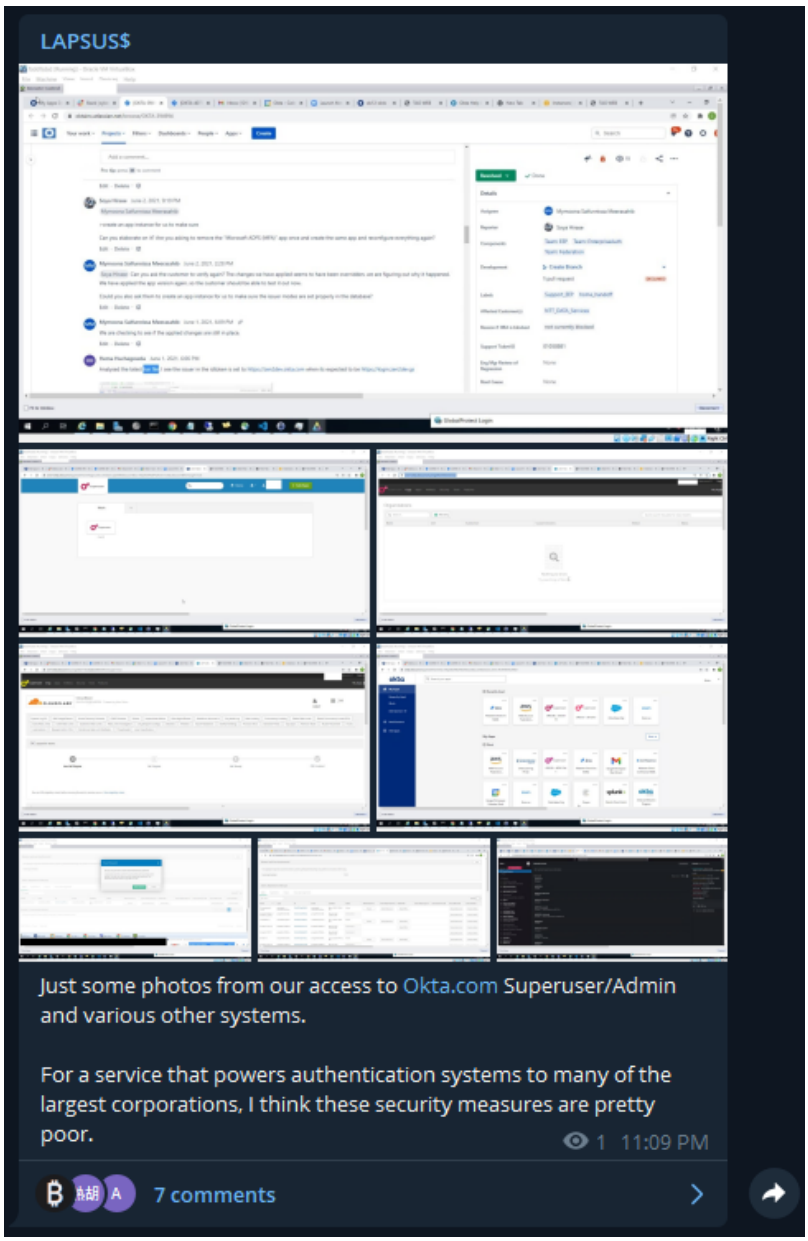
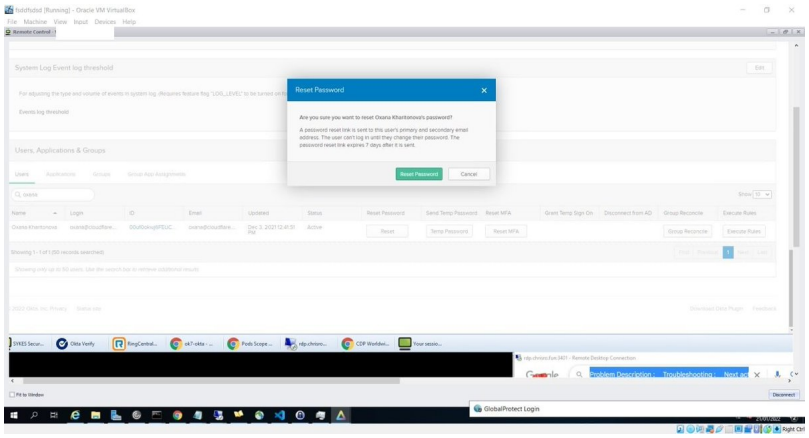
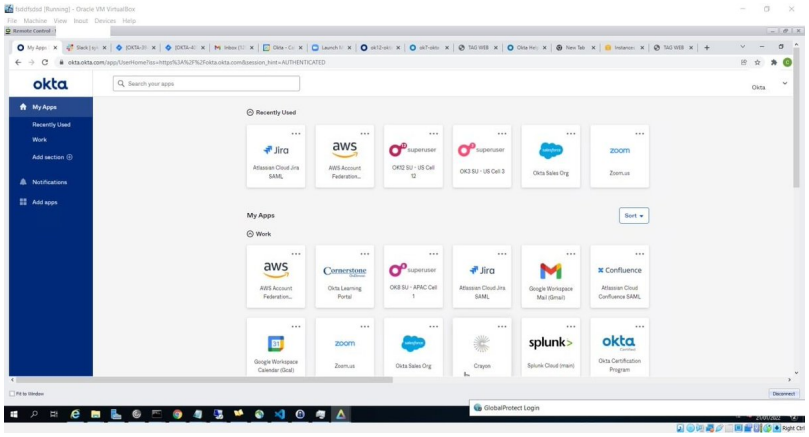
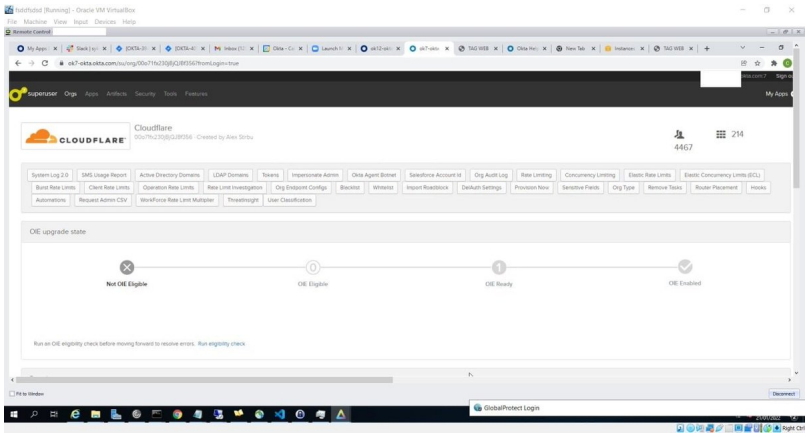
Bill Demirkapi **@BillDemirkapi** *Tue Mar 22 03:15:03 +0000 2022*

The LAPSUS$ ransomware group has claimed to breach Okta sharing the following images from internal systems. **https://t.co/eTtpgRzer7**

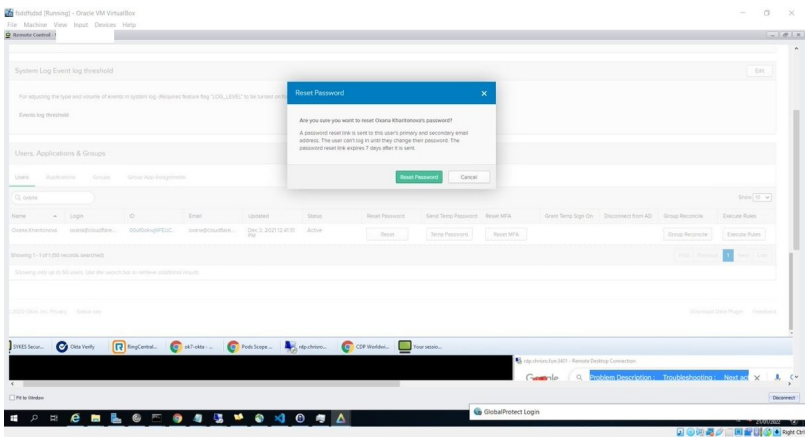


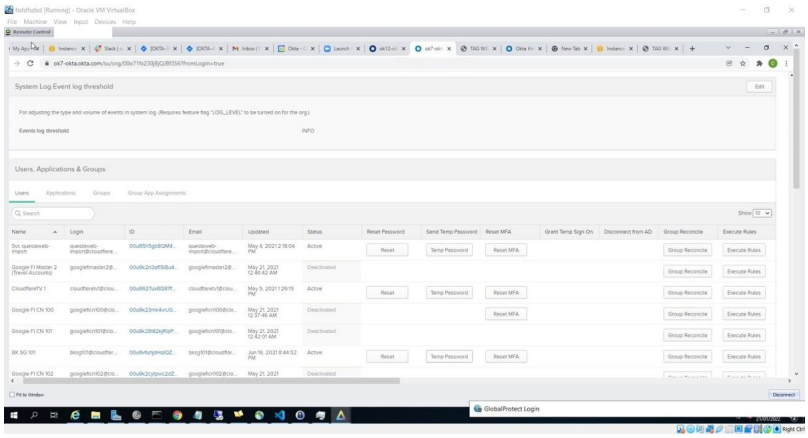


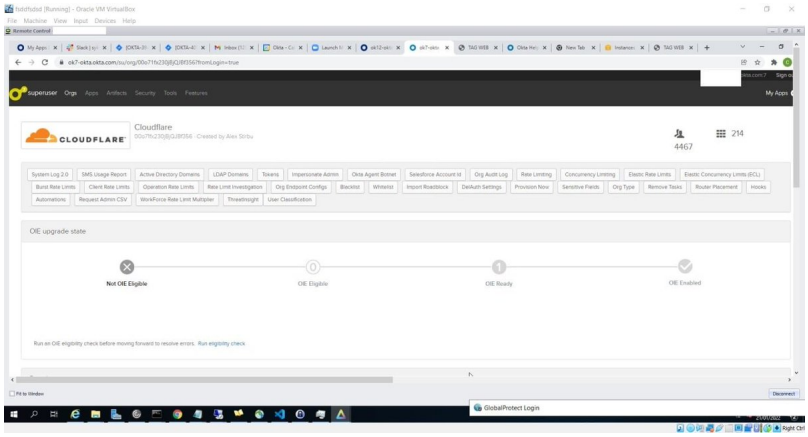




The screenshots are very worrisome. In the pictures below, LAPSUS$ appears to have gotten access to the @Cloudflare tenant with the ability to reset employee passwords: **https://t.co/OZBMenuwgJ**

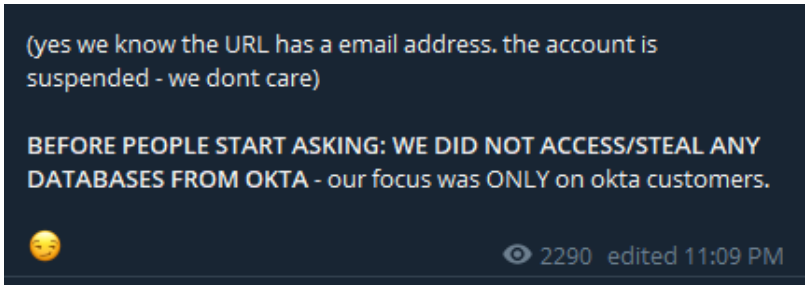




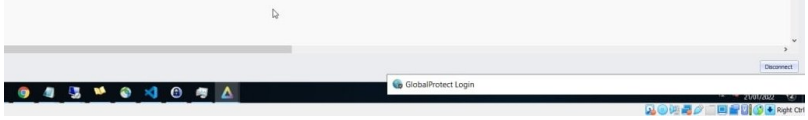


Another scary note is the date in the VM used in the screenshot consistently appears to be January 21st, 2022. If this date is correct, this would suggest @okta failed to publicly acknowledge any breach for at least two months. **https://t.co/g6RkONAgu4**

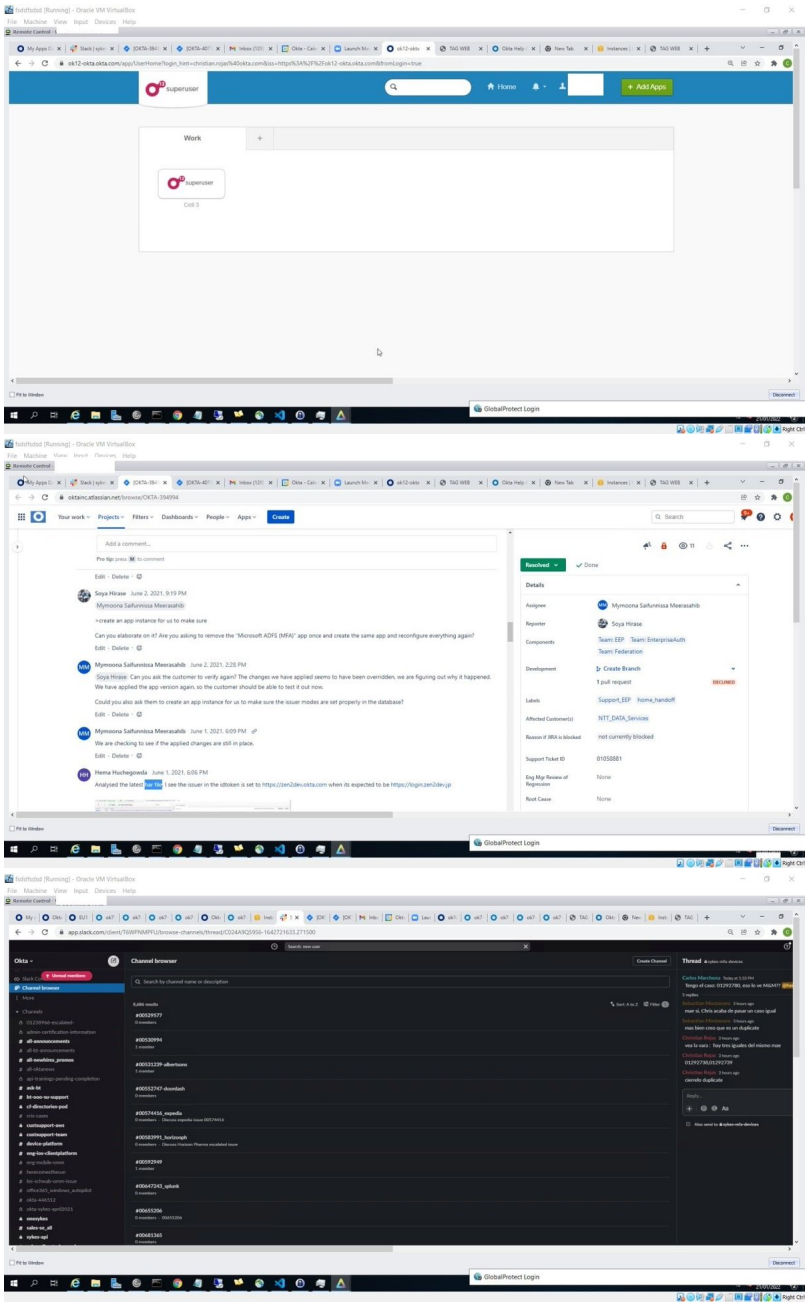
LAPSUS$ edited their message to clarify that they did not breach Okta's databases, but rather targeted Okta customers. **https://t.co/mYSlGCq6vt**



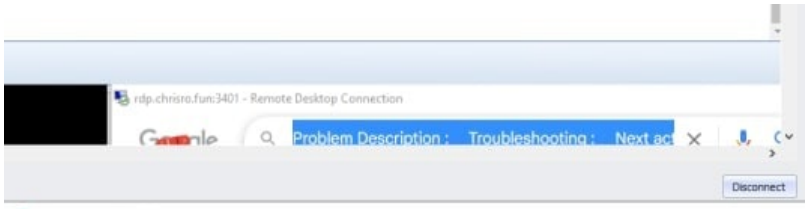
LAPSUS$ appears to have gained access to some company VPNs given the Cisco AnyConnect icon and the GlobalProtect window in this image. **https://t.co/GA0GWO8P2j**

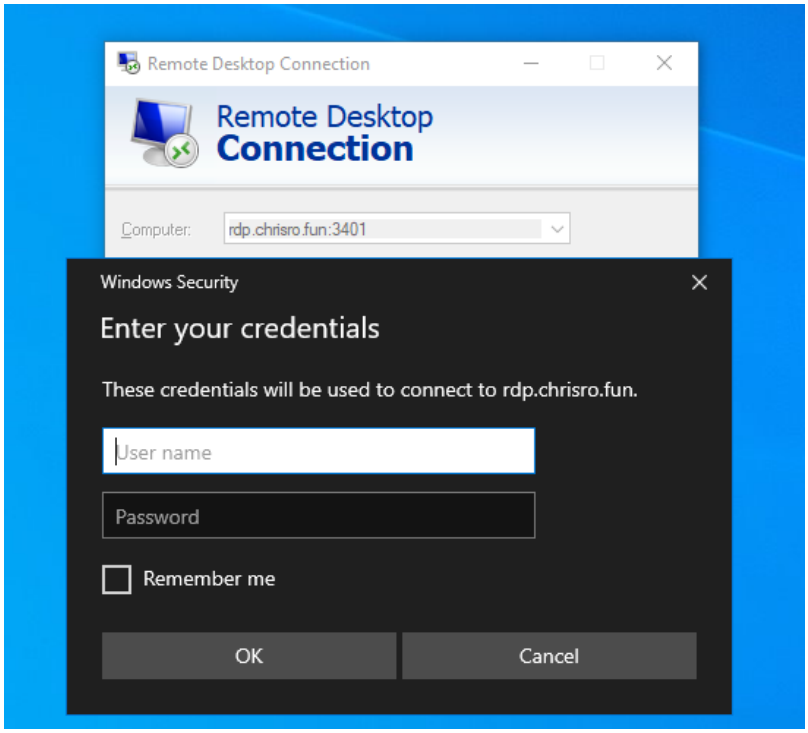


More screenshots demonstrating access to "superuser", perhaps Okta's administrative access panel? Other access includes Jira and Slack for Okta. **https://t.co/pEpPKEsARy**



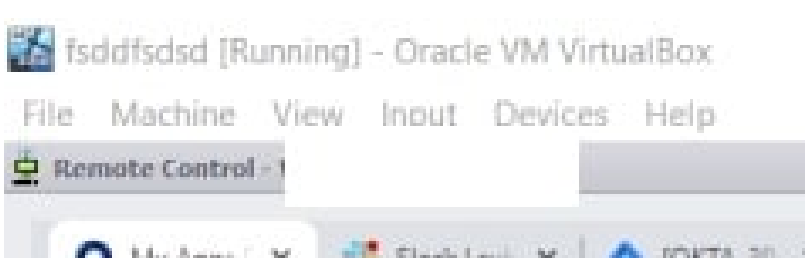
This RDP server in one of the screenshots "rdp[.]chrisro[.]fun" is still active. Perhaps part of LAPSUS$ internal infrastructure? Hosted in AWS (us-west-2) @awscloud @AWSSecurityInfo **https://t.co/OUwmm3y75A**

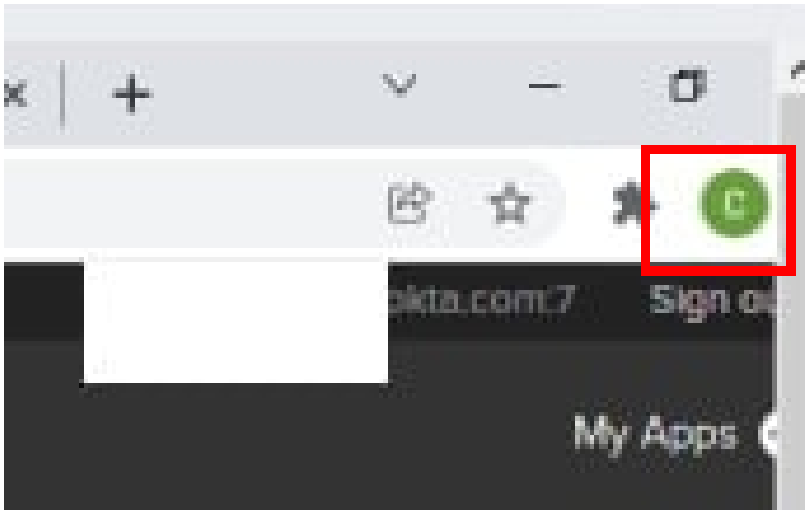




Interesting note. The "chrisro[.]fun" domain is registered to "SYKES LATIN AMERICA" and in this screenshot below we can see some tool in the taskbar named "SYKES Secur...". **https://t.co/Vw1AMDKg9m**

It is possible that LAPSUS$ might have gotten all this access by abusing Okta's own remote control tooling they use to spy on their employees. It would explain things like why the Chrome browser is signed into a user. **https://t.co/XGAn1l19RZ**





That rdp[.]chrisro[.]fun domain likely isn't part of LAPSUS$ infrastructure. It likely belongs to "Christian Rojas" from Okta whose account was compromised ("chrisro" = "Christian Rojas"). Pointing this out to clarify an earlier incorrect assumption. **https://t.co/hP5jQJeAuo**