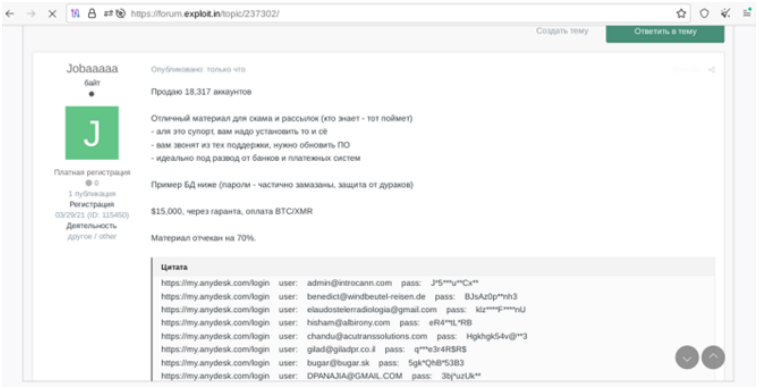
ANYDESK INCIDENT: CUSTOMER CREDENTIALS LEAKED AND PUBLISHED FOR SALE ON THE DARK WEB

Pierluigi Paganini February 04, 2024

Resecurity identified bad actors offering a significant number of AnyDesk customer credentials for sale on the Dark Web.

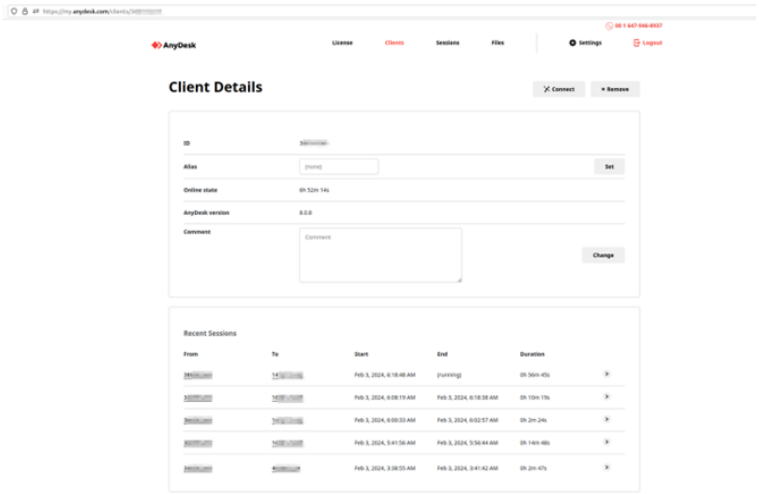
Such information being available for cybercriminals could act as a catalyst for new attacks, including targeted phishing campaigns. Having additional context about a particular customer, the probability of a successful compromise could increase significantly. For example, one possible scenario could involve these details being used in malicious emails sent on behalf of the software vendor, managed services providers (MSPs), or IT outsourcing companies with the goal of acquiring sensitive information – in such case, downstream damage may be significant. The sources and methods for acquiring data of this nature may vary depending on threat actors' unique Tactics, Techniques, and Procedures (TTPs). While this credential leak is widely believed to be the result of infostealer infections, this uncertainty nevertheless creates a new area of concern. Assuming the prevailing infostealer hypothesis is correct and considering the latest incident disclosure, timely password resets would be a mandatory mitigation measure for all AnyDesk customers. The end-users of AnyDesk include IT administrators, who are often targeted by threat actors. Thus, it is critical that AnyDesk ensures this cyberattack hasn't impacted access to any other critical

systems to which their IT admins may have privileged access.. By gaining access to the AnyDesk portal, bad actors could learn meaningful details about the customers – including but not limited to the used license key, number of active connections, duration of sessions, customer ID and contact information, email associated with the account, and the total number of hosts with remote access management software activated, along with their online or offline status and IDs.

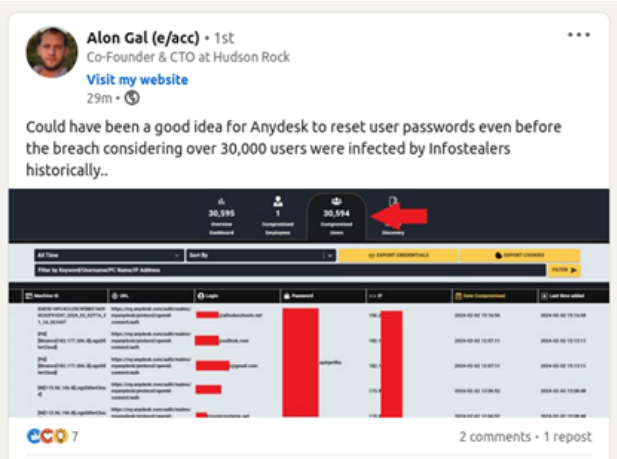


It is possible that cybercriminals familiar with the incident are hurrying to monetize available customer credentials via the Dark Web acquired from different sources, understanding that AnyDesk may take proactive measures to reset their credentials. Such data could be extremely valuable for both initial access brokers and ransomware groups familiar with AnyDesk, often abused as one of the tools following successful network intrusions. Notably, per additional context acquired from the actor, the majority of exposed accounts on the Dark Web didn't have 2FA enabled.

Notably, the timestamps visible on the shared screenshots by the actor illustrate successful unauthorized access with sessions dated Feb 3, 2024 (post-incident disclosure). Some users may not have changed their password, or this process might still be ongoing. Handling remediation, especially for a large customer base, is complex and may not be instantly executed.



Per a public statement from AnyDesk on February 2, 2024, “as a precaution, we (AnyDesk) are revoking all passwords to our web portal, my.anydesk.com, and we recommend that users change their passwords if the same credentials are used elsewhere.” However, there seems to be an issue with it. Other cybersecurity experts, such as Alon Gal, Co-Founder & CTO of Hudson Rock, have also noticed the issue and alerted the broader community. According to Gal, over 30,000 user credentials could be circulating on the Dark Web due to infostealer activity. Proper mechanisms should be considered to mitigate the risk of customer compromise, regardless of the past incident announcement.



Dark Web actors have expressed a strong interest in AnyDesk customer credentials. The opportunity to acquire them in bulk will be extremely attractive for actors involved in spam, online banking theft, scam, business email compromise (BEC), and account takeover (ATO) activities. The spectrum of cyber risks associated with this new development transforms proportionally, ranging from the use of this information in further fraudulent and scam campaigns to targeted phishing and malicious cyber activity.

Resecurity informed AnyDesk and notified multiple consumers and enterprises whose credentials have been exposed on the Dark Web.

Notably, the activity with AnyDesk comes right after Cloudflare announced it was targeted, along with Microsoft and Hewlett Packard Enterprise disclosing cybersecurity incidents conducted by a suspected nation-state attacker.

Additional details are available in the analysis published by cybersecurity firm Resecurity:

https://www.resecurity.com/blog/article/following-the-anydesk-incident-customer-credentials-leaked-and-published-for-sale-on-the-dark-web

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

Pierluigi Paganini

(**SecurityAffairs – hacking, AnyDesk**)

AnyDesk Cybercrime Dark Web Hacking hacking news information security news IT Information Security malware Pierluigi Paganini Security Affairs Security News