10 June 2022

Facts about the ransomware attack on Equis

What happened?

Recently our network monitoring system detected a multiple systems failure affecting certain of our back-up servers in Singapore. Upon investigation it was revealed that the source of the failure was a ransomware cyber-attack.

The preliminary results of our investigation indicate that a significant portion of our historic funds data covering the period from 2012 through 2020 was affected by "LockBit" encryption ransomware and potentially copied

We maintain unaffected and full back-ups of all compromised data. There is no ongoing threat to our systems from this attack and our ability to conduct business is unaffected.

Information Impacted?

We continue to ascertain the scope of the information affected by this event, however, we believe that no information after 5 January 2021 has been accessed, encrypted or illegally copied.

As particularly relevant to current and former employees of Equis and any of its affiliated companies, we identified that the personal data of staff employed by Equis between 2012 and 2020 maintained by HR in connection with staff employment has likely been compromised. Although we do not believe that any password data has been compromised, out of caution please consider changing passwords related to financial or other sensitive accounts.

Please be particularly cautious of any requests seeking to obtain further data or information from you or contact from individuals purporting to work with Equis.

Where can I obtain further information?

Please direct any questions to Data-info@equis.com

1 George Street, #23-03, One George Street, Singapore 049145
P: +65 6220 0040 | F: +65 6220 0042

2022 년 6 월 10 일

에퀴스 랜섬웨어 공격에 대한 안내문

무슨 일이 발생하였나요?

최근 당사는 내부 네트워크 모니터링 시스템을 통하여 싱가포르 일부 백업 서버에 영향을 미친 다수의 시스템 장애를 감지했습니다. 조사 결과, 해당 장애의 원인이 랜섬웨어 사이버 공격이라는 것이 밝혀졌습니다.

당사의 예비 조사 결과, 2012 년부터 2020 년까지의 기간에 해당하는 과거 펀드 데이터의 상당 부분이 "LockBit" 암호화 랜섬웨어의 영향을 받았으며 해당 데이터들이 복사되었을 가능성도 있음이 확인되었습니다.

당사는 손상된 모든 데이터를 피해 없이 완벽하게 백업하고 있습니다. 또한 현재 해당 공격으로 인한 진행중인 위협은 없으며 당사의 비즈니스 수행 능력도 영향을 받은 바 없습니다.

어떠한 정보가 유출되었나요?

당사는 해당 공격으로 인하여 유출된 정보의 범위를 지속적으로 파악 중에 있습니다만 2021 년 1 월 5 일 이후에 해당하는 그 어떠한 정보도 접근, 암호화 또는 불법 복제되지 않은 것으로 판단하고 있습니다.

특히 에퀴스 및 관계사의 전·현직 임직원 정보와 관련하여, 당사는 인사팀에서 보관 중이였던 2012 년부터 2020 년 사이에 고용관계가 있던 임직원의 개인정보가 유출되었을 가능성이 있음을 확인하였습니다. 비밀번호 데이터는 유출되지 않은 것으로 사료되지만, 만의 하나라도 있을지 모르는 피해를 예방하기 위하여 금융 또는 기타 민감한 계정과 관련된 비밀번호를 변경을 고려하여 주시기 바랍니다.

1 George Street, #23-03, One George Street, Singapore 049145
P: +65 6220 0040 | F: +65 6220 0042

귀하께서는 추가적인 데이터 또는 정보를 요구하거나 에퀴스와 함께 일한다고 사칭하는 자로부터의 연락에 각별히 유의하여 대처해주시기를 당부드립니다.

추가적인 정보는 어디서 얻을 수 있나요?

KR-Data-info@equis.com / equis@equis.com 으로 문의 주시기 바랍니다.

[*Followed by a Japanese version*]

1 George Street, #23-03, One George Street, Singapore 049145
P: +65 6220 0040 | F: +65 6220 0042

2022 年 6 月 10 日

当社サーバーに対するランサムウェア攻撃に関するお知らせ

経緯

先般、当社のネットワーク監視システムが、シンガポールに所在する当社のバックアップサーバーに異常を感知したため、調査を行ったところ、ランサムウェアによるサイバー攻撃を受けたことが発覚いたしました。

初期調査の結果、当社が過去に運用していたファンドの2021年から2020年までのデータの多くが LockBit ランサムウェアによって暗号化され、窃盗されたおそれのあることが判明しております。

当社は、影響を受けた全データについて、安全な形でバックアックを有しております。また、当社システムに対するサイバー攻撃の脅威はすでに排除されており、当社の事業継続性に対する懸念もございません。

影響を受けた可能性のあるデータ

攻撃の影響を受けたデータの範囲については、引き続き調査を行ってまいりますが、2021 年1月 5 日以降のデータについては、不正アクセスを受けておらず、暗号化も違法コピーもなされていない点は明らかになっております。

他方、2012 年から 2020 年の間に当社グループに在籍していた従業員の情報が、攻撃を受けたデータに含まれていた可能性が高いことが判明しております。パスワードが付されていた情報については、暗号化されていないものと思われますが、念のため、銀行口座など、機密性が高い情報に関するパスワードについては、お手数でございますが、変更をご検討いただきたく存じます。

今後、当社や当社の業務関係者を名乗る者から、更なる情報の提供を求める要請や接触がある可能性がございますので、関係各位におかれましては、十分な注意を払っていただきますようお願い申し上げます。

本件に関するお問合せ先

JP-Data-info@equis.com