INFORMATIONAL

Ransomware Data Leak Sites Report

TLP:GREEN

Apr 04, 2023

A valued colleague is providing this daily ransomware tracker as **TLP:GREEN** for purposes of increasing ransomware threat awareness. The body of the email contains newly added victims since the last update.

The information provided in the report is pulled from threat actor data leak sites ‘as is,’ meaning, it is shared as it has been posted by the threat group. They have been known to make mistakes, have typos, mis-name victims, or use other language aside from the victim name. The report shares the information ‘as is’ and neither the source of the report, nor our team, goes to the individual sites to verify the information, though it can be (and we sometimes do) cross referenced with other reporting sources. Neither the originator of the report, nor our team, is in direct discussion w/ the threat actors. There are cyber threat intelligence firms that do engage in cybercrime forums and can provide additional perspective of victims and ongoing discussions occurring in those forums.

We share the report for recipient awareness. Often times, a victim may be a supplier or have another third or fourth party relationship with recipients. We hope that recipients look for those relationships and then are able to inquire directly as may be appropriate with the supposed victim.

By the time a victim is identified in the name and shame report, it is reasonable to assume they have been contacted by the threat group and have either elected not to make payment or that some other issue has led the group to disclose the victim publicly. Victims that pay do not usually have their data made available publicly. We have not seen a significant amount of incidents that were deliberately falsely reported by threat groups, though, as noted above, they have made mistakes.

Please be advised the .txt and .csv attachments that typically accompany this report will no longer be provided per collection source.

This is your 2023-04-03 report for new victims listed on 'name and shame' or data leak sites (DLS).

BlackBasta

- Shively Bros., Inc., Automotive, United States
- Corporate Technologies LLC, Information Technology and Services, United States
- Precision Fabrics Group, Inc., Textile Manufacturing, United States

LockBit 3.0

- Revv Aviation, Airlines and Aviation, United States
- Errebielle Srl, Furniture, Italy
- Verne Technology Group, S.L., IT Services and IT Consulting, Spain
- The Ned, Hospitality, United Kingdom

Medusa

- SONDA S.A., IT Services and IT Consulting, Chile

Money Message

- Mid-American Glass, Inc., Consumer Goods, United States
- Guess who!

Nokoyawa

- Pueblo Mechanical & Controls, LLC, Construction, United States

Royal

- Steve Silver Company, Furniture, United States
- Teijin Carbon America, Inc. / Toho Tenax America, Chemicals, United States
- 5+design, Architecture and Planning, United States
- Sunstar Americas, Inc., Consumer Goods, United States
- Corizon Health, Inc., Hospitals and Health Care, United States

Stormous

- Archiplus, Architecture and Planning, Hong Kong
- Ocean Engineering Undergraduate Program, Bandung Institute of Technology, Higher Education, Indonesia
- Metal Work S.p.A., Automation Machinery Manufacturing, Italy
- The Wholesale House, Inc., Manufacturing, United States
- Sage
- TreeNovum S.L., Program Development, Spain

Release Date
1680667199

Alert ID 615a4551

View Alert

Tags Ransomware Data Leaks

TLP:GREEN Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

Access the Health-ISAC Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.