INFORMATIONAL

Ransomware Data Leak Sites Report

TLP:GREEN

Nov 23, 2021

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.

New victims listed:

::: Bonaci Group :::
==========
Victim / Company Name Date First Seen by Tracker
--- ---
Marshall Investigative Group 2021-11-22 19:05:01.963375+00:00

::: CL0P :::

==========
Victim / Company Name Date First Seen by Tracker
---------- ----------
EDAN[.]COM 2021-11-22 16:05:02.856525+00:00

::: Conti :::
==========
Victim / Company Name Date First Seen by Tracker
---------- ----------
Dealers Auto Auction Group 2021-11-22 00:05:03.069039+00:00
DKS Deutsch Kerrigan LLP 2021-11-22 12:35:02.458675+00:00

- The E-ISAC has recently come across information that the Conti ransomware group has claimed the New Orleans-based law firm Deutsch Kerrigan LLPas a victim on their leak site. The law firm provides services to businesses in a variety of sectors, including:
    - Aviation – “Deutsch Kerrigan attorneys have defended numerous claims arising from the aviation activities of both commercial and general operators”
    - Finance – “Deutsch Kerrigan provide legal services to banking institutions including closing commercial transactions, drafting and negotiation of contracts, mergers and acquisitions and representation in litigated matters including claims of lender liability, directors and officers liability, letters of credit, force placed insurance, cyber liability and labor and employment disputes.”
    - Commercial Real Estate – “Firm clients include contractors, developers, joint venturers, managers, property owners, investors, landlords and tenants, as well as lenders, borrowers, equity funds, public entities, and institutions.”
    - Healthcare – “Deutsch Kerrigan attorneys have extensive experience in defending medical practitioners, hospitals, nursing homes, assisted living centers and other affiliated medical providers.”
    - Maritime - Our admiralty and maritime attorneys routinely handle matters related to Death on the High Seas Act (DOSHA) claims, offshore platform casualties, marine insurance coverage opinions and disputes, Jones Act, collision, allision, fire, stranding, sinking, towage and property damage cases of all kinds, including pipeline, rig and platform damage arising from marine operations in the offshore petroleum industry.

    - Retail and restaurant – “Our attorneys counsel restaurants and retailers in the Gulf South region. Our team of attorneys is well-positioned to represent retailers and restaurant companies in a number of markets and jurisdictions.”
    - Transportation – “We represent trucking companies, commercial aviation companies, manufacturers of transportation products, rental car companies and insurers and numerous insurance companies.”
    - Oil and gas – “With a comprehensive team of attorneys, we focus on the many aspects of litigation and the law as it relates to the energy sector. If you are involved in the exploration, production, refinement, or marketing of oil & gas along the Gulf Coast, let Deutsch Kerrigan partner with you today.”
- As of the time of sharing, Conti have not specified on their leak site the quantity or nature of the data they have allegedly stolen from Deutsche Kerrigan.

::: Everest :::
==========
Victim / Company Name Date First Seen by Tracker
---------- ----------
Charlie Hebdo 2021-11-22 13:05:02.126161+00:00. The controversial French publication experienced a tragic terrorist act in Jan 2015.

::: Grief :::
==========
Victim / Company Name Date First Seen by Tracker
---------- ----------
Charley's Greenhouse Supply, LLC 2021-11-22 21:35:03.471322+00:00

::: HiveLeaks :::
==========
Victim / Company Name Date First Seen by Tracker
---------- ----------
GryphTech 2021-11-22 11:05:02.413900+00:00
The British Columbia Institute Of Technology 2021-11-22 12:05:02.674015+00:00

::: Karakurt :::

==========
Victim / Company Name Date First Seen by Tracker
---------- ----------
Yanmar 2021-11-22 16:05:02.856525+00:00

::: LV :::
==========
Victim / Company Name Date First Seen by Tracker
---------- ----------
reigroup[.]com 2021-11-22 17:05:01.767476+00:00

::: LockBit 2.0 :::
==========
Victim / Company Name Date First Seen by Tracker
---------- ----------
mecfond[.]com 2021-11-22 03:35:02.249344+00:00
roteritaly[.]com 2021-11-22 15:35:01.903541+00:00
wnrllc[.]com 2021-11-22 16:05:02.856525+00:00
planters-oil[.]net 2021-11-22 16:05:02.856525+00:00
fluidsealingproducts[.]com 2021-11-22 16:05:02.856525+00:00
kankakeetitle[.]com 2021-11-22 16:05:02.856525+00:00

- The E-ISAC recently came across information regarding a data breach carried out by the LockBit 2.0 Ransomware operators on Kankakee County Title Co. “Kankakee County Title Company was founded in 1910. The company's line of business includes searching real estate titles.” At the time of this writing, it does not appear any of the obtained files have been published to LockBit’s site, though it should be noted, the “date of publication” is scheduled for 11/26/2021. I have attached a screenshot from LockBit’s site for your reference.

::: Vice Society :::
==========
Victim / Company Name Date First Seen by Tracker
---------- ----------
Holy Family RC & CE College 2021-11-22 08:35:02.582549+00:00
City of Witten 2021-11-22 08:35:02.582549+00:00

Release Date
Nov 23, 2021

Alert ID c2ec6bac

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.

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**