ThreatMon

# Ransomware Group Activity Report

*05.11.2022 - 18.11.2022*

@threatmon

@MonThreat

# ThreatMon

# Ransomware Group Activity Report

ThreatMon Threat Intelligence created a report on **two weeks** of ransomware activity by tracking posts by ransomware groups on Dark Web leak sites.

According to ThreatMon's one-week security survey, there were **106** ransomware attacks. The United States was the most targeted country. In addition, the most targeted sectors are Industry, Technology and Finance.

ThreatMon will continue to share monthly ransomware reports. You can easily access these posts from our social media accounts.

## Key Points:

1. Number of Attacks by Ransomware Groups
2. Number of Attacks by Countries
3. Number of Attacks by Sectors
4. IOC List of Ransomware Groups

# Table of Contents

# 1. Number of Attacks by Ransomware Groups

The most active group during this one-week period was the **LockBit 3.0** ransomware group. LockBit 3.0 had **4** missing attacks compared to the number of attacks in the report last week, but it was the most active ransomware group in this week's period.

Targeting the **Technology** sector the most, **LockBit** took the **Real Estate** sector as the second target and the **Finance** sector as the third target.

Targeting the United States, the most as a country, LockBit targeted Canada as the second and United Arab Emirates as the third.

The second most active group during this one-week period was the **Royal** ransomware group. Royal carried out an equal number of attacks in the report last week, with a total of **18** attacks.

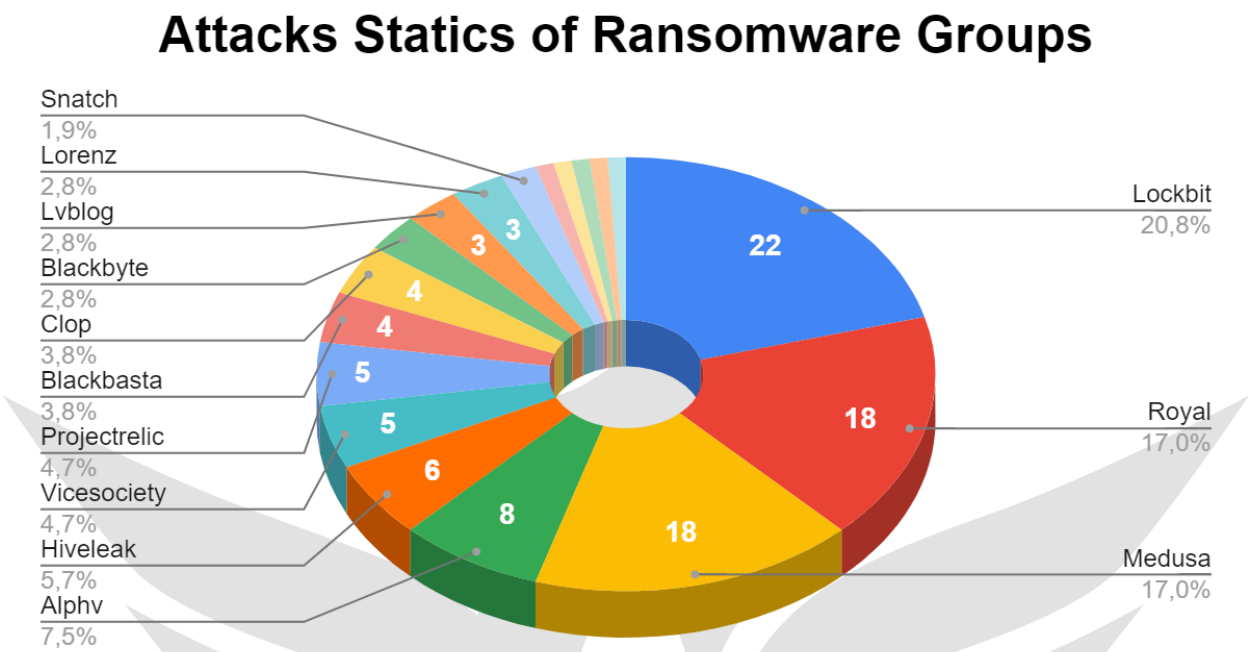
Targeting the **Industry** sector the most, **Royal** took the **Logistics** sector as the second target and the **Engineering** sector as the third target.

Targeting the **United States** the most as a country, **Royal** targeted **Canada** second and **Germany** third.

The third most active group during this one-week period was the **Medusa** ransomware group. Medusa did not appear as active in last week's report, but she carried out **18** attacks in this week's report.

Medusa, targeting the **Industry** sector the most, took the **Insurance** sector as the second target and the **Software** sector as the third target.

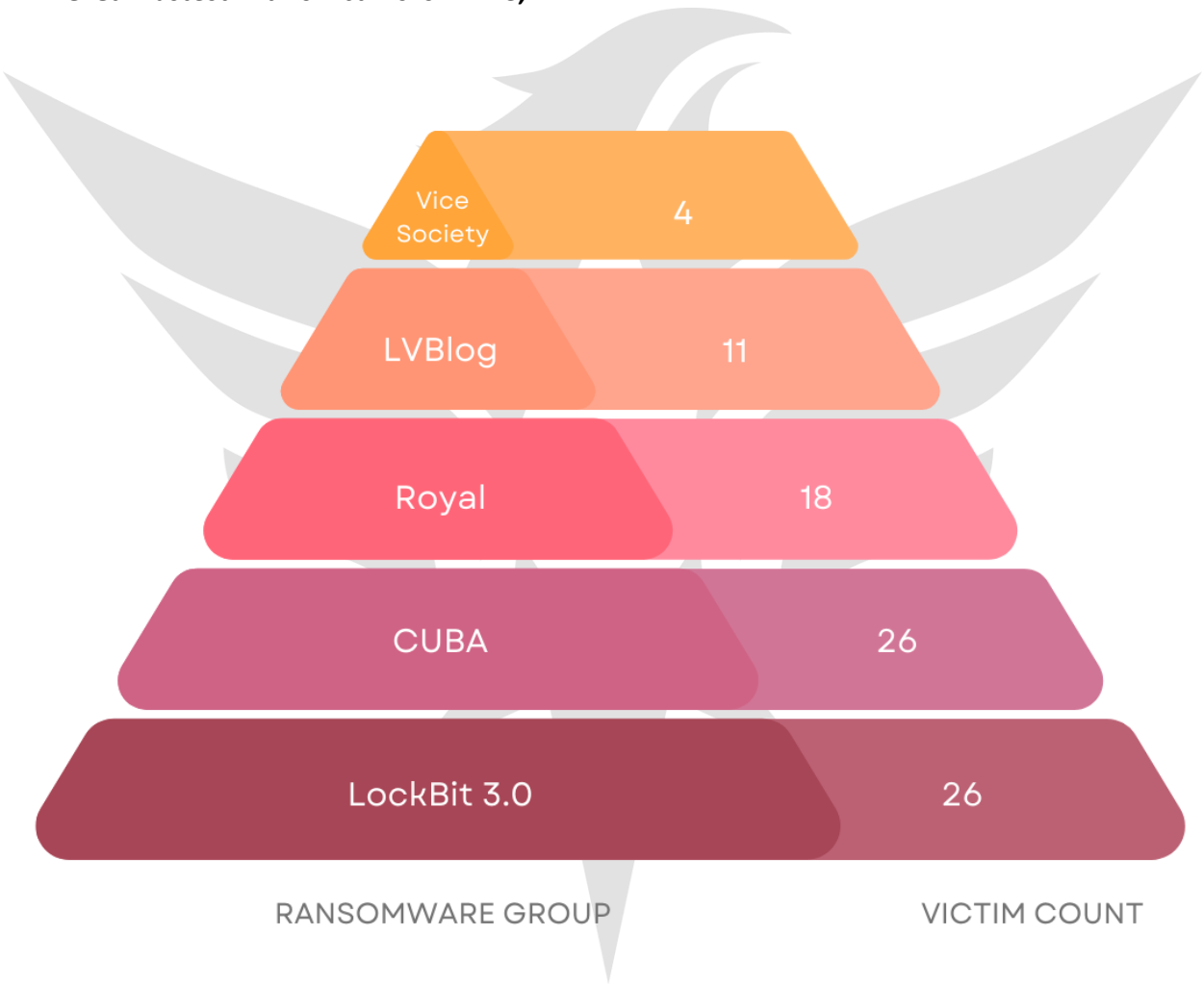
Targeting the **United States** the most as a country, **Medusa** targeted **Italy** second and **United Kingdom** third.




The table contains a graphical version of how many cases there are by ransomware groups. There is not much change in the groups compared to last week. Numerically, the total number of attacks is very close to each other.

The Ransomware Groups in the top ten are as in the image;

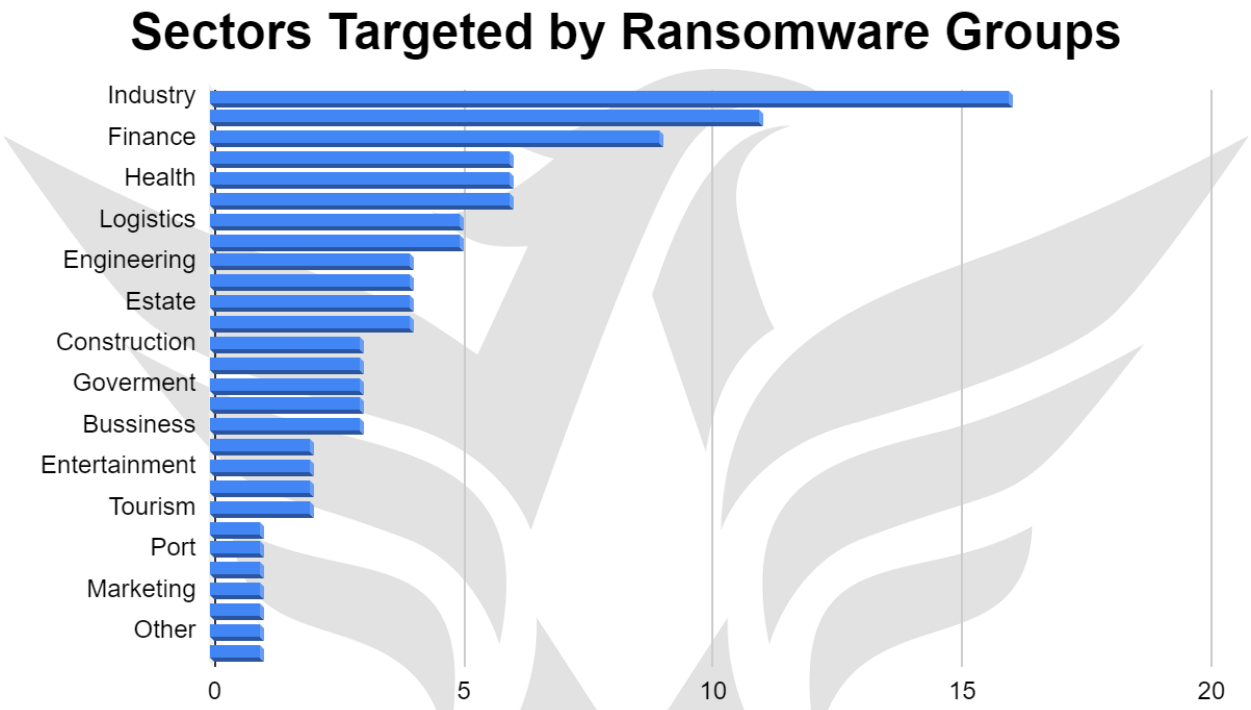
- **LockBit 3.0** is the first with 22 victims,
- **Royal** second, with 18 victims,
- **Medusa** third with 18 victims,
- **AlpHV** fourth with 8 victims,
- **HiveLeak** lastest with 6 victims is in line**,**



# 2. Number of Attacks by Sectors

Ransomware groups mostly prefer to attack **Industry** sectors in early October.

The second most attacked sector was the **Finance** sector.

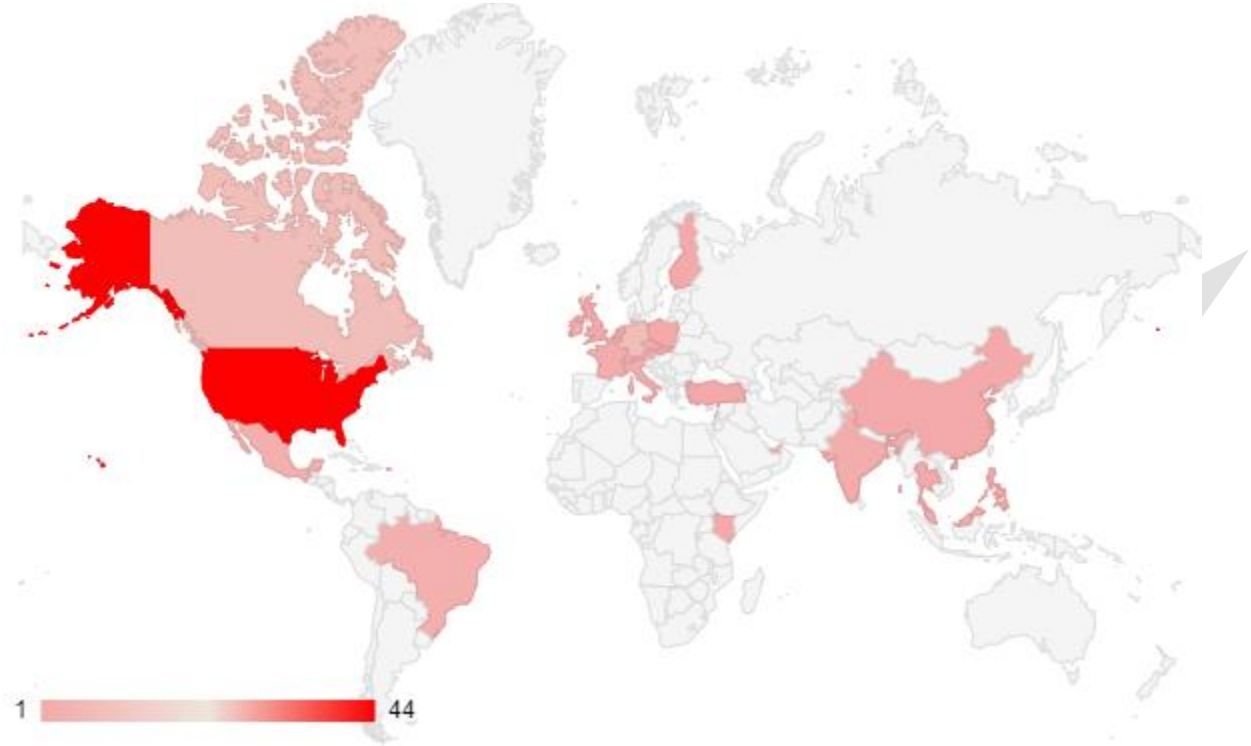



As in the previous report, there are not many sectors that have changed on a sectoral basis. The previous report had a lot of attacks on the **Industry** sector, but this week there are more attacks on the **Industry** sector.

The target of current attacks is **Industry**, **Finance** and **Healthcare** sectors.

# 3. Number of Attacks by Countries

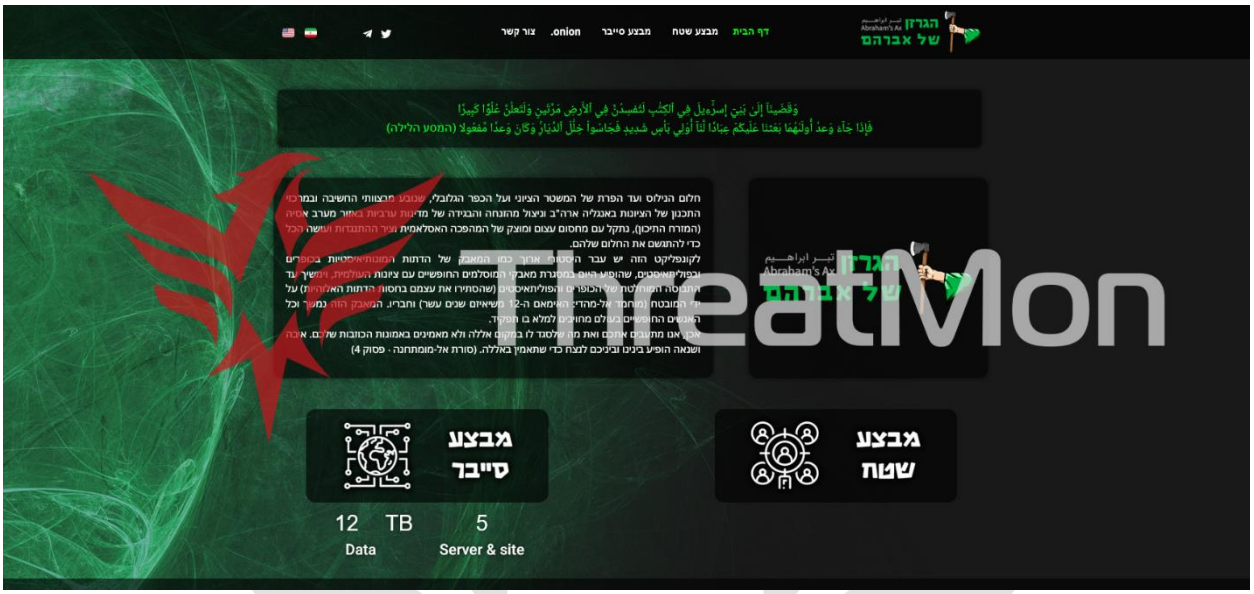
According to the study, the **United States** received a total of 44 attacks this week. The second of this week was **Canada** and **Germany** with 8 victim, and the third was the United Kingdom.



# Important Ransomware Group Activities

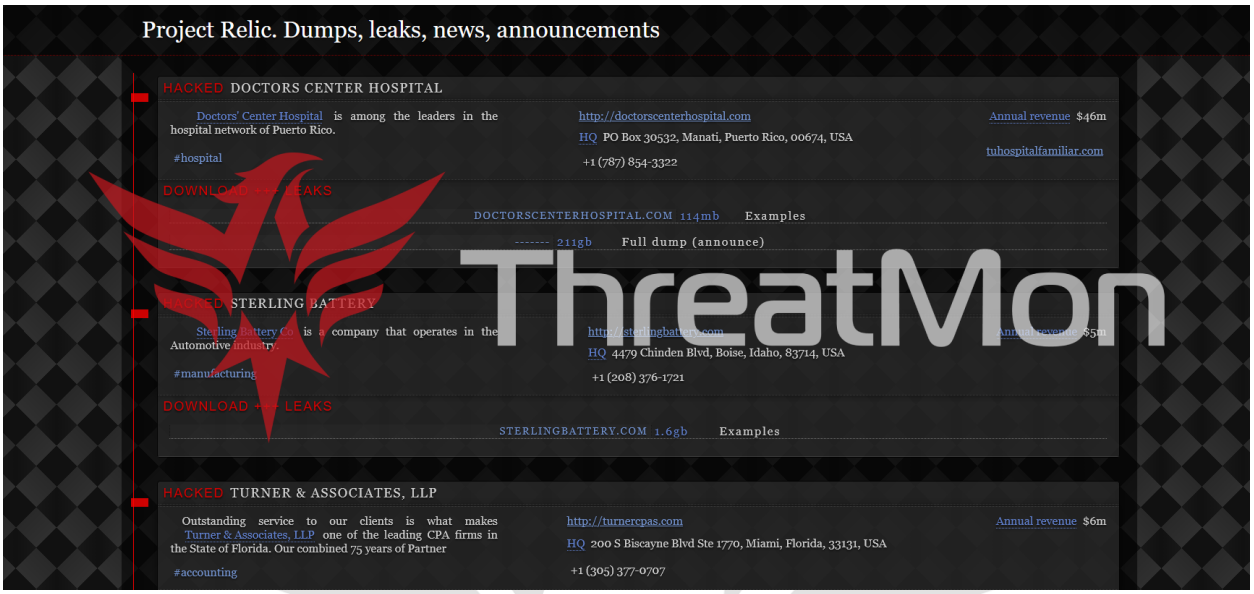
# Abrahams-AX

According to the DarkWeb Ransomware activity Detected by the ThreatMon Team, a newly launched Ransomware group has been detected. The **Abrahams-AX** Group is thought to be the successor of **Moses Staff**.



# ProjectRelic

According to DarkWeb Ransomware activity Detected by ThreatMon Team, a newly launched Ransomware batch has been detected. The group introduced its name as **ProjectRelic**.



# 5. IOC List of Ransomware Groups

**ThreatMonIT** recommends adding shared IOCs to your blacklists of security devices to avoid ransomware attacks. We will share with you as we reach new IOCs.

| Group Name | Type | Indicator |
|---|---|---|
| LockBit 3.0 | SHA-256 | F41ABD588CEF0ED3E46F91C73014CC17327200FB41CE2DEAFAACDE023FEDFE01 |
| LockBit 3.0 | SHA-256 | F6FBFA9FE38F69F8806D60072B7E8A9ACEACF4A2B27095F7297F529BA986EAB4 |
| LockBit 3.0 | SHA-256 | ED266B1B8B19DE457D48A7BFE4C6094557B35734CB63362A63A1A5392083BCE7 |
| LockBit 3.0 | SHA-256 | 9A0F32EB9DA6CD8F3F4DB8C49C87999374C5F045F51F8011CA29713743EC4CFF |
| LockBit 3.0 | SHA-256 | 190BD1403DF2F46BFC864957B211D49E3177A30D0CE816F6CC0425E43E346285 |
| LockBit 3.0 | SHA-256 | 367F5B45DA98215FF297E0856E4A961C9E831E4F06457F16453F60D0CF407449 |
| LockBit 3.0 | SHA-256 | A736269F5F3A9F2E11DD776E352E1801BC28BB699E47876784B8EF761E0062DB |
| LockBit 3.0 | SHA-256 | 58260A6687486E39DC46461270B391280B7D59997D84B6639230D95E3BDFCA23 |
| LockBit 3.0 | SHA-256 | A0DB5CFF42D0EE0DE4D31CFF5656ED1ACAA6B0AFAB07D19F9F296D2F72595A56 |
| LockBit 3.0 | SHA-256 | 4B8FBB8A6E46B9DB78BDF5AC1AA924F901270FE369411BF431FCE8A46C48CA2A |
| LockBit 3.0 | SHA-256 | FC50CC92D099A16505A820A7735AF7B31C10AFD55928F66D3172A36977A92F84 |
| LockBit 3.0 | SHA-256 | C154FF7027CC540DEA86B3390CABBFF4D817BCABD463082073763E8FA198C521 |
| | | |
| ROYAL | SHA-256 | 491C2B32095174B9DE2FD799732A6F84878C2E23B9BB560CD3155CBDC65E2B80 |
| ROYAL | SHA-256 | 7CBFEA0BFF4B373A175327D6CC395F6C176DAB1CEDF9075E7130508BEC4D5393 |
| ROYAL | SHA-256 | C24C59C8F4E7A581A5D45EE181151EC0A3F0B59AF987EACF9B363577087C9746 |
| ROYAL | SHA-256 | 5FDA381A9884F7BE2D57B8A290F389578A9D2F63E2ECB98BD773248A7EB99FA2 |
| ROYAL | SHA-256 | 312F34EE8C7B2199A3E78B4A52BD87700CC8F3AA01AA641E5D899501CB720775 |
| ROYAL | SHA-256 | F484F919BA6E36FF33E4FB391B8859A94D89C172A465964F99D6113B55CED429 |
| | | |
| MEDUSA | SHA-256 | B00BE4DDA45F8670B0E65D37CC7770FA791D869C7E567EA316D84D16283F8009 |
| | | |
| ALPHV | SHA-256 | 133E003CC510E3D2D0C7DF70A603448605641256C88CE64A3BCABB762295D622 |
| ALPHV | SHA-256 | 69417EC104C1DD07E5067110D6E7F3C643C534D14DB65A704BC0C14C223C3001 |
| ALPHV | SHA-256 | 0BA1FFAEE0EF23A65C80075495DDAF6F96D0F1241B71B13981EA094AC5F2796E |
| ALPHV | SHA-256 | 07CB251C6C4262876083E5AD6A02B1C022464A10BAB23C9582661DACC3D6730A |
| | | |
| BLACKBASTA | SHA-256 | 856B5DC509C17F5BE68186B6A8AB272FC0DD12000C978548D8488EE997B015E5 |
| BLACKBASTA | SHA-256 | E9FEFD053B8C77C7DB13D528B97D2B974DFD86775A8CC9C53B8EFDB07DB8842C |
| BLACKBASTA | SHA-256 | A083060D38984E7C6F36DCD2C57EC1AA3F50F9C201C8538257C8CBF2B3217E96 |
| BLACKBASTA | SHA-256 | 15ABBFF9FBCE7F5782C1654775938DCD2CE0A8EBD683A008547F8A4E421888C4 |
| BLACKBASTA | SHA-256 | A9503A3D998E705C37D3BEC7FEA0FF188BCF7E753833C8B4B195E590C4ED9625 |
| BLACKBASTA | SHA-256 | AFFCB453760DBC48B39F8D4DEFBCC4FC65D00DF6FAE395EE27F031C1833ABADA |
| BLACKBASTA | SHA-256 | C532D28F9700ABBA1A4803C3A9D886C8C4FB26F84CF2399C533D68CFDCEC4FA7 |
| BLACKBASTA | SHA-256 | CCE74C82A718BE7484ABF7C51011793F2717CFB2068C92AA35416A93CBD13CFA |
| BLACKBASTA | SHA-256 | D144B61C0626989039AA5EB56BD7D276A22959AEB19D1610CD35359A2EE85DC1 |
| BLACKBASTA | SHA-256 | D943A4AABD76582218FD1A9A0A77B2F6A6715B198F9994F0FEAE6F249B40FDF9 |
| BLACKBASTA | SHA-256 | 449D87CA461823BB85C18102605E23997012B522C4272465092E923802A745E9 |
| BLACKBASTA | SHA-256 | DC56A30C0082145AD5639DE443732E55DD895A5F0254644D1B1EC1B9457F04FF |
| BLACKBASTA | SHA-256 | 03309C90E6C60A2E3CD44374EFA3003AE10CD9E05BA6A39C77AA5289B32CB969 |

| | | |
|---|---|---|
| **Snatch** | SHA-256 | BF5F4D7B6EF1FDB903677E4EDE04FB49952E08CEE79822B9B53642BB5D1E6F02 |

**You can follow our GitHub Repository to get better IOC data!**

**GitHub Link:** [ThreatMon 05.11.2022 - 18.11.2022 Ransomware Report]

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166