Data leak sites (DLSs)

1. The Ransom Watch site provides a group index, recent DLS posts, group profiles, and statistic/graph pages:

   https://ransomwatch.telemetry.ltd/#/README

2. The Ransom Look site provides a group index, forum and market links, a listing of data leaks, telegram messages, and statistic/graph pages. The team also maintains a GitHub repo that you can review.

   https://www.ransomlook.io/
   https://github.com/RansomLook/RansomLook

3. The Ransom.Wiki site focuses more on allowing users to search for recent victims and/or ransomware groups by name:

   https://ransom.wiki/

4. Dark Feed provides several resources for identifying ransomware DLS and blog information:

   https://darkfeed.io/ransomwiki/
   https://darkfeed.io/ransomgroups/

5. Fastfire’s deepdarkCTI GitHub repo provides and maintains a list of ransomware group sites called “ransomware_gang.md”:

   https://github.com/fastfire/deepdarkCTI/blob/main/ransomware_gang.md

6. The “Ransomware Group Sites” Wiki is a .onion site and must be accessed via Tor. This site provides links to various data leak and victim portal sites:

   http://ransomwr3tsydeii4q43vazm7wofla5ujdajquitomtd47cxjtfgwyyd[.]onion/

Ransomware Playbook:
https://docs.google.com/spreadsheets/d/1lOrsSEUWze4lJyQkHSZXzS6iXsFtoNOFwXf1dYSXIw8/edit?gid=0#gid=0

Download large data:

1. This article aims to assist those attempting to download large data leaks over Tor and can be found

   https://0ut3r.space//2022/09/30/big-files-from-tor/

Communication channel:

1. Tox is an encrypted instant messaging system that uses Tor circuits to anonymize communications. Ransomware groups like LockBit 3.0 prefer Tox for its real-time, anonymous chat capabilities.

   https://tox.chat/

DFIR Report:

1. TheDFIRReport is an excellent resource for understanding how ransomware attacks unfold.

   https://thedfirreport.com/

Sysmon Related topic included configuration and Logging:

1. Michael Hagg maintains a fantastic repo containing a multitude of resources for Sysmon:

   https://github.com/MHaggis/sysmon-dfir

2. Yamato Security's "Ultimate Windows Event Log Configuration Guide for DFIR and Threat Hunting" GitHub. how to enable specific non-default log types that are conducive to ransomware response

   https://github.com/Yamato-Security/EnableWindowsLogSettings

3. Mathias Stuhlmacher's "Awesome Event IDs" GitHub. List of useful Event IDs including information pertaining to how to log the relevant events.

   https://github.com/stuhli/awesome-event-ids?tab=readme-ov-file#event-id-databases

Most Exploited Vulnerabilities:

https://github.com/fastfire/deepdarkCTI/blob/main/cve_most_exploited.md

Living Off Trusted Sites (LOTS) Project:

Sites used frequently for BYOT, data exfiltration, phishing, and other malicious activities. It’s essential to monitor and alert on such domains to prevent and detect these activities.

https://lots-project.com/

DLL Hijacking:
DLL Hijacking, where legitimate DLLs are replaced or hijacked by malicious actors.

https://hijacklibs.net/

Different Remote access tool during its setup and use:

https://www.synacktiv.com/publications/legitimate-rats-a-comprehensive-forensic-analysis-of-the-usual-suspects.html

Contains samples for various malware families, including ransomware families!

The VX-Underground team maintains many malware-related collections. One such collection they maintain is their “Families” collection, which contains samples for various malware families, including ransomware families!

https://vx-underground.org/#E:/root/Samples/Families

The team also maintains an archive with various builders, including ransomware builders!

https://vx-underground.org/

free decryptors for some ransomware variants:

https://www.nomoreransom.org/en/decryption-tools.html

Crypto Sheriff

No More Ransom also provides “Crypto Sheriff,” a tool you can use to determine what strain of ransomware.

https://www.nomoreransom.org/crypto-sheriff.php?lang=en

Encoded commands hunting:

PowerShell commands that begin with (note: begin with, not include within the string!) common characters.

https://gist.github.com/Neo23x0/6af876ee72b51676c82a2db8d2cd3639

AV un- quarantine script:

AV utilities will quarantine Luckily for us, we have resources to pull files out of quarantine!

https://hexacorn.com/d/DeXRAY.pl

In most cases this is done with LOLBAS commands rather than external malware or exploits. More details and examples of the **commands used can be found**

https://dfirtnt.wordpress.com/2020/11/25/detecting-ransomware-precursors/

Rule creation and detection Sigma:

which allow you to paste a Sigma rule in and convert it to multiple formats.

https://uncoder.io/