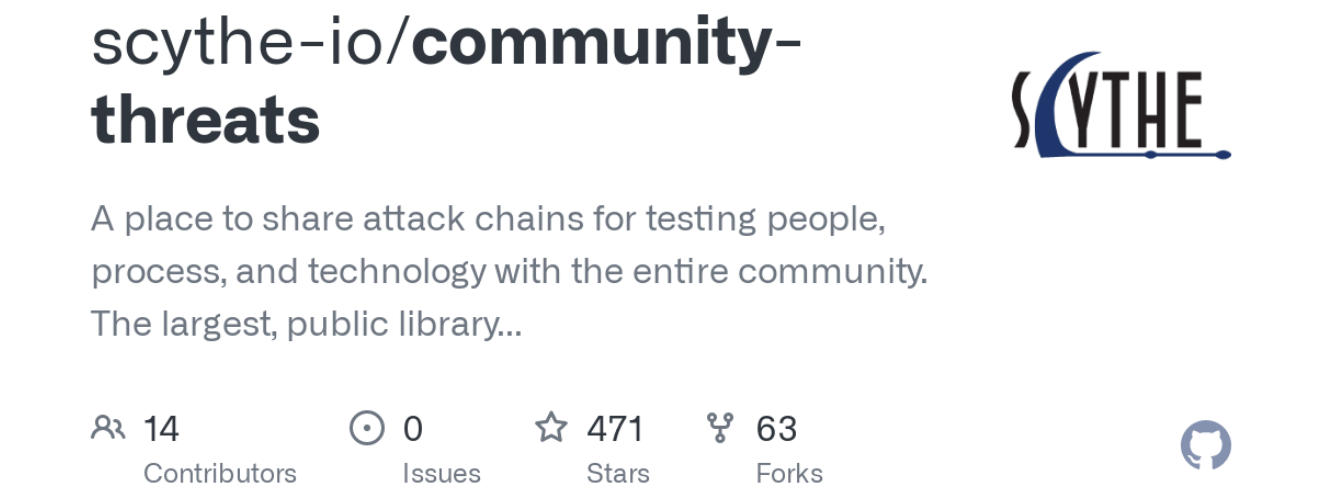
Ryuk Adversary Emulation Plan

github.com/scythe-io/community-threats/tree/master/Ryuk

scythe-io



This threat is explained further in SCYTHE Threat Thursday blog: https://www.scythe.io/library/threatthursday-ryuk

First and foremost, we would like to give a shout out to @TheDFIRReport for providing quality content to the community. SCYTHE is happy to announce we are supporters and encourage you to donate to industry resources that provide quality content. Visit them at https://thedfirreport.com/

We leveraged The DFIR Report's Cyber Threat Intelligence on Ryuk to create and share this adversarial emulation plan. Their report is available to everyone here: https://thedfirreport.com/2020/10/08/ryuks-return/

To emulate:

1. Download and import the threat in JSON format to your SCYTHE instance - https://raw.githubusercontent.com/scythe-io/community-threats/master/Ryuk/Ryuk_scythe_threat.json
2. Download the Virtual File System (VFS) files under Ryuk/VFS
3. Upload the VFS files to your SCYTHE VFS in the following location: VFS:/shared/threats/ryuk
4. Go to the Threat Catalog and select "Threat Thursday - Ryuk Ransomware"
5. Click "Create Campaign from Threat" to start your campaign