2019 - AIP - E72-781 - Ryuk Ransomware Similarity Analysis - Colin Cowie

CERIAS

The Center for Education and Research in Information Assurance and Security

Ryuk Ransomware Similarity Analysis

Colin Cowie and Prof. Anthony H. Smith

Department of Computer and Information Technology

Abstract

In August 2018 a new type of ransomware named "Ryuk" infected several enterprises and encrypted their files for ransom. Unlike traditional generic ransomware, Ryuk disables security controls and is strategically deployed in targeted and well planned attacks. Over $4,000,000 was paid in ransom within the first six months of Ryuk being discovered. There is currently no publicly known technique for decrypting files other than paying the ransom.

Initially Ryuk was misattributed to North Korea but it's now believed to be the efforts of various cybercrime organizations. There has been an increase in the number and variety of Ryuk samples spotted in the wild. This research aimed to track the developments and varieties in Ryuk ransomware overtime. Using python, code similarity analysis was performed to clusters different Ryuk variants.

Detection and Tracking

Yara, the pattern matching malware signature tool, was leveraged to identify and detect Ryuk ransomware. The figure below displays a Yara rule that is comprised of unique strings and regular expressions that are commonly associated with Ryuk. VirusTotal (VT) is an antivirus website and threat intelligence feed with hundreds of terabytes of malware data. Yara was leveraged with VT Intelligence to continuously monitor and alert on new submissions of Ryuk ransomware samples. VT Hunting was used to perform retroactive hunts for Ryuk samples that were previously uploaded to VirusTotal.

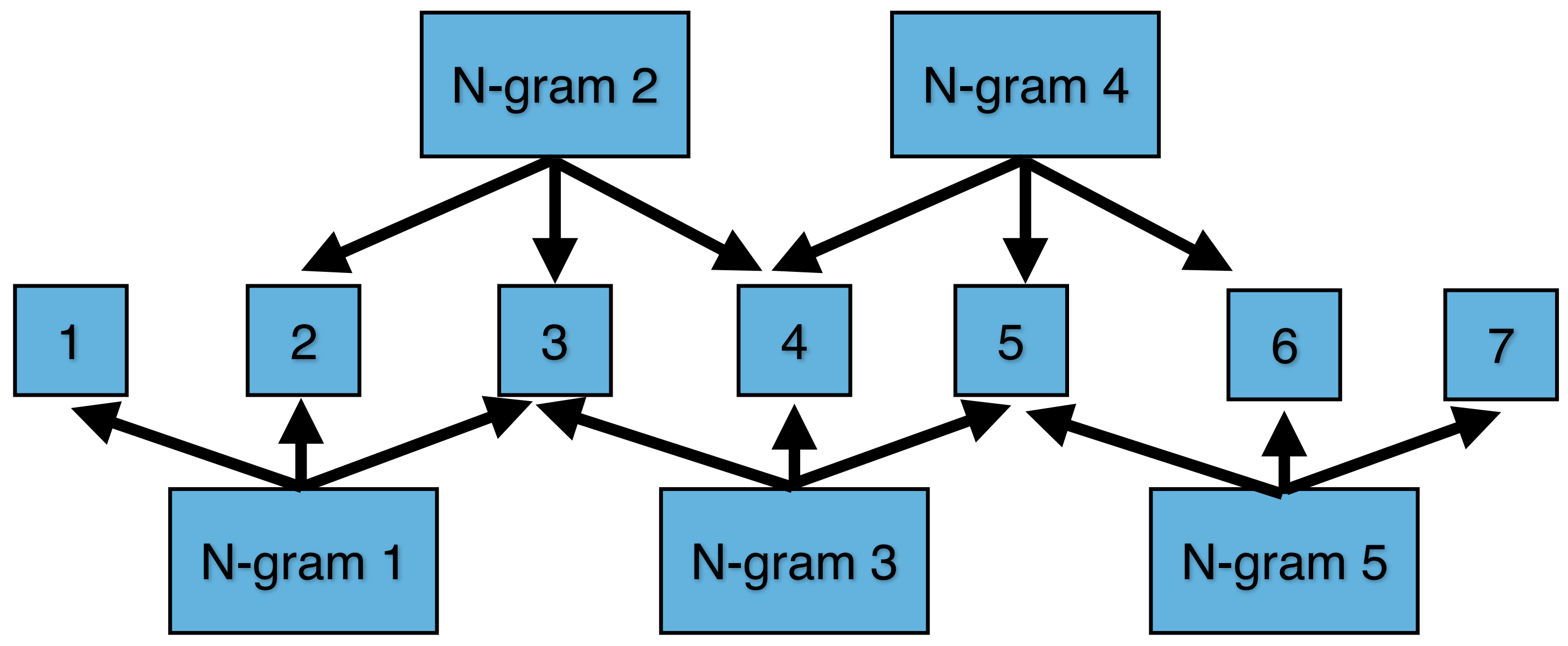
The Viper framework is an open source binary analysis and management framework. It enabled researchers to organize collections of malware. All files that matched the Yara rule detection were added to a viper database to be further analyzed and verified.

```
rule Ryuk_Generic{
   meta:
      description = "Detects Ryuk Ransomware"
      author = "Colin Cowie"
   strings:
      $re1 = /C:\\Users\\Admin\\Documents\\Visual Studio
2015\\Projects\\ConsoleApplication[a-zA-Z]{1-16}\\.pdb/
nocase wide
      $re2 = /^[a-zA-Z0-9]{9}\.dll/ ascii wide nocase
      $s1 = "UNIQUE_ID_DO_NOT_REMOVE" ascii wide
      $s2 = ".RYK" ascii wide
      $s3 = "RyukReadMe.txt" ascii wide
      $s4 = "2 files we unlock for free" ascii wide
      $s5 = "Backups were either encrypted" ascii wide
      $s6 = "HERMES" ascii wide
      $s7 = "AhnLab" ascii wide
      $s8 = "No system is safe" ascii wide
      $s9 = "vssadmin resize shadowstorage"  ascii wide
      $s10 = "\\users\\Public\\window.bat" ascii wide
      $s11 = "Main Invoked." ascii wide
   condition:
      3 of them or ($re1 and 1 of them)
}
```

Methodology

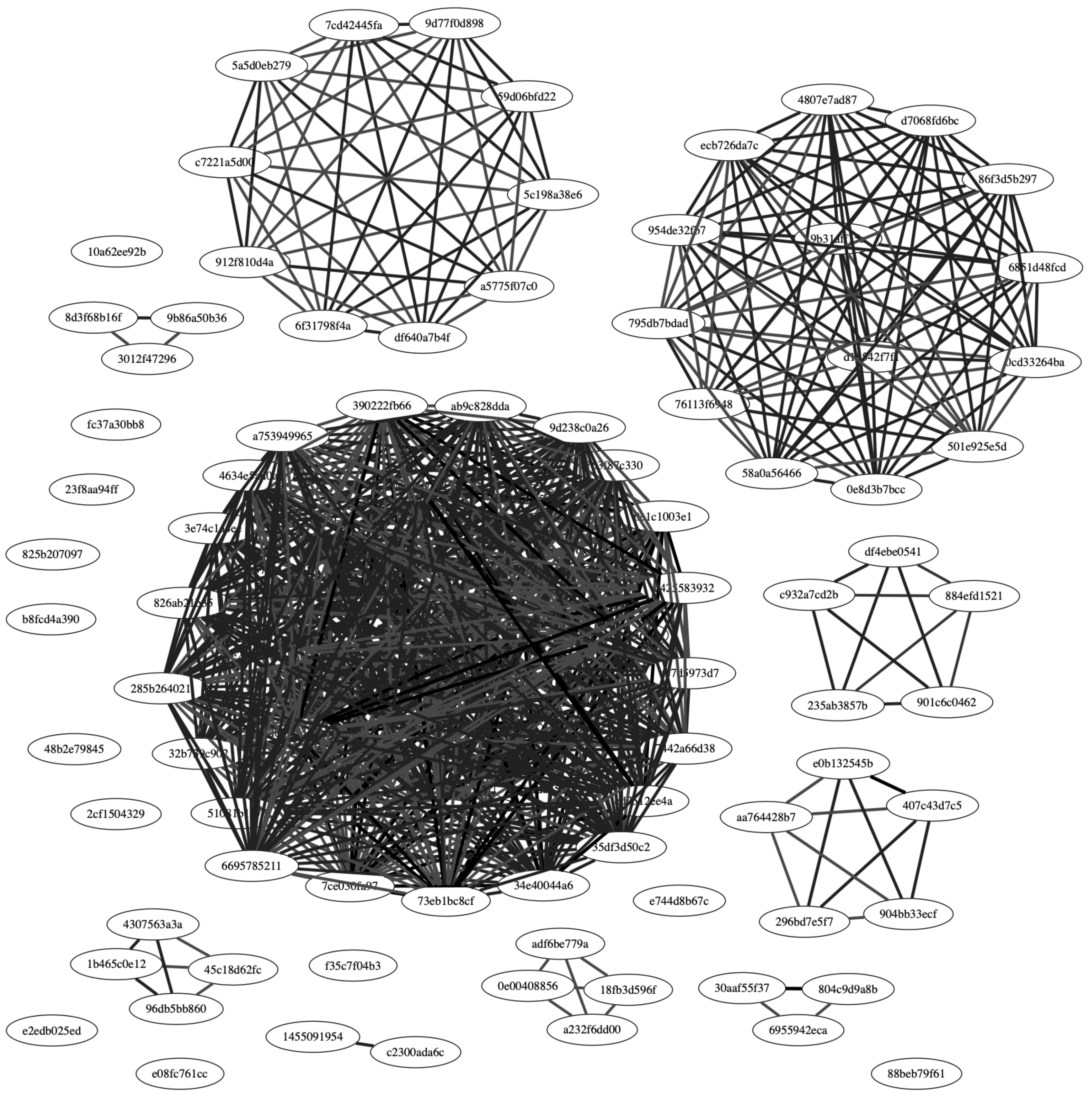
Similarity analysis estimates the amount of shared code between malware samples. It can help researchers better understand changes in development as well as relationships between different malware families. Instead of just comparing the behavior difference of malware, this research analyzed the order in which different malware behaved to improve the accuracy of the results.

N-grams are subsequences of events that have specific lengths. A plugin for the Viper framework was developed to iterate a sequence of events and record the subsequence events at each index. These were classified as N-grams or malware features. N-grams of sequential static strings content was analyzed to classify the malware features. This research compared shared features between malware samples. The number of shared attributes was divided by the total attributes to determine a Jaccard index used to express the degree of overlap between two malware samples



Results

The graph below visualizes malware code similarity among 100 different Ryuk samples. Correlations were drawn among files with a jaccard index of 0.75 or higher.



PURDUE UNIVERSITY Discovery Park

CERIAS