Measuring Crime as a Service Ecosystem

Degree programme: BSc in Computer Science | Specialisation: Digital Business Systems
Thesis advisor: Prof. Dr. Emmanuel Benoist
Expert: Prof.Andreas Fischer

This thesis aims to collect data from the darknet using a web crawler, and to then analyze this data in order to gain insight into cybercriminal operations. In order to accomplish this, darknet pages are first crawled and saved as HTML files. In a second step, these HTML files are programmatically analyzed by extracting relevant data and saving it to a database. In a final step, this data can be queried and compiled into graphs and diagrams.

Jonas Schlegel

Objectives

The tor network, commonly referred to as the darknet, is the perfect place for cybercriminals to conduct business due to its anonymizing nature. The goal of this thesis was to adapt a darknet crawler to gather data on a variety of cyber criminality related darknet pages. The main focus was put on Ransomware-as-a-Service (RaaS) groups, but it also includes a few markets/forums. Goals included measuring the activity of cybercriminals, determining the country of origin of ransomware victims and finding links between ransomware operations and darknet markets/forums.

Crime as a Service

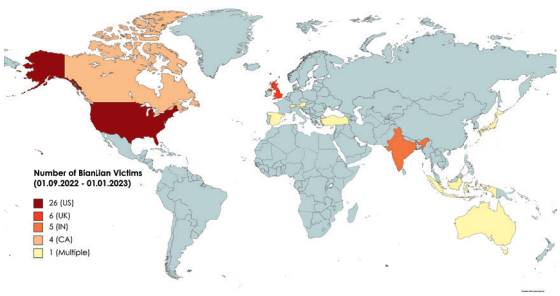
Crime as a Service is a model where criminal services and resources are offered in exchange for money. It is the cybercriminal equivalent of modern IT concepts like Software as a Service (SaaS) and Infrastructure as a Service (IaaS). It is a way for criminals to scale up their operations and make more money than if they were working alone. There are different ways of categorizing Crime as a Service. Usually, multiple types CaaS will be combined to form an economic chain of criminal services.

Results

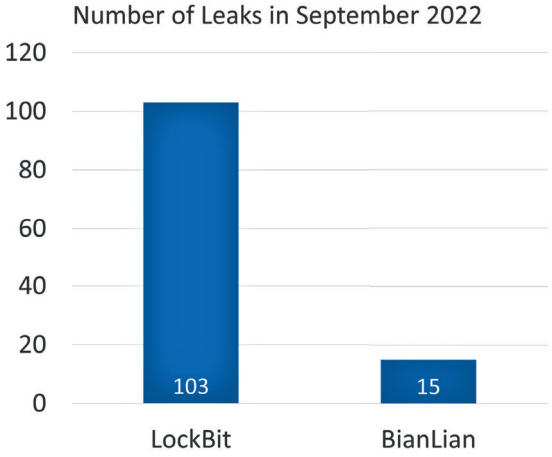
The darknet crawler was successfully used to track the activity of a wide variety of ransomware groups and some forums/markets. Some links between criminal groups and forums could be established. Drawing comparisons between different groups is difficult, as the type and amount of information available varies drastically from site to site. The following is a comparison between one exceptionally active and one moderately active group.

BianLian is a relatively new ransomware group that started its activity around late 2021 to early 2022. It has since grown to be among the most active ransomware groups on the planet. The below map shows countries affected by BianLian between 01.09.2022 and 01.01.2023. As with most other ransomware groups, businesses located in North America and Europe are their main target, however businesses in Asia and Oceania were affected as well. One thing to note is that ransomware victims in the CIS region are exceptionally rare.

One group that stands out among the others that were analyzed is LockBit. LockBit is one of the most active ransomware groups in the world, having leaked the files of over 100 victims in the month of September alone. The below chart shows a comparison of LockBit and BianLian activity in the month of September 2022.



Countries affected by BianLian between 01.09.2022 and 01.01.2023



Number of LockBit and BianLian victims in September 2022