**Ransomware Analysis of Ryuk and REvil ransomware**

By – Harsh Sharma

**What is a ransomware?**

A ransomware is a malicious software when injected into a system can steal the data and encrypt it for better foothold in favour of threat actors.

**How the whole scene works out?**

Threat actors demands some ransom to reverse the attack, if not paid then they will (in most cases) reveal the data in the public forums and dark net. Where the data is used for scams and phishing.

**Ryuk Ransomware**

**History:**

Ryuk Ransomware is derived from Hermes Ransomware. It was first coming in to light on August 2018. Made by Russian e-crime group “Wizard Spider.” The average ransom demanded by Wizard Spider is more than $2,90,000 dollars.

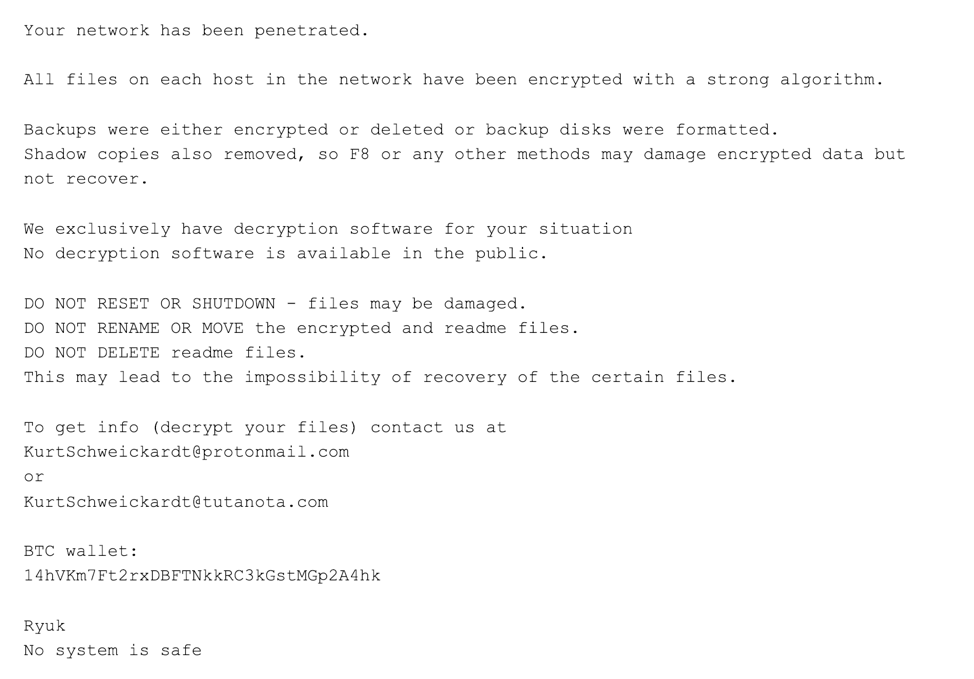
Ryuk Ransomware is used to target big industries, Wizard Spider call this methodology as “Big Game Hunting”.

**Ryuk is specifically used to target enterprise environments.** Code comparison between versions of Ryuk and Hermes ransomware indicates that Ryuk was derived from the Hermes source code and has been under steady development since its release. Hermes is commodity ransomware that has been observed for sale on forums and used by multiple threat actors. However, Ryuk is only used by WIZARD SPIDER and, unlike Hermes, Ryuk has only been used to target enterprise environments. Since Ryuk’s appearance in August, the threat actors operating it have **netted over 705.80 BTC across 52 transactions for a total current value of $3,701,893.98 USD.**

**Anatomy of Ryuk:**

The ransomware comes with 2 parts first is the dropper and the second one is executable payload.

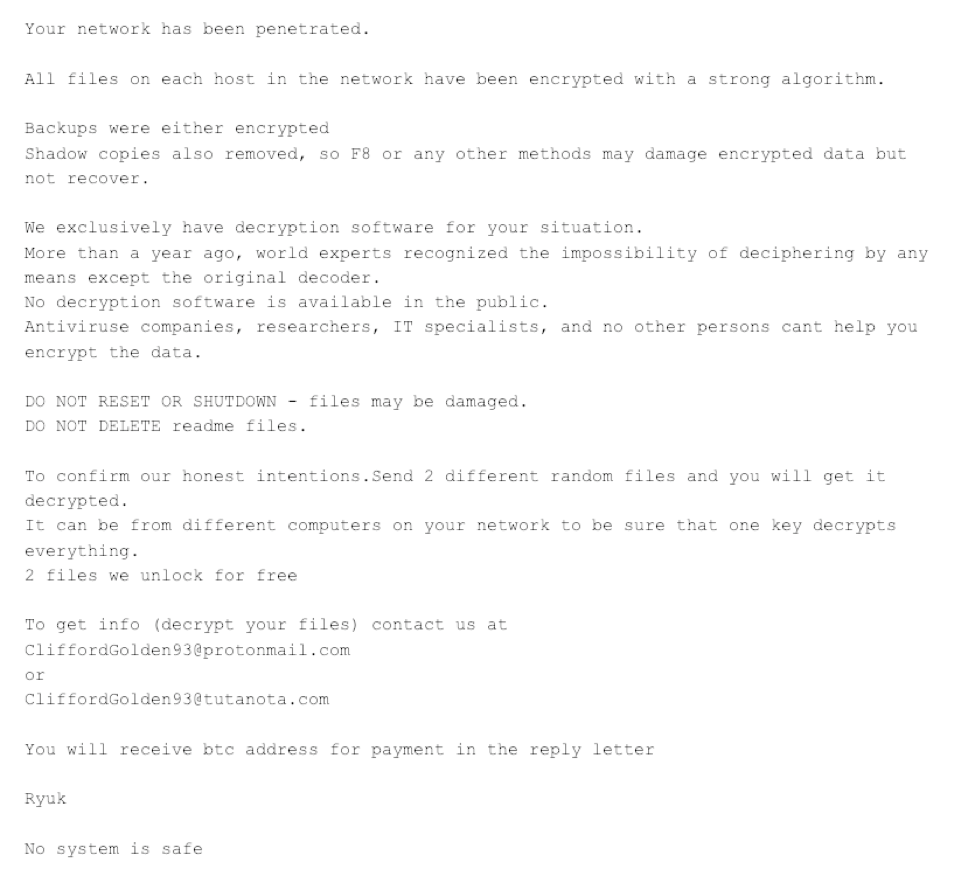
1. Dropper – It is the malware that setups Ryuk on the victim’s system.
2. Executable payload – Part of the payload is to delete the dropper from the system and encryption of data. So that it cannot be retrieved and analysed.



Glimpse of a machine compromised by Ryuk

The ransom email used by Ryuk is unique for each executable. But during the investigation it came to light that their BTC address was same on most ransom notes.

But in the recent variants of Ryuk BTC address is not mentioned and can only be received by contacting the email stated in the ransom notes of Ryuk Ransomware.



Ransom notes of Ryuk Ransomware

Early Ryuk binaries with the removal of BTC address contained a PDB path of

C:\Users\Admin\Documents\VisualStudio2015\Projects\ConsoleApplication54new

crypted try to clean\x64\Release\ConsoleApplication54.pdb.

The PDB path started appearing on Nov 29, 2018.

**REvil Ransomware**

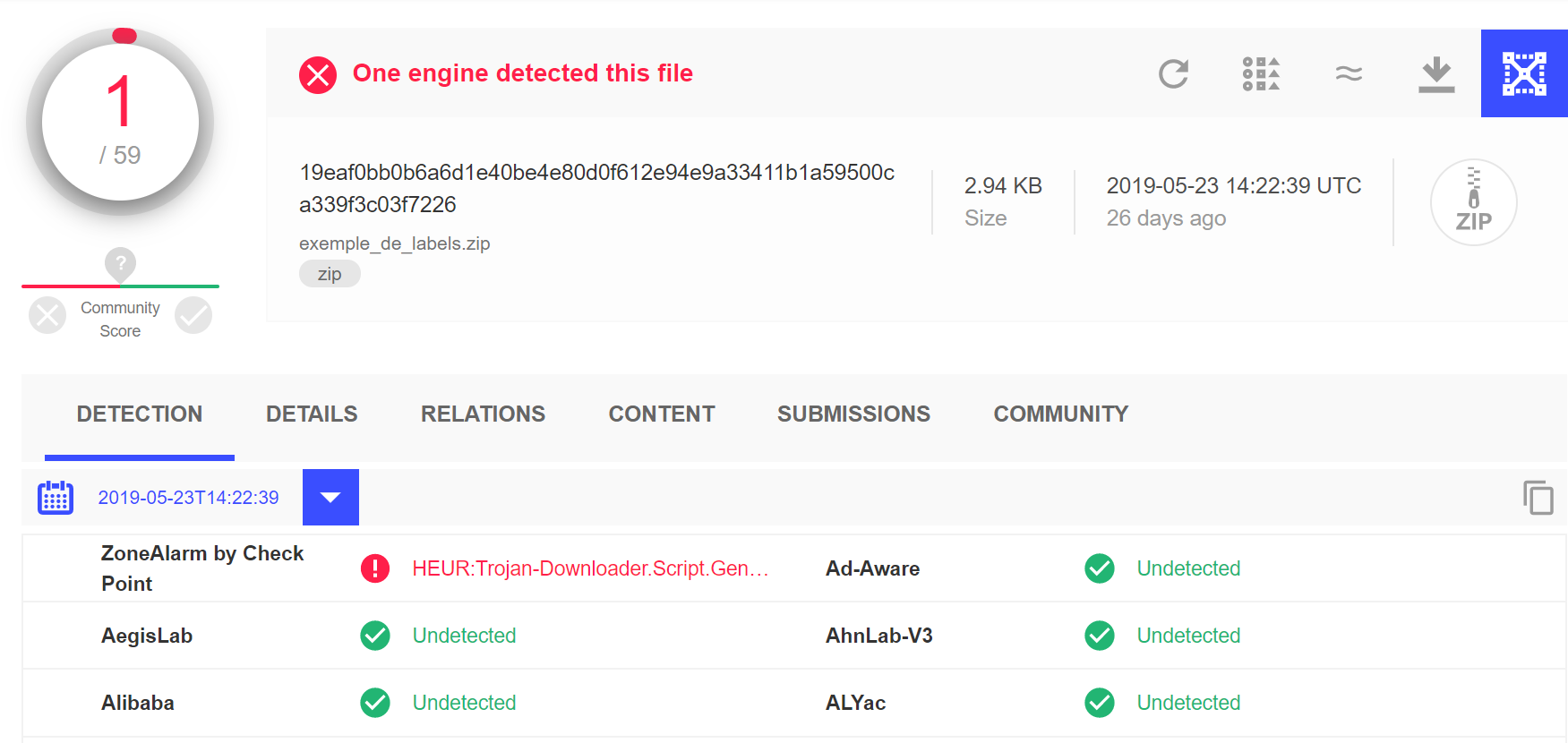
**History:**

REvil word was derived from Resident Evil Franchise (Sodinokibi) and is a RaaS. It is distributed using several different methods including malicious spam email, exploit kits, and RDP vulnerabilities. It has a twist in their Ransom notes stating that “if the ransom is not paid on the time the ransom will be doubled.” The REvil group even offers a “trial offer” to prove the decryption of data collected. It was first coming into light in April 2019 and is one of the most widespread ransomware families in 2020.

**Anatomy of REvil:**

REvil is built upon an older codebase, most likely GandCrab. REvil is very configurable, allowing each user to modify the code to their end goal. According to Secureworks, malicious actors can use the ransomware to exploit CVE-2018-8453 to elevate privileges and exfiltrate host information.

The initial infection vector used by the threat actor is a phishing email containing a malicious link. When pressed, the link downloads a supposedly legitimate zip file that is malicious. REvil / Sodinokibi zip files have a very low detection rate on VirusTotal, which signals that most antivirus vendors do not flag the initial payload as malicious.

Since the initial REvil / Sodinokibi payload can pass undetected, the first layer of defense for many organizations is immediately bypassed: 

REvil zip file detection rate on VirusTotal is low