#RansomAware

Share your story

TALION

Top 5 Ransomware Strains

/ 2021

01 \ RYUK

Origin: 🇰🇵 🇷🇺 *

First seen: **2018**

Est. Revenue: **$150 million in 2020**

Unarguably one of the most active strains on the scene, this crypto-locking variety usually doubles up on malware strains during infiltration, with TrickBot seemingly the favoured weapon of choice for RYUKs operators.

The strain has previously targeted government agencies and large organisations whom the operators know will be able to pay their huge ransom demands.

02 \ Revil AKA Sodinokibi

Origin: 🇷🇺 *

First seen: **2019**

Est. Revenue: **Over $100 Million by 2021**

The infamous banking trojan, has been operating since early 2019. It is believed this strain dominates 11% of all successful attacks and holds the record for the largest ransom payment to date at $50 million from Acer in March this year.

This strain quickly captured the community's attention for its legitimate uses of CPU functions to bypass detection services.

Typically delivered via email attachment, the modular malware is utilised to deliver further strains such as TrickBot or IcedID onto the compromised network.

03 \ NetWalker

Origin: 🇷🇺 *

First seen: **2019**

Est. Revenue: **$29 Million as of August 2020**

A fileless ransomware written in PowerShell and executed directly in memory accounting for around 10% of all attacks. This strain targets large organisations in the energy and logistics sector and saw a return of $25 million, after emerging onto the scene in late 2020.

*of North Korean origin, but recently suspected of being devised by Russian criminal cartels

talion.net/ransomaware

04 \ Conti

Origin: 🇰🇵 🇷🇺 *
First seen: **2018**
Est. Revenue: **$20 Million in 2020**

A Ransomware-as-a-Service (RaaS) that was first observed in December 2019, Conti has been successfully utilised against major organisations and government agencies.

What is unique with this strains is its offering to help the company with its own cyber security post compromise & payment from the target.

Demands from this strain range around the $40 million mark and has successfully compromised a number of high-profile targets, including a school in the United States and the Irish public health system.

05 \ Dopplepaymer

Origin: 🇷🇺 *
First seen: **2019**
Est. Revenue: **Approx. $15 Million in 2020**

Making up for around 9% of attacks is a strain from the creators of the infamous banking trojan Dridex. Dopplepaymer has a number of successes since its emergence targeting government, healthcare and the education sector worldwide.

One of the most known attacks from this strain was the compromise of Mexico's state-owned oil company, Pemex, with a ransom demand of $4.9 Million in 2019.

#RansomAware
Share your story

*of North Korean origin, but recently suspected of being devised by Russian criminal cartels