THE HISTORY OF RANSOMWARE

HOW IT WORKS AND HOW MUCH MONEY IT MAKES

RYUK

Ryuk ransomware was derived from the Hermes source code. Hermes isavailable for sale on forums as a commodity for mass-scale attacks but Ryuk targets large enterprises for big ransom payments.

Notable victims include: Mitsubishi Aerospace, Data Resolution and Tribune Publishing.

NOTPETYA

Like WannaCry, NotPetya also used the EternalBlue exploit. It earned a relatively paltry $10,000 because paying the ransom didn't return the victims their data.

It's aim wasn't to make money – it was destruction. The White House estimate the cost was more than $10 billion in damages. It was most likely an act of cyberwar, against the Ukraine by Russia.

Notable victims include: The Maersk, WPP and Merck & Co.

LOCKY

Locky was the big money-maker. It was delivered via a malicious email attachment (a Word doc with a macro Trojan).

Aside from the usual advice of "patch", "update anti-virus and anti-spam" and "educate your users" it reminds us of another fundamental lesson – "disable macros"

CERBER

Cerber is the best example of ransomware as a service.

Developers build the malware and sell the 'kits' to would-be cybercriminals (who don't need any technical skills) to launch the attack.

The developers of the ransomware then earn a cut of the takings.

2019 $3,700,000

2018 $720

2017 $10,000

2016 $140,000

2015 $7,800,000

2014 $6,900,000

2013 $3,000,000

THANATOS

Although it didn't earn much, Thanatos is an interesting ransomware case for two reasons:

1. In addition to being distributed by email it also used Discord the voice and text chat app for gamers.

2. Unlike most ransomware, Thanatos didn't demand payment in Bitcoin. Instead, it used less common cryptocurrencies including Bitcoin Cash, Zcash and Ethereum.

WANNACRY

WannaCry propagated through the EternalBlue exploit and DoublePulsar backdoor implant tool.

EternalBlue exploited a vulnerability in the Server Message Block protocol for Microsoft systems.

It is a "worm" because it automatically spreads itself around the network.

EternalBlue was originally developed by the NSA and was leaked by the hacking group the Shadow Brokers.

WannaCry famously had a built-in "killswitch". The ransomware would check a particular url before acting. As long as the domain was unregistered and inactive it would continue. British security researcher (and hacker) Marcus Hutchins spotted it and registered the domain effectively shutting down WannaCry.

Notable victims include: The NHS, Nissan and Telefónica.

CRYPTOLOCKER

CryptoLocker was spread by the Gameover ZeuS botnet which was also used for banking fraud.

CryptoLocker infected over 500,000 machines for a ransom of $300 or €300.

HOW TO PROTECT AGAINST RANSOMWARE

- Patch and update your systems
- Use anti-virus and anti-spam software
- Don't click links or open attachments from unsolicited emails and unknown senders
- Don't enable macros from email attachments
- Restrict user permissions to install and run software
- Backup your data!

Databarracks

www.databarracks.com