FEB 2020 - VOLUME I

The Evolution of Ransomware as a Service (RaaS)

Cyber criminals netted over $1 Billion in 2017

INTUITION Publishing PTE Limited

The dreaded ransomware

Ransomware is a type of Malware (Malicious Software) that holds the victim to ransom. The origins of Ransomware date back to 1989, when 20,000 diskettes were distributed to attendees of the World Health Organisation International AIDS Conference. The primary mechanism of Ransomware, once infected, is to lock a user out of their system and deny access to the data. This is achieved in several ways, most commonly by encrypting all files on the computer. Once the files have been encrypted, they are unable to be opened without a decryption key. Modern variants will also encrypt all external drives connected to the system, thus rendering some backup devices ineffective.

Economic enablement

Early viruses caused destruction for entertainment or infected a system so they could be used as a staging platform for further attacks. Ransomware is a much more direct approach to extorting money from victims. The first strains of effective ransomware developed in Russia would encrypt the ‘My Documents’ folder, or identified and moved certain file types to a password protected Zip folder, which would only be unlocked when the victim transferred a few hundred dollars to the attacker via E-Gold — electronic currency before Bitcoin. Now we live in the time of Bitcoin, a fully decentralised electronic payment system. This has enabled anonymous online transactions and marketplaces to flourish, giving rise to modern Ransomware demanding payment in Bitcoin. The 2012/13 CryptoLocker Ransomware campaign generated some $27 Million in Bitcoin payments. These early campaigns relied on mass untargeted attacks, such as spam emails and phishing campaigns.

Fast to act

To make more money with your Ransomware efforts, you need to infect many systems as quickly as possible. This was made very easy for cyber criminals in 2017 when hackers hacked the NSA and leaked their arsenal of tools. One such tool was a zero-day Windows exploit named EternalBlue. Ransomware developers realised that this new exploit could be used to spread their infections, and within days had repackaged their Ransomware and were using the new exploit. This led to over 200,000 computers being infected in days. Luckily a U.K. security researcher found a kill switch in the code and managed to halt the spread, but researchers estimate that cyber criminals netted over $1 Billion in 2017 via ransoms.

Targeted attacks

Due to the monetary success of their early campaigns, cyber criminals decided to up the ante and perform targeted attacks. They realized that an infected corporate network with all computer systems offline could demand a larger ransom to recover their systems. Thus, targeting large corporations, hospitals, airports and public utilities became common, with little regard for the damage caused.

From ransom to data-breach

Enter to the frame, REvil/Maze Ransomware gang's, who are taking things to a whole new level. Firstly, they gain access to a large network and begin exfiltration of data, then encrypt the computers and begin their extortion demands. Alongside the consequences of the victim’s computers being disabled, they are also threatened with the public release of the exfiltrated data. One of their most prominent attacks was on Southwire, one of the largest private US companies with revenues in excess of $6 Billion. They exfiltrated 120GB of data and infected over 800 computers, demanding a ransom of 850 Bitcoins ($6 Million), and publishing some of the exfiltrated data as proof of the breach.

Ransomware as a service

How to grow a billion-dollar business? By enticing affiliates to assist with the infiltration and infection of victims. Ransomware authors are now offering their tools as a service for a percentage of the ransoms paid. The potential profit for ransomware authors and operators also drives rapid innovation and ruthless competition amongst cyber criminals. This potential for large financial gain introduces a new threat vector; people with access to networks, with no hacking skills, can now cause severe damage with the potential for high monetary reward. It is concerning to think that disgruntled employees, troubled students, and corporate affiliates can now become involved in this form of espionage. With tools and services such as these readily available on the internet, now anyone can become a cyber-criminal.

Intuition-Blended Learning

The Intuition online learning library consists of several tutorials related to this article:

- **Cyber Security Awareness**
  - Passphrases
  - Preventing Identity Theft
  - Device Security
  - Malware & Breach Recovery
  - Social Engineering
  - And more…

For Intuition blended learning related to this article, some of our popular workshops include:

- Cyber-Warfare the Fourth Dimension of War
- Human Cyber-Security Risk
- Holistic Technology Risk Management Framework
- Artificial Intelligence
- Digital Banking Masterclass
- Insights into GRC in New Digital Age and Impact on Financial Advisory and Capital Market Representatives

Get in touch with your Intuition account manager at apacinfo@intuition.com for more details

Download the Asia Perspectives free app to get the latest articles.

Related News Articles

- New Ransomware targets US and European companies – FT 12 Aug 2019
- Hackers cripple airport currency exchanges, seeking $6 million ransom – NYT 09 Jan 2020

The topics covered in Intuition Asia Perspectives are current developments or topics currently in the market. Intuition Asia provides bespoke learning solutions, both eLearning and Instructor-led courses. These can also be blended in a program to provide the most effective form of learning. These workshops can be structured as lunch & learns, webinars or full day deliveries. Clients can use these to keep their workforce updated with the latest developments in the market and complete their mandatory CPD learning hours.