illusive

Rãnsømwäre

What is a ransomware attack?

Attackers want your money. Ransomware is malware that encrypts your files, making the data inaccessible. Attackers then deliver extortion demands, leveraging your need to access the encrypted data and continue daily operations.

In a targeted ransomware attack, attackers deliberately select sensitive network locations for encryption, such as those that hold business-critical information.

What is the risk?

Attackers take network assets hostage, wreaking havoc on businesses of all sizes. Victims then need to choose between paying extremely high mitigation fees and freezing production for several days while reverting to backed-up data.

How does the attack operate?

1. Network breach - usually achieved by exploitation or spam campaigns

2. Distribution - spread the program across network endpoints, and gain access to organizational-data such as shared folders and backups

3. Encryption - scan for specific pre-defined file-types, and encrypt the files

4. Notification - notify users of payment details and deadline (up to 72 hours)

What are the challenges to detection?

Ransomware is significantly faster than other types of malware; critical assets can be encrypted in hours or even minutes.

Signature-based detection is ineffective due to the variety of ransomware families.

As with APTs, targeted ransomware uses lateral movements to seek sensitive organizational assets. Security solutions struggle to identify these without raising false-positive alerts.

What would minimize the risk?

Immediate detection and ransomware-diversion would give Incident Response teams time to save network data. Automatically suspending ransomware processes would keep data safe.

illusive is the only vendor that neutralizes ransomware activity on source hosts.

The illusive Advanced Ransomware Guard ™ uses agentless technology to create transparent ransomware-specific deceptions that are only accessed by ransomware programs. These deceptions divert the attack giving you the time you need to take action before your most critical data is encrypted.

Statistics

A ransomware attack in March 2016 caused a regional hospital in Kentucky pay $17,000 to unlock patient files.

In 2016, multiple hospitals across the US had their systems shut down following successful Ransomware attacks.

- 7,700 public complaints regarding ransomware since 2005, totaling $57.6 million in damages (Source: Kaspersky Labs, covering Kaspersky clients worldwide)
- Those damages include ransoms paid - generally $200 to $10,000, according to the FBI - as well as costs incurred in dealing with the attack and estimated value of data lost (Source: Kaspersky Labs, covering Kaspersky clients worldwide)
- In 2015 alone, victims paid over $24 million across nearly 2,500 cases reported to the IC3 (Source: Kaspersky Labs, covering Kaspersky clients worldwide)
- Q1 2016: $209 million in costs associated with ransomware (Source: Kaspersky Labs, covering Kaspersky clients worldwide)
- Ransomware was #2 in quantity of crimeware breaches in 2015, up from #7 in 2014 (Verizon 2016 DBIR).
- Number of Ransomware victims rose by ~20% in the last year, reaching 2.3 million users.