Newly detected ransomware employs BitLocker technology to encrypt victim data

Description

ShrinkLocker ransomware has been discovered by security researchers, using the BitLocker feature in Windows to encrypt victim data. BitLocker, a full-volume encryptor introduced in Windows Vista in 2007, has seen upgrades in newer versions of Windows to enhance its security features.

Researchers from Kaspersky found ShrinkLocker being used to encrypt data in Mexico, Indonesia, and Jordan, renaming it for its use of BitLocker and its partition shrinking capabilities. This ransomware is not the first to exploit BitLocker, with previous incidents reported in Iran and Russia.

ShrinkLocker uses a VisualBasic script to resize disks and encrypt data, disabling BitLocker key protections in the process. The ransomware generates a 64-character encryption key using various elements and encrypts data on the system. Recovery without the attacker-supplied key is challenging due to the unique values used in key generation.

To protect against ShrinkLocker attacks, Kaspersky recommends robust endpoint protection, proactive threat scanning, strong password usage for BitLocker, minimal user privileges, network traffic monitoring, script logging, offline backups, and frequent testing. Organizations can use provided indicators to determine if they have been targeted by ShrinkLocker.

Overall, the threat of ransomware continues to evolve, with attackers finding new ways to evade detection and cause disruptions to systems.

Warning: Trying to access array offset on false in **/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-qustions.php** on line **76**

Warning: Trying to access array offset on false in **/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-qustions.php** on line **76**

Warning: Trying to access array offset on false in **/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-qustions.php** on line **76**

Warning: Trying to access array offset on false in **/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-qustions.php** on line **76**

Warning: Trying to access array offset on false in **/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-qustions.php**

on line **76**

Warning: Trying to access array offset on false in **/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-qustions.php** on line **76**

Vocabulary List:

1. **ransomware** // (noun): Software designed to deny access to a computer system or data until a ransom is paid.
2. **encrypt** // (verb): To convert information or data into a code to prevent unauthorized access.
3. **victim** // (noun): A person who is harmedinjuredor killed as a result of a crime or other event.
4. **exploit** // (verb): To make full use of and derive benefit from a resource.
5. **endpoint** // (noun): A device that serves as a connection or communication point in a network.
6. **indicators** // (noun): Signs or signals that point to a particular condition or result.

Vocabulary quizzes

Multiple Choice (Select the Correct answer for each question.)

1. What term is used to describe the curved path of a celestial object around a star?

Option: Swirling
Option: Orbits
Option: Congestion
Option: Deorbiting

2. What is defined as the beliefs or opinions that are generally held about someone or something?

Option: Formation
Option: Reputation
Option: Insights
Option: Alignment

3. What term is used to describe the process of converting information into a code to prevent unauthorized access?

Option: Victim
Option: Encrypt
Option: Flexibility
Option: Mitigate

4. What is the gradual development of something especially from a simple to a more complex form?

Option: Orbital

Option: Evolution
Option: Lessened
Option: Remediation

5. In cybersecurity what does the term "endpoint" refer to?

Option: Exploit
Option: Ransomware
Option: Endpoint
Option: Disk

6. What is the ability to adapt or be adapted to changing circumstances?

Option: Spectators
Option: Cost-effective
Option: Flexibility
Option: Commitment

7. Who are individuals watching an event or performance called?

Option: Conferencing
Option: Spectators
Option: Attendance
Option: Insights

8. What term is used to describe the overcrowding or blockage of something?

Option: Congestion
Option: Vulnerable
Option: Iconic
Option: Cost-effective

9. What is the term used to describe the action of reducing the severity or seriousness of something?

Option: Orbital debris
Option: Mitigate
Option: Orbital
Option: Attendance

10. What term is used to describe the arrangement in a straight line or in correct relative positions?

Option: Alignment
Option: Formation
Option: Remediation
Option: Discovery

Gap-Fill (Fill in the blanks with the correct word from the vocabulary list.)

11. _____ is a storage device used for storing and retrieving digital information.

12. The impact of the new regulations significantly _____ the company's profitability.

13. The _____ at the concert was much higher than expected.

14. The Eiffel Tower is considered to be one of the most _____ landmarks in the world.

15. Prompt _____ of the security breach helped prevent further data loss.

16. The _____ of the new government brought hope for positive change.

17. The company implemented a _____ solution to reduce operational expenses.

18. Market research provided valuable _____ into consumer preferences.

19. Efforts to clean up _____ in space are crucial to prevent collisions with satellites.

20. The satellite was intentionally maneuvered for _____ to ensure it would burn up in the atmosphere.

Matching Sentences (Match each definition to the correct word from the vocabulary list.)

21. The of the new planet was a result of cosmic processes over millions of years.
22. Without the latest security updates your computer may be to cyber attacks.
23. His long-term to the project earned him the respect of his colleagues.
24. The team would in their victory after a hard-fought game.
25. The high at the conference indicated widespread interest in the topic.
26. is a type of malicious software that blocks access to a computer system until a sum of money is paid.
27. Cybercriminals often vulnerabilities in software to gain unauthorized access to systems.
28. Unusual network activity could be one of the of a potential security breach.
29. Using open-source software can be a solution for small businesses with limited budgets.

30. The team worked in perfect to achieve their common goal.

Answer

Multiple Choice: 1. Orbits 2. Reputation 3. Encrypt 4. Evolution 5. Endpoint 6. Flexibility 7. Spectators 8. Congestion 9. Mitigate 10. Alignment
Gap-Fill: 11. Disk 12. Lessened 13. Attendance 14. Iconic 15. Remediation 16. Formation 17. Cost-effective 18. Insights 19. Orbital debris 20. Deorbiting
Matching sentence: 1. Formation 2. Vulnerable 3. Commitment 4. Rejoice 5. Attendance 6. Ransomware 7. Exploit 8. Indicators 9. Cost-effective 10. Alignment

CATEGORY

1. Sci/Tech - LEVEL3

Date Created
2024/05/25
Author
aimeeyoung99