NASUNI

Incident Report

Get transparency to know what happened, when it happened, and how to fix it fast.

A Comprehensive Report is promptly generated upon detecting an incident, serving purposes of reporting, compliance, and cyber-insurance. Key details extracted from the report seamlessly feed into Nasuni's Targeted Restore process, facilitating a streamlined restore operation.

Attack Summary
Key details to understand the source and scope of the attack

Full Attack Timeline
Including the Last Clean Snapshot for Recovery

Confidence Levels Reached

List of Files Impacted

NASUNI

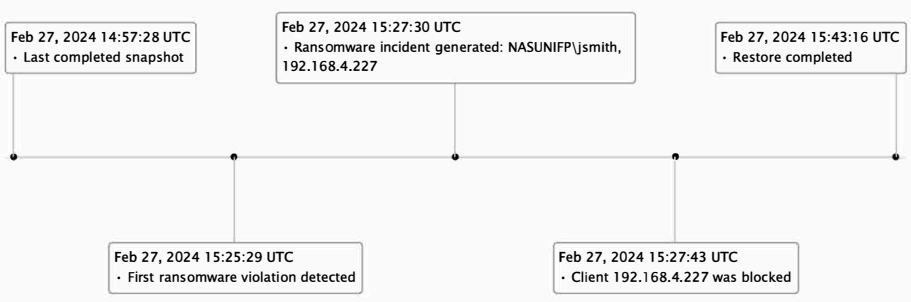
Ransomware Incident Report - Feb 27, 2024 16:03:04 UTC

1 Attack Summary

On Feb 27, 2024 15:27:30 UTC, Nasuni detected a ransomware attack on corpdata volume on the nea1 Filer. The attack originated from user NASUNIFP\jsmith's client. 351 files were impacted. The attack was mitigated and the client was blocked from accessing the nea1 Filer.

CATEGORY	VALUE
Incident ID	111
Impacted Volume	corpdata
Affected Filer	nea1
Affected Filer Serial Number	08bc6f07-1bd4-44cc-a913-59408f837101
User Involved	NASUNIFP\jsmith
Detected Confidence Level	High (4)
Client Blocked	Yes
# of Files Affected	351
Attack Signature (extension)	--

2 Event Timeline



Timeline Details

DATE	DESCRIPTION
Feb 27, 2024 14:57:28 UTC	Last completed snapshot
Feb 27, 2024 15:25:29 UTC	First ransomware violation detected
Feb 27, 2024 15:27:30 UTC	Ransomware incident generated: NASUNIFP\jsmith, 192.168.4.227
Feb 27, 2024 15:27:43 UTC	Client 192.168.4.227 was blocked
Feb 27, 2024 15:42:47 UTC	admin initiated a Targeted Ransomware Restore job for the ransomware attack detected at Feb 27, 2024 15:27:30 UTC on volume corpdata.
Feb 27, 2024 15:43:16 UTC	Targeted Ransomware Restore job successfully restored 351 files for the ransomware attack detected at Feb 27, 2024 15:27:30 UTC on volume corpdata. For more details, refer to the restore log file located in the .nasuni/restore_results directory at the root of the volume.

3 Ransomware Detection Confidence Level

DETECTED CONFIDENCE LEVEL
High (4)

CONFIGURED CONFIDENCE LEVEL	VALUE
Incident Creation	Medium (3)
Block Clients	High (4)

Detected Clients Status

IP ADDRESS	STATUS	BLOCKED BY	BLOCKED DATE
192.168.4.227	Blocked	Mitigation Policy	Feb 27, 2024 15:27:43 UTC

4 Affected Files

The first 100 impacted files since incident creation. A complete list of files along with additional details about the user and client device involved, can be found in the ransomware violations log file located in the .nasuni/ransomware_violations directory at the root of the volume.

TIMESTAMP	EVENT TYPE	PATH
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0000.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0001.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0002.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0003.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0004.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0005.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0006.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0007.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0008.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0009.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0010.jpg
Feb 27, 2024 15:26:15 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0011.jpg
Feb 27, 2024 15:26:16 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0012.jpg
Feb 27, 2024 15:26:16 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0013.jpg
Feb 27, 2024 15:26:16 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0014.jpg
Feb 27, 2024 15:26:16 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0015.jpg
Feb 27, 2024 15:26:16 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0016.jpg
Feb 27, 2024 15:26:16 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0017.jpg
Feb 27, 2024 15:26:16 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0018.jpg
Feb 27, 2024 15:26:16 UTC	Rename	./Ransomware Test Data Set/natural_images/airplane/airplane_0019.jpg
Feb 27, 2024 15:26:16 UTC	Rename	./Ransomware Test Data Set/natural_images/car/car_0000.jpg
Feb 27, 2024 15:26:17 UTC	Rename	./Ransomware Test Data Set/natural_images/car/car_0001.jpg
Feb 27, 2024 15:26:17 UTC	Rename	./Ransomware Test Data Set/natural_images/car/car_0002.jpg
Feb 27, 2024 15:26:18 UTC	Rename	./Ransomware Test Data Set/natural_images/car/car_0003.jpg
Feb 27, 2024 15:26:18 UTC	Rename	./Ransomware Test Data Set/natural_images/car/car_0004.jpg
Feb 27, 2024 15:26:18 UTC	Rename	./Ransomware Test Data Set/natural_images/car/car_0005.jpg