



Oracle Recovery Appliance against Ransomware

Most valuable data stored in Oracle DB needs proper protection.



Cristian Termure

Oracle Cloud Systems

Technology Summit 2022





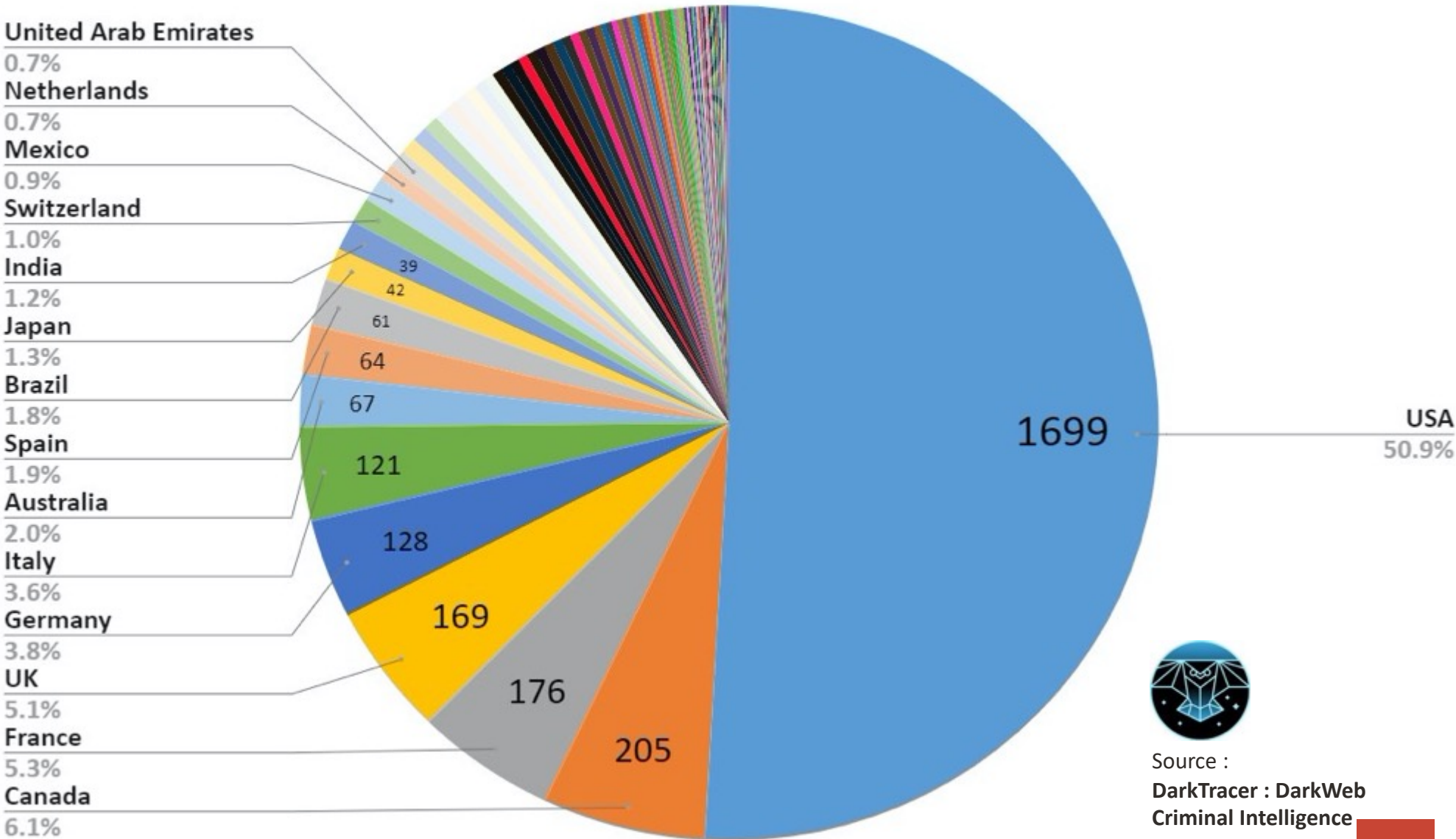
Hackers have an advantage !!

*It's much easier to find a
open windows than to
keep all windows closed.*

Same is true on security

USA	1699
Canada	205
France	176
UK	169
Germany	128
Italy	121
Australia	67
Spain	64
Brazil	61
Japan	42
India	39
Switzerland	33
Mexico	31
Netherlands	22
United Arab Emirates	22
South Africa	21
Taiwan	20
Austria	19
Belgium	17
China	15
Indonesia	15
South Korea	15
N/A	14
Chile	13
Saudi Arabia	13
Argentina	12
Israel	12
Norway	12
Peru	12
Portugal	12
Sweden	12
Thailand	12
Colombia	11
Turkey	11
New Zealand	10
Singapore	10
Hong Kong	9
Czech Republic	7
Ireland	7
Poland	7
Romania	7

Statistics on countries affected by darkweb ransomware



Source :
DarkTracer : DarkWeb
Criminal Intelligence



Setting The Scene

Basics about Ransomware

Ransomware attack : a kidnap of complete environments and data.

It often includes also:

- Massive **Data Breaches** – which is all about stolen data
- Distributed Denial of Service (**DDoS**) - to overload attacked systems getting them to collapse the environments

The Options Victim has:

1. Pay
2. Negotiate
3. Do NOT Pay (our aim)

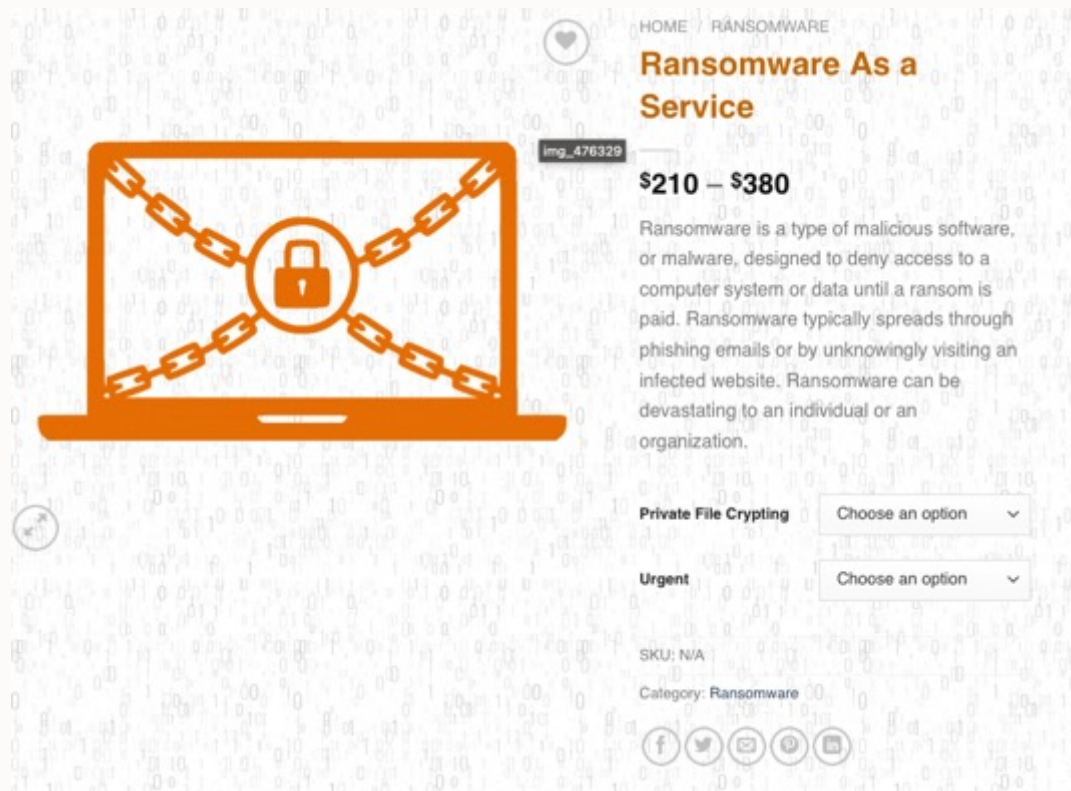


**WANNA
CRY**



Ransomware-as-a-Service (RaaS)

You don't even need to be an expert



HOME / RANSOMWARE

Ransomware As a Service

img_476329

\$210 – \$380

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Ransomware can be devastating to an individual or an organization.

Private File Crypting

Urgent

SKU: N/A

Category: Ransomware

[f](#) [t](#) [e](#) [p](#) [i](#)

DESCRIPTION ADDITIONAL INFORMATION

Now you will pay Ransomware available as a service.

Price includes:

- 1 exe file with your payment information

You will receive the .exe file which includes the ransomware payload. You will have to send the file to your victim through your own methods. Once the computer is infected it will be crypted instantly.

You get 1 key for full computer decrypt.

File will be detected by Antivirus as a malware unless you order the Private Crypt option or use your own crypter to make it FUD!



Think you can avoid Ransomware nightmares with a backup?

You are wrong!

Customers basically think about Backup as countermeasure for Ransomware.

They also believe that the best protection against these sorts of attacks is solid offline backups.

It was appropriate for 2019 but the way ransomware attacks are conducted today has changed

Ransomware are now able to discover your backup architecture and attack it, wherever is located.

SOPHOS

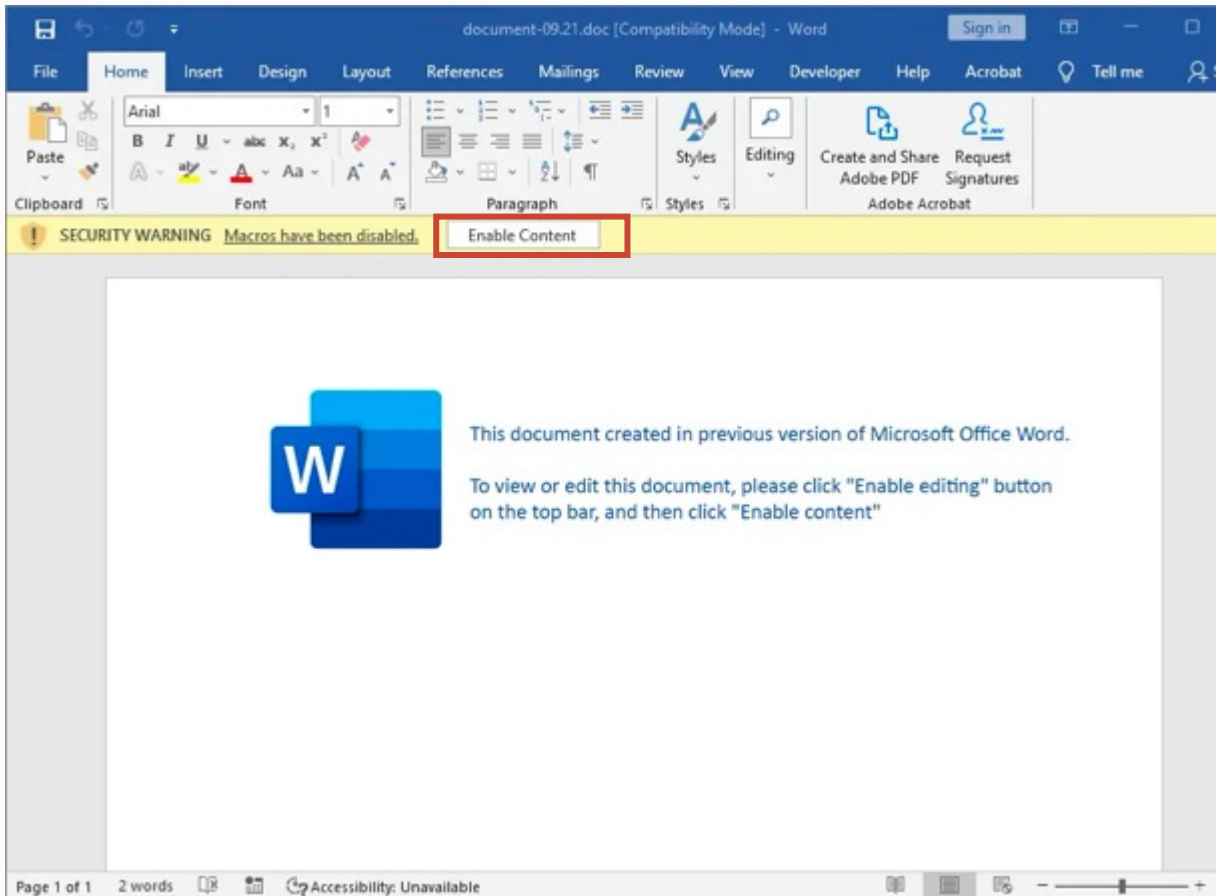


Quantum.



Lateral Movement:

Planting malicious payload in any storage



NetApp Product Security

HOME ADVISORIES BULLETINS CONTACT POLICY RESOURCES CERTIFICATIONS

Home > Advisory > CVE-2021-29631 FreeBSD Vulnerability in NetApp Products

CVE-2021-29631 FreeBSD Vulnerability in NetApp Products

i NetApp will continue to update this advisory as additional information becomes available. This advisory should be considered the single source of current, up-to-date, authorized and accurate information from NetApp.

Advisory ID: NTAP-20210923-0004 **Version:** 2.0 **Last updated:** 09/29/2021 **Status:** Interim.
CVEs: CVE-2021-29631

Overview Affected Products Remediation Revision History

Summary

Clustered Data ONTAP incorporates FreeBSD. All supported versions of FreeBSD are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Impact

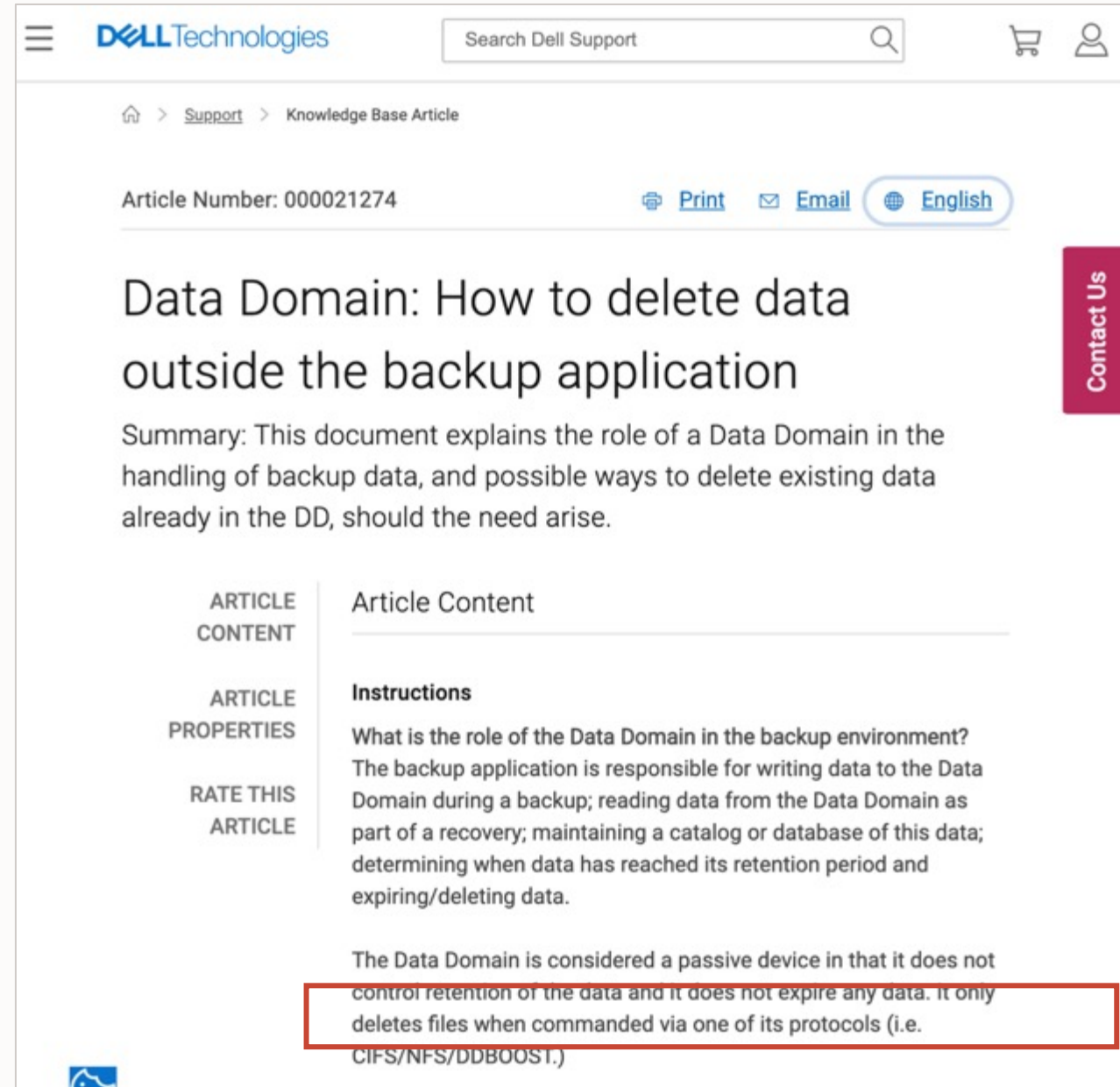
Successful exploitation of this vulnerability could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Lateral Movement: Infecting Backup Devices

Hacking team will search for backup visible mount points, such as CIFS or even DDBOOST and will enter the backup devices using backdoors

Alternatively, will just wait for the tampered files to be backed up

Last stage of the attack is the erasure of any backup data



The screenshot shows a Dell Technologies Knowledge Base article. The header includes the Dell Technologies logo, a search bar, and navigation icons. The article title is 'Data Domain: How to delete data outside the backup application'. Below the title is a summary: 'Summary: This document explains the role of a Data Domain in the handling of backup data, and possible ways to delete existing data already in the DD, should the need arise.' The article content is divided into sections: 'ARTICLE CONTENT', 'ARTICLE PROPERTIES', and 'RATE THIS ARTICLE'. The 'Instructions' section explains the role of the Data Domain in the backup environment. A red box highlights a specific sentence in the instructions: 'The Data Domain is considered a passive device in that it does not control retention of the data and it does not expire any data. It only deletes files when commanded via one of its protocols (i.e. CIFS/NFS/DDBOOST.)'.

DELL Technologies

Search Dell Support

Home > Support > Knowledge Base Article

Article Number: 000021274

Print Email English

Data Domain: How to delete data outside the backup application

Summary: This document explains the role of a Data Domain in the handling of backup data, and possible ways to delete existing data already in the DD, should the need arise.

ARTICLE CONTENT

ARTICLE PROPERTIES

RATE THIS ARTICLE

Instructions

What is the role of the Data Domain in the backup environment? The backup application is responsible for writing data to the Data Domain during a backup; reading data from the Data Domain as part of a recovery; maintaining a catalog or database of this data; determining when data has reached its retention period and expiring/deleting data.

The Data Domain is considered a passive device in that it does not control retention of the data and it does not expire any data. It only deletes files when commanded via one of its protocols (i.e. CIFS/NFS/DDBOOST.)

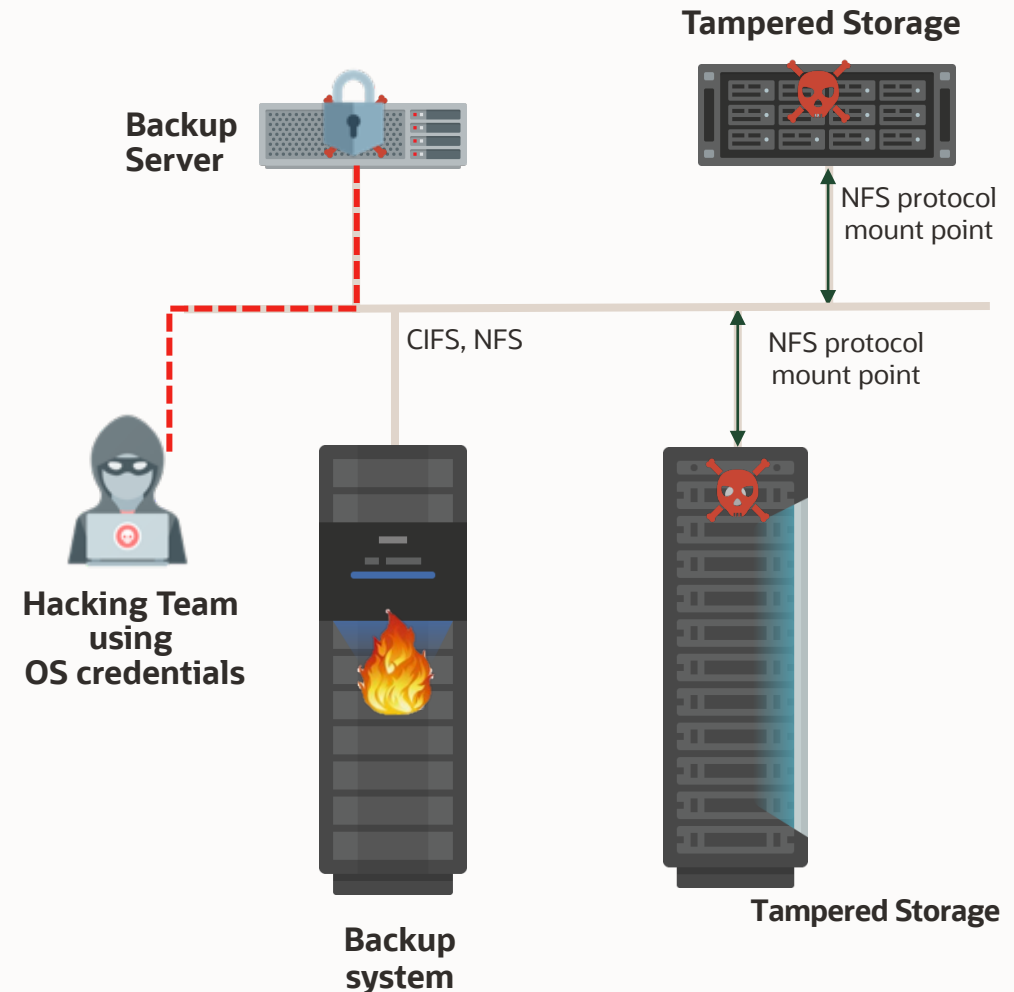
Contact Us

Lateral Movement: Infecting Backup Servers

Same kind of attack can be done by tampering the **Backup Server** whether is on-prem software or deployed in cloud



The Hacking team connects to the backup server and deletes the backup **and/or encrypts the catalog**





Recap:

Ransomware *is not magic!*
In order to do its job it makes use of :

1. Visible mount points and files
2. Visible OS commands
3. Visible OS user credentials

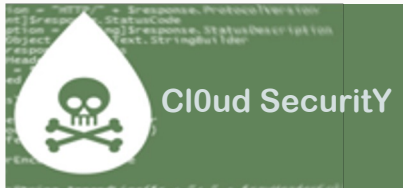
**Ransomware won't easily affect
what is *Invisible***

Which Ransomware operate at Storage level

Ransomware family



- eCh0raix is brute-forcing NAS devices
- infect and encrypt documents
- It target both primary file storage and backup storage



- Attacks management interface exposed on the internet
- Delete all of the files on NAS devices
- Alternatively, files are hidden
- a ransom note was left in their place.



- brute-forcing NAS devices that use weak passwords for the built-in phpMyAdmin service
- encrypt users' files and save a copy of the decryption keys on ransomware command and control (C&C) server.

Excerpts from Attack

```
README_FOR_DECRYPT.txt - Notepad2
File Edit View Settings ?
1 All your data has been locked(encrypted).
2 How to unlock(decrypt) instruction located in this TOR website:
3 http://sg3dwqfpmr4s15hh.onion/order/
4 Use TOR browser for access .onion websites.
5 https://duckduckgo.com/html?q=tor+browser+how+to
6
7 Do NOT remove this file and NOT remove last line in this file!
8
```

YOUR FILES HAVE BEEN ENCRYPTED AND MOVED TO A SAFE LOCATION. IF YOU NEED THEM BACK PLEASE SEND 0.03 BITCOIN TO THIS ADDRESS:
13gMN3sJFxoLvDzyGxq31sr4k9P2qqMDQ
YOU HAVE UNTIL THE 1st OF AUGUST 2019 TO MAKE THE PAYMENT OR YOUR FILES WILL BE GONE FOR GOOD.

```
HOW_TO_RESTORE_FILES.txt - Notepad2
File Edit View Settings ?
1 Hello,
2
3 Unfortunately a malware has infected your QNAP and a large number of your files has been encrypted using a hybrid encryption scheme.
4 File names were also encrypted.
5
6 You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.
7
8 Send email to [redacted] with subject "[redacted]" and we will talk.
9
```

EXAMPLES or somethin Which Ransomware operate at Backup level

Ransomware family



- BitPaymer Source Code is a Fork of DoppelPaymer Ransomware and Dridex 2.0
- Encrypt and/or Delete backups



- Ransom amounts vary from 2 Bitcoin to 100 Bitcoin (almost 1,000,000 USD)
- Encrypt and/or delete backups



- Gain Admin access to local backup system
- Encrypt and/or delete backups
- When Maze finds backups stored in the cloud, they also attempt to obtain the cloud storage credentials

Excerpts from Attack

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm. Backups were either encrypted or deleted or backup disks were formatted. No free decryption software is available in the public. Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files. This may lead to the impossibility of recovery of the certain files.



Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm . Backups were either encrypted or deleted or backup disks were formatted.



- Ransomware operators published on their leak site the Admin user name and password for a non-paying victim's backup software
- was used as a warning to the victim that the ransomware operators had full access to their network, including the backups

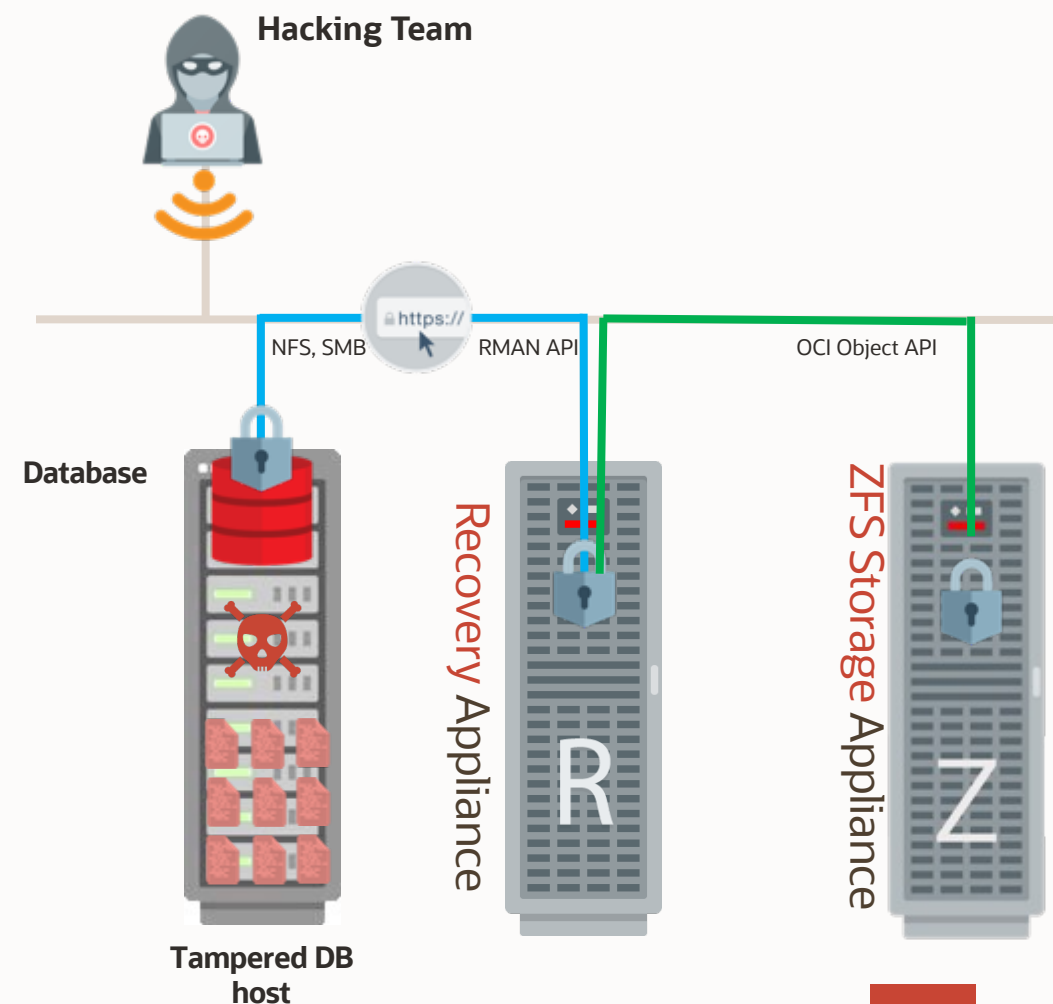


ZDLRA does not use any visible mount point and does not work on raw files.

Database accesses ZDLRA through an hidden channel built on top of a proprietary API and managed by an agentless backup module.

Communication between DB and ZDLRA can also can be encrypted, preventing any intrusion

Offload to ZFS using OCI Object Storage

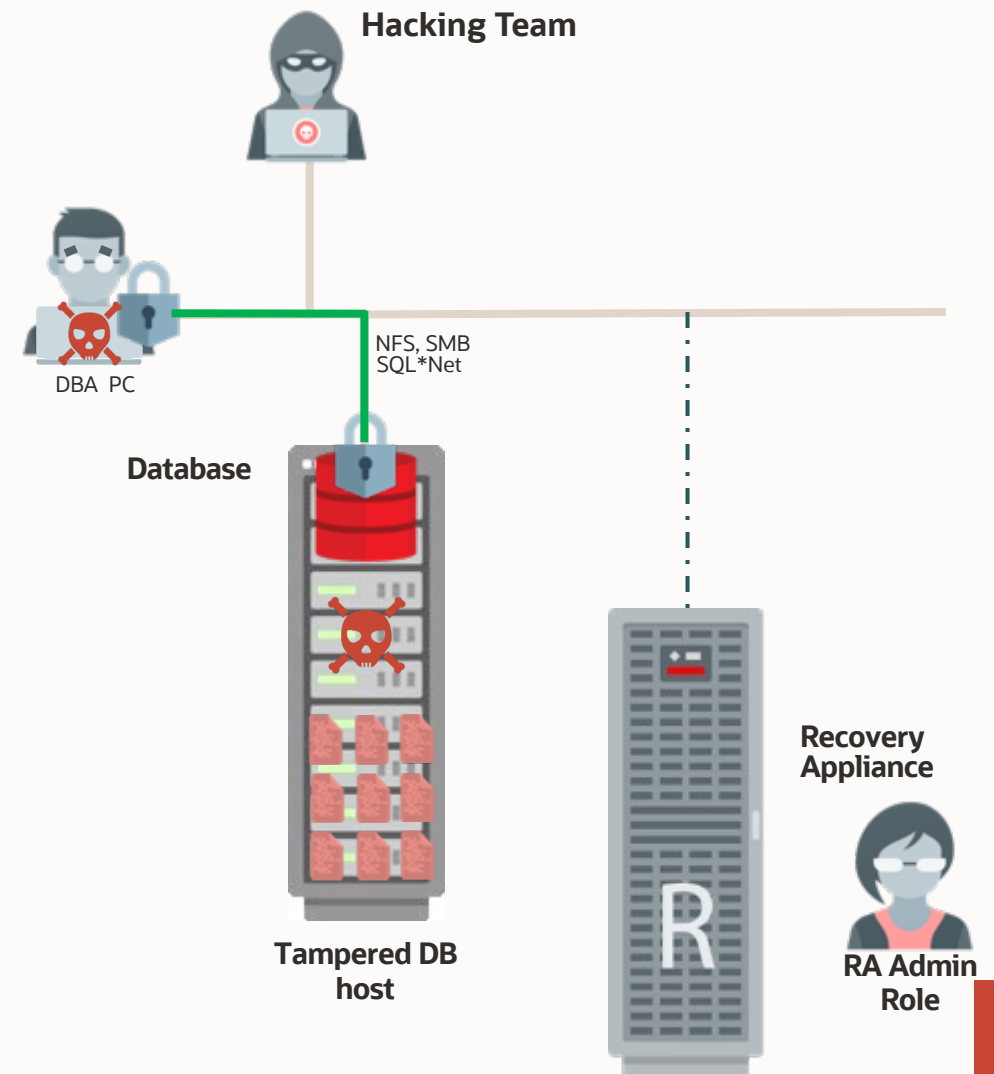


ZDLRA does not use visible Admin credentials to get the job done.

If hackers make it to compromise a vulnerable PC client and crack DBA credentials, this will not harm the restore.

DBA has no permissions to delete backup volumes from ZDLRA.

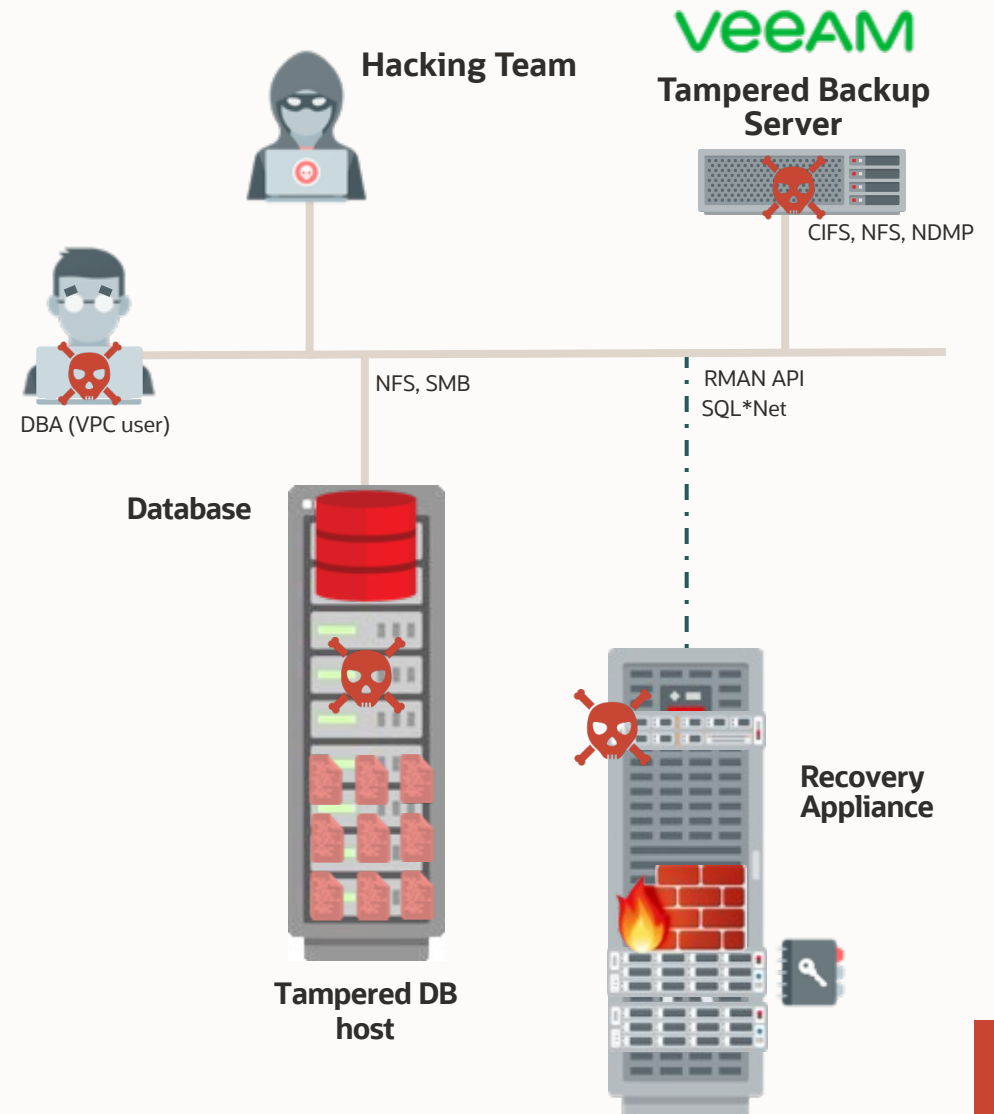
ZDLRA Dedicated Admin role is stored in a segregated place




ZDLRA is resilient to backup server tampering

If hackers successfully log into a backup server, and bounce into ZDLRA compute nodes, an internal firewall hides and protects the storage cells where backup data is stored.

The ZDLRA has his own metadata which contains catalog





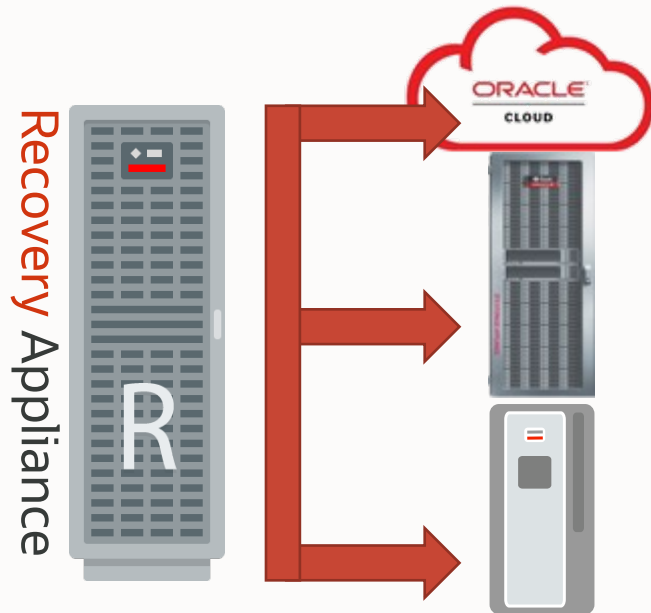
Backup is invisible now.
Is protecting your most valuable data.

**All the security features presented here are
included in the ZDLRA.**

Backups Are Safer With ZDLRA

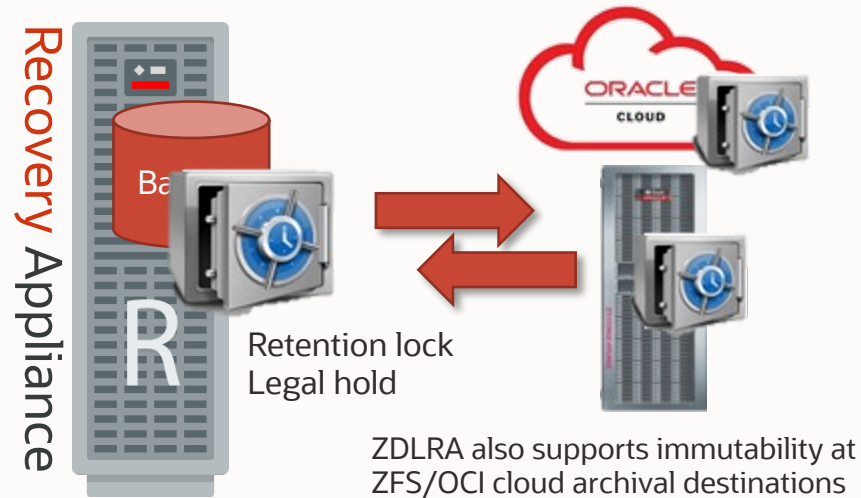
7. External Copies

RA can create additional copies on external mediums



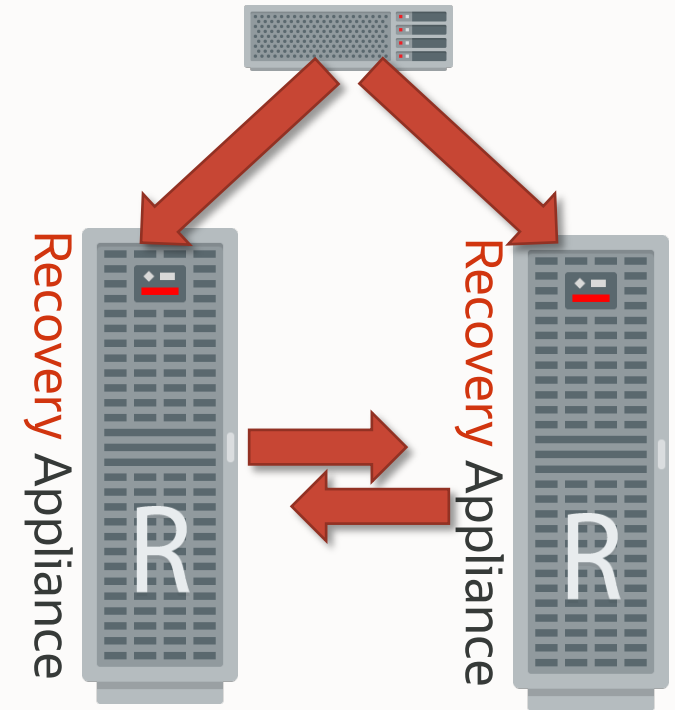
Several options to create more copies
Fully automated retention management

8. Immutable External Copies



ZDLRA supports archiving to ZFS and OCI object storage and these locations also have immutability capabilities, both retention lock and legal hold.

9. DB Aware Replication



DB aware replication topologies for extra protection
Backup anywhere capability



Ransomware Cannot Affect What Is **Invisible**

Thank You

Cristian Termure

cristian.termure@oracle.com

