Ransomware Attackers Use Your Cloud Backups Against You

bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/

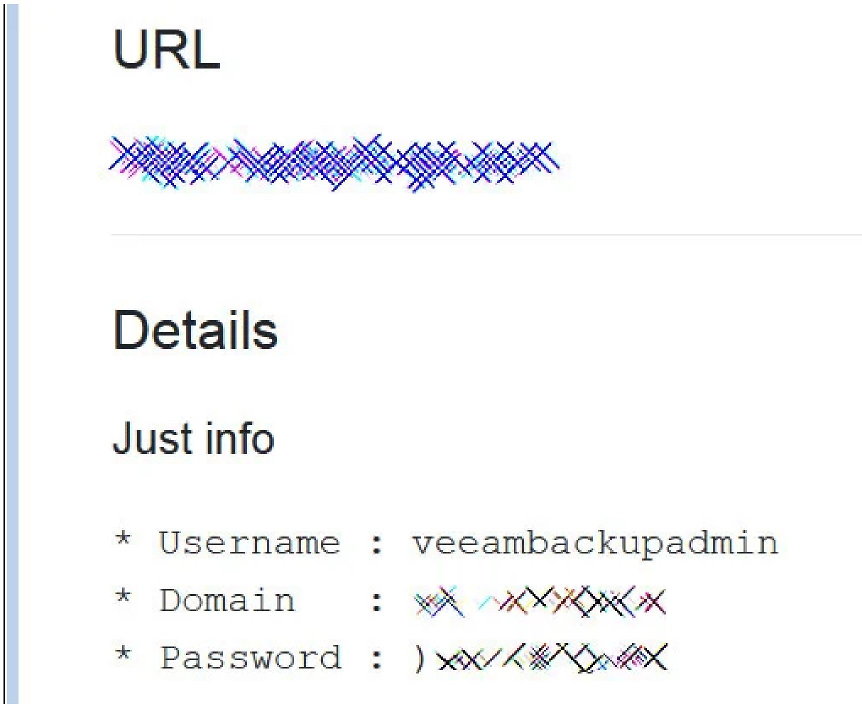
Lawrence Abrams

By
Lawrence Abrams

- March 3, 2020
- 04:36 PM
- 1

Backups are one the most, if not the most, important defense against ransomware, but if not configured properly, attackers will use it against you.

Recently the DoppelPaymer Ransomware operators published on their leak site the Admin user name and password for a non-paying victim's Veeam backup software.



URL

[redacted]

Details

Just info

```
* Username : veeambackupadmin
* Domain   : [redacted]
* Password : [redacted]
```

Leaked Veeam Account

This was not meant to expose the information to others for further attacks but was used as a warning to the victim that the ransomware operators had full access to their network, including the backups.

After seeing this information, I reached out to the operators of the DoppelPaymer and Maze Ransomware families to learn how they target victim's backups and was surprised by what I learned.

It should be noted that in this article we will be focusing on the Veeam backup software. Not because it is less secure than other software, but simply because it is one of the most popular enterprise backup products and was mentioned by the ransomware operators.

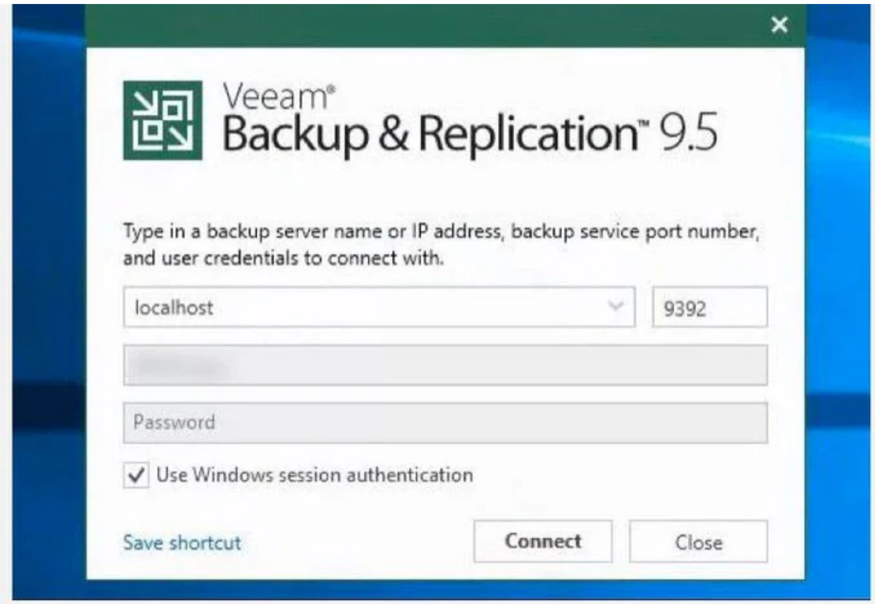
Attackers first use your cloud backups to steal your data

During ransomware attacks, attackers will compromise an individual host through phishing, malware, or exposed remote desktop services.

Once they gain access to a machine, they spread laterally throughout the network until they gain access to administrator credentials and the domain controller.

Using tools such as Mimikatz they proceed to dump credentials from the active directory.

According to Nero Consulting, an MSP and IT Consulting company based out of New York City who assisted me with this article, this could allow the attackers to gain access to backup software as some administrators configure Veeam to use Windows authentication.



Veeam® Backup & Replication™ 9.5

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

localhost | 9392

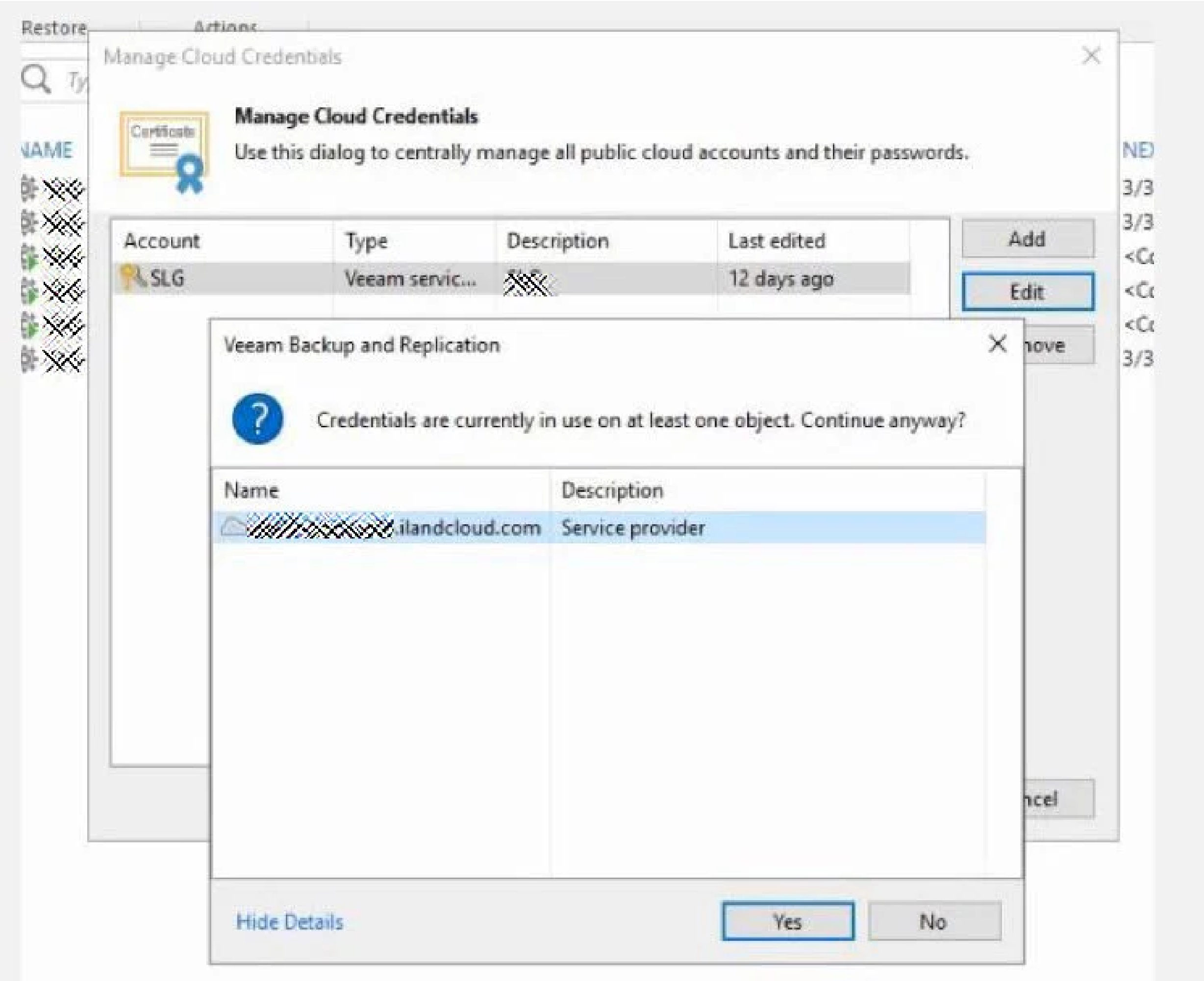
[redacted]

Password

☑ Use Windows session authentication

Log in to Veeam using Windows authentication

Once they gain access, the Maze Ransomware operators told BleepingComputer that if cloud backups are configured, it is very useful when stealing data from their victims.



Manage Cloud Credentials

Manage Cloud Credentials

Use this dialog to centrally manage all public cloud accounts and their passwords.

Account	Type	Description	Last edited
SLG	Veeam servic...	[redacted]	12 days ago

Veeam Backup and Replication

Credentials are currently in use on at least one object. Continue anyway?

Name	Description
[redacted].ilandcloud.com	Service provider

Configured cloud provider

When Maze finds backups stored in the cloud, they attempt to obtain the cloud storage credentials and then use them to restore the victim's data to servers under the attacker's control.

"Yes, we download them. It is very useful. No need to search for sensitive information, it is definitely contained in backups. If backups in the cloud it is even easier, you just login to cloud and download it from your server, full invisibility to "data breach detection software". Clouds is about security, right?"

As the attackers are restoring directly from the cloud to their servers, it won't raise any red flags for the victim as their servers appear to be operating normally with no logs being created in their backup software.

The Maze operators did not elaborate on how they gain access to the cloud credentials, but DoppelPaymer told us they use "all possible methods".

This could include keyloggers, phishing attacks, or by reading locally saved documentation on the backup servers.

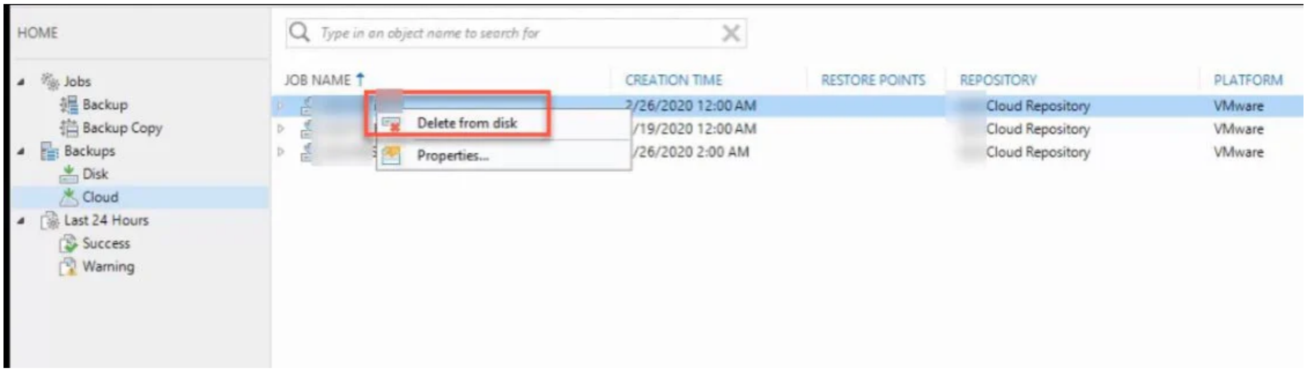
Deleting backups before ransomware attacks

Regardless of whether the backups are used to steal data, before encrypting devices on the network the attackers will first delete the backups so that they cannot be used to restore encrypted files.

DoppelPaymer told BleepingComputer that even though cloud backups can be a good option to protect against ransomware, it is not 100% effective.

"Cloud backups are a very good option against ransom but do not 100% protect as cloud backups are not always good configured, offline backups often outdated - the system of backups is really nice but human factor leaves some options," DoppelPaymer told us via email.

Unless you subscribe to service add-ons such as immutable backups, as the actors have full access to the local install of backup software, they can simply delete any backups that exist in the cloud.



JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY	PLATFORM
[redacted]	2/26/2020 12:00 AM		[redacted] Cloud Repository	VMware
[redacted]	/19/2020 12:00 AM		[redacted] Cloud Repository	VMware
[redacted]	/26/2020 2:00 AM		[redacted] Cloud Repository	VMware

Deleting a cloud backup in Veeam

With a victim's data now stolen and their backups deleted, the attackers deploy their ransomware throughout the compromised network using PSExec or PowerShell Empire typically during off-hours.

This usually leads to a company opening the next day to an encrypted network.

Protecting your backups

In emails with Rick Vanover, Senior Director, Product Strategy at Veeam Software, we were told that it does not matter what software you use, once an attacker gains privileged access to the network, everything is at risk.

"We have advocated, even in a published 2017 whitepaper that I wrote I've recommended separate accounts for Veeam installations and components. Additionally, I recommend Veeam installations to use non-domain accounts for components as well to add more account-based layers of resiliency. Additionally, Veeam has recommended that the Veeam deployment not have Internet access or otherwise be on an isolated management network," Vanover told BleepingComputer.

To prevent ransomware attackers from gaining complete leverage over a victim, Veeam recommends that companies follow a 3-2-1 Rule when configuring backups.

"Whether it is ultra-resilient backup data like S3-immutable backups in the cloud, encrypted backups on tape or encrypted backups on removable offline storage; customers need to have multiple copies of data. We have advocated for a long time the 3-2-1 Rule, which advocates having 3 different copies of data on 2 different media with one of them being off-site. Couple in 1 copy being on an ultra-resilient technique such as an immutable backup, offline backup or otherwise air-gapped; data can be protected against nearly any failure scenario – including ransomware. Additionally, Veeam also has a technology called Secure Restore; which will perform a threat scan with almost any tool to ensure that a restored system or data does not re-introduce a threat," Vanover continued.

Like Veeam, Nero Consulting also strongly recommends users should purchase the immutable storage or redundant storage protection options if available when using cloud services.

Using this option, even if the data is deleted from the cloud storage provider, the immutable storage service will make the data recoverable for a certain amount of time.

As for protecting a network from data exfiltration, the best solution is to prevent the attackers from gaining access to your network in the first place and to monitor for suspicious activity.

This would include utilizing network monitoring software, intrusion detection systems, and geographic and IP access control for cloud storage providers if available.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Quantum ransomware seen deployed in rapid network attacks

Austin Peay State University resumes after ransomware cyber attack

LockBit ransomware gang lurked in a U.S. gov network for months

Snap-on discloses data breach claimed by Conti ransomware gang

- Backup
- Cloud
- Cyber Attack
- Data Exfiltration
- Hacker
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

wifinomad - 2 years ago

It's perhaps a little ironic that the header image of this article is a picture of destroyed LTO Ultrium tape. Ironic because tape is arguably one of the strongest forms of "last line of defence protection" against ransomware. A useful recommendation is to follow the 3-2-1-1 rule: three copies of data on two different media types, one stored offsite and one stored offline. Ransomware can't infect data that is inaccessible behind an air gap. That's why LTO Ultrium tape is so effective!

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: