When SysAdmins go rogue...

It's a nightmare scenario; one of your trusted SysAdmins/ Super Users goes bad. How much damage can they do? How would you know it was happening and who it was? How could you recover from it?

We've all heard of Edward Snowden… well, he had just a bit of Privileged Access, and used social engineering to acquire other user's passwords. Your SysAdmin/Super User/Root User has all that access legitimately. It's a job that comes with a great deal of trust, but what if one went rogue? What could they do and how would they do it?

This article examines these hard-to-impossible to spot attacks, focusing on illegal data acquisition and data breaches.

Online attacks

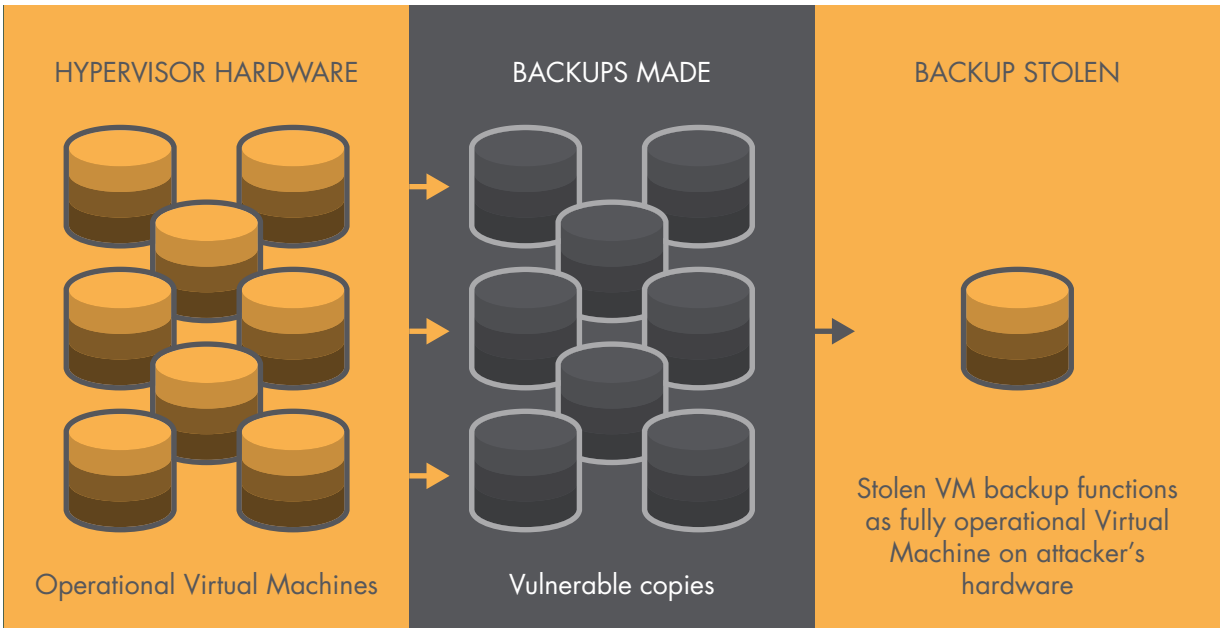
There are many ways a rogue SysAdmin may manipulate their privilege online. One example involves adding Privileged Accounts to systems. These new additions are typically given innocuous names that are easily mistaken for legitimate functions:

- Backup
- backup
- Backup_Daemon
- Tape_Management
- System
- system
- postgres
- sql
- <AV product names>

Only by careful examination can someone tell if these accounts are bogus, for example by looking for interactive login rights. Moreover, to identify these details, the person looking needs to be a capable SysAdmin to start with.

cont. overleaf

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password lifecycle management, and then hand the pre-prepared session back to the incoming request ready for system management. The session can be recorded, subject to time windows and device group separation. We have delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.



Another common approach is to create trust relationships between systems so that backup@systemA can operate as backup@systemB. It's so easy to get into a mess with trust relationships that it can be hard to tell the difference between oversight and premeditated malice.

A more complex attack sees API keys used to gain access to applications, such as a script that behaves like a recognised client part of an application. As an attack type, creating backdoor access is very difficult to detect. When does the legitimate need for management access cross over into malice? A typical case is the use of extra ports on firewalls, because it is so easy to get locked out whilst defining rules. Using remote access to systems because a SysAdmin wants to run a backup from home - where do we draw the line? Perhaps the VPN has been set up using a PBX system rather than the corporate firewall? Maybe a cloud service like GoToMyPC using a personal account? There could even be more complex cases of connecting to several other systems before making the jump to their own workstation.

Deleting log files is another classic cause for concern. Was this done to 'save the day' because the system was out of disk space, or does it hide a more nefarious activity?
Using other people's accounts can also be a sign, particularly while they are away, because they are a great way of hiding trails (à la Edward Snowden). The SysAdmin changes the password, then the rightful user assumes they forgot their password or missed a mandatory refresh.

Offline attacks

And if the online attacks are difficult to trace, then the offline versions take this to a whole new level.

An offline attack refers to breaking into a copy of an online system. Since our SysAdmin is responsible for backups, they have plenty to choose from.

You may have a well-secured system running as a virtual machine, either on your own infrastructure, or the cloud. Though the passwords for the system and applications may well be not known to the SysAdmin, they can use a copy of that virtual machine in a separate instance (at home or their corner of the cloud). They can boot the system into single user mode, and then change any password they wish.

cont. overleaf

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password lifecycle management, and then hand the pre-prepared session back to the incoming request ready for system management. The session can be recorded, subject to time windows and device group separation. We have delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.

A stolen virtual machine can be subjected to many brute force hacks. The system itself may complain, generating warning syslogs, but with nowhere for the warnings to go your organisation is not aware of the attacks in the 'parallel universe'.

If a password is compromised it will work against the live system, appearing as a legitimate user that logs in without error. Any API keys on the remote system may also be valid. However often they are locked against IP addresses, those that lock against MAC addresses are easily defeated since the stolen VM can simply be configured to have the same MAC address.

Imagine what would be available to the attacker if the virtual machine they copied was an Active Directory domain controller… They would have access to the SAM database and therefore be able to run brute force attacks against all of your user accounts. Senior Staff accounts would have access to sensitive emails and would be accessed in a seemingly legitimate manner.

How the Osirium PxM Platform mitigates these issues

It's essential your organisation takes stock of the data that is really sensitive. There are obvious data sets:

Finance Files,

Customer Records (particularly GDPR sensitive),

Personnel and Payments data,

Board Meeting Minutes.

The next stage is to work out who you can trust with administrative access to these. You'll need to understand that a zero-trust policy, whilst possible, is expensive and slow to operate.

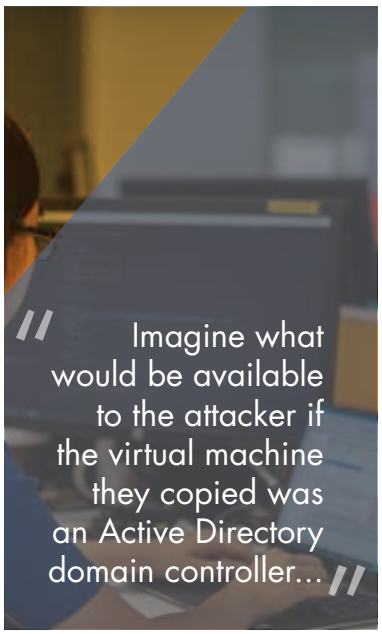
From the examples we've given, you can see that most of the problem relates to Privileged Credentials in that those that have them can make copies of critical systems. It's still possible to make copies without credentials, but physical access is required, and the systems in question would need to be taken offline so that disks could be copied.

Our Privileged Access Management solution, the Osirium PxM Platform, separates people from passwords and applies Enterprise Class Password Life Cycle management. This means that people do not know the passwords in the first place, and if they obtain them through the break-glass function, not only is this logged to their identity, but the lifetime of the password is limited. A regular review of who used the break-glass function is a vital part of your security posture.

A key takeaway is that security of your hypervisor/cloud estate is more critical than the security of individual virtual machines. This security should also extend to your NAS and online storage solutions.

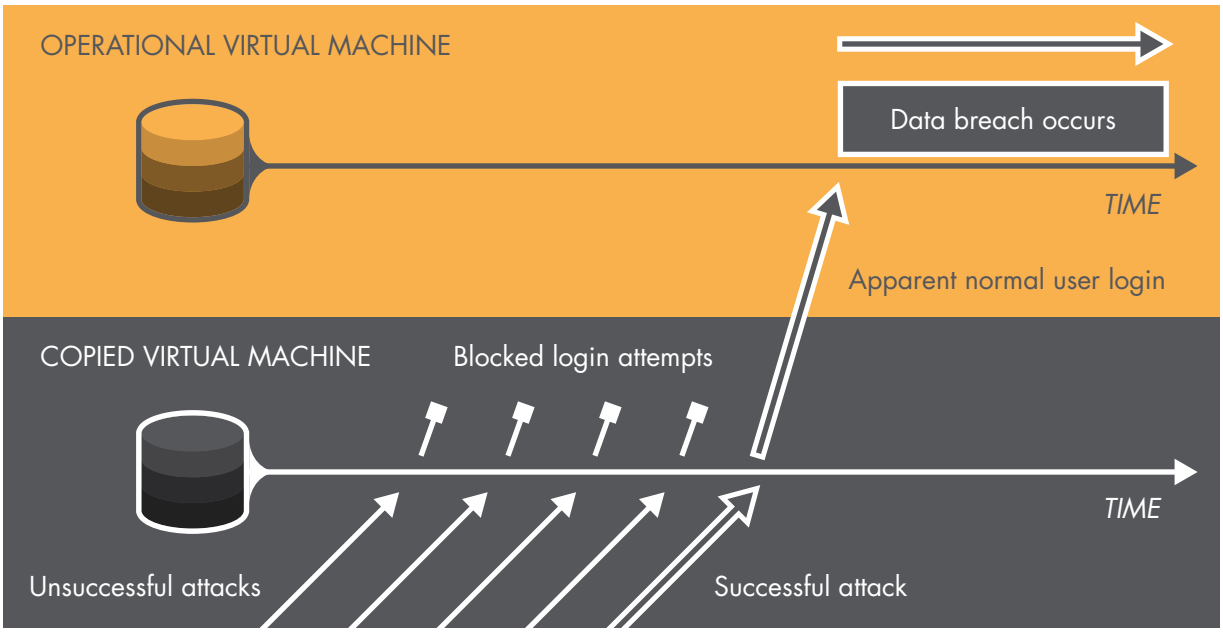
You need to think about the state and format of your backups. Are these a latent threat? If they were stolen, are they easy to access? Could they be encrypted, and if so, what would need to be in place for private key security? We need to remember that the most important part of backup is recovery, and encrypted backups put extra risk around the recovery process. This increases the need for both commissioning and periodic testing. In particular, an organisation needs to take extra care when certificates (and their keys) are changed. Old backups will use the old keys, so losing the keys means that historical backups are rendered useless.

The PxM Platform regularly audits devices for new accounts and flags those not expected. This helps eliminate back door accounts. However, this is only the case if you have someone listening to the alerts. As the saying goes, who shall guard



cont. overleaf

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password lifecycle management, and then hand the pre-prepared session back to the incoming request ready for system management. The session can be recorded, subject to time windows and device group separation. We have delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.



Above: A copied Virtual Machine experiences a different timeline...

the guards themselves? You must review who is in access profiles and why.

The PxM Platform also deals with session recording. Due to the way that recordings are checksummed, it's difficult to remove or change a recording. This in itself is a great deterrent.

How to recover from an attack

When a SysAdmin goes rogue, you have to assume that they know every password of every person and every account, and that they have a copy of your Active Directory Domain Controller. With the PxM Platform in place, you'd know two things:

If the Break Glass function was used.

The date that every privileged account password was changed.

Every account needs its password changed. This is easy enough with the PxM Platform where you can simply use the regenerate account password task for each device. You should deal with devices on an infrastructure-first basis, since if you don't fix that level the rogue can continue with the same attack path.

Did the rogue have access to any Master Encryption Keys (MEK)? If so, they need to change. Using the PxM Platform, this involves a backup and restore of the previous master to a fresh install (thus regenerating on a new MEK). It's good practice to get the MEK away from any SysAdmin as soon as possible.

If your VPNs are AD and/or certificate-driven, you might need to think about changing the certificate.

You then need to freeze out and secure all the logs on all the systems (don't forget those Hypervisors and NAS - even if they are in the cloud). You'll need the logs for legal action, but perhaps of greater importance are the lessons they contain. The absence of any log files should always raise the red flag of suspicion.

Of course, we hope you never experience a SysAdmin 'going rogue' and never need to refer to this article... But if you do, we also hope that you have the PxM Platform.