GLOBAL PRIVILEGED ACCESS MANAGEMENT INNOVATORS

Do you really have to accept that breaches are inevitable?

The process of criminal change in the cyber world is continuous with occasional sharp movement brought about by exploitation of new technologies.

It is a truism that if a weakness is made good then the attackers will be driven to a different route. Over the last three years we have seen a huge decline in brute-forcing passwords mirrored by an increase in stealing credentials. By refactoring the Verizon 2014 breach reports into related methods, we find the previous state of privileged account abuse to be:

- 86% stolen
- 10% phished
- 4% brute forced

Since credential theft is making up the majority of successful attacks, we'll examine it further. Most incursions start with C2 crimeware, C2 refers to 'command and control'. In 84.4% of breach cases C2 Crimeware infections were found. It is thought that the bulk of these are opportunistic and many are related to DOS (Denial of Service) attacks.The use of keyloggers and spyware has been falling (6%).

Once an attacker has control, there are many ways in which privileged account credentials can be stolen; some are obvious, for example simply viewing spreadsheets of passwords, trawling through network shares or searching through emails. More advanced techniques rely on what we loosely term 'the dangerous desktop'.

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.

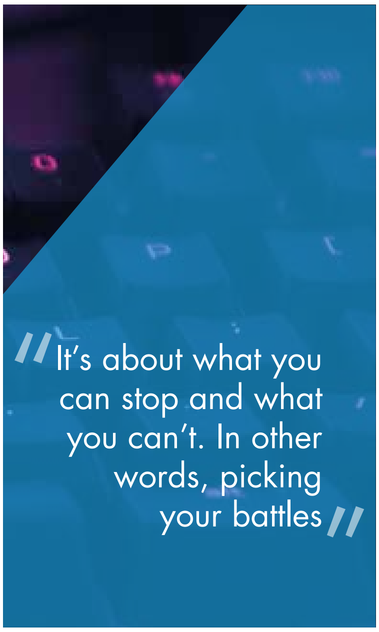
The Dangerous Desktop

Many common applications allow for credentials to be saved, the most obvious example are web browsers. Here we're concerned with the quality of credential storage, for example Firefox has a 'master password' feature that when used, overrides the default encryption key. This means that all Firefox users that don't use this option are using the same key set and therefore their stored credentials are easily decrypted. For reference, Firefox is one of the better applications; some store in plain text and many just base64 encode or use a bit-shift and encode.

There are more advanced techniques. Whenever a user has an RDP session, or a network share to a remote system, a hash of their credentials is available. This hash is the result of a one-way algorithm. The internet has a number of sites that have taken billions of common password combinations as a reverse lookup table from hash to password. One site claims to have 131 billion reverse lookups.

The compromised desktop can be used to view network traffic, either directly or through mirrored ports on network switches, it can scope and test internal defences as well as deploy malware as traps for others. This is why it is so important to manage the credentials of secondary and infrastructure systems. If a criminal can't access your database but can take a copy of the disks it runs from, the attack is still effective.

From the report we can see that 95% of malware is only prevalent in the wild for a few weeks. Attacks however, tend to be launched up to a year later. It is believed that attacks are launched only once sufficient knowledge, credentials and resources are built up. After all, any attacker would be lucky to stumble across your database credentials first time.



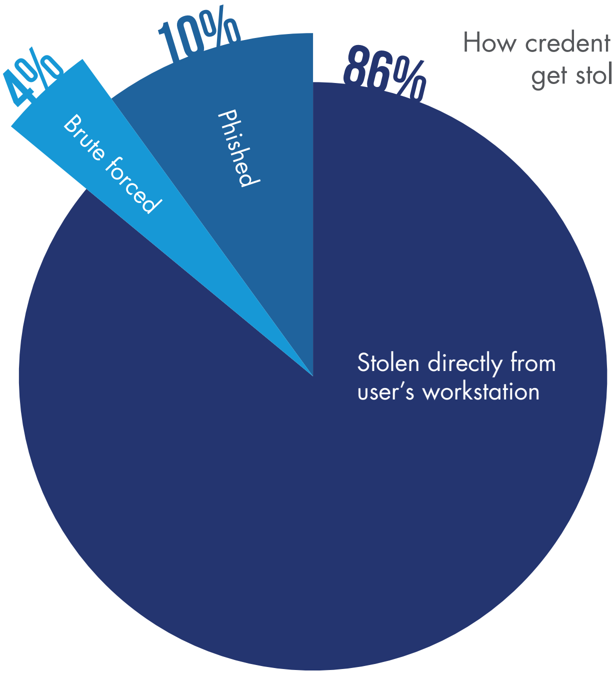
"It's about what you can stop and what you can't. In other words, picking your battles"

The progress of criminal attacks is the same; collect enough privileged credentials, find the data that can be monetised, then exfiltrate it as quickly as possible.

You need a serious strategy, not pixie dust

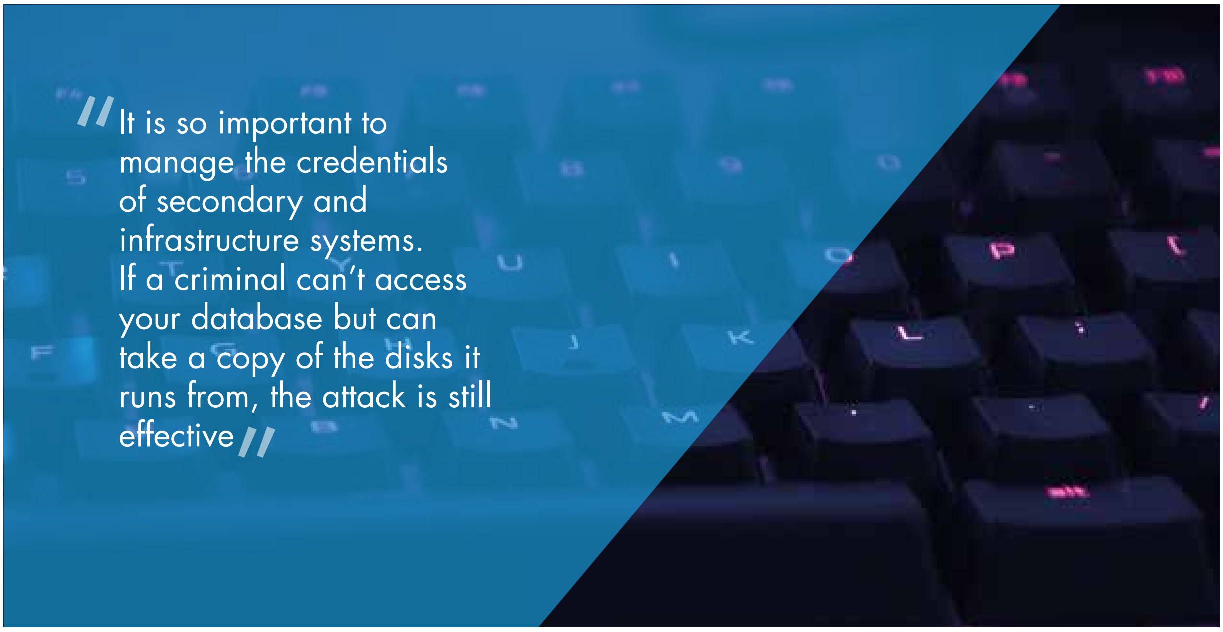
It's about what you can stop and what you can't, in other words picking your battles. The malware tidal wave combined with phishing and social engineering means that we need to look at a different part of the chain.

How credentials get stolen:



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.



> “It is so important to manage the credentials of secondary and infrastructure systems. If a criminal can’t access your database but can take a copy of the disks it runs from, the attack is still effective”

Separating the people from their passwords

Yes, it’s that simple. If people never get access to the passwords of privileged accounts they cannot be stolen or phished. If those passwords never enter the user’s domain, they are never vulnerable to malware.

Identity in, role out

In these days of the race to the bottom for pricing on IT support, it’s often the case that the lowest paid person ends up with the highest privileges on your systems. When outsourcers outsource, it’s difficult to know who really does have access to your infrastructure. That’s why it’s important to know the identity of everyone on your systems. Those identities need to be mapped to roles, and those roles should have the least privileges needed to perform them.

Defence in depth is the best solution, however organisations should consider that their user networks are always in a compromised state. Therefore, it is vital to keep passwords away from user systems as much as possible. Some passwords will always escape, but if you have enterprise class password management you can be sure that the escapees validity is always less than a month.

Osirium’s PxM Platform is about users arriving with an identity and leaving with a role. The role is defined by the account used and the passwords never enter the user’s systems. Passwords can be refreshed on short cycles without burdening the human user’s memory. When denied access to working credentials the attacker can’t strike.

“It is so important to manage the credentials of secondary and infrastructure systems.

If a criminal can’t access your database but can take a copy of the disks it runs from, the attack is still effective.”