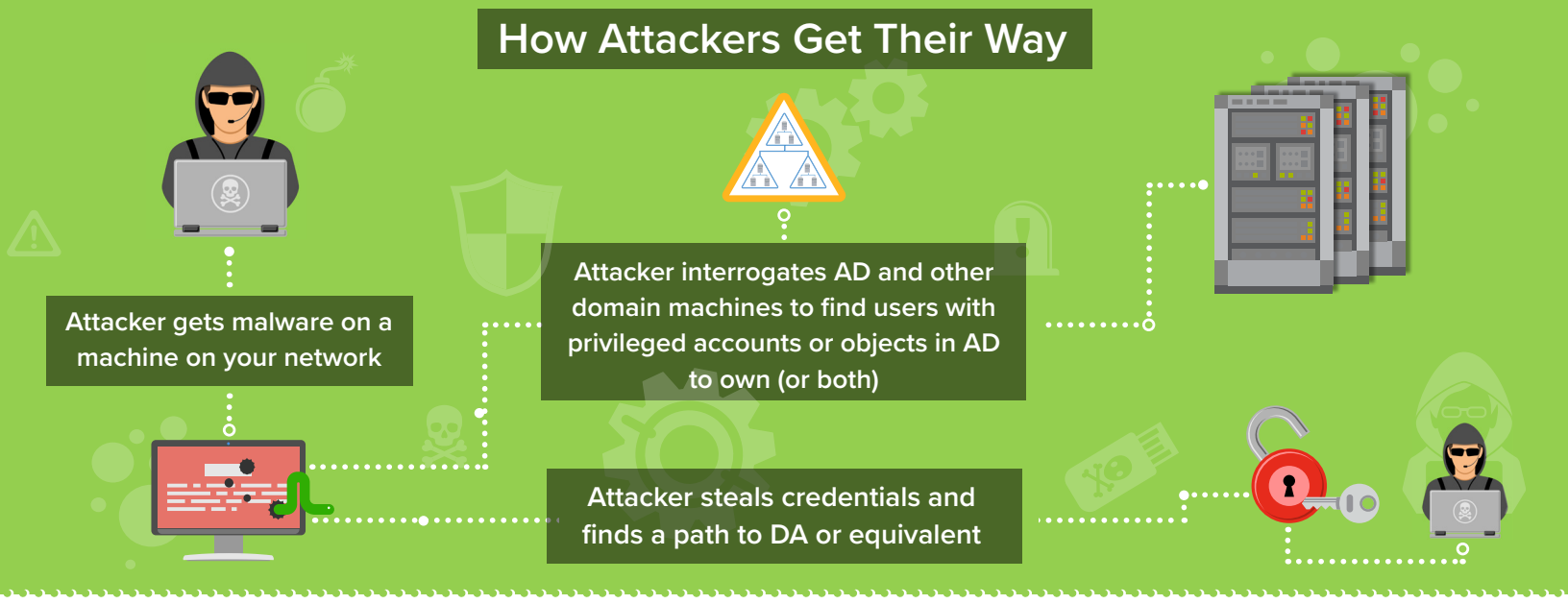
5 Tips for Securing Active Directory from a Cyber Attack

How Attackers Get Their Way



Active Directory Protection Tips

1- Harden Privileged AD Groups

Active Directory “red team” tools, like Bloodhound, look for memberships in interesting AD groups (i.e. Domain Admins, Enterprise Admins, etc.), which allow them to build a graph of group memberships and determine where access has been granted in the environment.

TIP

Harden privileged AD groups to prevent world-readable membership lists (i.e. Authenticated User groups). Remove readability on the members attribute for any user/group who doesn’t need it.

2- Harden AD ACLs on Privileged Objects

One of the recent advancements in Bloodhound is the discovery of access control list (ACL) attack paths, where permissions can be exploited to allow privileged access to your Active Directory.

TIP

Look for delegations that grant these permissions on privileged objects to “lower-tier” users and consider removing them: Reset Password, Change Group Membership, Full Control, Write All Properties, Modify Owner, Modify Permissions, All Extended Rights.

3- Harden Sensitive GPOs and GPO Delegation

While Group Policy Objects (GPOs) aren't commonly thought of as a path to attack, they are indeed exploitable. There are GPOs in your environment that contain settings that grant privileged access and provide a map of who has what access in your environment. Attackers are also able to exploit weak edit permissions on GPOs to inject policies that distribute malware to the entire organization.

TIP

You can download a script that searches all your GPOs for vulnerable GPOs that contain privileged access policies like restricted groups, and are "world-readable." You can use this information to harden the GPOs. It's also critical to control who can edit GPOs- limit delegating edit permissions on GPOs to those who really need it or only delegate when needed and revoke afterwards.

4- Use Admin Tiering and PAWs to Control Where Credentials are Left

Highly privileged accounts logging onto untrusted low-privilege user workstations to perform tasks are at risk of credential theft.

TIP

Implement administrative tiering strategy where separate accounts are used for performing different tasks in order to limit where administrators are leaving their credentials. Privileged Access Workstations (PAWs) further prevent the spread of hashes by ensuring that when admins log in, they log in from more secure machines.

5- Reduce "Query-ability" of Sessions and Local Admins

Another hallmark of tools like Bloodhound is that they interrogate machines on your network to determine active sessions, and from where, using older APIs. The NetSessionEnum API gives you a map of user to machine and SAM-based APIs help find local admin members on machines.

TIP

Microsoft has a script that allows you to re-permission the NetSession Enum API and allows you to remove Authenticated Users from being able to query sessions.

Enable Group Policy Setting to restrict SAM-based APIs -> Computer Configuration/ Policies/Windows Settings/Security Settings/Local Policies/Security Options/Network access: Restrict clients allowed to make remote calls to SAM with a restricted ACL.

Bonus Tip! – Avoid "Kerberoasting"

Kerberoasting is the process of grabbing the NTLM hashes of arbitrary user service accounts that have Service Principal Names (SPNs) defined in AD. These service accounts are often privileged accounts which are forgotten about and tend to have non-expiring passwords (potentially even easy-to-crack passwords).

TIP

You can download a script that easily finds Kerberoastable users and ensure that these accounts have complex, frequently-rotating passwords.

To learn more about how to protect your organization, please visit www.semperis.com